BIONUMERICS Tutorial:

Setting up users and passwords

1 Aim

In a multi-user environment, security tools and user restrictions are indispensable to keep the database clean and manageable and avoid abusive changes. BIONUMERICS contains a comprehensive set of user and security tools, including the creation of ***User Groups*** defining specific privileges and ***Users*** with logins and passwords. In this tutorial you will learn how to create ***Users***, how to assign logins and passwords to the created users, and how to grant and deny ***privileges*** to ***User groups***.

2 Introduction to the user management components

BIONUMERICS uses three key concepts for user management: users, user groups and privileges (see Figure 1):

- A ***user*** corresponds to a physical person who accesses the BIONUMERICS database. Each user is authenticated via his/her own unique user ID and optionally a password.
- A ***user group*** should be thought of as a number of users (i.e. persons), all fulfilling the same or a very similar role. Users are assigned to one or more user groups, to each of which a specific set of privileges is granted.
- ***Privileges*** apply for *modification* of data. Privilege management is accomplished by setting up an ordered list of allow/deny rules for each user group.

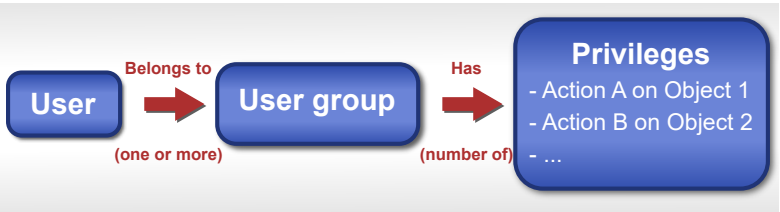

Figure 1: Relations between the three key concepts in user management: users, user groups and privileges.

3 Preparing the database

The **DemoBase Connected** will be used in this tutorial and can be downloaded directly from the *BIONUMERICS Startup* window or restored from the back-up file available on our website:

1. To download the database directly from the *BIONUMERICS Startup* window, click the button, located in the toolbar in the *BIONUMERICS Startup* window. Select **DemoBase Connected** from the list and select ***Database*** > ***Download*** (). Confirm the download action.

2. To restore the database from the back-up file, first download the file `DemoBase_Connected.bnbk` from `https://www.applied-maths.com/download/sample-data`, under 'DemoBase Connected'. In the *BIONUMERICS Startup* window, press the button, select ***Restore database***, browse for the downloaded file and select ***Create copy***. Specify a name and click <***OK***>.

In contrast to other browsers, some versions of Internet Explorer rename the `DemoBase_Connected.bnbk` database backup file into `DemoBase_Connected.zip`. If this happens, you should manually remove the `.zip` file extension and replace with `.bnbk`. A warning will appear ("If you change a file name extension, the file might become unusable."), but you can safely confirm this action. Keep in mind that Windows might not display the `.zip` file extension if the option "Hide extensions for known file types" is checked in your Windows folder options.

4 The User management window

1. In the *BIONUMERICS Startup* window, double-click on the **DemoBase Connected** database to open it.

2. Select ***Database*** > ***User management...*** to call the *User management* window (see Figure 2).

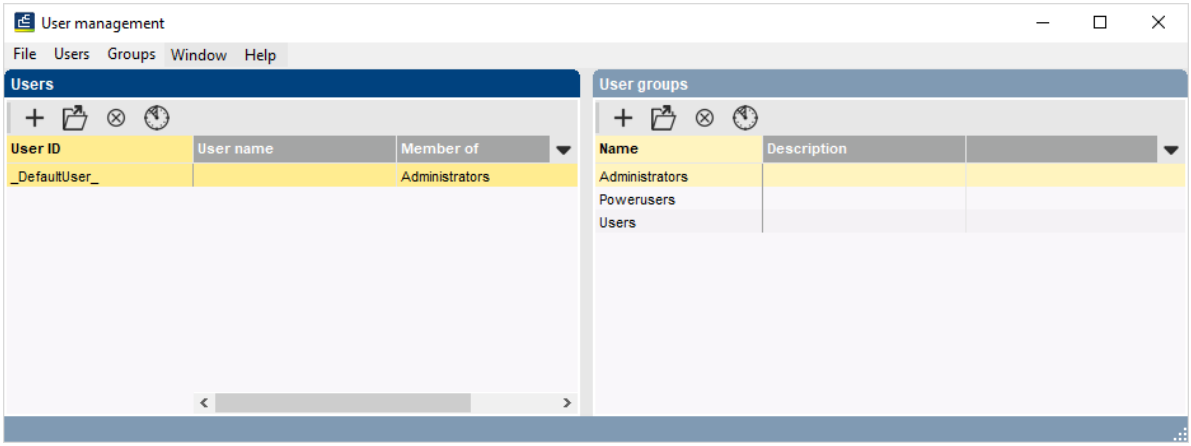

Figure 2: The *User management* window: default view.

In the *User management* window, the database users are listed in the *Users* panel (left panel in default configuration) and the user groups are shown in the *User groups* panel (right panel).

Three user groups are automatically created by BIONUMERICS (**Administrators**, **Powerusers**, and **Users**) as is one user labeled _**DefaultUser**_. This default user is assigned to the **Administrators** group.

3. Double-click on the **Users** user group in the *User groups* panel to open the *Account group settings* dialog box (see Figure 3).

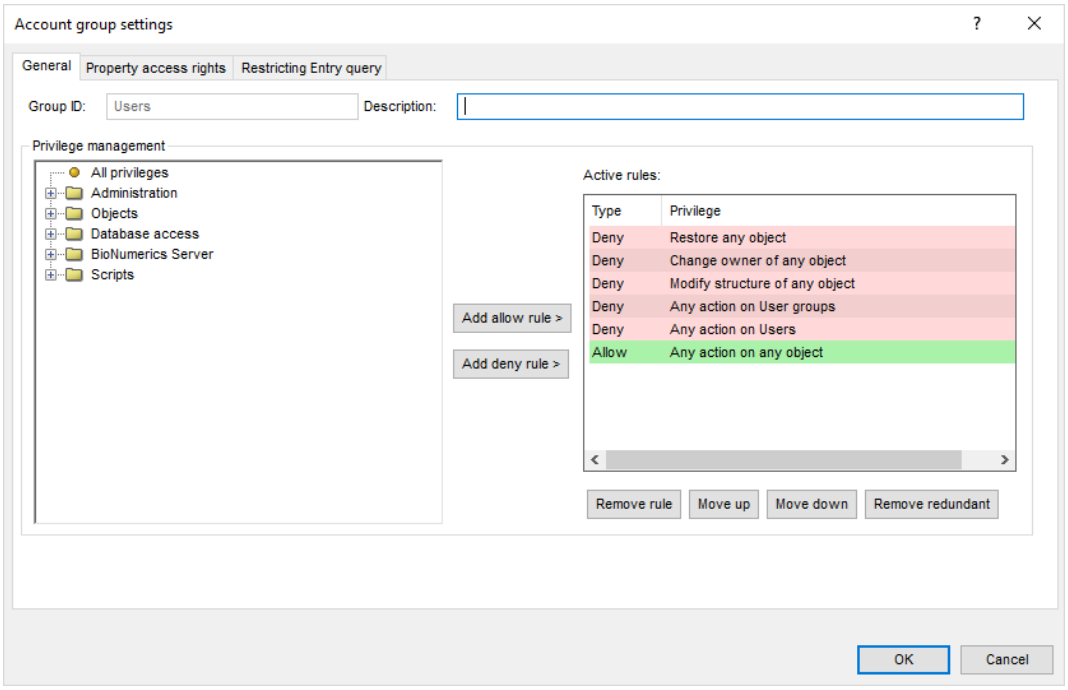

Figure 3: The *Account group settings* dialog box, showing the general settings for the default user group **Users**.

The ***Active rules*** appear in an ordered list, with the most general rule at the bottom of this list. Towards the top of the list, the rules get more and more specific, i.e. they form exceptions to the more general rules below them. When a user that is assigned to the user group performs an action on the database, the ***Active rules*** will be checked from top to bottom. If the privilege of the first (i.e. most specific) rule covers the action, the rule will be applied and the action is either allowed or denied. If the privilege does not cover the action, the second rule is checked, etc.

- Users assigned to the default user group **Administrators** can by default do everything (***Allow All privileges*** is default the only active rule for this group).
- **Powerusers** can by default do everything except database system changes (e.g. change the audit trail settings) and user management alterations.
- Users assigned to the **Users** group (see Figure 2) can by default only do the normal day-to-day work in the database (e.g. they cannot make new information fields or remove them, or cannot change the ownership of objects (see 8.2), etc.).

4. Click on the *Property access rights tab* of the *Account group settings* dialog box (see Figure 4).

All entry information fields and experiment types present in the database as well as custom scripts and plugins stored in the database through *Plugins* dialog box are listed in the grid, with their ***Name*** and two access rights:

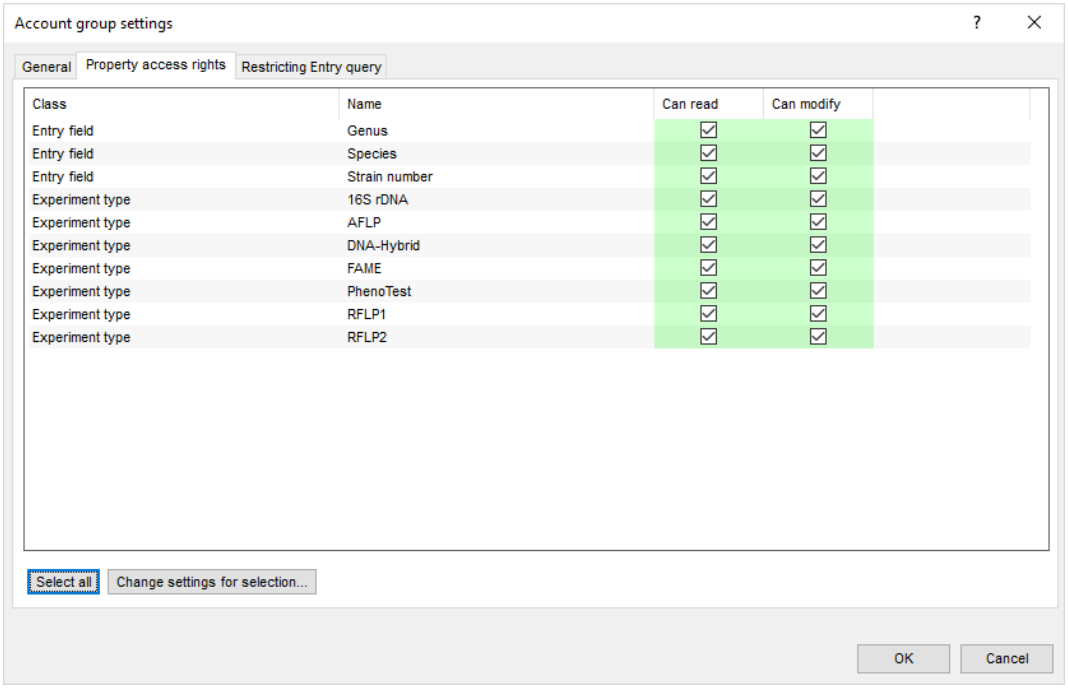

Figure 4: Property access rights.

- ***Can read***: If checked, the information will be visible to members of this user group. If unchecked, the information will not be displayed (appears as hatched areas). Note that unchecking this option will also uncheck the ***Can modify*** access right.
- ***Can modify***: If checked, members of this user group can make modifications to the information. Checking this option will also uncheck the ***Can read*** access right. If unchecked, information will not be editable (entry fields) or it will not be possible to save any changes to the database (experiments).

5. Click on the *Restricting entry query tab* of the *Account group settings* dialog box.

All query-based entry Views that are available in the database will be listed (see Figure 5). A view can be selected that will act as a *restricting query*: only those entries that are included in the selected view will be visible for the current user group. When "<All entries>" is selected, no restriction will be applied. More information about views can be found in 8.3.

6. Close the *Account group settings* dialog box.

5 Adding users to the database

When a new database is created, one user labeled **_DefaultUser_** is automatically created and is assigned to the **Administrators** group. The status bar at the bottom of the *Main* window displays the name of the user that is currently logged on: Database: Example database (connected, _DefaultUser_). The **_DefaultUser_** is assigned to the default user group **Administrators** and can by default do everything, including user management alterations.

As an example, we will add a new member to the **Administrators** and **Users** user groups.

1. In the *User management* window select ***Users*** > ***Add new...*** (+) to add a new user to the list. This brings up the *User settings* dialog box (see Figure 6).

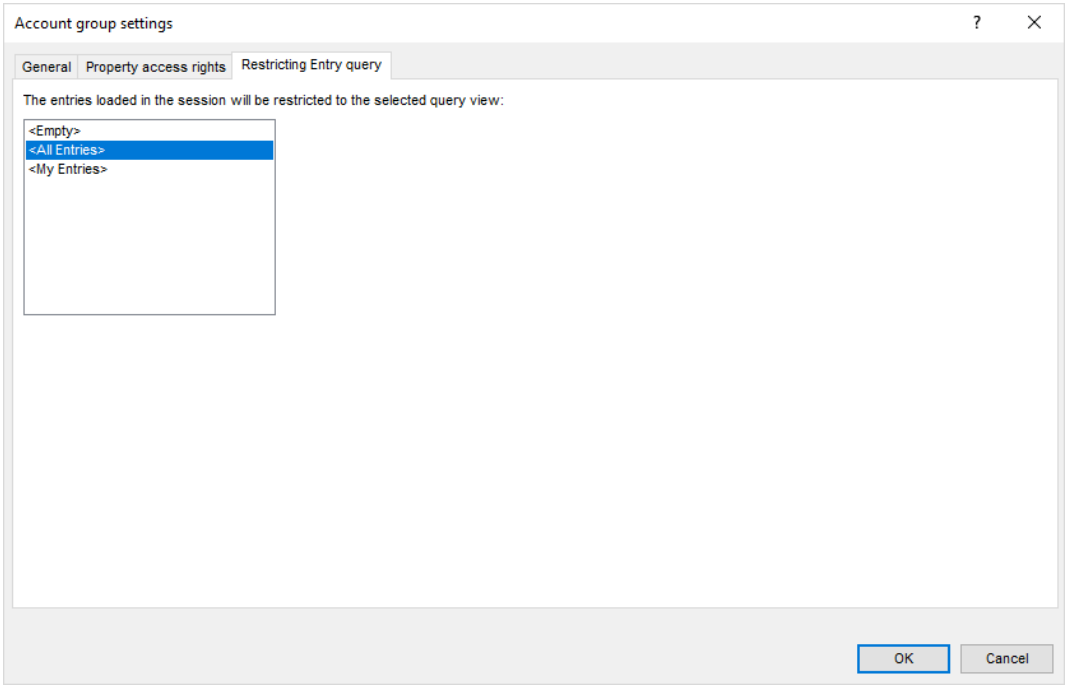

Figure 5: Entry views.

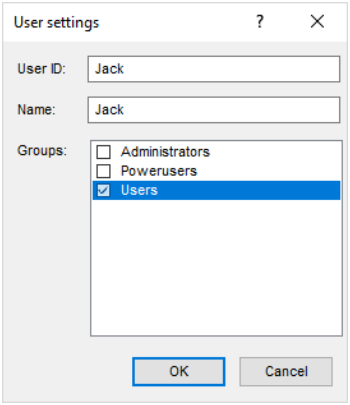

Figure 6: Add a new user to the database.

This dialog box allows you to specify a unique ***User ID*** for a new user, which cannot be changed later on. Optionally, a ***Name*** can be entered for the user. The bottom part of the dialog lists all user groups that are defined in the database. Via the check boxes, one or more groups that the user should be belong to, can be selected.

2. Specify a unique ***User ID***, (e.g. **Admin**), optionally a ***Name***, check the **Administrators** group and press <***OK***> to add the user to the *Users* panel of the *User management* window.

3. Select ***Users*** > ***Add new...*** (+) again, specify a unique ***User ID***, (e.g. **Jack**), optionally a ***Name***, and check the **Users** group. Press <***OK***> to add the user to the *Users* panel of the *User management* window.

As soon as more than one user is defined in the database, one can switch between different users by closing and reopening the database.

4. Close the *User management* window and the *Main* window. Reopen the database.

The *User* dialog box pops up (see Figure 8) prompting for the ***User ID*** and ***Password***. By default,

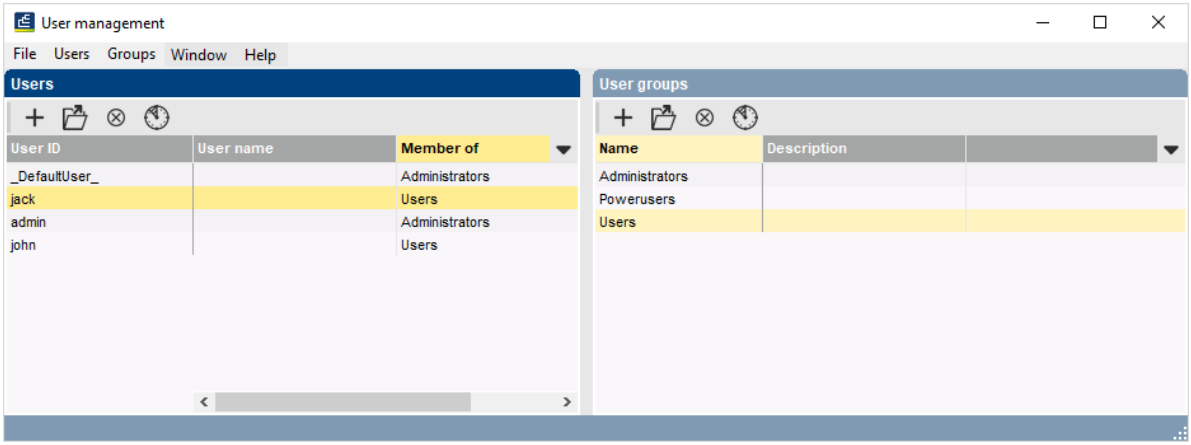

Figure 7: New users added to the database.

the name of the Windows user is displayed in the ***User ID*** text box. When no ***Passwords*** have been assigned to the users (see 6), this field can be left blank.

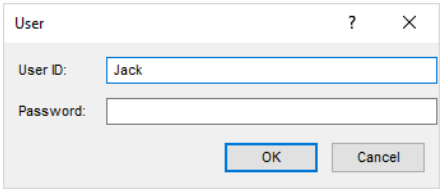

Figure 8: The *User* dialog box.

5. Specify the correct User ID for a user belonging to the **Administrators** (e.g. **Admin** in this tutorial) and press <***OK***>.

The status bar at the bottom of the *Main* window displays the name of the user that is currently logged on.

6. Select ***Database*** > ***User management...*** to call the *User management* window.

7. Select ***Users*** > ***Add new...*** (+) again. This brings up the *User settings* dialog box.

8. Select the **_DefaultUser_** from the list of users and select ***Users*** > ***Remove highlighted...*** (⊗) and confirm the removal of the default user.

9. Close the *User management* window and the *Main* window. Reopen the database.

10. Login with a user that belongs to the ***Users*** group (e.g. **Jack** in this tutorial) and press <***OK***>.

11. When logged in as **Jack**, belonging to the **Users** user group, check that no user management alterations (among many other modifications) are allowed for this group by selecting ***Database*** > ***User management...***.

A dialog box is displayed, indicating that this user is not allowed to access the user management settings (see Figure 9).

Figure 9: Error message.

6 Assigning passwords to users

Assigning passwords to users is optional in BIONUMERICS, but it is recommended for security reasons.

1. To define (or change) a password for the user that is currently logged on to the database select ***Database*** > ***Current user*** > ***Change password...*** and confirm the action.

This calls the *Change password* dialog box.

2. Type the current password of the user next to ***Current password***. If no password has been assigned to the user, leave this field blank.

3. Type the ***New password*** and re-enter the new password for confirmation (***Confirm new password***).

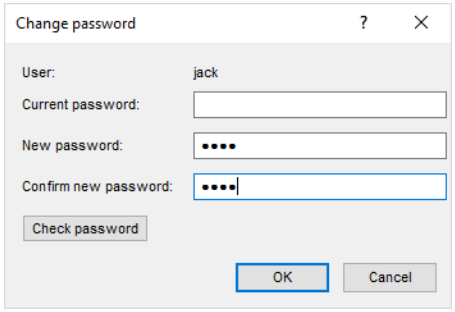

Figure 10: Enter and confirm the new password.

4. Press the <***Check password***> button to check if the new password meets the password criteria. Standard user passwords should be at least 4 characters long. Improved security can be achieved when *strong* user passwords are enforced in the database (see further in this section).

5. Press <***OK***> to save the new password of the current user in the database.

BIONUMERICS encrypts the password in such a way that the original password can not be recovered.

A user belonging to the ***Adminstrator*** user group can change the user authentication settings (e.g. enforce a (strong) password for every user that tries to log on, change passwords after a certain period of time, etc.).

6. Close the *Main* window and reopen the database.

7. Login as a user belonging to the ***Administrator*** user group, e.g. **Admin** in this tutorial.

8. Select ***Database*** > ***Database settings...*** to open the *Database settings* dialog box and click the *Security tab*.

9. Check ***Require passwords*** to enforce a standard user password of at least 4 characters long.

All users having no password in the database, are prompted to specify a password when logging on to the database.

10. Improved security can be achieved when checking the option ***Require strong passwords***.

A strong user password in BIONUMERICS should be at least 8 characters long, including as least two alphabetic characters, and should have a complexity score of 20. The complexity score is calculated using following scoring rules: new alphabetic character: **+2**; alphabetic character: **+1**; new non-alphabetic character (e.g. numeric characters, %, ?): **+4** points; non-alphabetic character: **+2**. When the option is checked, all *new* passwords specified in the database, have to meet the strong password criteria. Passwords that were stored in the database *before* the option ***Require strong passwords*** was checked, and that do not meet the strong password criteria, can still be used in the database. Users having no password in the database, are prompted to specify a strong password when logging on to the database.

11. Change the number of days in the ***Password validity time*** text box to set an expiration date for passwords.

The passwords assigned to users in the database will only be valid for the period specified. When the validity time of a user's password has expired, the software will prompt for a new password when logging on to the database.

12. Close the *Main* window and reopen the database.

13. Login as a user belonging to the ***Administrator*** user group, e.g. **Admin** in this tutorial. When no password is linked to the user, a new (strong) password is prompted for. Enter a new password and confirm.

Sometimes users forget the password they need to log into the database. When this happens, users must request assistance of another user that belongs to a user group that has the privilege to reset a password in the database (***Allow Modify Users*** rule). Users assigned to the default user group **Administrators** are able to reset passwords in the database.

14. To reset a password for a user, select ***Database*** $>$ ***User management...*** to call the *User management* window. Highlight the user in the *Users* panel of the *User management* window (e.g. **Jack**), select ***Users*** $>$ ***Reset password...*** and confirm the action. When a password is reset, it will effectively be blank.

A new password should be specified by first logging as the user whose password was reset:

15. Close the *User management* window and *Main* window and reopen the database.

16. The ***User ID*** should be entered in the *User* dialog box and the password field left blank. Next, press $<$***OK***$>$.

17. Leave the ***Current password*** field blank, type the ***New password*** and re-enter the new password for confirmation (***Confirm new password***). Press $<$***OK***$>$ to set the new password.

7 Logging user activity

Sometimes institutes might want to keep track of the different BIONUMERICS users that are logging onto a database. In addition, failed authentication attempts and changes made to the database system parameters might be of interest. A user belonging to the ***Adminstrator*** user group can activate the logging of the user activity in the database.

1. Close the *Main* window and reopen the database.

2. Login as a user belonging to the ***Administrator*** user group, e.g. **Admin** in this tutorial.

3. Select ***Database*** > ***Database settings...*** to open the *Database settings* dialog box and click the *Security tab*.

4. Check the option ***Log user activity*** and close the *Database settings* dialog box.

Every user logged on the database can now consult the logged user activity actions.

5. Select ***Database*** > ***Current user*** > ***Show user activity log...*** in the *Main* window.

This action will load the user log events in the *User activity log* window (see Figure 11).

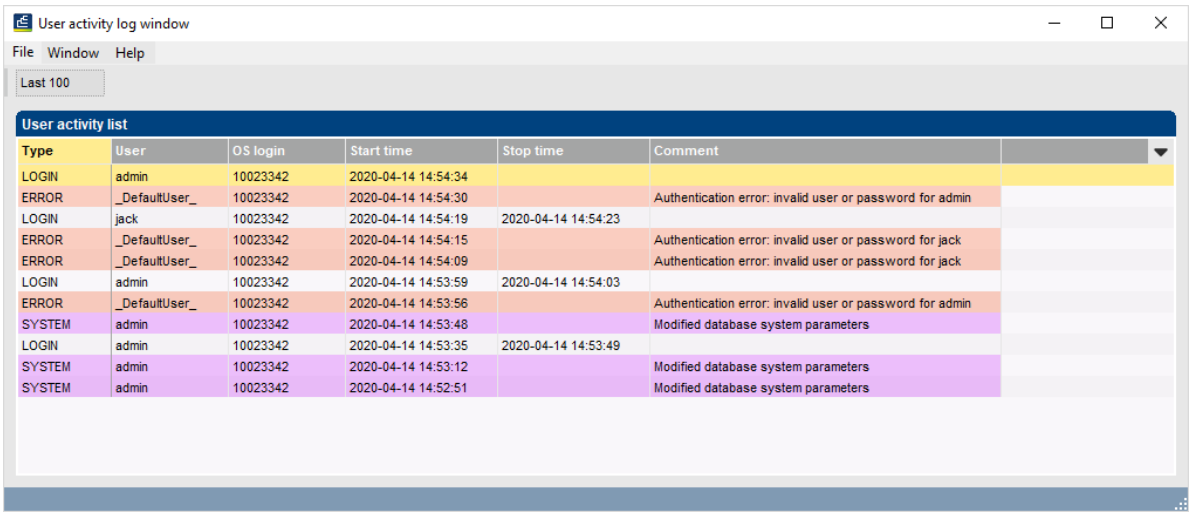

Figure 11: User activity log.

The type of activity that is recorded is displayed in the 'Type' column (LOGIN, INFO, ERROR or SYSTEM). Each type of activity is displayed in a different color.

- A LOGIN type activity is created each time the database has successfully been loaded by one of the users. The user is displayed in the 'User' column, and the time the database was opened and closed is shown in the 'Start time' and 'Stop time' columns respectively. The Windows user is shown in the 'OS login' column.
- Every change of current user in the database is reported as an INFO action in the list. The name of the newly logged on user is shown in the 'User' column, and the time the change occurred is displayed in the 'Start time' column. Timestamps are indicated following the ISO 8601 notation, optionally with indication of the time zone. The windows user is shown in the 'OS login' column.
- Changing settings in the *Database settings* dialog box is recorded as a SYSTEM type activity. The user who has made the changes in the database is displayed in the 'User' column, the Windows user is shown in the 'OS login' column. The 'Start time' reflects the time the database system parameters were saved in the database.
- Every unsuccessful login and failed attempt to sign an object (see BIONUMERICS reference manual for more details) is reported as an ERROR action. The User ID is displayed in the 'Comment' field and the time the error occurred is displayed in the 'Start time' column. The Windows user is shown in the 'OS login' column.

6. Close the *User activity log* window with ***File*** > ***Exit***.

8 Users and objects

8.1 Introduction to objects

In a BIONUMERICS database, all major data classes are seen as *objects*. In many cases, an object corresponds to a single record in a single table. Examples of such objects are database entries, fingerprint files, comparisons, etc.. However, an object can also correspond to a set of records, even from different tables. Examples are character experiments and sequences in case the sequences were assembled from trace files. Lists of BIONUMERICS database objects are often displayed in *object grid panels*. The grid consists of information fields organized in columns and database objects of a certain type in rows.

8.2 Object access settings

Any object in the database can be locked or unlocked, and has ownership and sharing settings. These settings are referred to as *object access settings*. The owner of each database object, which is by default the user who created the object, is displayed in the ***Owner*** column in each object grid panel.

1. To display the ***Owner*** column in a panel (e.g.. the *Experiment types* panel), click on the column properties button in the information fields header and select ***Set active fields*** (see Figure 12).

2. Check ***Owner*** from the list and press <***OK***>.

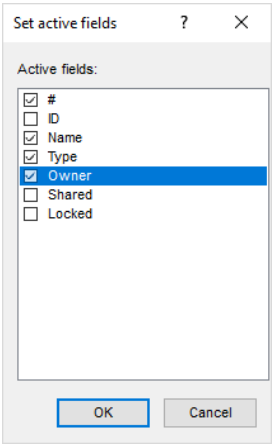

Figure 12: Set active fields.

The ***Owner*** column is now added to the *Experiment types* panel.

3. Double-click on an experiment in the *Experiment types* panel and choose ***File*** > ***Object access status...*** to call the *Object access* dialog box.

All object access settings of an object are displayed in the *Object access* dialog box. The *Object access* dialog box allows to change the ***Object access status*** and ***Object ownership*** for an individual object (see Figure 13).

Under ***Access privileges***, all possible actions on an object are listed and whether or not this action is allowed for the user that is currently logged in. If an action is not allowed, the reason why is displayed. The ***Access privileges*** cannot be modified in the *Object access* dialog box (the list is read-only) and should be set at the level of user management.

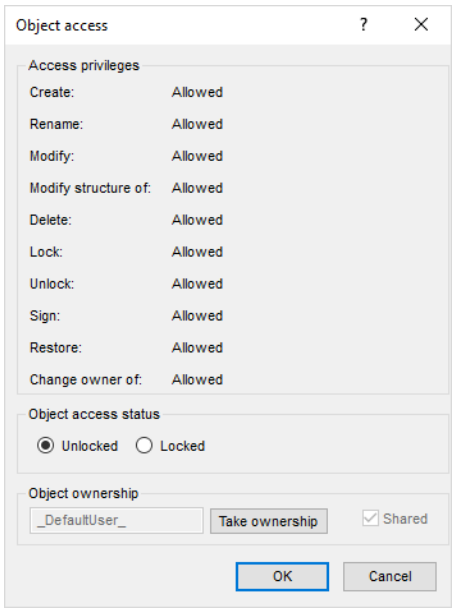

Figure 13: The *Object access* dialog box.

The ***Object access status*** of an object can be either ***Unlocked*** or ***Locked***. If an object is locked, it will not be possible to overwrite the object in the database, until the lock is reset by a user with this privilege.

Each object in the database has an *owner*, which is by default the user who created the object. The current user can be made owner of the object by pressing <***Take ownership***>, if he/she has the privilege to do so. An object can furthermore be made ***Shared*** or not by checking the corresponding check box. Objects that are not shared can only be edited by their respective owners; shared objects can be edited by any user who has the ***Access privileges*** to do so.

When the object is locked by checking ***Locked*** followed by <***OK***>, a ”padlock” icon ( ) will be displayed left of the object. If now the object information is modified and an attempt is made to save the changes to the database, the save action will be prevented and an ”Invalid action” error message generated.

8.3 Object views

An object grid panel does not necessarily displays all available database objects of a certain type. Instead, it provides a dynamical *view* on the objects. One can easily switch from one view to the other via the Views drop-down list, displayed in the toolbar of the object grid panel.

4. Make sure the ***Owner*** column is displayed in the *Experiment types* panel (click on the column properties button in the information fields header, select ***Set active fields***, and check ***Owner***).

5. Click on the ***Views*** drop-down list in the toolbar of the *Experiment types* panel (see Figure 14).

6. Select the <My Experiment types> view from the list.

The <My Experiment types> view will display all objects of which the currently logged-in user is the ***Owner***.

7. Click on the ***Views*** drop-down list in the toolbar of the *Experiment types* panel again but now choose <Manage user defined views. . . >.

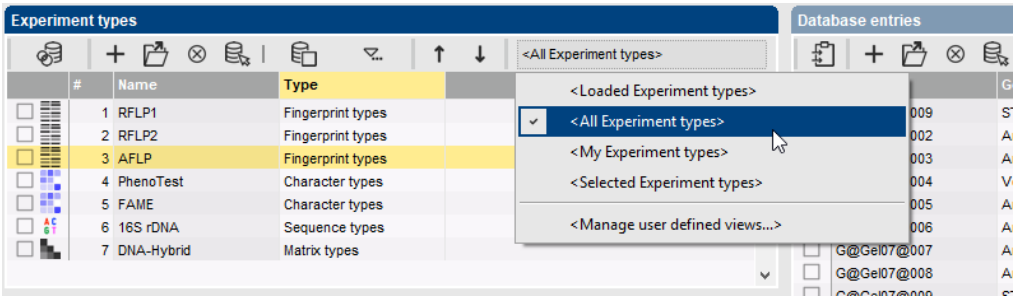

Figure 14: An example of a Views drop-down list, here from the *Experiment types* panel.

This will display the *Manage user views* dialog box. Under ***Show predefined views***, all predefined views are listed. The drop-down list ***Startup view for*** <***Database Level***> displays a list of all available views (predefined and custom views), of which one can be selected as the startup view, i.e. the view that will be used when the database is opened.