

AFO 611 - Passwords

611.1 Introduction

The system has a number of refined security mechanisms, password control being the most important. You can optimize your system's security using AFO 611, password control.

Function and characteristics of a password

When logging in, you must enter a password. This password has the following functions:

- it controls the user permissions within the system;
- it determines the language in which the system communicates with the user (Dutch, English or French).

Passwords can be a minimum of three and a maximum of ten characters long. A password may consist of numeric characters, alphanumeric characters or a combination of the two. Punctuation marks are not permitted.

- The following data is linked to a password:
 - a name, which is displayed at login;
 - the language in which the system communicates with the user;
 - the files to which the password has access;
 - the settings to which the password has access;
 - a so-called extra - secret - code; this is optional;
 - the AFOs to which the password has access;
 - the default editing method to be employed by the user;
 - the permissions to start processes in 'memory' (that is, at a later time).

The system distinguishes the following types of passwords:

- the system password;
- 'ordinary' passwords.

System password

The system password differs from other passwords in a number of ways. The distinctive features are:

The system password provides extra options at specific points in the system, such as password control.

The system password can override locks set by the system at specific places in the software. This is particularly true of AFO 111, 'Cataloging', where the system password has access even to locked descriptions. This is one of the reasons why it is best not to use the system password for normal functions.

Special password AAA

Bibliographic records and items that you add as 'new', will automatically be stored in a savelist under the system assigned user 'Automatic Savelists' (usercode AAA). Lists are stored to track the first items added to a bibliographic record as well as new items added (by year and by month).

The savelist AFVGPK contains a list of the bibliographic records which no longer contain a shelfmark (all items have been deleted).

This system user is generally available for viewing to all similar to the 'General Use' profile. Anyone can view the savelists by using the 'View savelists of user' (PW) option.

Only users with SYS! Privileges for AFO141 will be allowed to modify / delete the Automatic savelists contents. (Similar to the functions of the data stored under General Use).

'Normal' passwords

This are all other passwords.

Authorisation

Different types of permissions are associated with each password, all of which are described below:

Access to files

Each bibliographic file is characterised by a number. These numbers are linked to each password that offers access to the files.

Access to settings

Each setting within the system is expressed by a code. These codes are linked to each password that offers access to these settings.

Access to AFO's

Data is linked to each password giving the password access to the different AFO's.

Note!

A password that has access to AFO 611 'Password administration' can grant access to only those AFO's that the password itself has access to. In contrast, the system password can give access to all AFO's.

Access to options within AFO's

For specific 'core' AFO's such as cataloguing, subject headings control, borrowers and circulation administration, it is possible to limit specific options to specific passwords. A few examples for cataloguing are: permission to delete descriptions, permission to enter new subject headings, etc. In fact, these are permissions at the field level.

Extra security

In addition to passwords, the system also contains other security mechanisms. These are described below.

'Extra' code

A so-called 'extra' code can be linked to every password. This code is invisible within the system. Within password administration you can specify for every password whether or not the extra code is required at login. A user can change this extra code himself. This is done outside password administration, since this extra code is invisible, even to the system administrator. The relation between the password and the extra code is comparable to the distinction 'username/password' in operating systems such as Windows NT and Unix. This extra code only plays a role at login; the permissions and such are linked to the password, not the extra code. In addition, the period of validity for this code can be limited. If this period expires, the user must change the access code at login. The system alerts the user at login a few days before the access code expires.

'Special' access code

A so-called 'special' access code can be assigned to each activity. This provides extra security for these activities. The user must enter this special code before gaining access to AFO's secured in this manner.

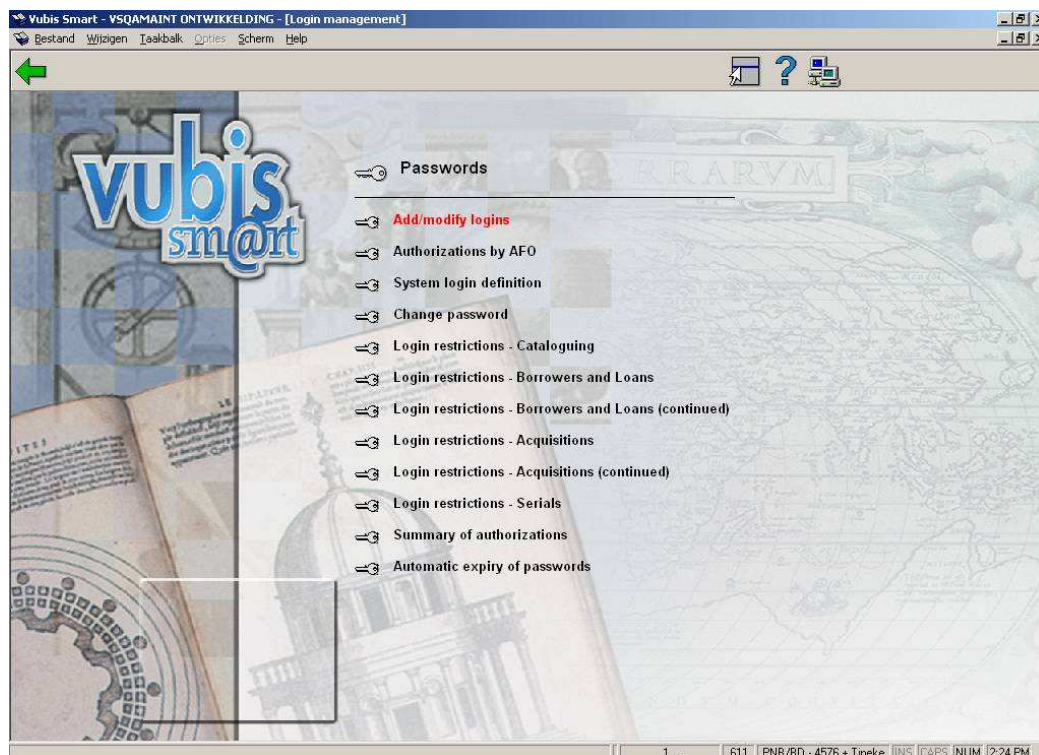
Display and system facilities

The system distinguishes between viewing display and system facilities for AFO 243 'Base funds control', AFO 423 'Item control', AFO 461 'Administrators control', AFO 475 'Patron statistics' and AFO 478 'Freely definable circulation statistics'. A password that only gives the user permission to view facilities also only allows the user to view and print data. A password with system facilities can also delete, update, add and enter data.

Blocking AFO's

You can block access to AFO's per (logical) port: you can specify which AFO's may and may not be accessed from a port (workstation). This is defined in AFO 612 'Ports'. Thus, you can assign a password to specific (logical) ports as a standard. Then the system will no longer request a password at login, but will automatically select the password associated with that port.

After you start AFO 611, a menu screen is displayed:

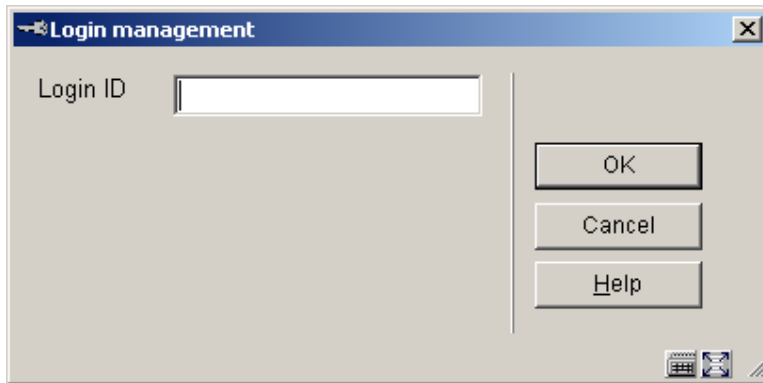


The menu options are discussed separately in the following paragraphs.

611.2. Add/modify logins

You can create and delete passwords and specify password permissions with this menu option.

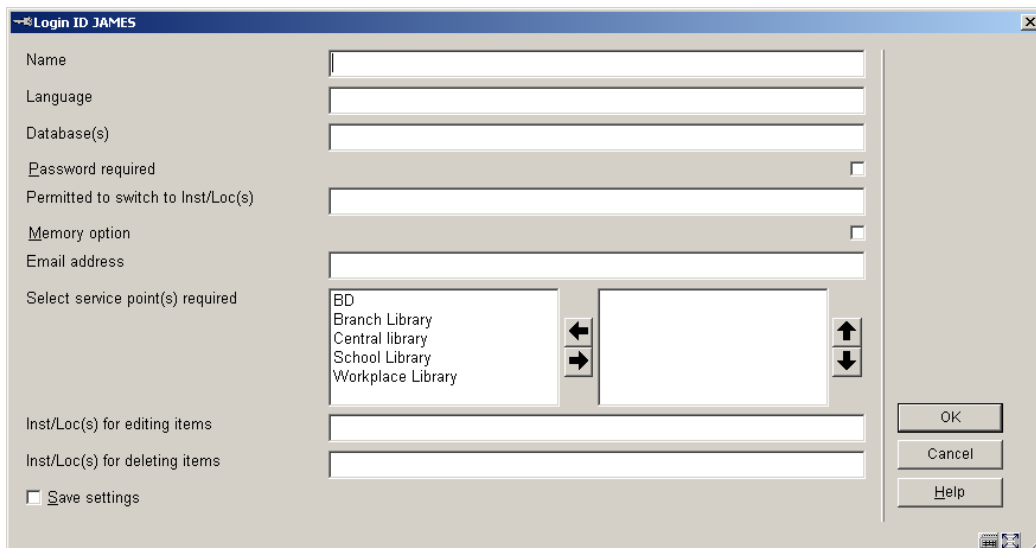
If you select this menu option, an input screen appears:



Enter an ID. A login ID may contain a minimum of three and a maximum of ten letters or digits. Punctuation marks are not permitted. No distinction is made between capital and small letters: the system automatically converts all ID's to capital letters.

If you enter a login ID that does not exist, the system automatically switches to the new input screen.

If you enter an existing login ID, an overview screen appears with a list of the data associated with that login ID, which you can change, if necessary.



Fields on the screen

Name: Enter the name associated with this login ID. This name may not contain any punctuation marks and may be a maximum of 20 characters.

Language: Enter the language the user will use to communicate with the system. Valid codes are dut (Dutch), eng (English) and fre (French).

Database(s): Enter the databases this login ID may log in to. Databases are indicated by a digit. Separate multiple digits with commas. The main database number is generally "2".

Password required: Specify whether an extra access code must be entered after the login ID has been entered.

Permitted to switch Inst/Loc(s): Enter the settings and/or locations to which this login ID has access. Examples: OBG/C, OBG/W or OBG/*, etc. Enter nothing if the login ID provides access to all institutions and/or locations. Separate institution and location codes by a / (forward slash); separate multiple institutions/locations by commas.

Memory option: Specify whether this login ID may use the memory option. This means that processes may be started later.

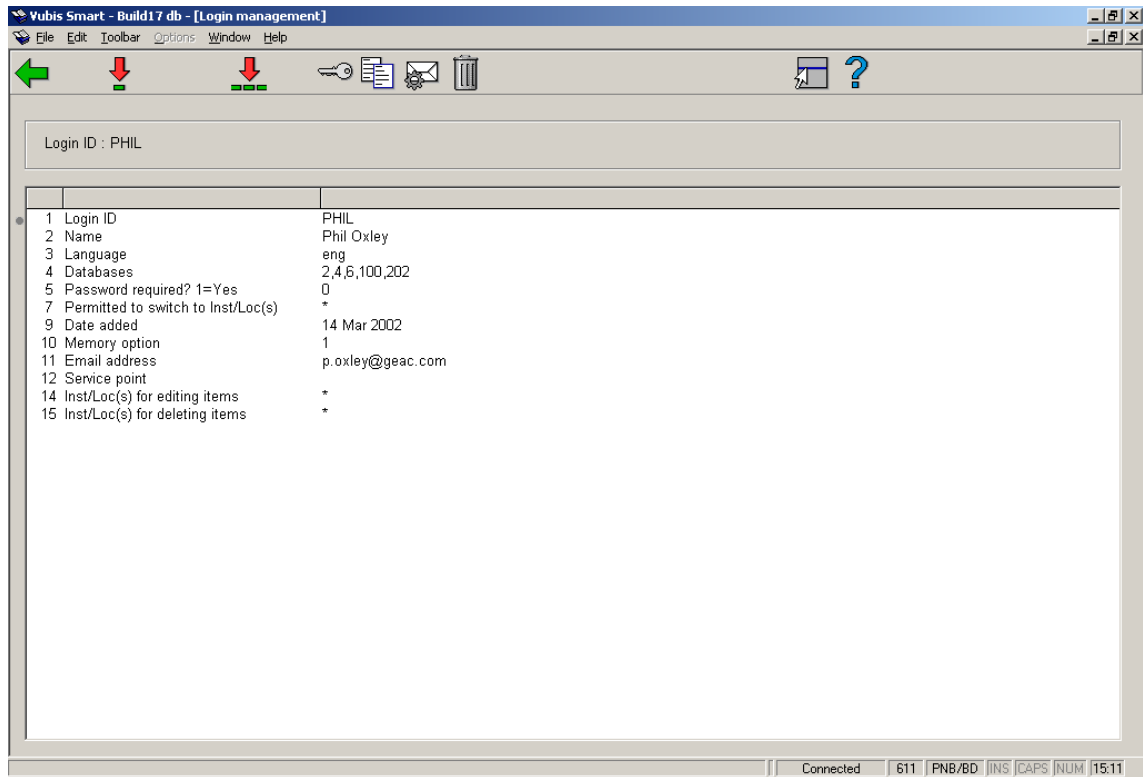
Email address: Optionally enter the email address. This can be used elsewhere in the system, e.g. on the technical overview screen of a bibliographic record.

Select service points required: when service desk are used for reservations messaging (see the Help on AFO 618 for more information) you can specify here which service desks are linked to this user.

Inst/Loc(s) for editing items: Specify for which institutions/locations this user can modify item information.

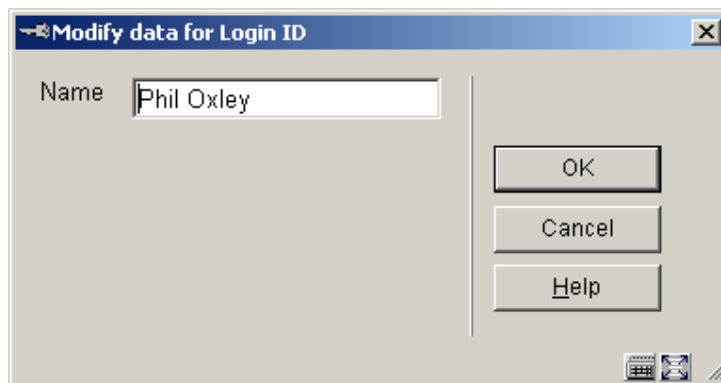
Inst/Loc(s) for deleting items: Specify for which institutions/locations this user can delete items.

Once you have entered the data, an overview screen appears:



Options on the screen

Modify line no. (+):Select a line number and then select this option to change the data:



Modify all data: Select this option to change all data for this password:

Modify data for Login ID PHIL

Name: Phil Oxley

Language: eng

Database(s): 2,4,6

Password required:

Permitted to switch to Inst/Loc(s): *

Memory option:

Email address: p.oxley@geac.com

Select service point(s) required: deb's Desk (English)

Inst/Loc(s) for editing items:

Inst/Loc(s) for deleting items:

OK Cancel Help


Note

If you wish to change the ID itself, you must first delete the existing one and then add the new form. For example, if you want to change the login ID 'ABC' to 'XYZ', you must first delete 'ABC' and then add 'XYZ'.

Delete: Select this option to delete the login ID.

Email parameters: Choose this option to set the email parameters:

Email parameters for acquisitions [X]






Check the first box of each pair to send notices by email.
Check both boxes to send notices by post and email.

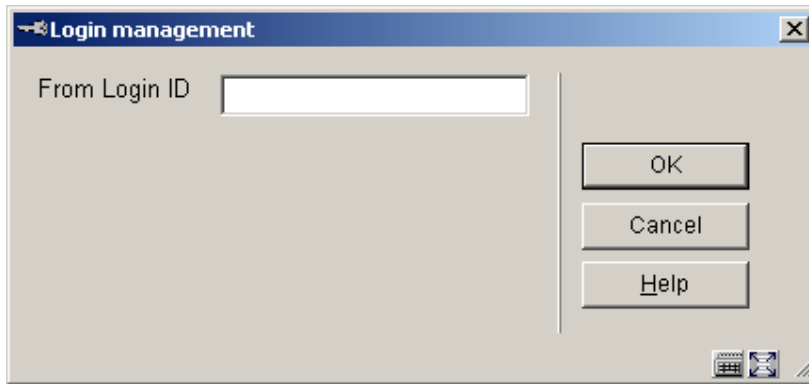
<u>N</u> ormal orders	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>E</u> xpress orders	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>U</u> rgent orders	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>F</u> irst claim	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>S</u> econd claim	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>C</u> ancellation notification	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>N</u> otification for users	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>N</u> otification for suppliers	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>R</u> eceipt notification	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>
<u>R</u> eceipt notification for individual documents	<input type="checkbox"/>
<u>S</u> till send by post	<input type="checkbox"/>

Save settings

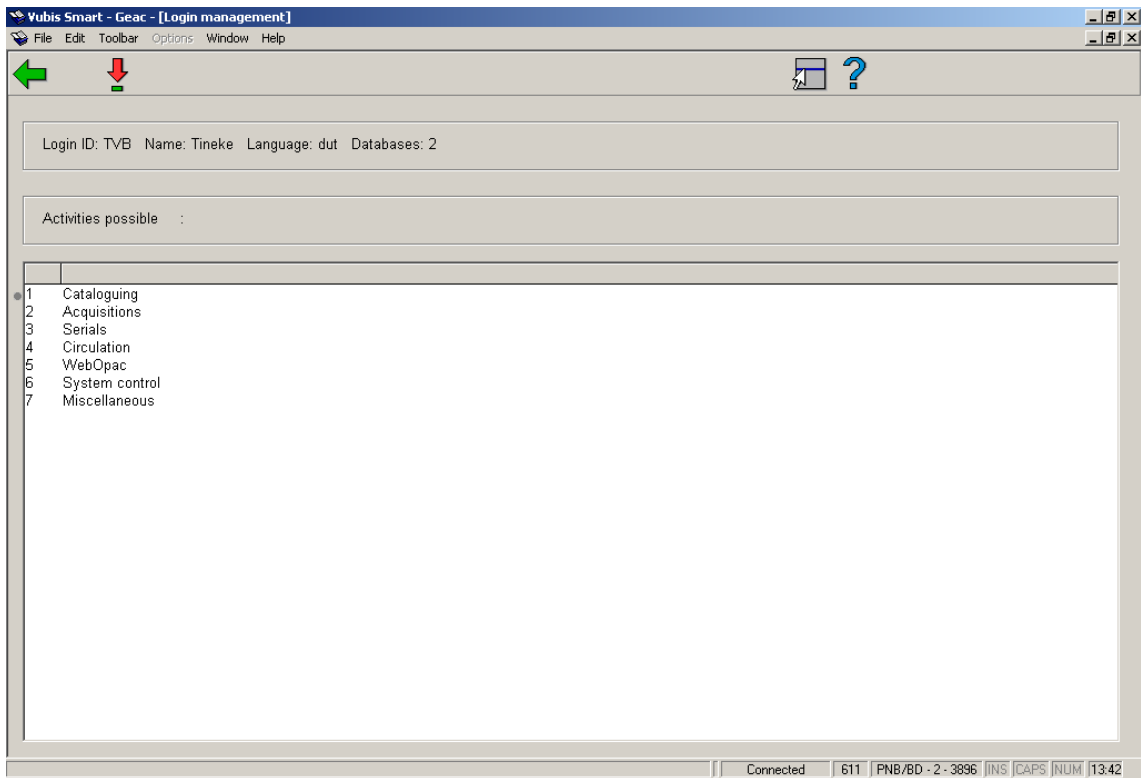
OK
Cancel
Help

Copy: Select this option to copy the permissions associated with another login ID to the login ID on the screen. An input screen appears. Here you enter the login ID whose permission data you wish to copy to the login ID on the screen. The login ID to which you are copying the data is granted access to the same AFO's as the login ID from which you have copied the data:



Modify authorisations: Choose this option to modify the authorisations for this login ID. An overview screen with all modules is displayed:

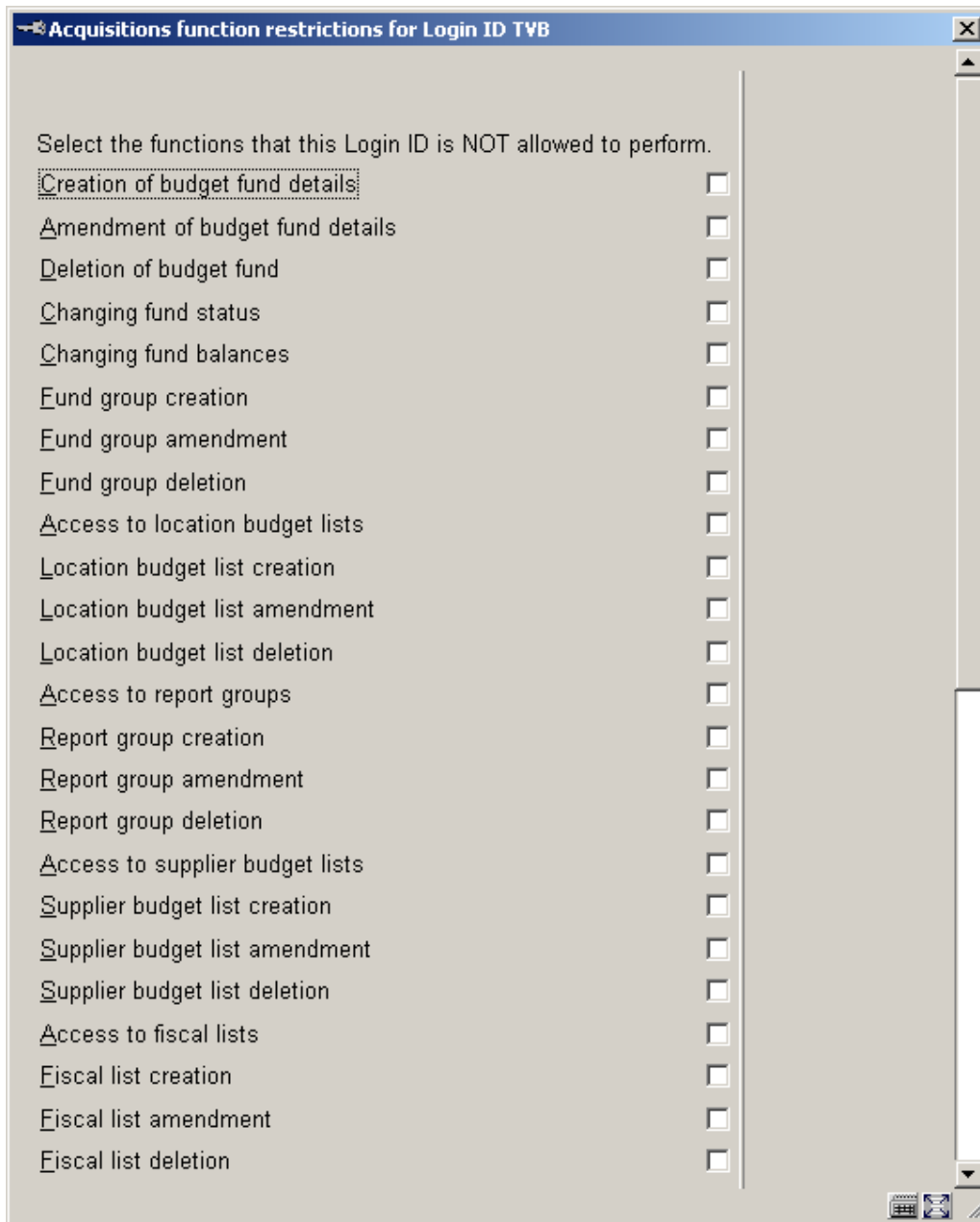


Choose AFO (+):Select the desired module from this list. An input screen appears with the AFO's for this module. Now you can select all the AFO's to which this password should be given access:



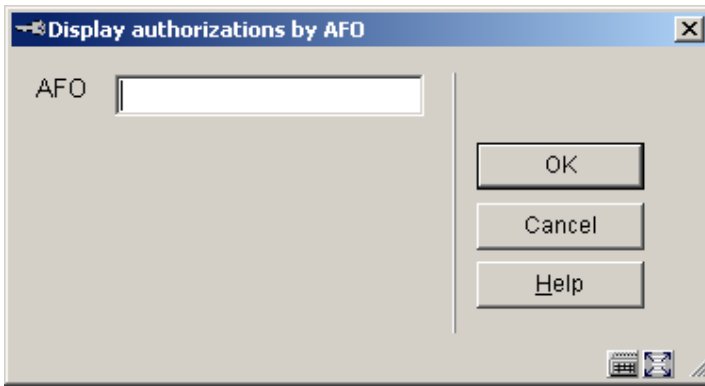
Note

For some modules (acquisitions, circulation, serials) a second screen is displayed. Here you can specify which functions the login ID may NOT perform:

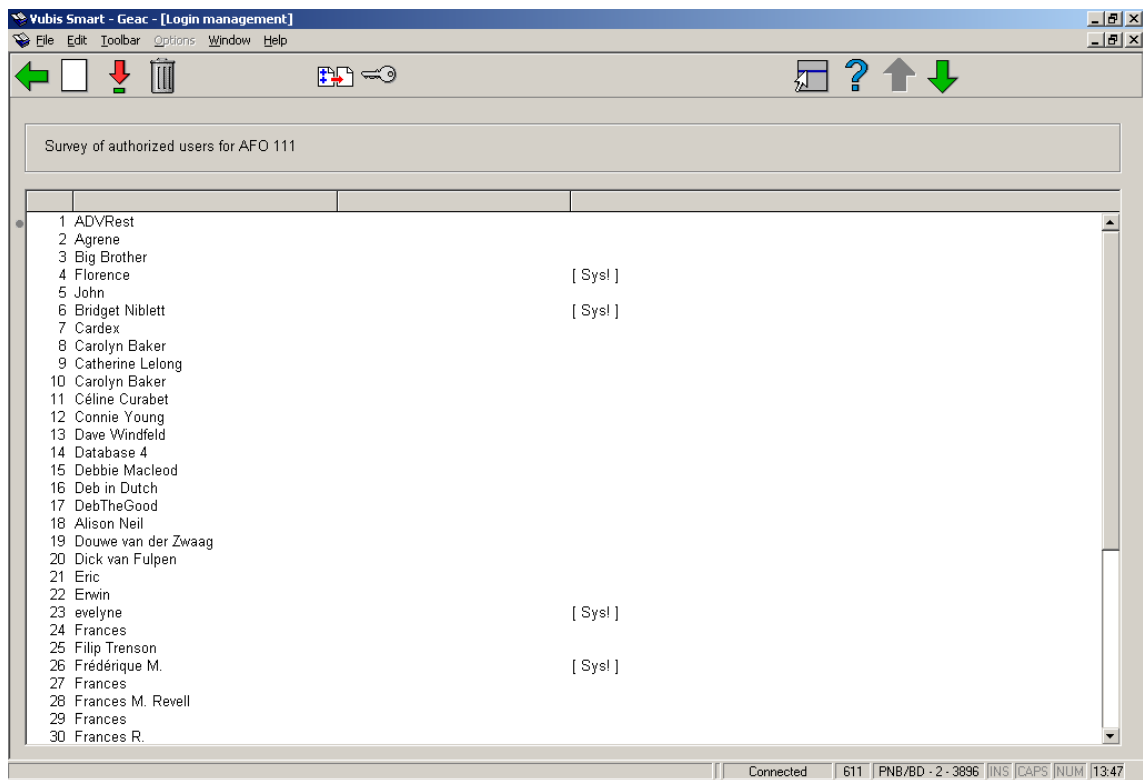


611.3 Authorisations by AFO

This menu option provides an overview of the login ID's that have access to an AFO. If you select this menu option, an input screen appears:



AFO: Enter an AFO number. An overview screen appears of all the login ID's that have access to the AFO specified:



Notes

If you have logged in with the system login ID, the system displays the permissions for this login ID in sequence, followed by the actual login ID. If you have logged in using an 'ordinary' login ID, the system only shows the name associated with the login ID.

In the last column, the system indicates whether the password has permissions for system facilities in the AFO. If the last column is empty, the password has only permission to view

facilities. If a password has system facilities, this is indicated by the word '[Sys!]' in the last column.

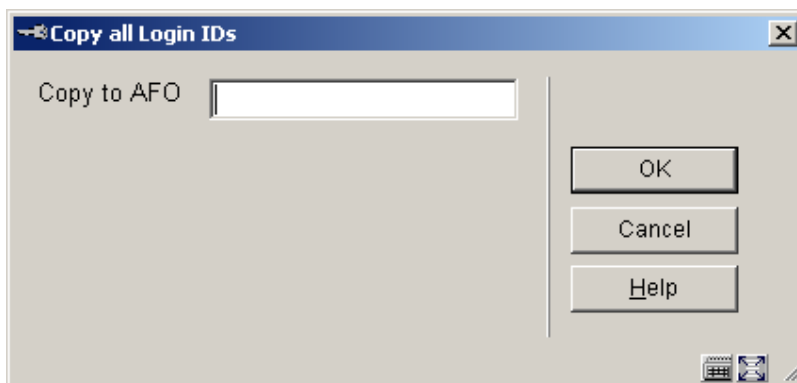
Options on the screen

Add login ID: Select this option to add a login ID to the list. An input screen appears, in which you can enter the ID to be added.

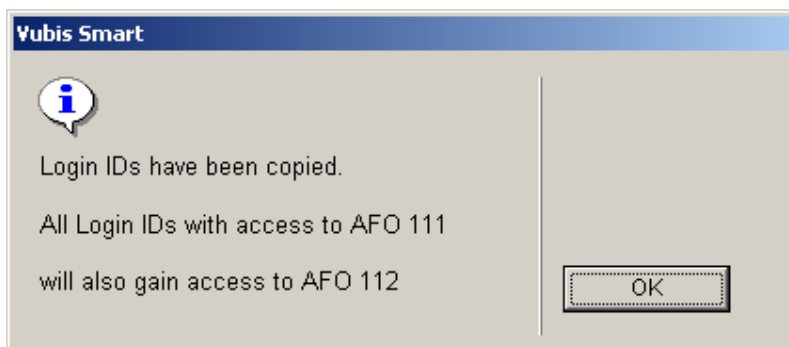
System privileges (+):Select a line number and then select this option to turn the system facilities for the AFO on or off for this login ID.

Delete login ID from list (+):Select a login ID and select this option to delete a login ID from the list.

Copy all login ID's to AFO: Select this option to copy all login ID's in this list to another AFO. An input screen appears. Here you can enter the AFO number to which the login ID's must be copied. The login ID's copied are added to the list with login ID's that are already displayed for this AFO:



The screenshot shows a dialog box titled "Copy all Login IDs". It features a text input field labeled "Copy to AFO" which is currently empty. To the right of the input field are three buttons: "OK", "Cancel", and "Help". The "Help" button has a small 'H' underlined. In the bottom right corner of the dialog box, there are three small icons: a keyboard, a mouse, and a help icon.

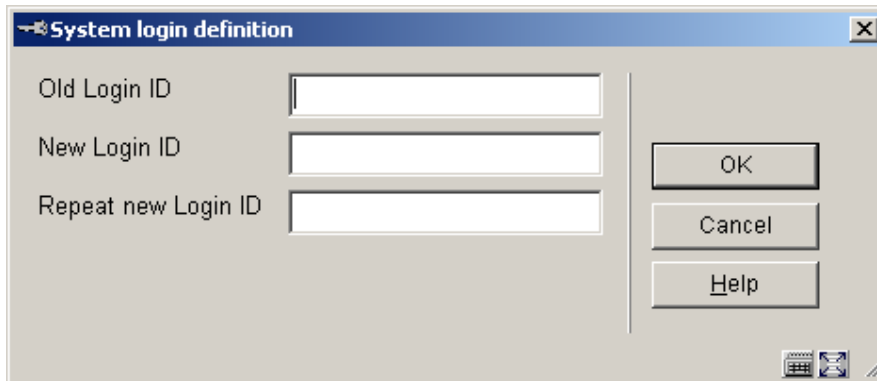


The screenshot shows an information dialog box titled "Vubis Smart". It contains an information icon (a lowercase 'i' in a blue circle) at the top left. Below the icon, the text reads: "Login IDs have been copied." followed by "All Login IDs with access to AFO 111" and "will also gain access to AFO 112". At the bottom right of the dialog box is an "OK" button.

Extra access code: A so-called 'special' access code can be assigned to each activity. This provides extra security for these activities. The user must enter this special code before gaining access to AFO's secured in this manner.

611.4 System login definition

You can change the system password. If you select this menu option, an input screen appears:



Fields on the screen

Old login ID: Enter the old system password.

New login ID: Enter the new system password.

Repeat new login ID: Enter the new system password again. If the code entered is not identical to the code in the previous field, the procedure is interrupted and the system issues a message stating that the system password has not been changed.

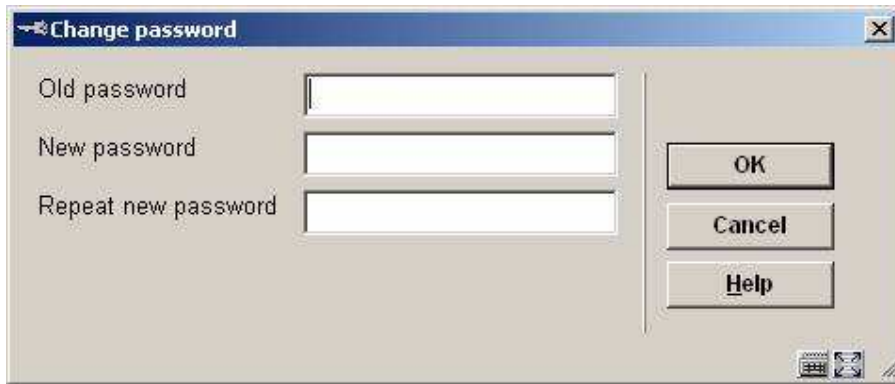
Notes

The passwords entered are not displayed on the screen.

Do not forget that the system password must also be defined as an ordinary login ID so that you can log in using it.

611.5 Change password

You can change the special password. If you select this menu option, an input screen appears:



Fields on the screen

Old code: Enter the old code.

New code: Enter the new code.

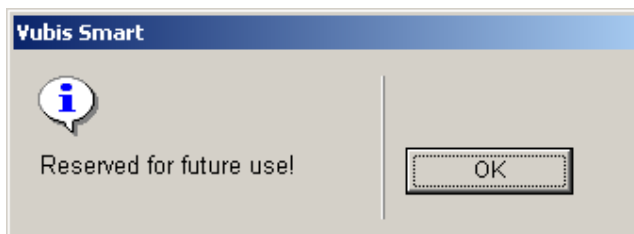
Repeat new code: Enter the new code again. If the code entered is not identical to the code in the previous field, the procedure is interrupted and the system issues a message stating that the code has not been changed.

Note

The passwords entered are not displayed on the screen.

611.6 Login restrictions - Cataloguing

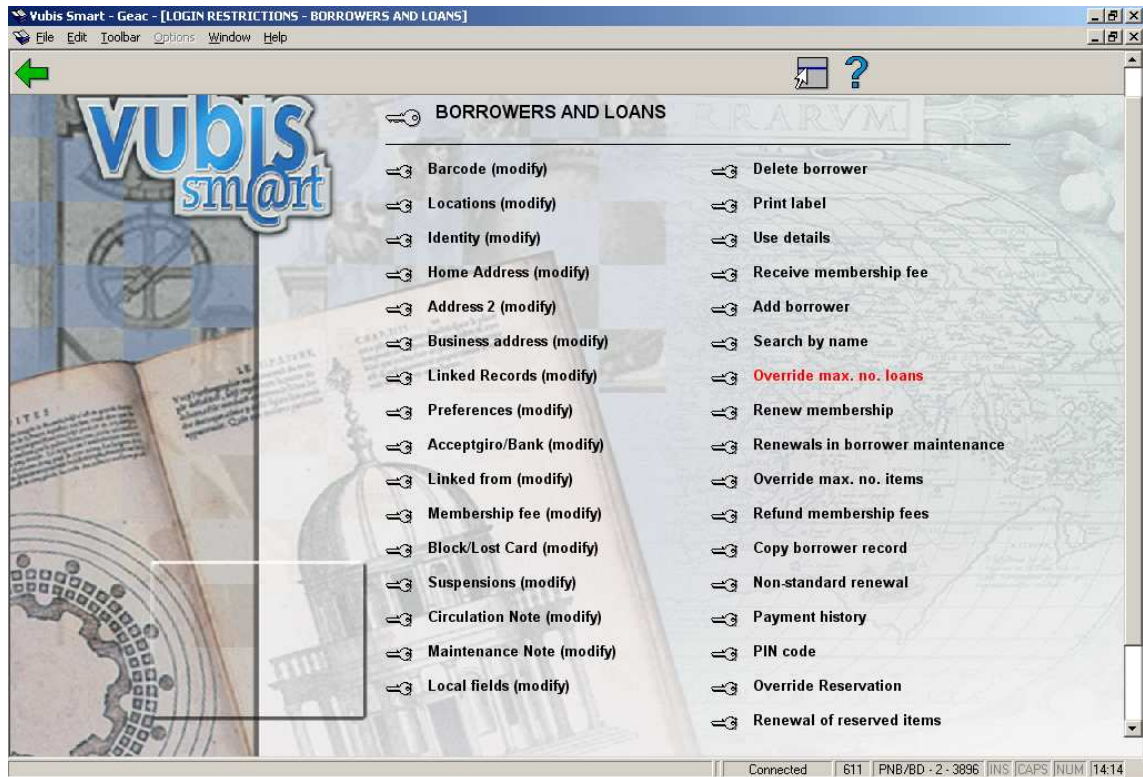
This option is not in use.



611.7 Login restrictions – Borrowers and loans

This menu option allows you to link specific options to a login ID. You can deny login ID's access to options within the circulation and borrower administration. This option involves AFO 411 ('Loans') and AFO 431 ('Borrower administration').

If you select this menu option, a menu appears with the options that can be linked to a login ID:



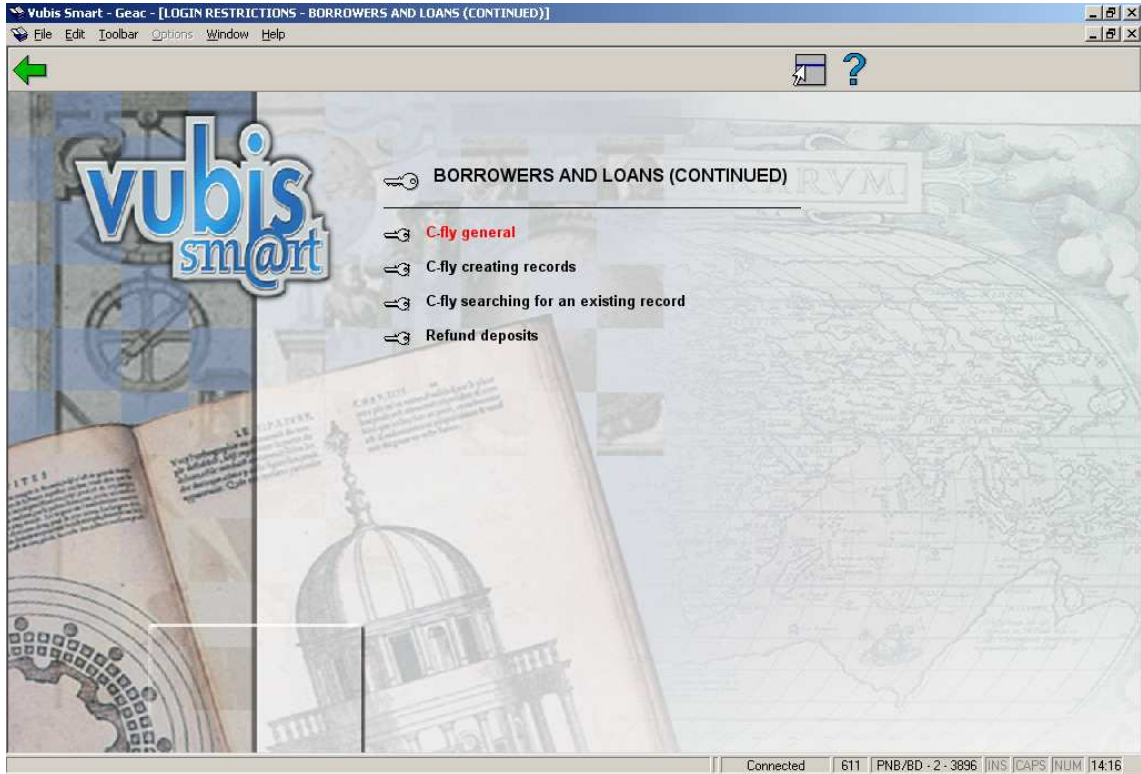
Menu options on the screen

Select the desired menu option. Now you can add login ID's with an input screen or add or delete login ID's that are denied access to an option via this screen.

Note

Defining options is a 'negative' process. That is to say: in principle all login ID's have access to this option, except those you include in this list.

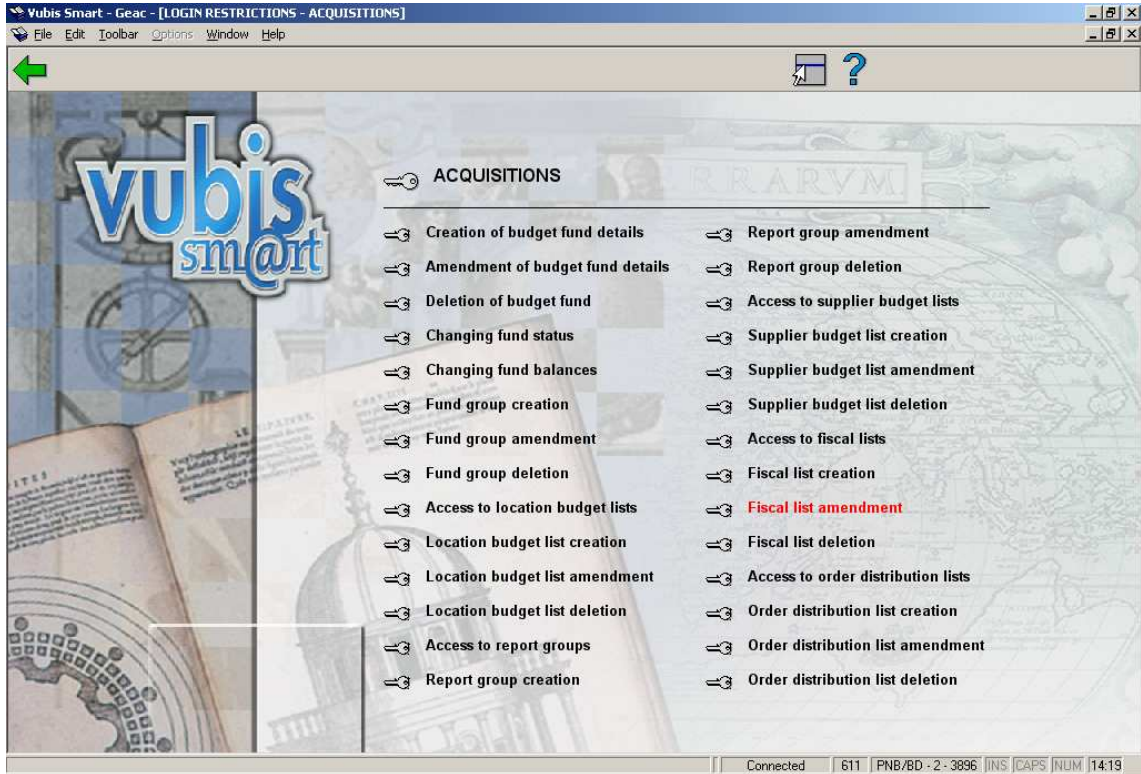
611.8 Login restrictions – Borrowers and loans (continued)



The procedure is the same as for "Login restrictions – Borrowers and Loans".

611.9 Login restrictions - Acquisitions This menu option allows you to link specific options to a login ID. You can deny login ID's access to options within the acquisitions module. This option relates to AFO 243 (Budget control) and 277 (Acquisitions lists).

If you select this menu option, a menu appears with the options that can be linked to a login ID:



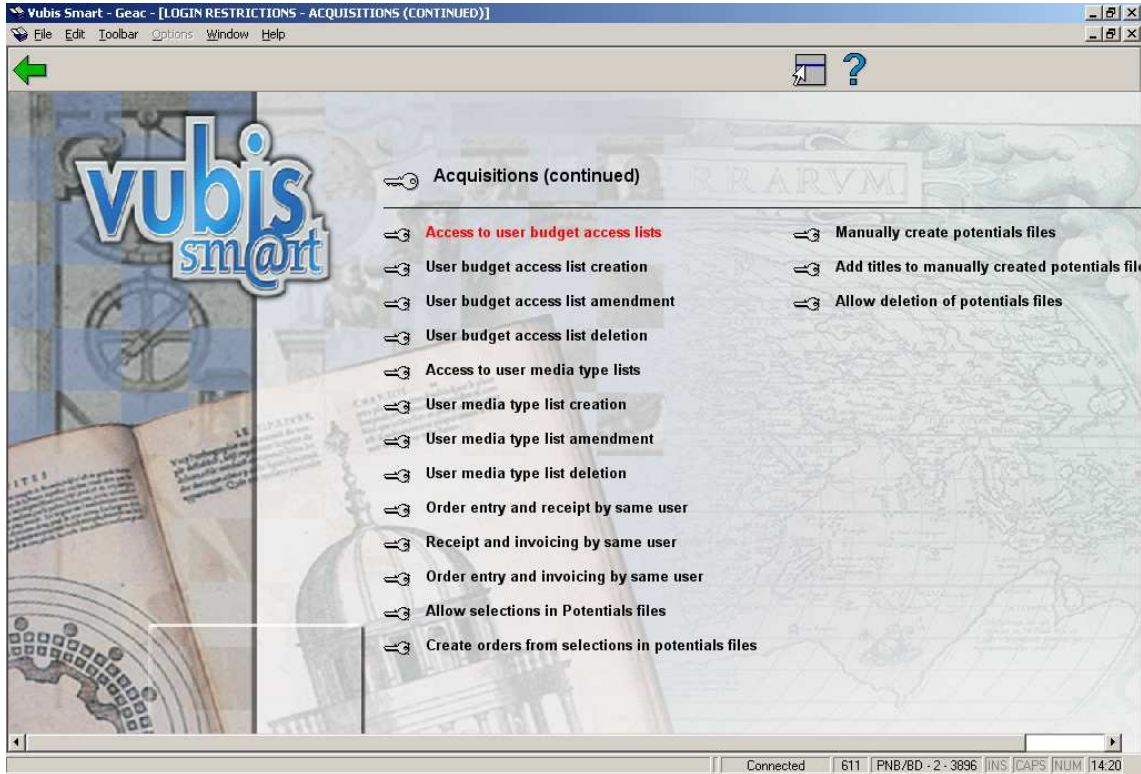
Menu options on the screen

Select the desired menu option. Now you can add login ID's with an input screen or add or delete login ID's that are denied access to an option via this screen.

Note

Defining options is a 'negative' process. That is to say: in principle all login ID's have access to this option, except those you include in this list.

611.10 Login restrictions - Acquisitions (continued)

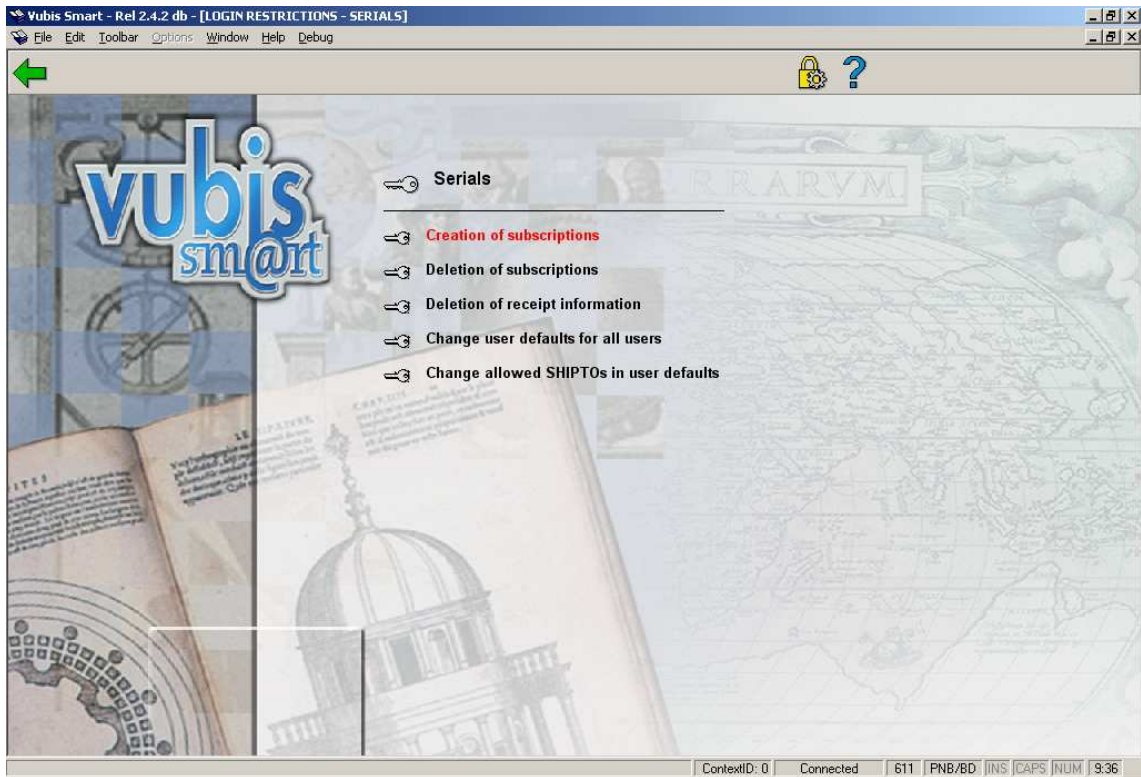


The procedure is the same as for "Login restrictions – Acquisitions".

611.11 Login restrictions - Serials

This menu option allows you to link specific options to a login ID. You can deny login ID's access to options within the serials module. This option relates to AFO's 311, 321 and 368.

If you select this menu option, a menu appears with the options that can be linked to a login ID:



Menu options on the screen

Select the desired menu option. Now you can add login ID's with an input screen or add or delete login ID's that are denied access to an option via this screen.

Note

Defining options is a 'negative' process. That is to say: in principle all login ID's have access to this option, except those you include in this list.

611.12 Summary of authorisations

Using this menu option you can view or print the permissions for one or more login ID's. If you select this menu option, an input screen appears:

The image shows a Windows-style dialog box titled "Summary of authorizations". It has a standard title bar with a close button (X). The dialog contains three text input fields stacked vertically. The first is labeled "From Login ID", the second "To Login ID", and the third "For inst./loc." which contains an asterisk (*). Below these fields is a checkbox labeled "Save settings". To the right of the input fields are three buttons: "OK", "Cancel", and "Help". The dialog box has a light gray background and a blue title bar.

Fields on the screen

From login ID: Enter the login ID from which to start the overview.

To login ID: Enter the login ID that ends overview.

Note

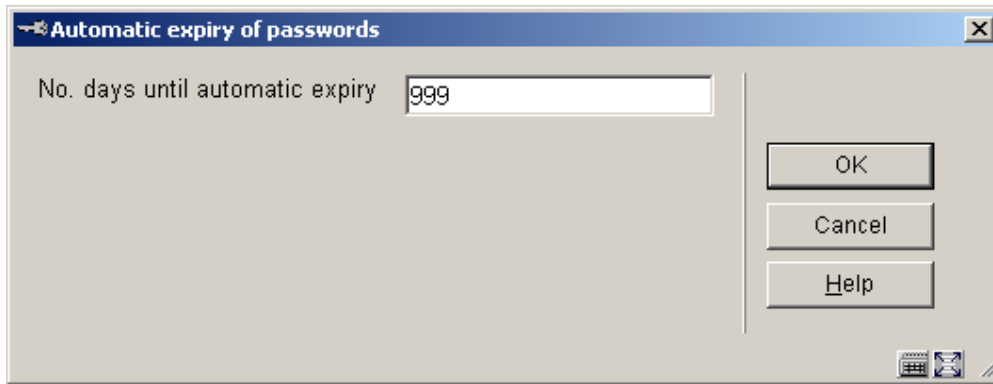
If you wish to create a list of all login ID's, leave the fields 'From login ID' and 'To login ID' blank.

For inst./loc.: Enter one or more agency and/or location codes (separated by commas) for which the list must be created. If you enter an "*" (asterisk) here, a survey will be created for all locations.

After you enter this data, the standard dialog box for generating output will be presented.

611.13 Automatic expiry of passwords

This menu option allows you to restrict the validity period for access codes (passwords). If you select this menu option, an input screen appears:



Fields on the screen

No. days until automatic expiry: Enter the number of days an access code (password) is to remain valid. When this period expires, the user will be forced to change his access code at login. The system will alert the user a few days before the access code expires.

- **Document control - Change History**

Version	Date	Change description	Author
1.0	unknown	creation	
2.0	September 2006	updates for release 2.4.1 build 17	
3.0	November 2006	merged in changes for release 2.4.2 serials maintenance updates	
4.0	March 2007	changed "access code" to "password", new screen shot	