User Administration

for InkFormulation 6
and ColorQuality 6
with

UserAdministrator 2.1

Content

1 User Administration

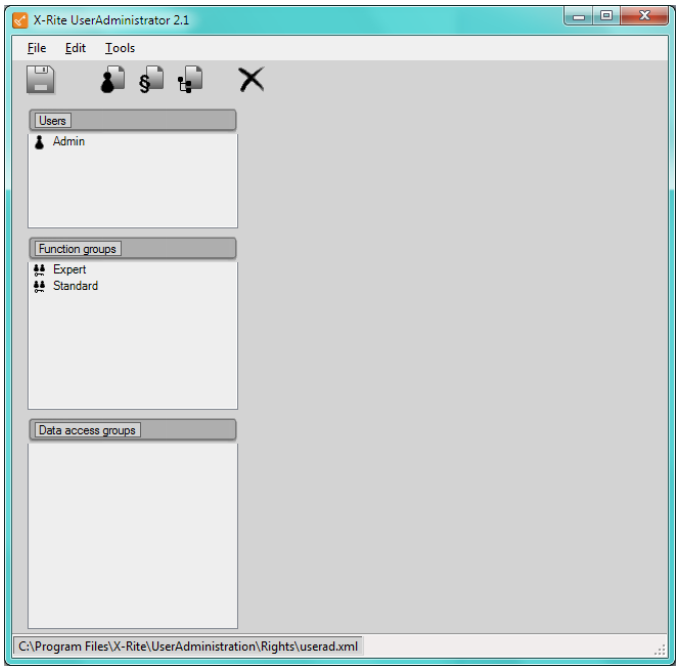
X-Rite UserAdministrator is additional software enabling you to define the access rights of the individual users to the functions of X-Rite InkFormulation and ColorQuality.
The UserAdministrator software displays all functions of InkFormulation and ColorQuality. However, only those functions can be switched on and off which are authorized by the copy protection pin.
UserAdministrator also allows users to be assigned to particular data access groups. This means that application data can be easily used jointly and protected from unauthorized access.

1.1 Launching UserAdministrator

The UserAdministrator can be launched from **Start > Programs > X-Rite > UserAdministrator**.

Remark: If you are using Windows XP SP2, NET 2.0 needs to be installed from the InkFormulation/ColorQuality 6 Installation CD (DotNet20_forWinXPSP2) on your PC.

2 Screen Structure



2.1 Function groups

Function groups define access rights to specific functions of InkFormulation and/or ColorQuality for the groups in question.
New groups can be added and existing ones deleted.

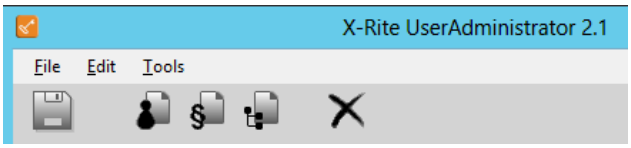
2.2 Users

Each user can be assigned to one or more rights groups. A user who belongs to several rights groups disposes of the cumulated access rights granted to those rights groups.
New users can be added and existing ones deleted.

2.3 Data access groups

Data access groups define the structure for access rights to data. Any user can be a member of a data access group (but only to one single data access group at a time, not to several simultaneously). A higher-ranking group has read and edit rights to all the data of a lower-ranking group. A lower-ranking group has read-only rights to all the data in the group. No group can read or edit the data of an adjacent group.
Data access groups can be added or deleted.

3 Menu list



The following functions can be carried out on the various menus:

File	Backup and restore user data
	Close the program
Edit	Undo
Tools	Settings: Select language

3.1 Symbols list

Save user data

Create new users

Create a new function group

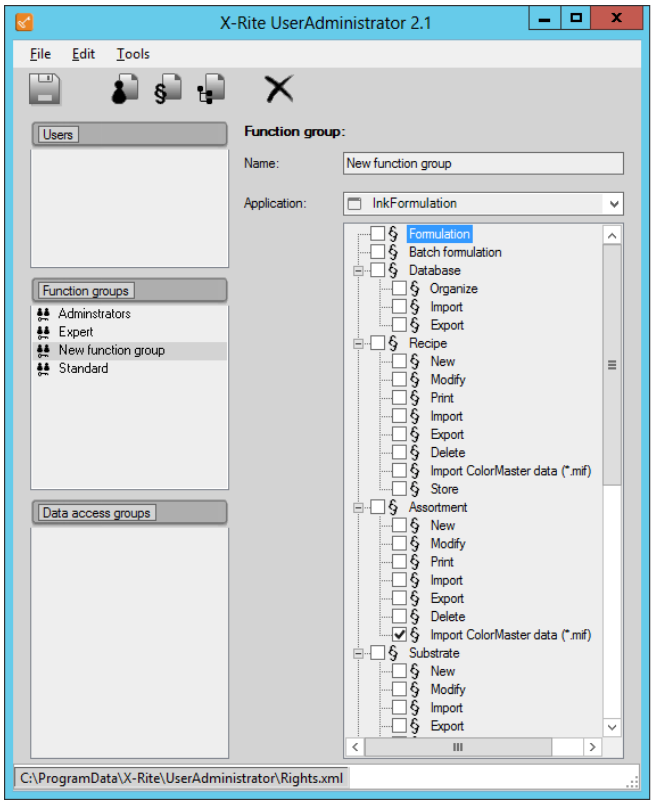
Create a new data access group

Delete

4 Entering new authorization groups

Procedure:

1. Click on the symbol New function group



2. Enter a designation for the function group
3. Select the desired application: ColorQuality or InkFormulation
4. Activate the check boxes for the functions to which the new group is to have access

Note: If you activate the check box for the main directory of a program, all subordinate functions will also be activated. Open the subdirectories to activate/deactivate the individual functions.
Functions which are not authorized by the copy protection pin cannot be activated.

5. Click on the Save symbol in the main window to activate the entries you have made.

Note The current user data can be saved in any directory and loaded when required.

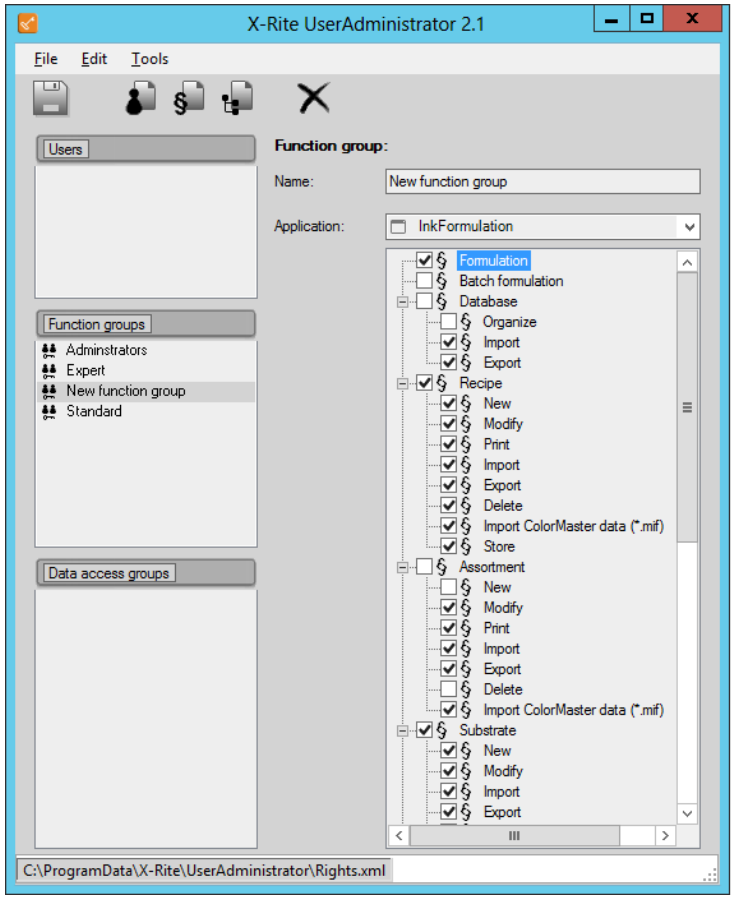
4.1 Processing function groups

The access rights for a group can also be changed later.

Procedure:

1. Highlight the relevant function group on the left side of the window. On the right side you see automatically the directory tree with all activated functions.

2. Deactivate or activate the check boxes for the required programs/functions



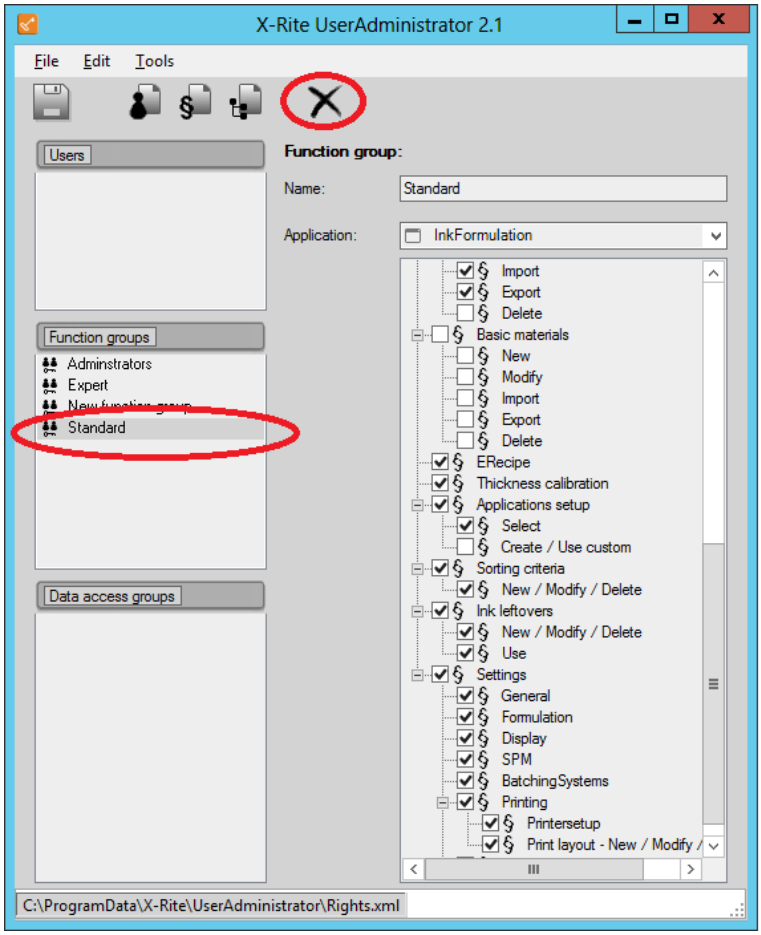
3. Click on the **Save** symbol to activate the entries you have made.

4.2 Delete function groups

Function groups can be deleted anytime.

Procedure:

1. Highlight the relevant function group in the directory tree on the left side, you want to delete.
2. Click on **Delete** to delete the function group.

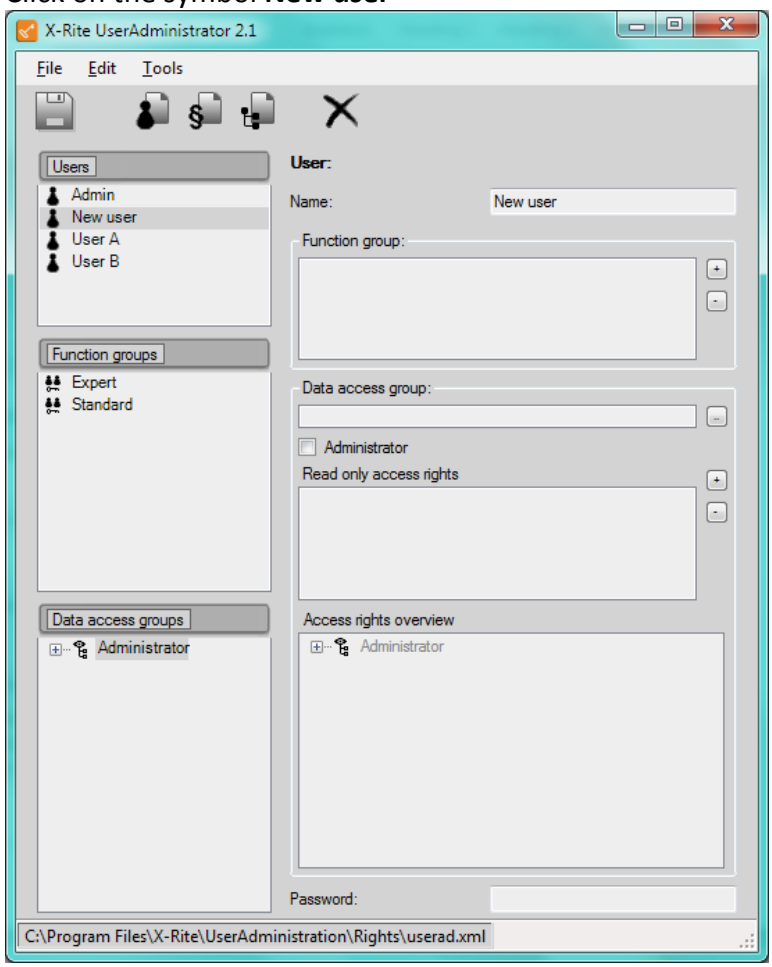


5 Processing user data

5.1 Entering a new user

Procedure

1. Click on the symbol **New user**



2. Enter the user name
3. Select the function group, to which the user should be assigned

Note	A user can be assigned to more than one rights group.

Assigning to a data access group **by highlighting** the relevant data access group.

Note The membership of a user to a certain data access group is identified by a colored background (). This symbol will not be immediately displayed upon assigning a user to a data access group, but can be verified after saving the settings by menu **User/Group > Modify**.

If the current windows user name is found in the UserAdministrator, it is automatically selected and the password dialog box is omitted, regardless whether a password is set or not.

If the current windows user is not found in the UserAdministrator, the password dialog box will be appear. We recommend a password.

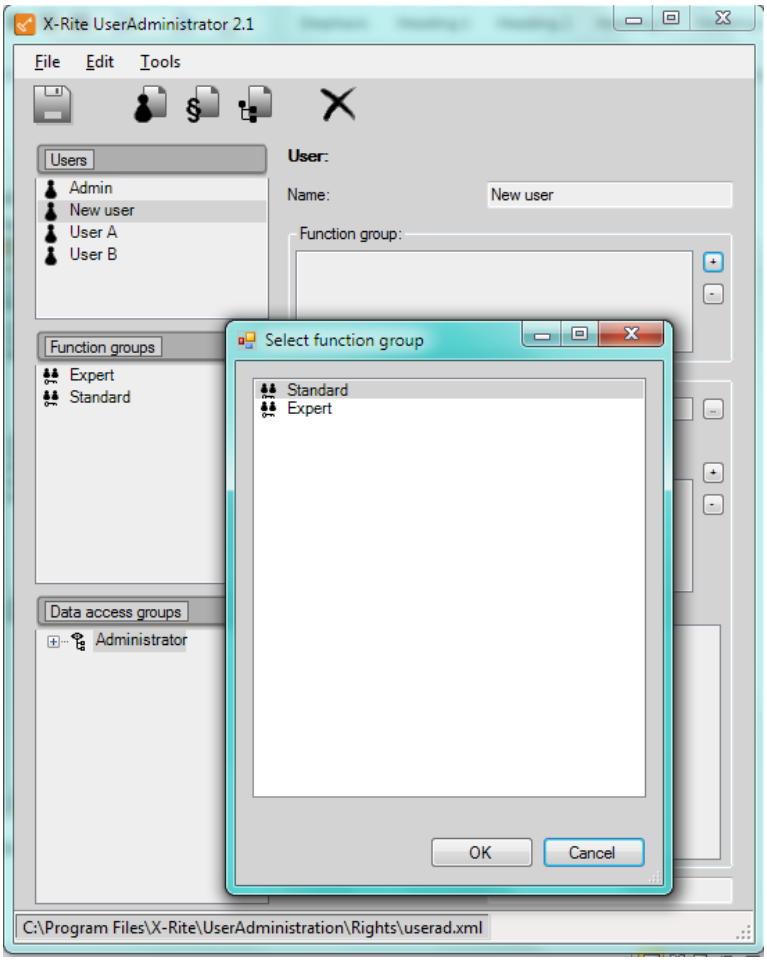
Click on the **Save** symbol to activate the entries you have made.

5.2 Processing user rights

The access rights for a user (defined by his membership to a certain user group or multiple user groups) can also be modified at a later time.

Procedure:

1. Highlight the relevant **user** on the left side.
2. Select the desired function group on the right side via **+** button.
3. Select in the „Select function group“ window the desired group of rights. Then click **OK**.



4. Click on **Save** symbol to activate the entries you have made

5.3 Entering or changing user information later

User information can be entered or altered at a later time.

Procedure:

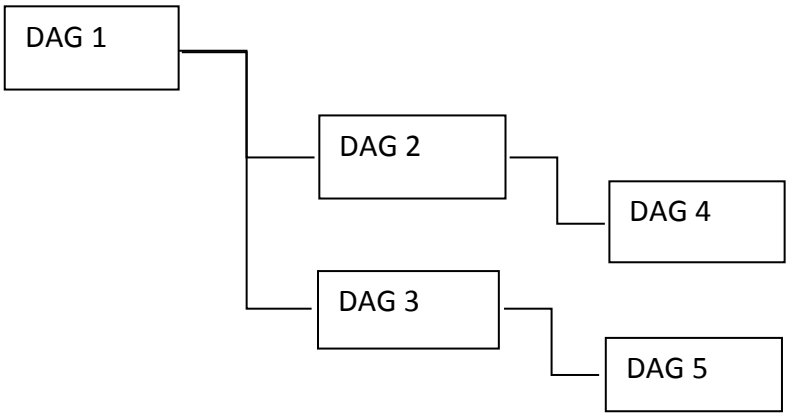
1. Highlight the user
2. On the right side the user information are displayed. You can modify or delete this information anytime
3. Click on **Save symbol** to activate the entries you have made

6 Structure and hierarchy of data access groups

The aim of data access groups is to provide privacy to users of data access groups of different trees. Basically data created by members of a data access group (DAG) of one tree cannot be seen (read) or accessed by members of a data access group of another tree. But since version 2.1 it is possible to give users read only access to other data access groups, not in the same tree.

By activated the User Administration, the user can store the recipes in different data access groups. It is only possible to store in those groups, where the user is or in groups below:

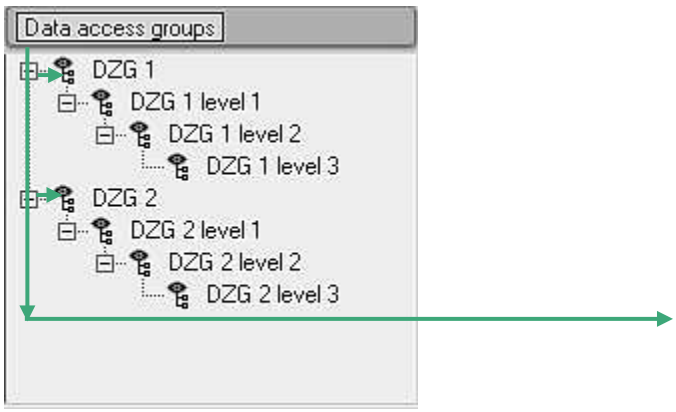
DAG 1 can store recipes in each DAG.
DAG 2 can store recipes in DAG 2 and DAG 4.
DAG 3 can store recipes in DAG 3 and DAG 5.
DAG 4 can store only in DAG 4
DAG 5 can store only in DAG 5.



A higher-ranking group has read and edit rights to all data of a lower-ranking group. A lower-ranking group has read-only rights to all data in the group. No group can edit data of an adjacent group, regardless whether it is on the same level, on a higher or on a lower level. Users optionally can be given read only access to adjacent groups.

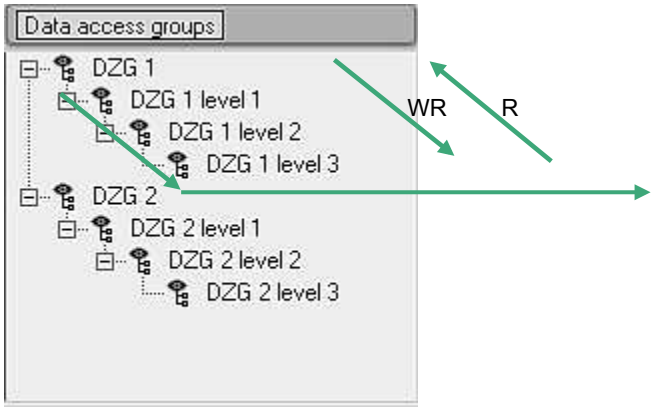
Note	Data which was present in the database before data access groups were built can be seen by all data access groups.

Example:



Members of a higher- ranking data access group (e.g. an administrator being member of the top level «Data access group») can read and access data of all lower-ranking data access groups, as far as they are granted to do so by the authorization group which they are member of

Note Whether a member of a higher-ranking data access group can **alter** or **delete** data created by members of lower-ranking data access groups depends on the rights granted by the **authorization group** which he is member of!



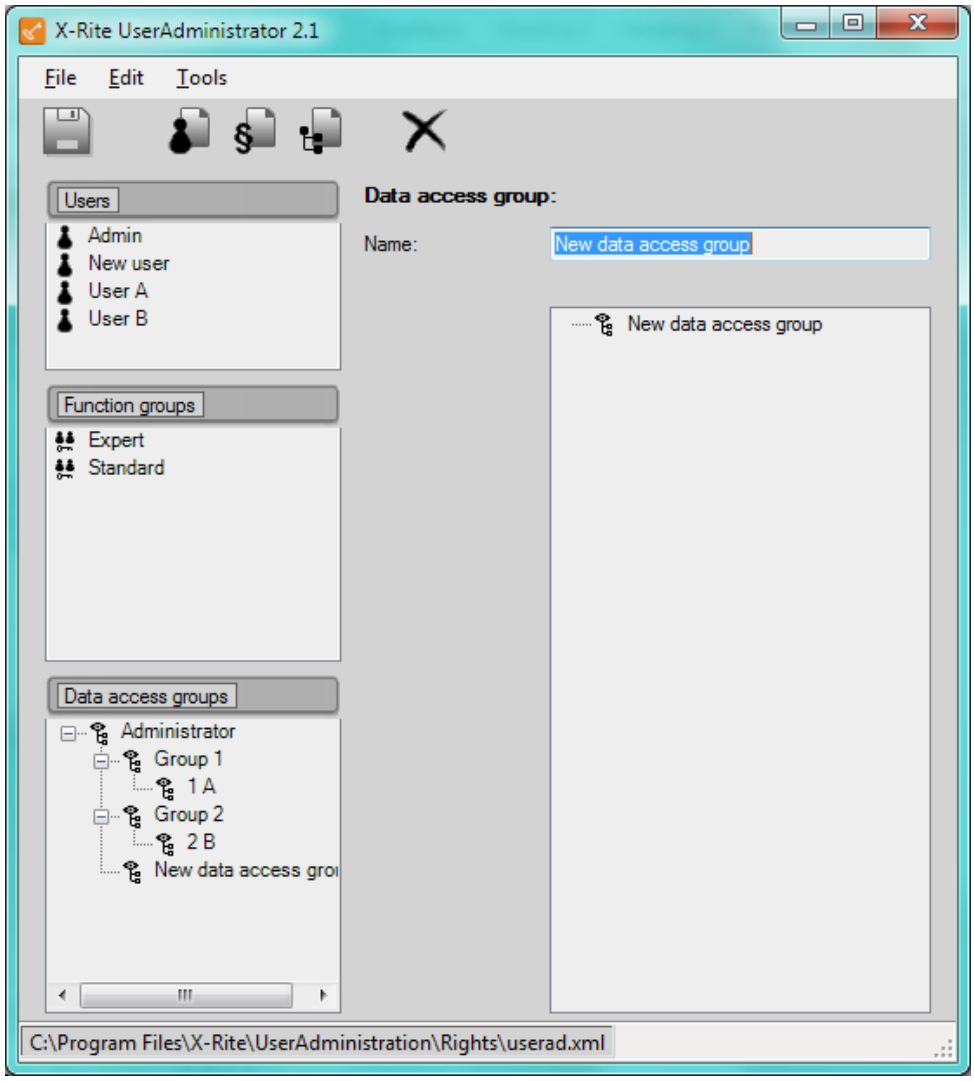
Members of a same tree can read all data of the different levels of this tree.
However, members of lower-ranking levels have read access (R) only to data created by members of higher-ranking data access groups, while members of higher-ranking levels have read and write access (WR) to data created by members of lower-ranking data access groups.

Note No user can be member of more than one data access group at a time but can have read only access to other data access groups.

6.1 Defining a new data access group

Procedure:

1. Highlight the data access group on the left side that will be the higher ranking group. The new data access group will be defined directly under that group.
2. Click on the symbol **New data access group**

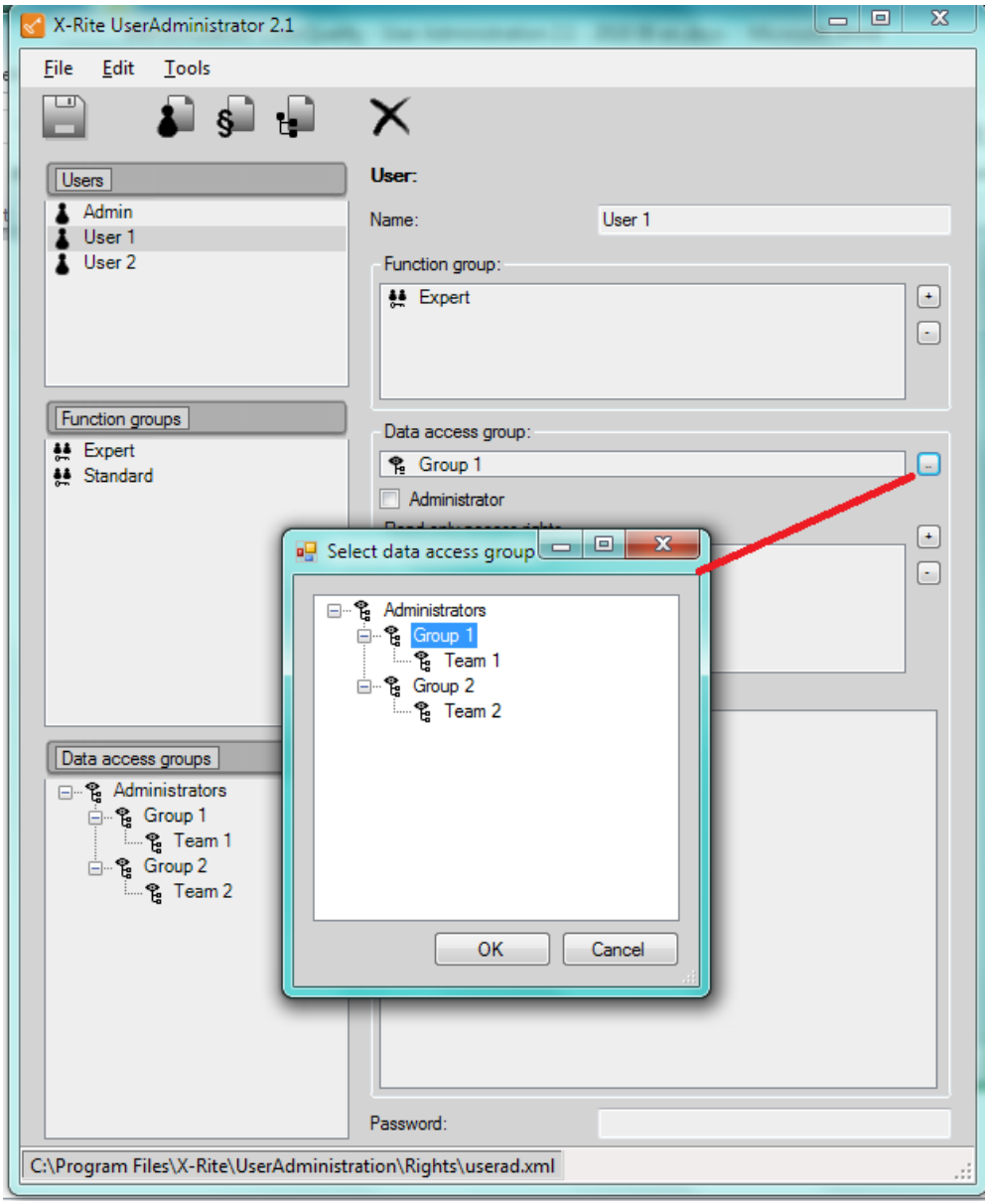


3. Enter the name of the data access group
4. Click on the **Save** symbol to activate the entries you have made

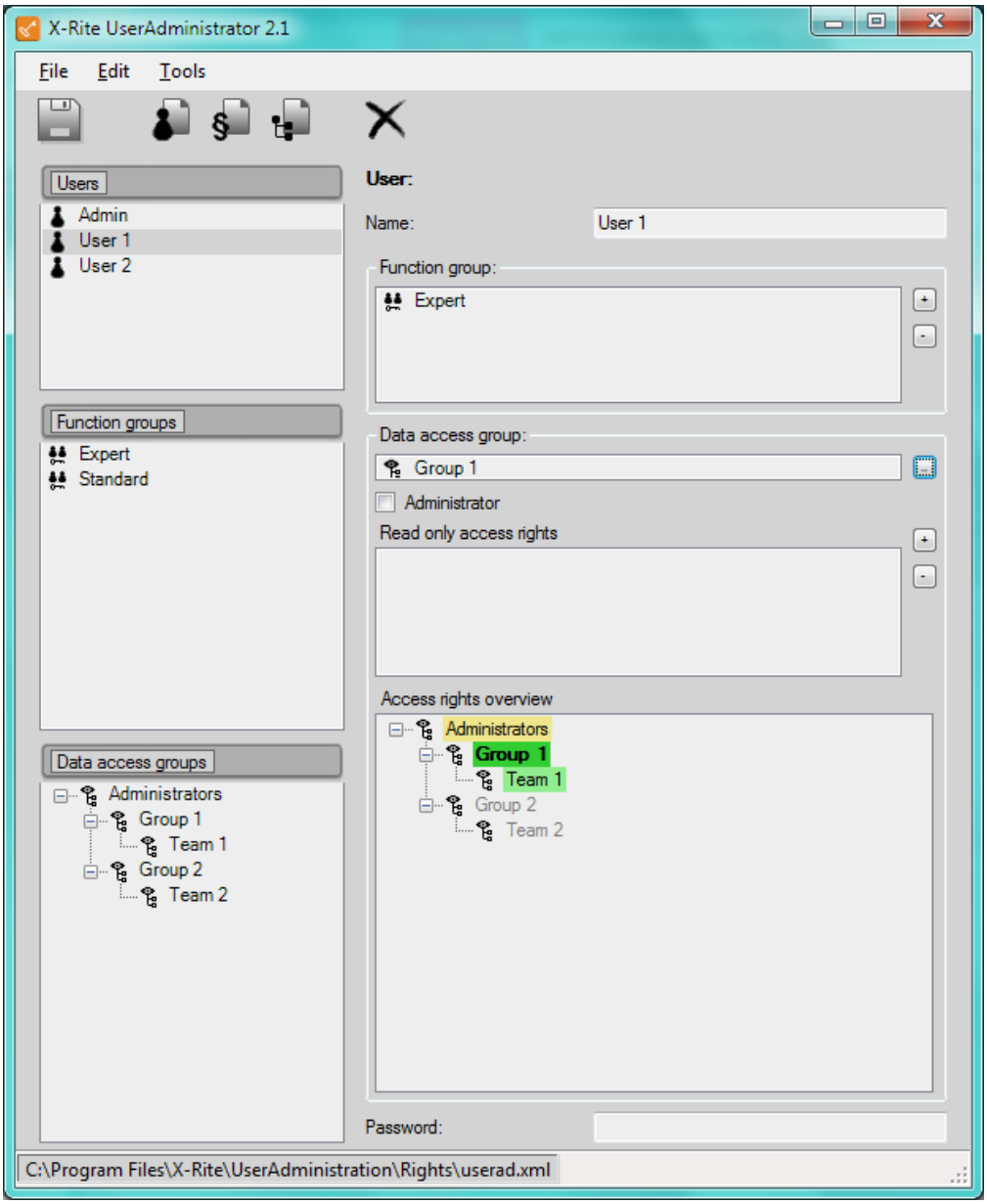
6.2 Assign a data access group

Procedure:

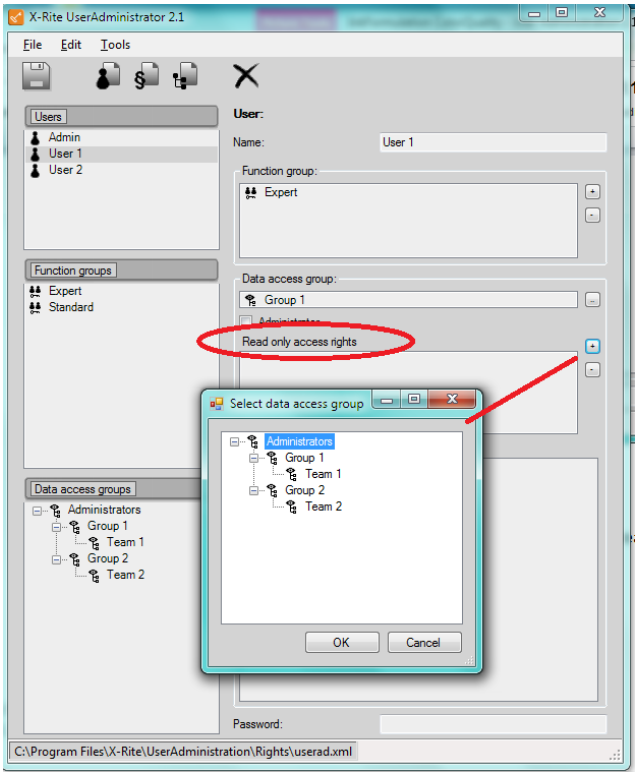
1. Select the user you want to assign to a data access group
2. On the right side you can modify the data of the user. Click on the button next to the list box Data access group.
3. Select the desired data access group and click on OK.



4. The assigned Data Access Group will be highlighted in dark green for the user, also full access rights to lower ranking groups (bright green) and read only access to higher ranking groups (yellow).



5. Optionally a user can be assigned to another Data Access Group with read only access.



6. Read only access is yellow highlighted.