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 50 characters long. A password may consist of numeric characters, alphanumeric characters as well as special characters or a combination thereof. The only characters not permitted are ^ and ~.

- 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 login ID’s

The system has several pre-defined special login ID’s that allow access to specific data sets.

AAA – Automatic savelists: 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).

General Use: 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.

VUBISWEB – WebOpac user: this can be used to retrieve circulation transactions information.

PUB – WebOpac Public user: this can be used for SSP reporting of WebOpac and ILL requests from WebOpac.

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.

Password encryption

This feature provides a mechanism to allow customers to use encrypted passwords for login into the application (as well as WebOpac Preferences).
The encryption feature is optional. The parameter is not interactive and can only be set by Infor staff.

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.

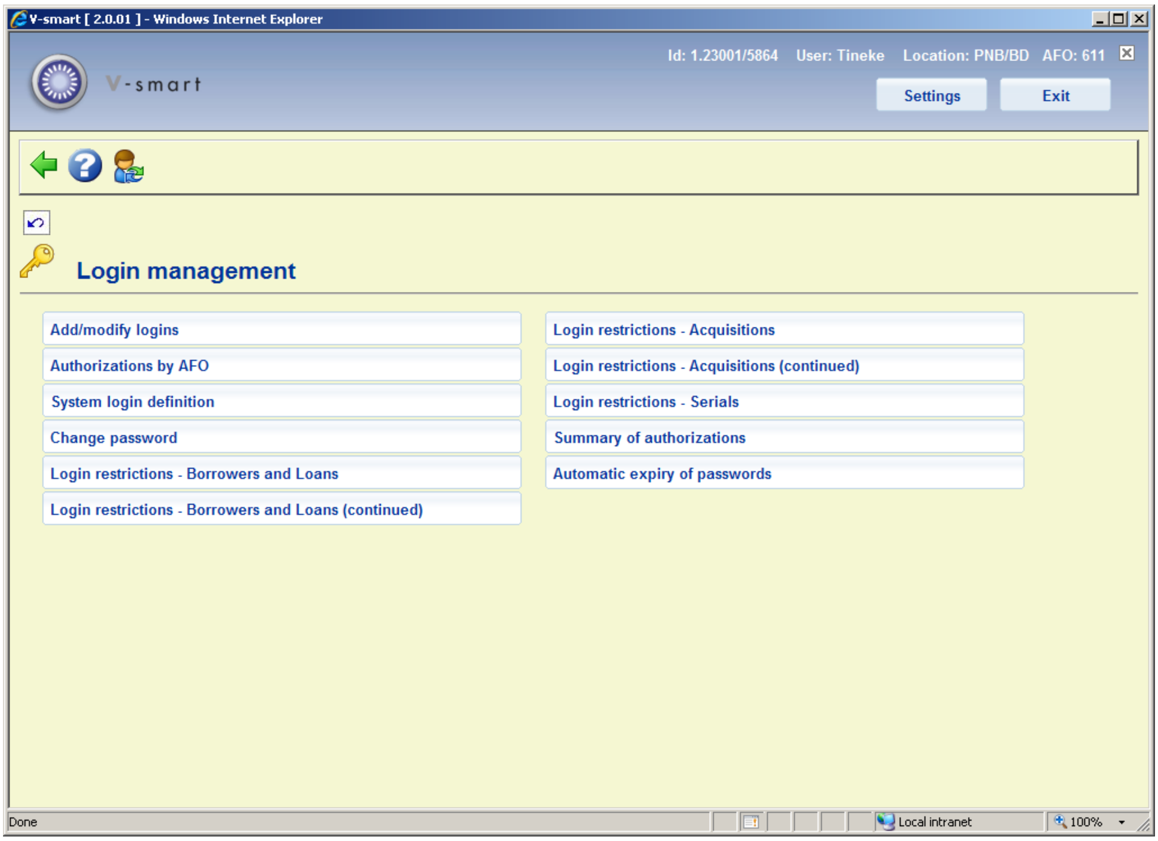
Display and system facilities

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:


V-smart [2.0.01] - Windows Internet Explorer
V-smart
Id: 1.23001/5864 User: Tineke Location: PNB/BD AFO: 611
Settings
Exit
Done
Local intranet
100%

Login management

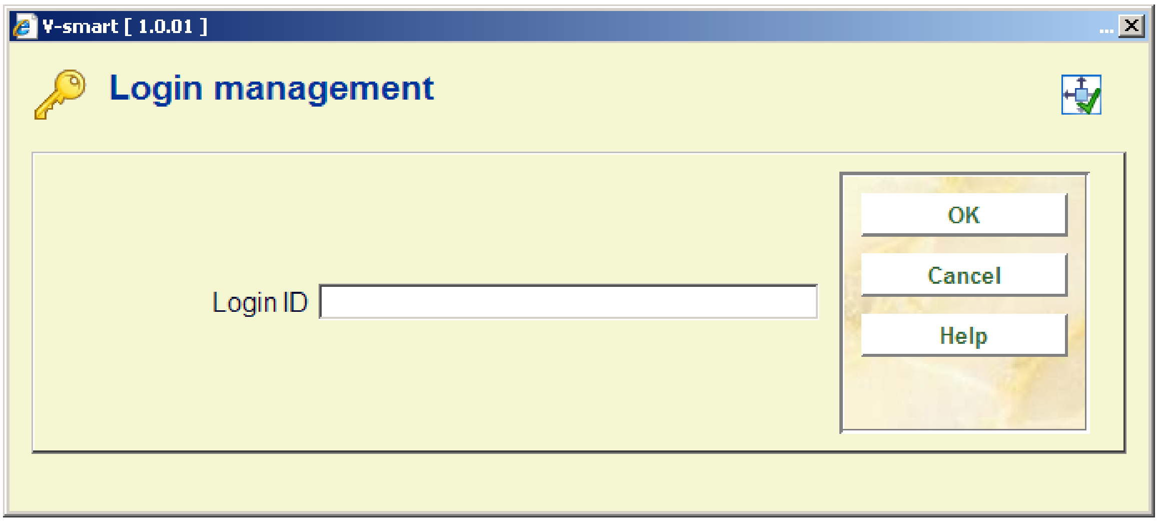
- Add/modify logins
- Authorizations by AFO
- System login definition
- Change password
- Login restrictions - Borrowers and Loans
- Login restrictions - Borrowers and Loans (continued)
- Login restrictions - Acquisitions
- Login restrictions - Acquisitions (continued)
- Login restrictions - Serials
- Summary of authorizations
- Automatic expiry of passwords

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:

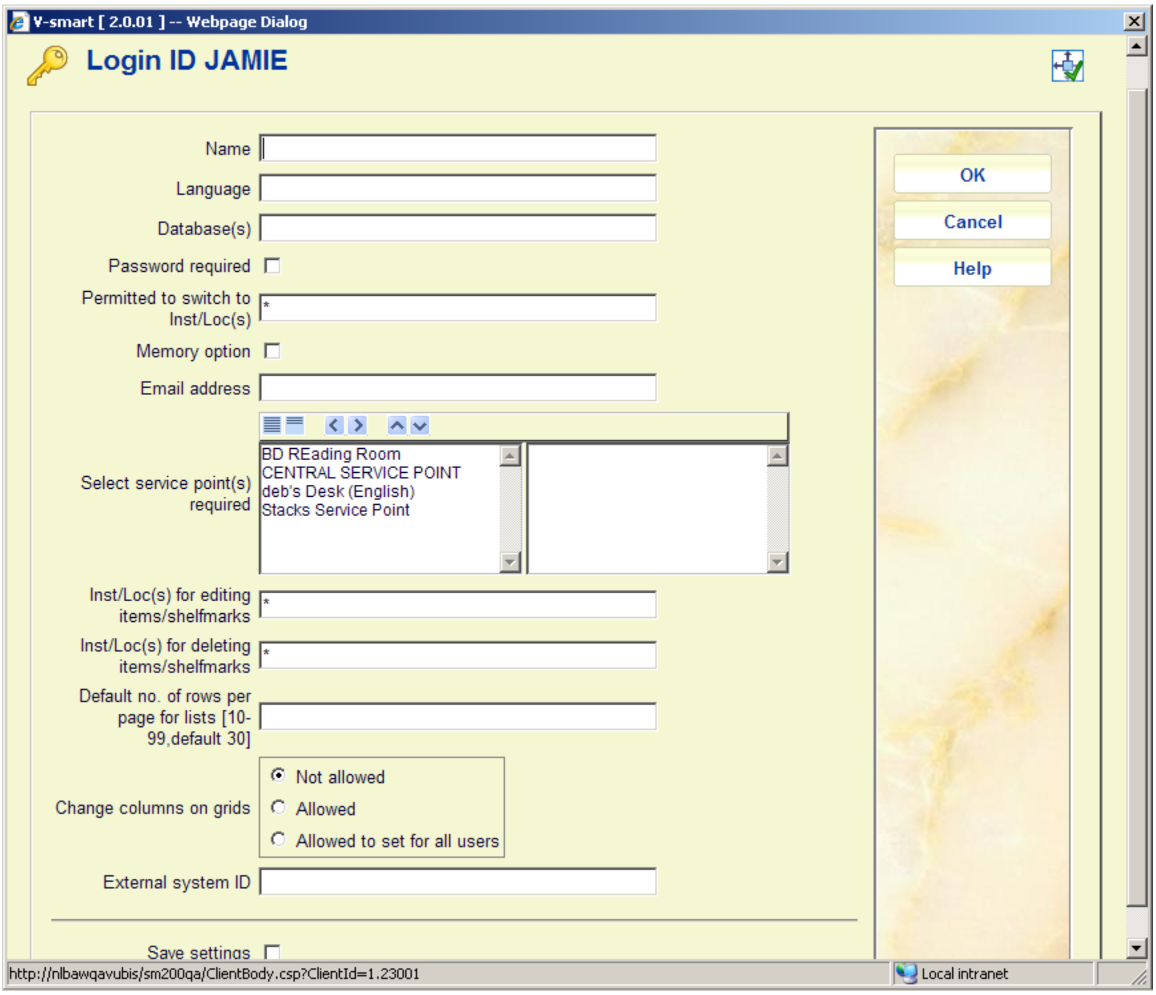


Login ID

Enter an ID. A login ID may contain a minimum of 3 and a maximum of 50 letters or digits. The characters ^ and ~ 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.



V-smart [2.0.01] -- Webpage Dialog

Login ID JAMIE

Name

Language

Database(s)

Password required □

Permitted to switch to Inst/Loc(s) *

Memory option □

Email address

Select service point(s) required

BD REading Room
CENTRAL SERVICE POINT
deb's Desk (English)
Stacks Service Point

Inst/Loc(s) for editing items/shelfmarks *

Inst/Loc(s) for deleting items/shelfmarks *

Default no. of rows per page for lists [10-99,default 30]

Change columns on grids
● Not allowed
○ Allowed
○ Allowed to set for all users

External system ID

Save settings □

http://nlbawqavubis/sm200qa/ClientBody.csp?ClientId=1.23001

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).
The language setting in the Preferences for a user, takes precedence over the language defined here. As long as no cookies are saved, the AFO 611 setting will still be used.

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 servcie desk are userd 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/shelfmarks: Specify for which institutions/locations this user can modify item and shelfmark information. You can enter INST/* for all locations in an instution or just * for system wide.

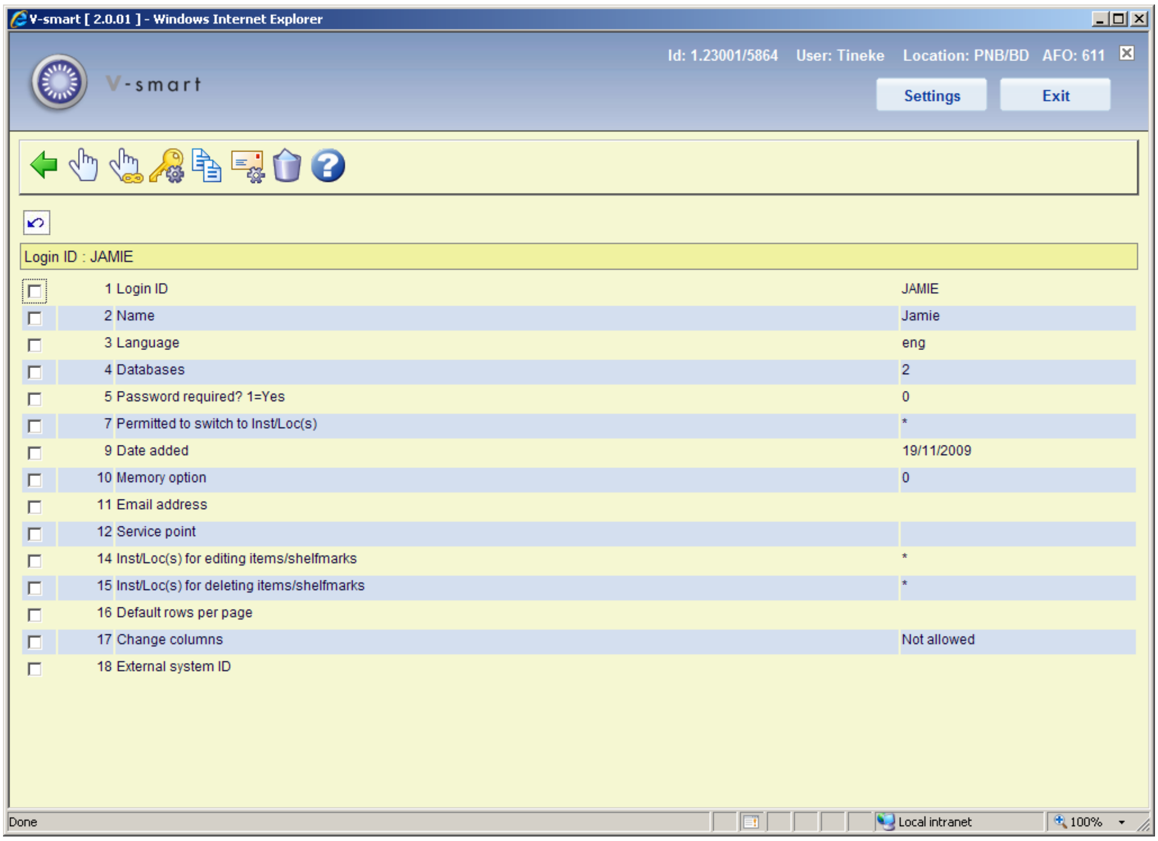
Inst/Loc(s) for deleting items: Specify for which institutions/locations this user can delete items and shelfmarks. You can enter INST/* for all locations in an instution or just * for system wide.

Default no. of rows per page for lists [10-99, default30]: The default value of 30 will be overriden by any other setting (between 10 and 99) in this field, for this user.

Change columns on grids: This option tells the system whether this user is allowed to change the column positioning on any grid. In addition to “allowed” or “not allowed”, a third option allows this user to apply their changes to ALL users.
See the general introduction to Vubis Smart for more information on this feature.

External system ID: This field is related to Smartcard Webservices for logging in. This field can contain the external login ID associated with the Vubis Smart user ID shown on the entry screen. This external ID will not be mandatory and if present will NOT be validated against any list.

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


V-smart [2.0.01] - Windows Internet Explorer
Id: 1.23001/5864 User: Tineke Location: PNB/BD AFO: 611
V-smart
Settings
Exit
Done
Local intranet
100%

Login ID : JAMIE

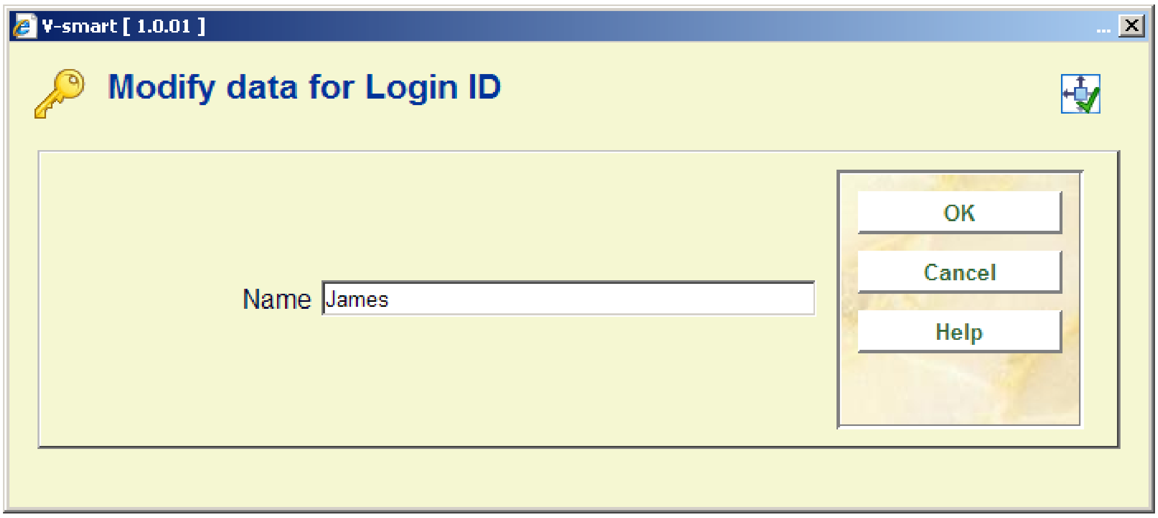
□	1 Login ID	JAMIE
□	2 Name	Jamie
□	3 Language	eng
□	4 Databases	2
□	5 Password required? 1=Yes	0
□	7 Permitted to switch to Inst/Loc(s)	*
□	9 Date added	19/11/2009
□	10 Memory option	0
□	11 Email address	
□	12 Service point	
□	14 Inst/Loc(s) for editing items/shelfmarks	*
□	15 Inst/Loc(s) for deleting items/shelfmarks	*
□	16 Default rows per page	
□	17 Change columns	Not allowed
□	18 External system ID	

Note

When your library has eID (Electronic Identification) enabled it is possible to login using an eID card. See the separate documentation on eID (in the General section) for more information.

Options on the screen

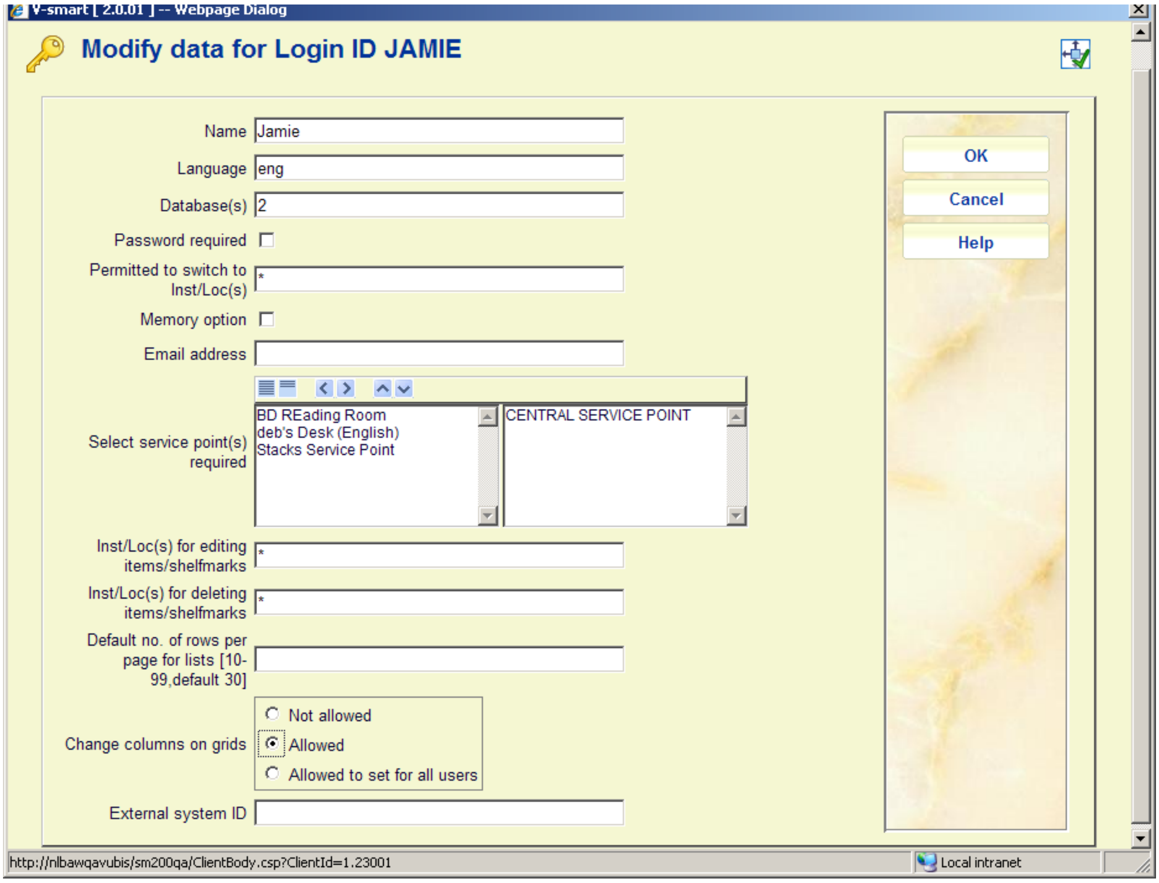
Modify line no. (+):Select a line number and then select this option to change the data:



Modify data for Login ID

Name James

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



Modify data for Login ID JAMIE

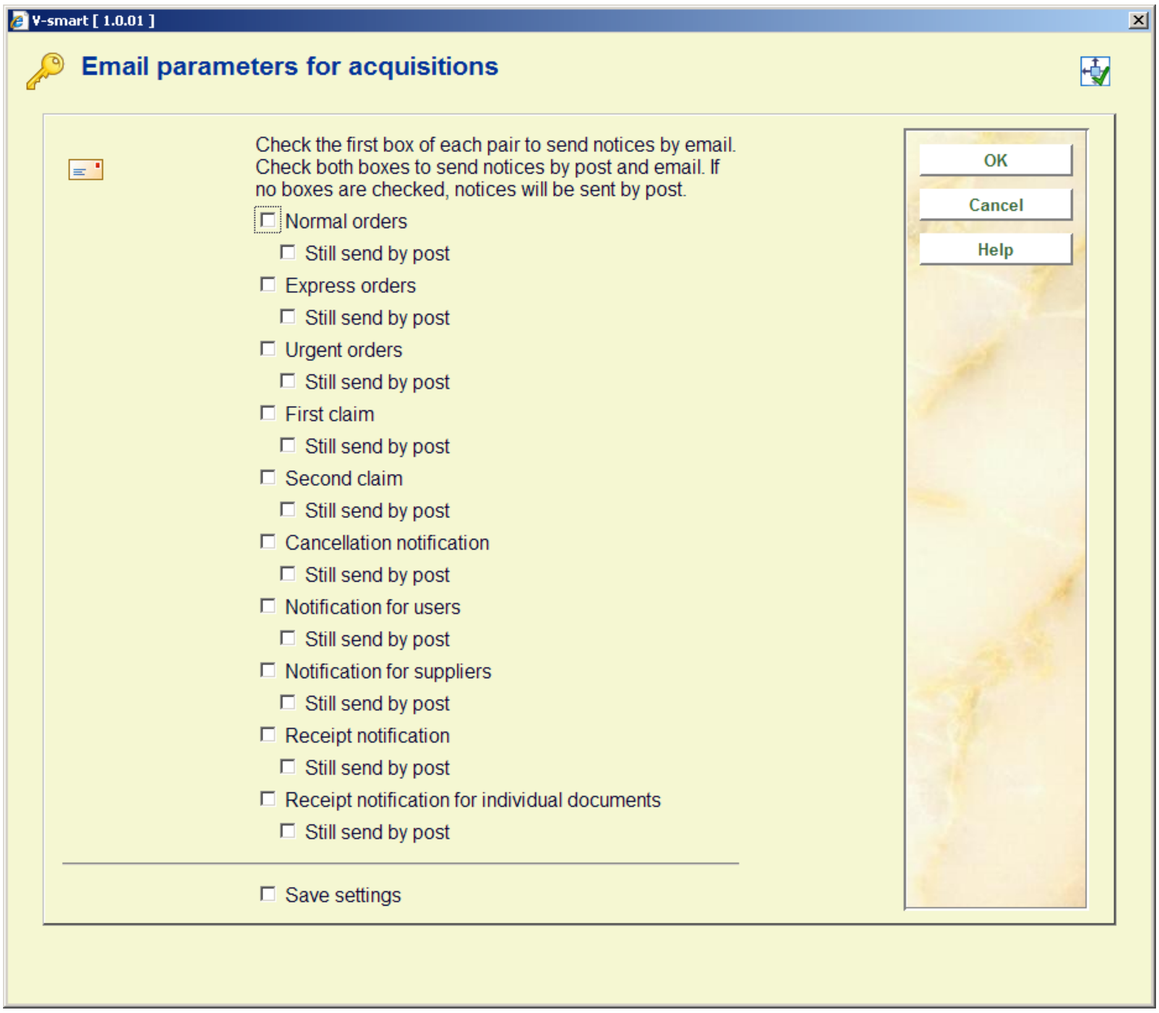
Name	Jamie
Language	eng
Database(s)	2
Password required	□
Permitted to switch to Inst/Loc(s)	*
Memory option	□
Email address	
Select service point(s) required	BD REading Room deb's Desk (English) Stacks Service Point CENTRAL SERVICE POINT
Inst/Loc(s) for editing items/shelfmarks	*
Inst/Loc(s) for deleting items/shelfmarks	*
Default no. of rows per page for lists [10-99,default 30]	
Change columns on grids	○ Not allowed ● Allowed ○ Allowed to set for all users
External system ID	

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:



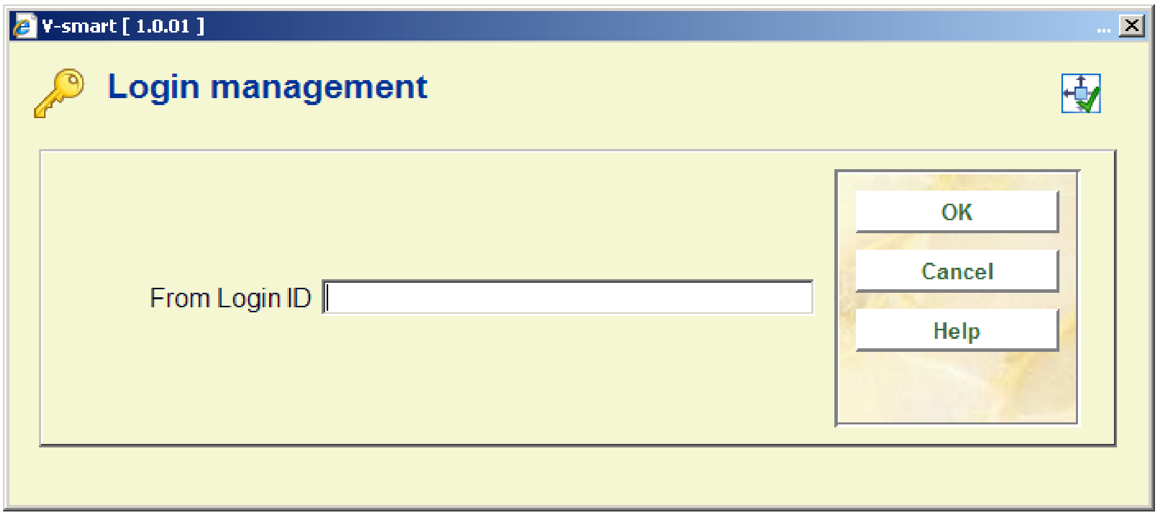
Email parameters for acquisitions

Check the first box of each pair to send notices by email. Check both boxes to send notices by post and email. If no boxes are checked, notices will be sent by post.

☐ Normal orders
 ☐ Still send by post
☐ Express orders
 ☐ Still send by post
☐ Urgent orders
 ☐ Still send by post
☐ First claim
 ☐ Still send by post
☐ Second claim
 ☐ Still send by post
☐ Cancellation notification
 ☐ Still send by post
☐ Notification for users
 ☐ Still send by post
☐ Notification for suppliers
 ☐ Still send by post
☐ Receipt notification
 ☐ Still send by post
☐ Receipt notification for individual documents
 ☐ Still send by post

☐ Save settings

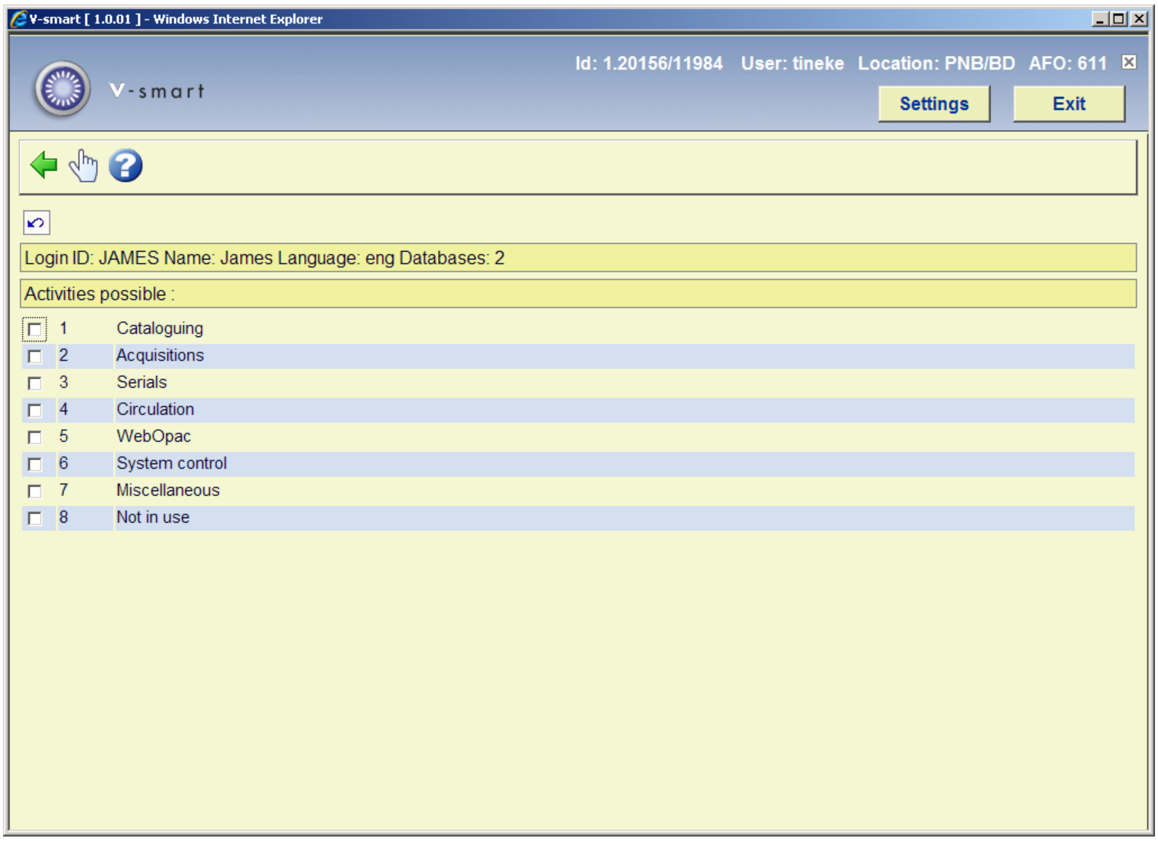
Copy: Select this option to copy the permissions associated with another login ID to the login ID on the screen. An input screen appears. Here you enter the login ID whose permission data you wish to copy to the login ID on the screen. The login ID to which you are copying the data is granted access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



Login management

From Login ID

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

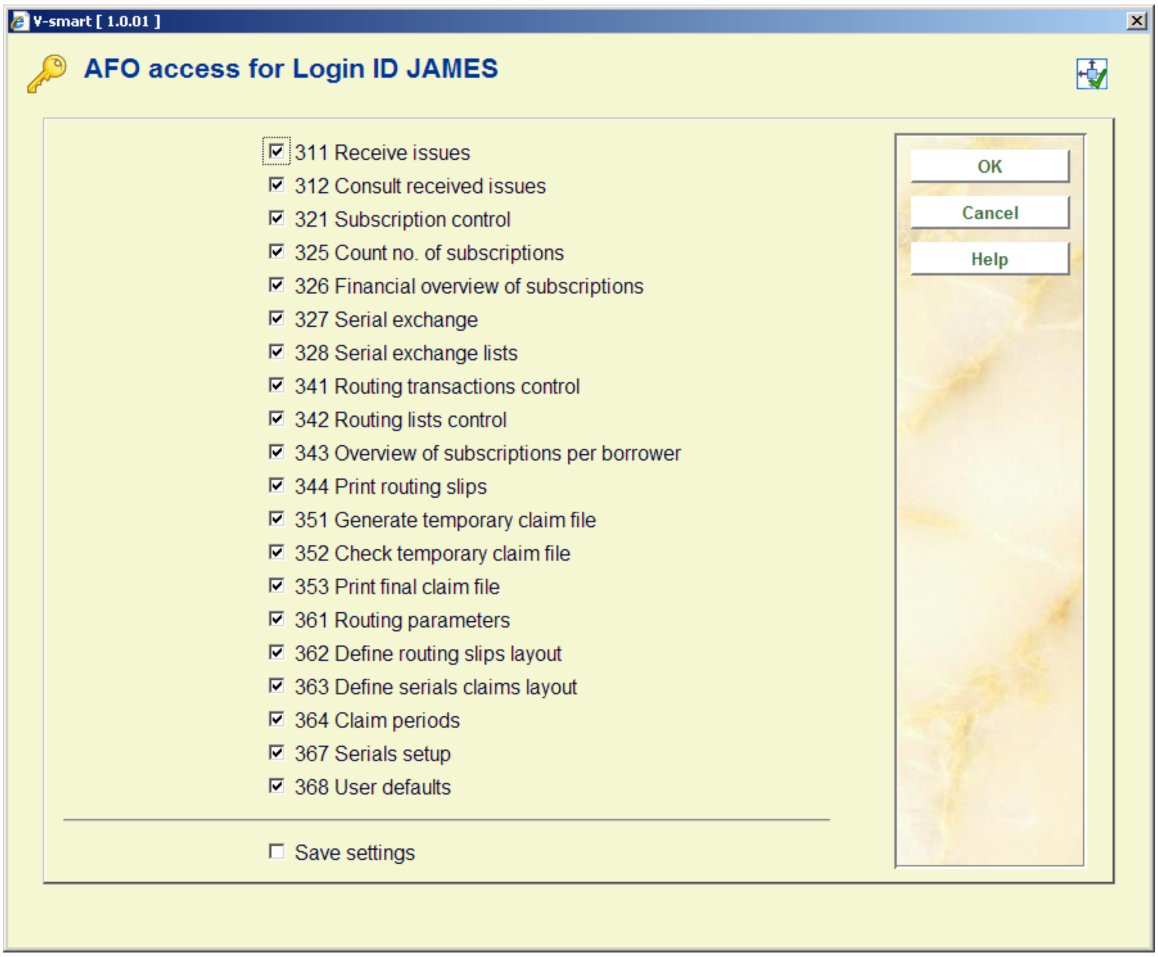

V-smart [1.0.01] - Windows Internet Explorer
V-smart
Id: 1.20156/11984 User: tineke Location: PNB/BD AFO: 611
Settings
Exit

Login ID: JAMES Name: James Language: eng Databases: 2

Activities possible :

□	1	Cataloguing
□	2	Acquisitions
□	3	Serials
□	4	Circulation
□	5	WebOpac
□	6	System control
□	7	Miscellaneous
□	8	Not in use

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:



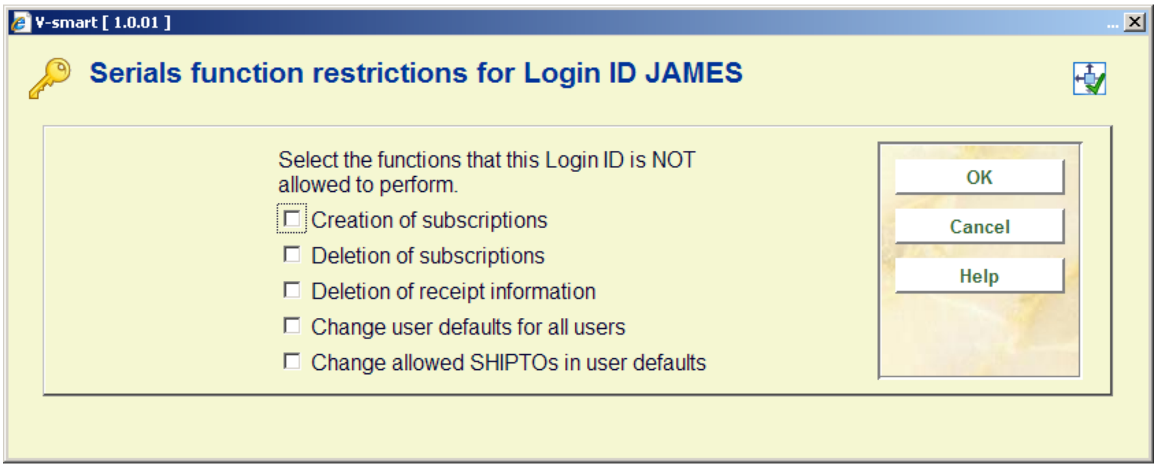
AFO access for Login ID JAMES

☑ 311 Receive issues
☑ 312 Consult received issues
☑ 321 Subscription control
☑ 325 Count no. of subscriptions
☑ 326 Financial overview of subscriptions
☑ 327 Serial exchange
☑ 328 Serial exchange lists
☑ 341 Routing transactions control
☑ 342 Routing lists control
☑ 343 Overview of subscriptions per borrower
☑ 344 Print routing slips
☑ 351 Generate temporary claim file
☑ 352 Check temporary claim file
☑ 353 Print final claim file
☑ 361 Routing parameters
☑ 362 Define routing slips layout
☑ 363 Define serials claims layout
☑ 364 Claim periods
☑ 367 Serials setup
☑ 368 User defaults

□ Save settings

Note

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



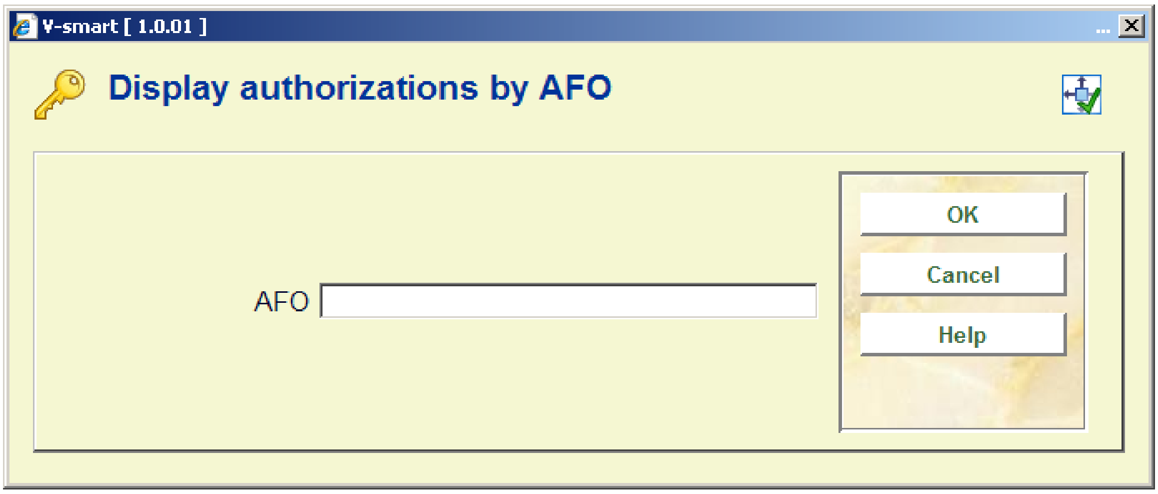
Serials function restrictions for Login ID JAMES

Select the functions that this Login ID is NOT allowed to perform.

□ Creation of subscriptions
□ Deletion of subscriptions
□ Deletion of receipt information
□ Change user defaults for all users
□ Change allowed SHIPTOs in user defaults

611.3 Authorisations by AFO

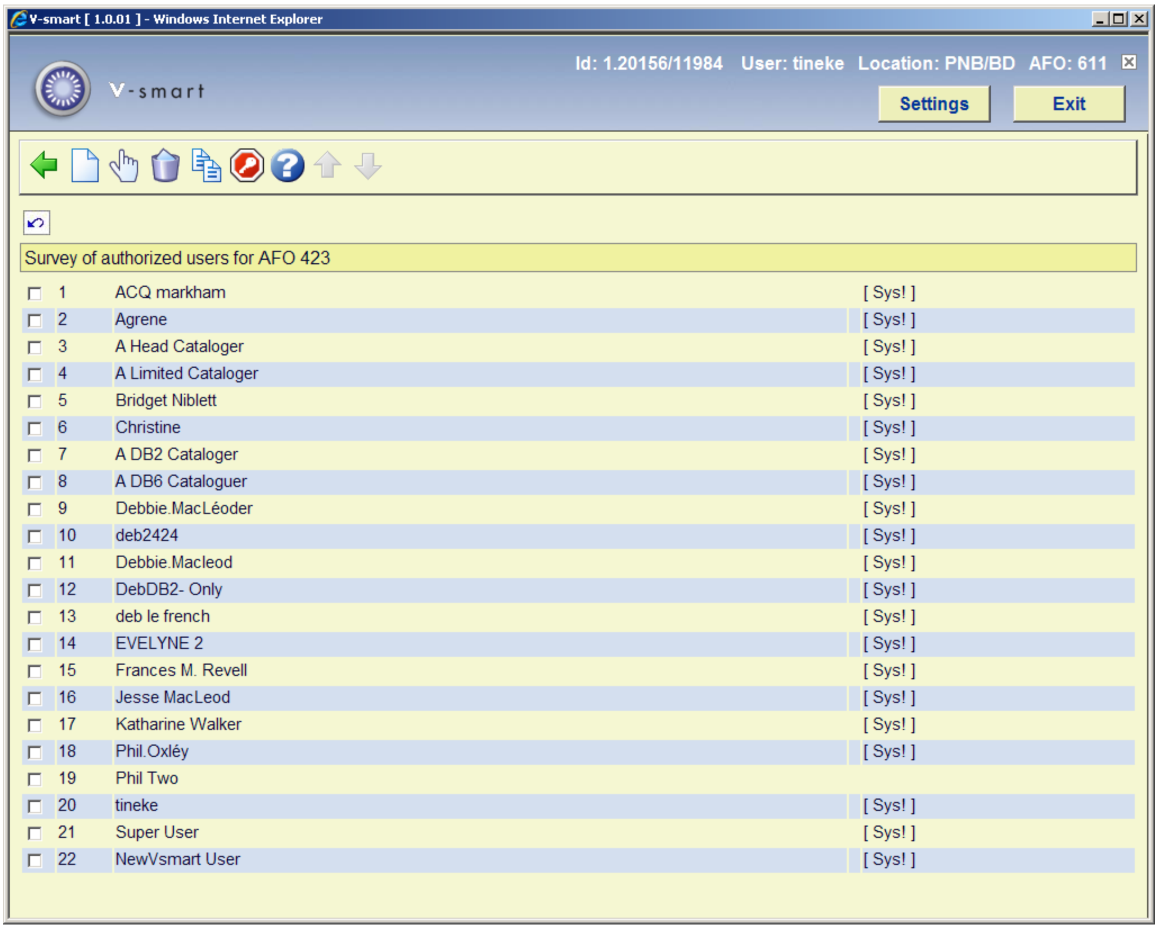
This menu option provides an overview of the login ID's that have access to an AFO. If you select this menu option, an input screen appears:



Display authorizations by AFO

AFO

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



Id: 1.20156/11984 User: tineke Location: PNB/BD AFO: 611

Survey of authorized users for AFO 423

□	1	ACQ markham	[Sys!]
□	2	Agrene	[Sys!]
□	3	A Head Cataloger	[Sys!]
□	4	A Limited Cataloger	[Sys!]
□	5	Bridget Niblett	[Sys!]
□	6	Christine	[Sys!]
□	7	A DB2 Cataloger	[Sys!]
□	8	A DB6 Cataloguer	[Sys!]
□	9	Debbie.MacLéoder	[Sys!]
□	10	deb2424	[Sys!]
□	11	Debbie.Macleod	[Sys!]
□	12	DebDB2- Only	[Sys!]
□	13	deb le french	[Sys!]
□	14	EVELYNE 2	[Sys!]
□	15	Frances M. Revell	[Sys!]
□	16	Jesse MacLeod	[Sys!]
□	17	Katharine Walker	[Sys!]
□	18	Phil.Oxléy	[Sys!]
□	19	Phil Two	
□	20	tineke	[Sys!]
□	21	Super User	[Sys!]
□	22	NewVsmart User	[Sys!]

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.

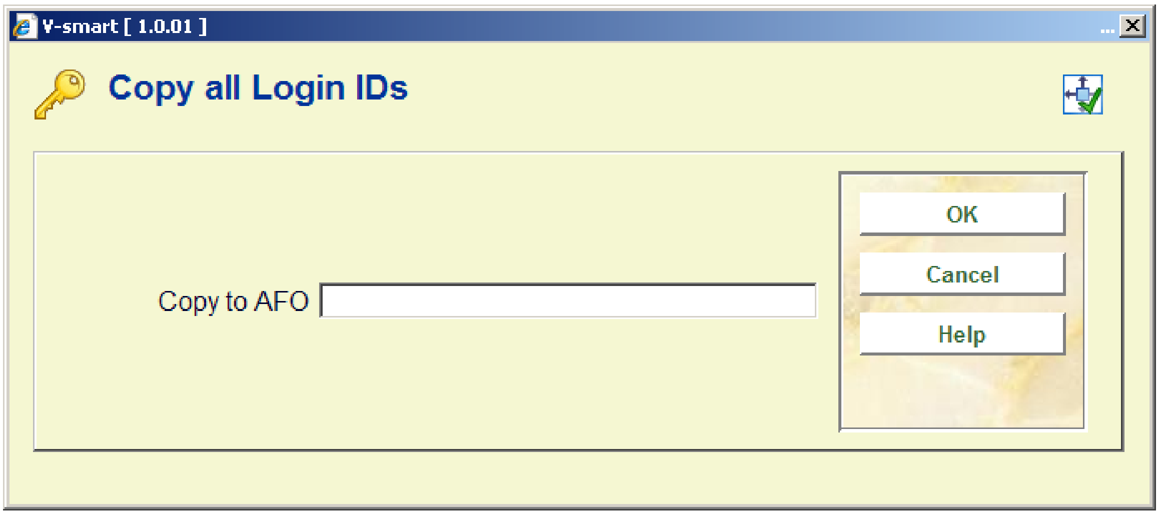
Options on the screen

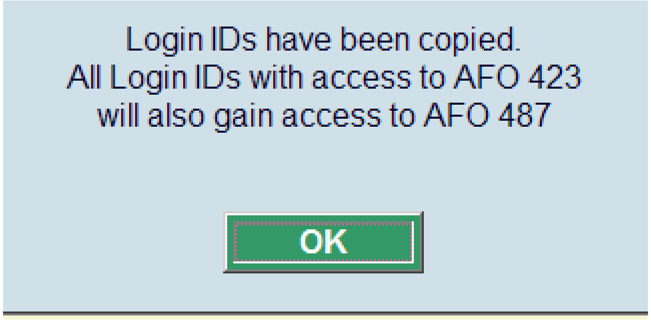
Add login ID: Select this option to add a login ID to the list. An input screen appears, in which you can enter the ID to be added.

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:



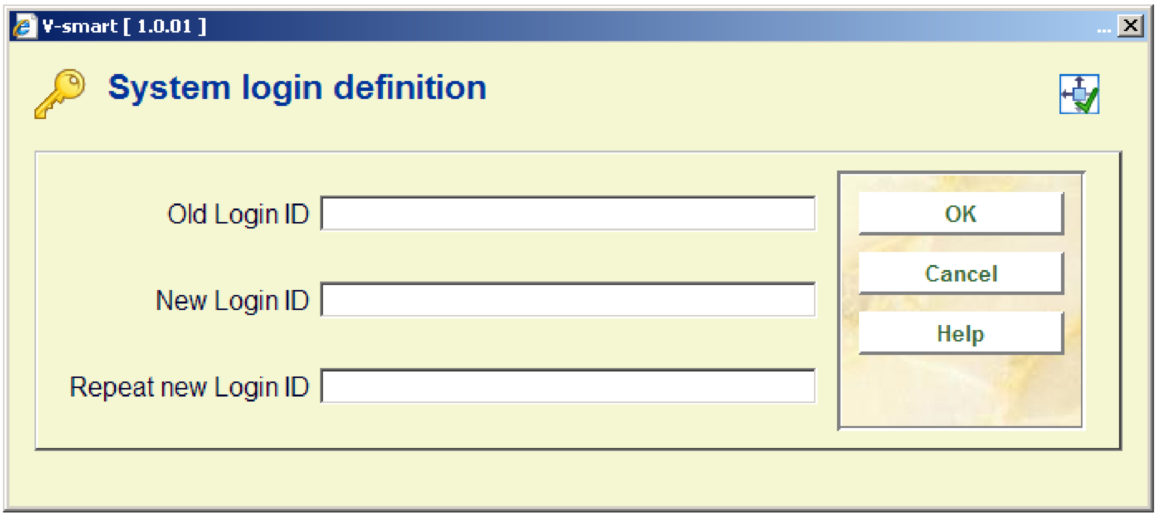


Login IDs have been copied.
All Login IDs with access to AFO 423
will also gain access to AFO 487

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.

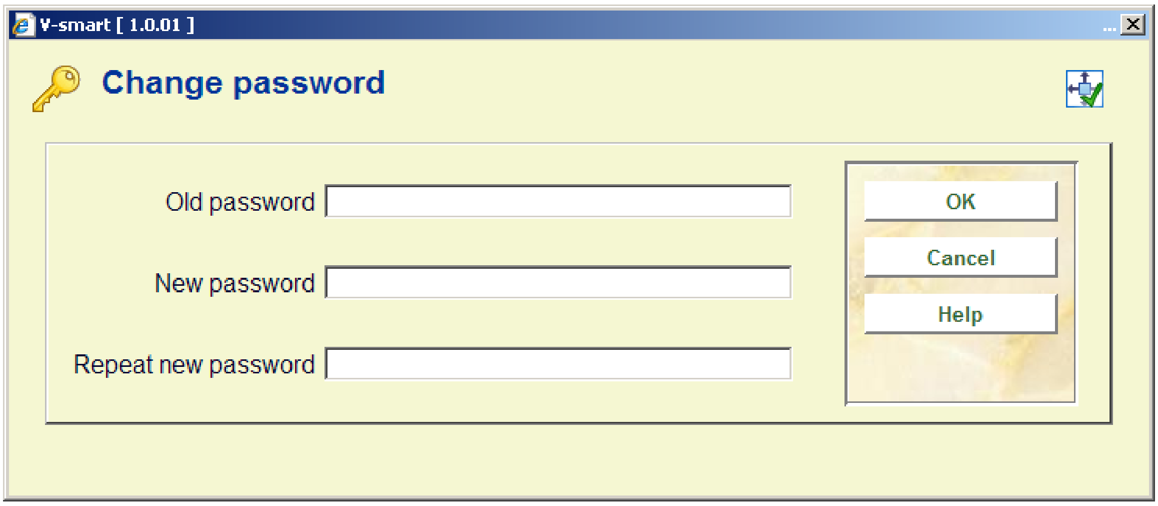
Notes

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.

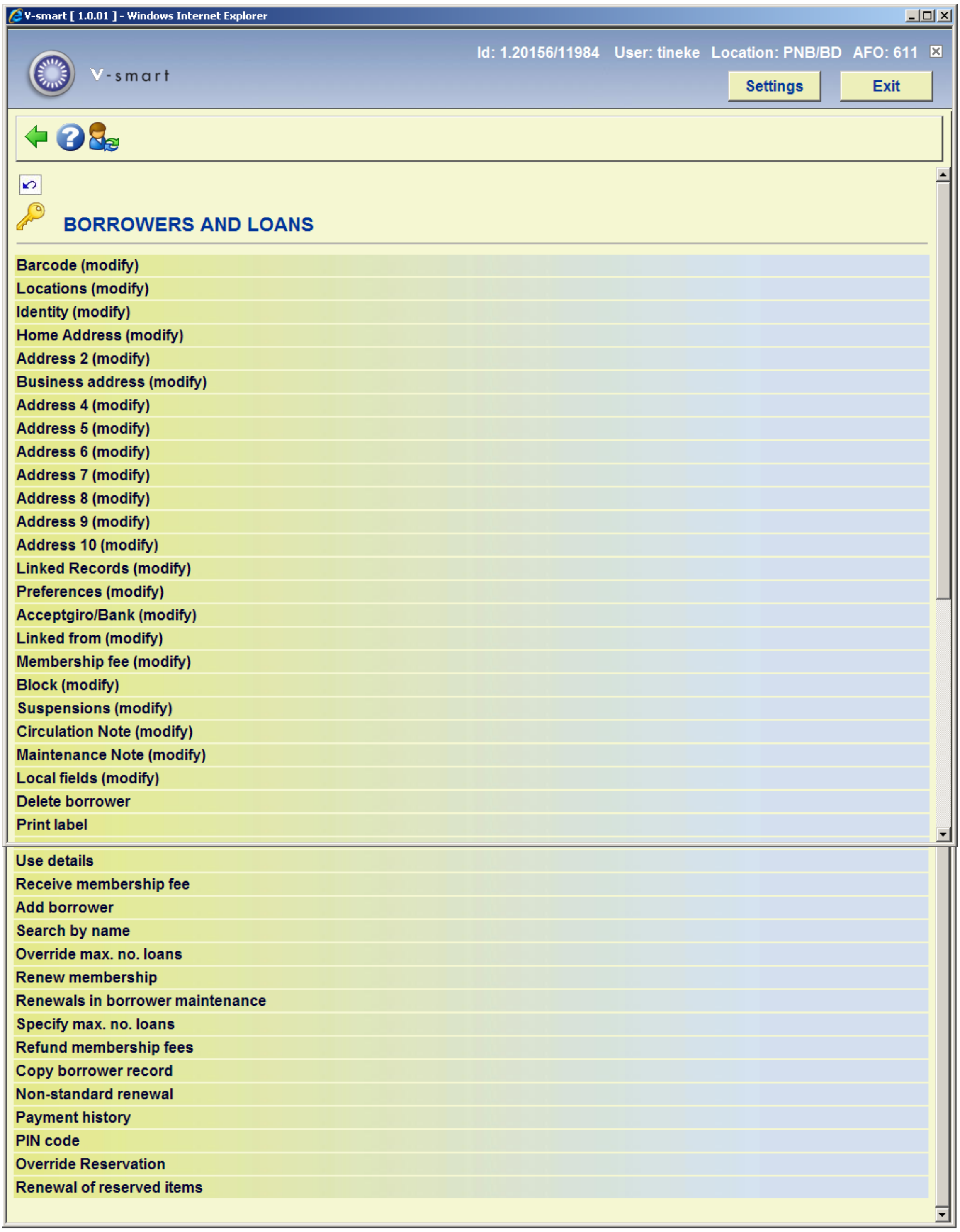
Note

The passwords entered are not displayed on the screen.

611.6 Login restrictions – 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:


V-smart [1.0.01] - Windows Internet Explorer
Id: 1.20156/11984 User: tineke Location: PNB/BD AFO: 611
V-smart
Settings
Exit

BORROWERS AND LOANS

Barcode (modify)
Locations (modify)
Identity (modify)
Home Address (modify)
Address 2 (modify)
Business address (modify)
Address 4 (modify)
Address 5 (modify)
Address 6 (modify)
Address 7 (modify)
Address 8 (modify)
Address 9 (modify)
Address 10 (modify)
Linked Records (modify)
Preferences (modify)
Acceptgiro/Bank (modify)
Linked from (modify)
Membership fee (modify)
Block (modify)
Suspensions (modify)
Circulation Note (modify)
Maintenance Note (modify)
Local fields (modify)
Delete borrower
Print label
Use details
Receive membership fee
Add borrower
Search by name
Override max. no. loans
Renew membership
Renewals in borrower maintenance
Specify max. no. loans
Refund membership fees
Copy borrower record
Non-standard renewal
Payment history
PIN code
Override Reservation
Renewal of reserved items

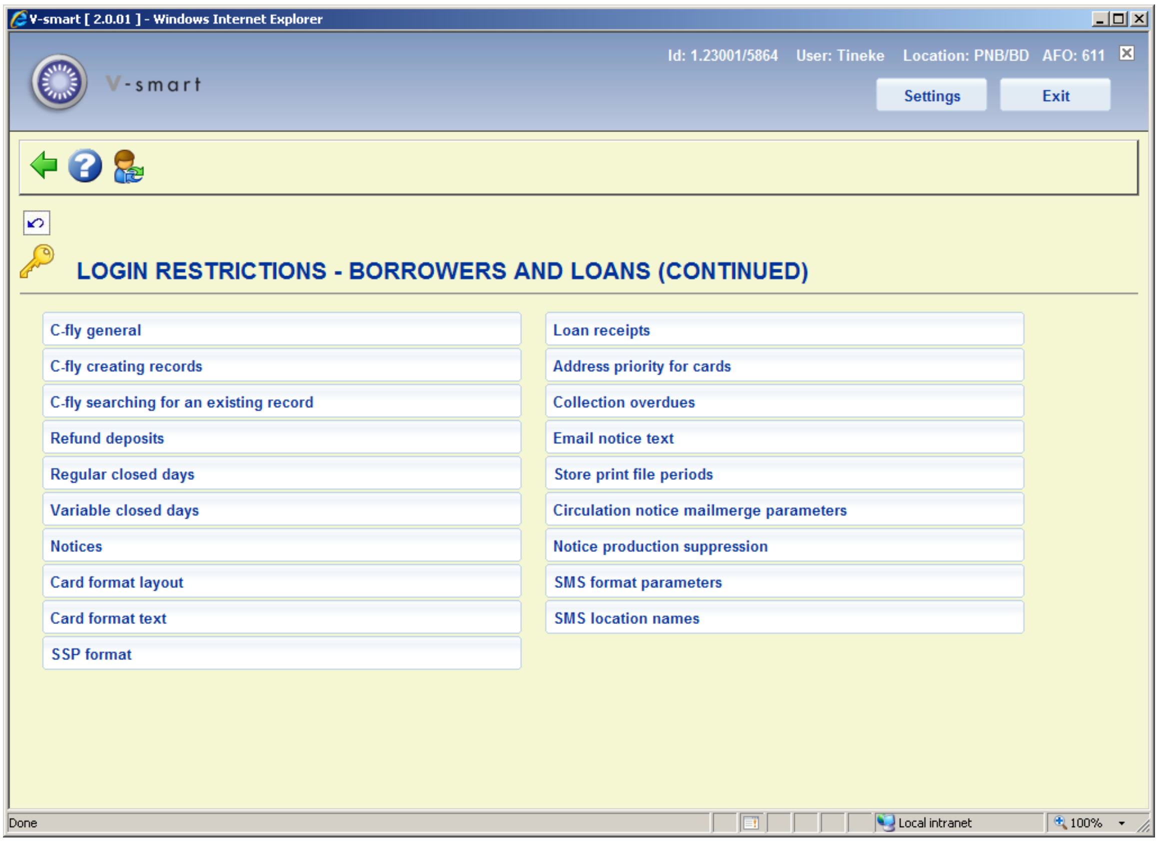
Menu options on the screen

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.

611.7 Login restrictions – Borrowers and loans (continued)

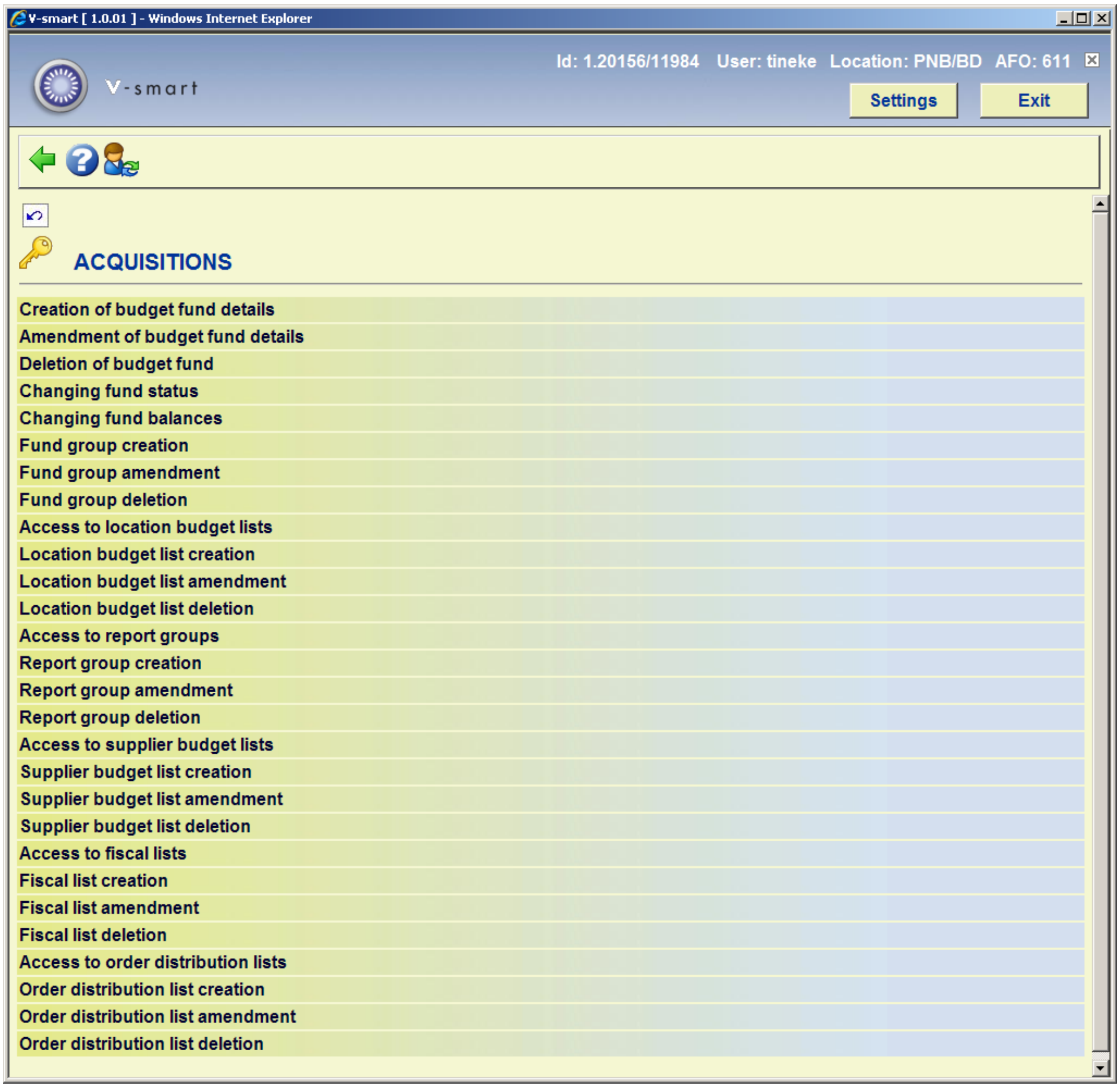


The procedure is the same as for ”Login restrictions – Borrowers and Loans”.

611.8 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 acquistions 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:


V-smart [1.0.01] - Windows Internet Explorer
V-smart
Id: 1.20156/11984 User: tineke Location: PNB/BD AFO: 611
Settings
Exit

ACQUISITIONS

Creation of budget fund details
Amendment of budget fund details
Deletion of budget fund
Changing fund status
Changing fund balances
Fund group creation
Fund group amendment
Fund group deletion
Access to location budget lists
Location budget list creation
Location budget list amendment
Location budget list deletion
Access to report groups
Report group creation
Report group amendment
Report group deletion
Access to supplier budget lists
Supplier budget list creation
Supplier budget list amendment
Supplier budget list deletion
Access to fiscal lists
Fiscal list creation
Fiscal list amendment
Fiscal list deletion
Access to order distribution lists
Order distribution list creation
Order distribution list amendment
Order distribution list deletion

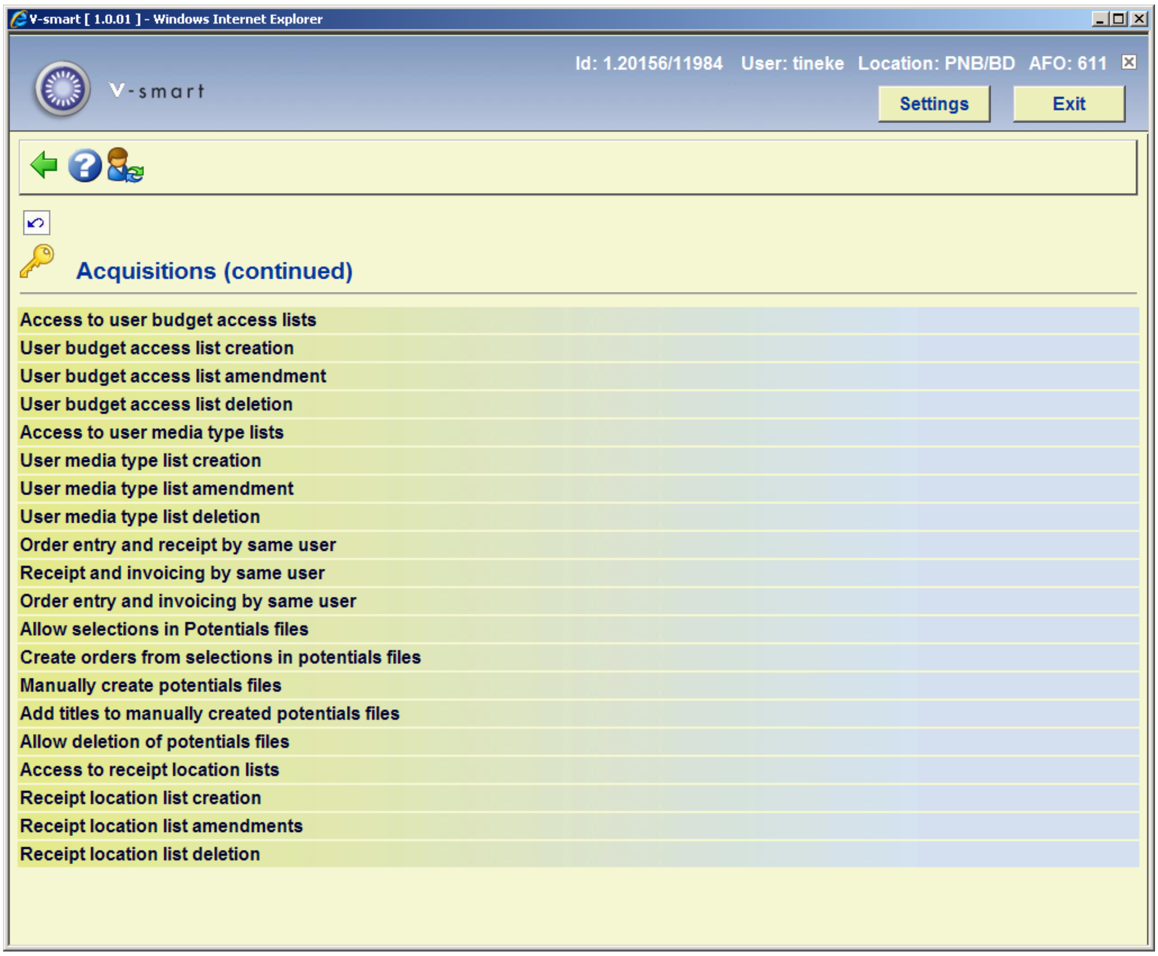
Menu options on the screen

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.

611.9 Login restrictions - Acquisitions (continued)



V-smart [1.0.01] - Windows Internet Explorer
V-smart
Id: 1.20156/11984 User: tineke Location: PNB/BD AFO: 611
Settings
Exit

Acquisitions (continued)

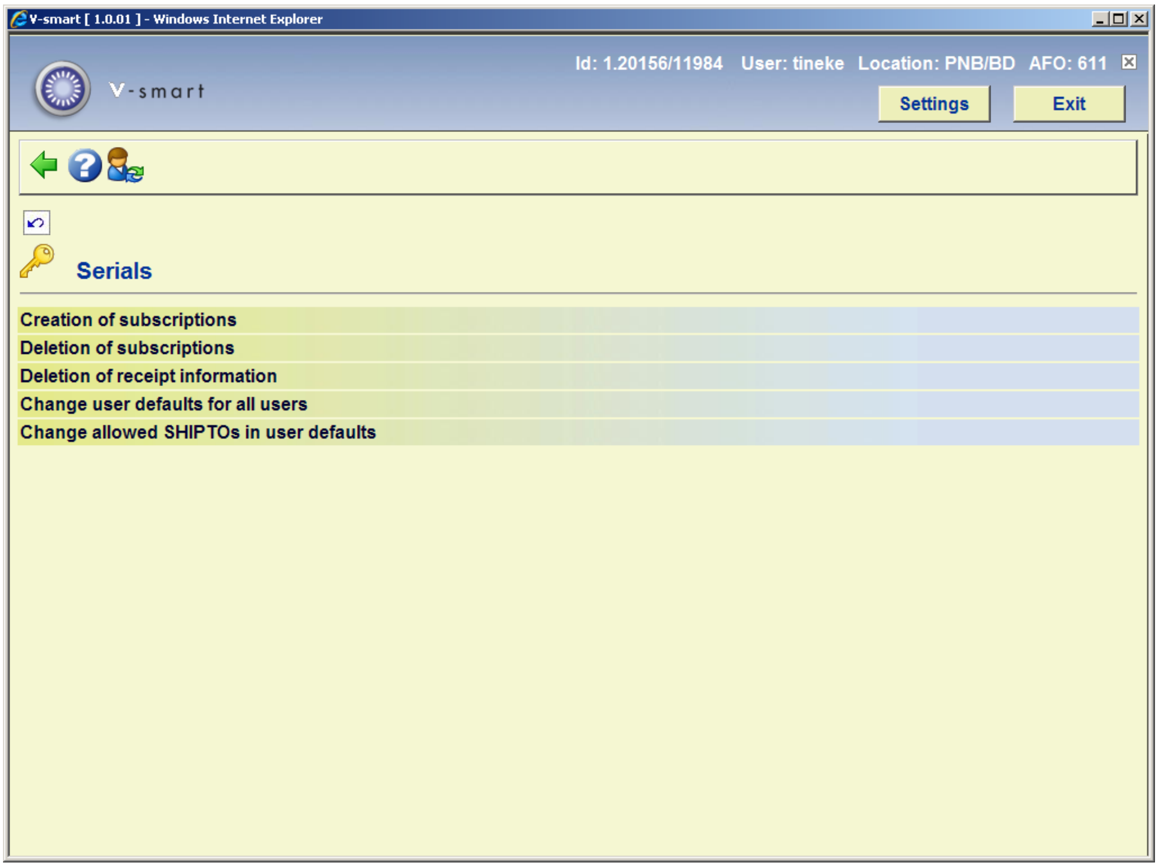
- Access to user budget access lists
- User budget access list creation
- User budget access list amendment
- User budget access list deletion
- Access to user media type lists
- User media type list creation
- User media type list amendment
- User media type list deletion
- Order entry and receipt by same user
- Receipt and invoicing by same user
- Order entry and invoicing by same user
- Allow selections in Potentials files
- Create orders from selections in potentials files
- Manually create potentials files
- Add titles to manually created potentials files
- Allow deletion of potentials files
- Access to receipt location lists
- Receipt location list creation
- Receipt location list amendments
- Receipt location list deletion

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

611.10 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:


V-smart [1.0.01] - Windows Internet Explorer
V-smart
Id: 1.20156/11984 User: tineke Location: PNB/BD AFO: 611
Settings
Exit

Serials

Creation of subscriptions
Deletion of subscriptions
Deletion of receipt information
Change user defaults for all users
Change allowed SHIPTOs in user defaults

Menu options on the screen

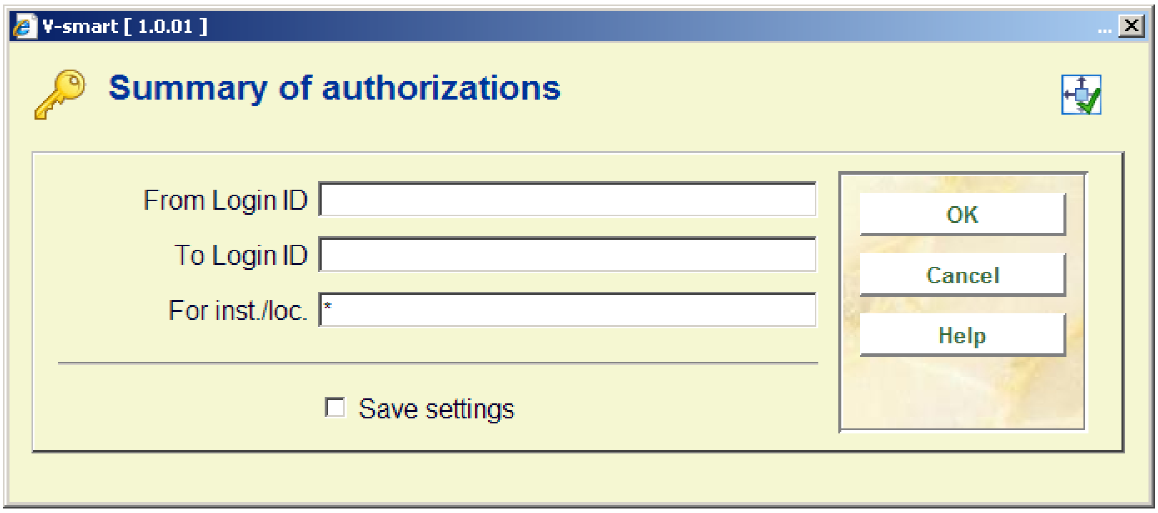
Select the desired menu option. Now you can add login ID’s with an input screen or add or delete login ID’s that are denied access to an option via this screen.

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.

611.11 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:



V-smart [1.0.01]

Summary of authorizations

From Login ID

To Login ID

For inst./loc. *

□ Save settings

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

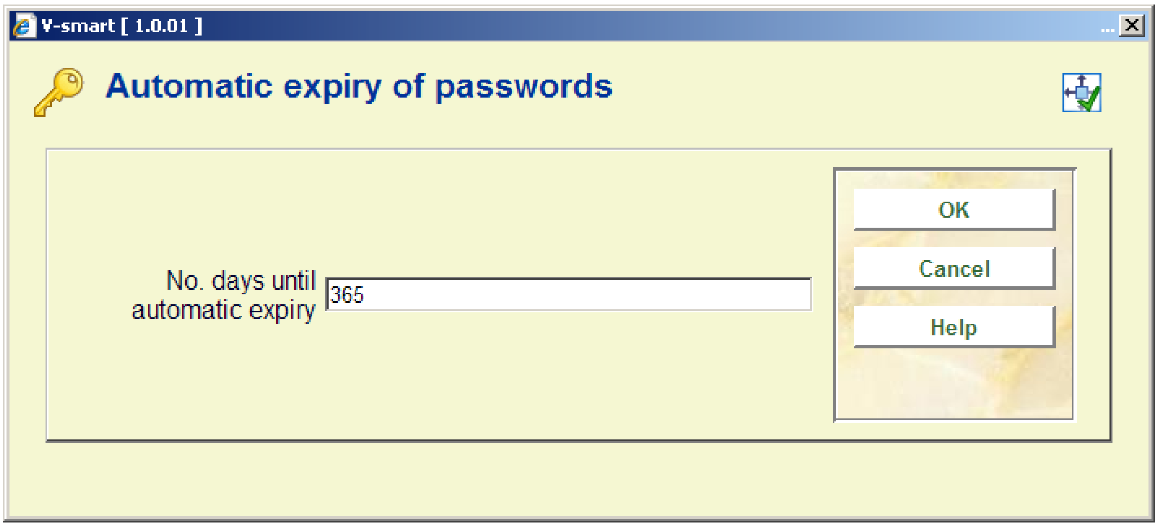
If you wish to create a list of all login ID's, leave the fields 'From login ID' and 'To login ID' blank.

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.

611.12 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:



No. days until automatic expiry 365

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	June 2008	creation	
2.0	June 2009	new option for encryption; new screen shots; textual corrections, Cataloguing restrictions removed part of 2.0 updates	
3.0	March 2011	new user PUB; updated section on special login ID's part of 3.5 updates	