

# WAY4™ User Management

# Contents

INTRODUCTION	2
CHAPTER 1. WAY4 USERS	3
Classification of WAY4 users	3
User groups	4
CHAPTER 2. CREATING USER WORKPLACES	5
"User Management" Window	5
User group parameters	6
User account parameters	6
Privileges	7
Buttons	9
Editing user groups	11
Adding a new user group	11
Modifying user groups	11
Assigning a user group to a higher-ranking group	11
Deleting a user group	12
Menu root group	12
List of privileges required for access to the menu root group	13
Updating user group privileges	13
Privileges required to open menu root group objects	14
Editing the user list	15
Creating a user account	15
Changing user account parameters	16
Assigning a user to a new user group	16
Deleting a user from the list	17
Locking an Oracle DB user account	17
Unlocking an Oracle DB user account	17
Deleting an Oracle DB user account	17
Changing user password	18
Configuring additional privileges for menu item DB objects	19
Configuring privilege packages	19
Assigning a package of additional privileges to a menu subitem	21
Initialization of local constants	21
CHAPTER 3. LOGGING	24
Process logging	24
Logging changes to records made in grid forms	24
Recovering deleted records	24
User login history	25
Locking inactive accounts	26
CHAPTER 4. PRIVILEGES FOR WAY4 DIRECTORIES	28
Standard WAY4 directories	28
Privileges for standard WAY4 directories	28
APPENDIX 1. LIMITING DATA ACCESS WITH USER PASSWORD ENCRYPTION	30
APPENDIX 2. AMENDMENT REPORT	31



# Introduction

This document describes the main concepts of user administration in WAY4™.

When working with this document, it is recommended to use the following resources from the OpenWay documentation series:

- "WAY4 Manager Manual"
- "WAY4 Manager Menu Editor"
- " WAY4 Manager Form Editor"
- "PCI DSS Security Recommendations for WAY4™"
- "Working with WAY4™ Remote Access"
- "WAY4™ Global Parameters"

The following conventions are used throughout this document:

- Field labels in screen forms are displayed in *italics*.
- Button labels in screen forms are shown in square brackets, as in [Approve].
- User menu selection sequences are given using arrows, as in Issuing → Contracts Input & Update.
- Sequences for selection of items from the system menu are shown using another type of arrow, as in "Database => Change password".
- Key combinations used in working with WAY4 Manager are displayed in angular brackets, for example <Ctrl>+<F3>.
- Values such as directory and file names, as well as file paths which vary for each local instance of the program are also shown in angular brackets, as in <OWS\_HOME>.
- Warnings that there is a risk of making an incorrect action are marked with the  sign.
- Messages marked with the  sign contain information about important features, additional facilities, or the optimal use of certain functions of the system.

## Chapter 1. WAY4 Users

This section discusses the classification of WAY4 users and describes their DB object access privileges.

### Classification of WAY4 users

The table below Table 1 shows the classification of WAY4 users according to their function, as well as the required DB access privileges for each class of users.

*Table 1. Classification of WAY4 database users*

User type (name)	Function	DB access privileges	Number
Scheme owner "Owner", (Administrative user)	Creation of WAY4 DB objects	Full privileges for all scheme objects (data and metadata)	1
Main security administrator (Administrative user)	Creation of users (including security administrators) and user groups, granting access privileges to users and user groups	Full privileges to view, edit and delete WAY4 DB data	1
Security administrator	Creation of users and user groups, granting access privileges to users and user groups	Partial privileges to view, edit and delete data in the WAY4 DB	Several
Administrator	Creation, editing and deletion of user views, screen forms, pipes, editing menu groups and user menu items	Partial privileges to view, edit and delete data	Several
Operator (Clerk)	Work with data in the granted menu group	Rights to view, edit and delete information accessible from the granted user menu group	Unlimited
Auditor	Viewing data available from the granted menu group	Privilege to view data available from the granted user menu group	Unlimited
NetServer user (Administrative user)	Online authorisation	Right to execute several stored procedures	1



WAY4 administrative users usually have the following names:

- Scheme owner – "OWS";
- Main security administrator – "OWS\_A";
- NetServer user– "OWS\_N".

Administrators, operators and auditors (hereinafter simply referred to as WAY4 users, as opposed to administrative users; see the table above Table 1) work with WAY DB data using the WAY4 Manager application (see the "WAY4 Manager Manual").

The scheme owner (Owner) is the owner of all tables, user views and procedures. After system setup (execution of a procedure to switch to multi-user mode) the scheme owner is automatically denied access to the system using WAY Manager.

The main security administrator (Super Security Administrator) is created once when the system is switched to multi-user mode. The main function of the Super Security Administrator is to create WAY4 users, including security administrators.

The role of security administrator is assigned to WAY4 users (administrators and operators). Specific roles are given to users by assigning them the corresponding privileges (see "Privileges"). The main function of a user with security administrator privileges is the creation of other WAY4 users.

## User groups

To facilitate administration, WAY4 users are united in groups. Each user group is granted a user menu group (see the "User Menu" section of the "WAY4 Manager Manual"). Access to other user menu groups is denied.



Each WAY4 user can belong to one user group only.

Each user group is also granted a set of DB access privileges. When executing the "Update Grants" operation (see "Creating user workplaces") for each user group two roles are automatically created in the DB (corresponding to the granted access privileges), that include DB access privileges necessary and sufficient for work with the given user menu group. These roles are granted to all users in the given group.

## Chapter 2. Creating user workplaces

To create a WAY4 user workplace, it is necessary to register an account for the given user in the appropriate group (see "User groups"). Moreover, on the user account level, the user can be assigned privileges determining the user role (administrator, operator, auditor or security administrator). Access privileges for the user menu group are granted on the user group level.

Access to user menu groups is granted using the following mechanisms:

- For each user group, creation of its own group-specific user menu group.
- Granting users and/or user groups privileges registered in the system, which are also set for menu groups (see the section "Editing the User Menu" of "WAY4 Manager Menu Editor").

Access to data available to users when working with WAY Manager forms is granted using static and dynamic filters (see the section "Form Editor Window. "Fields" Tab" of the document "WAY4 Manager Form Editor"), as well as the redetermination of these filter values (see the section "Initialization of local constants").

### "User Management" Window

User accounts are managed in a special dialog window "User Management" (see Fig. 1), opened from the menu item "Full → DB Administrator Utilities → Users & Grants → User Groups and Users - Edit".

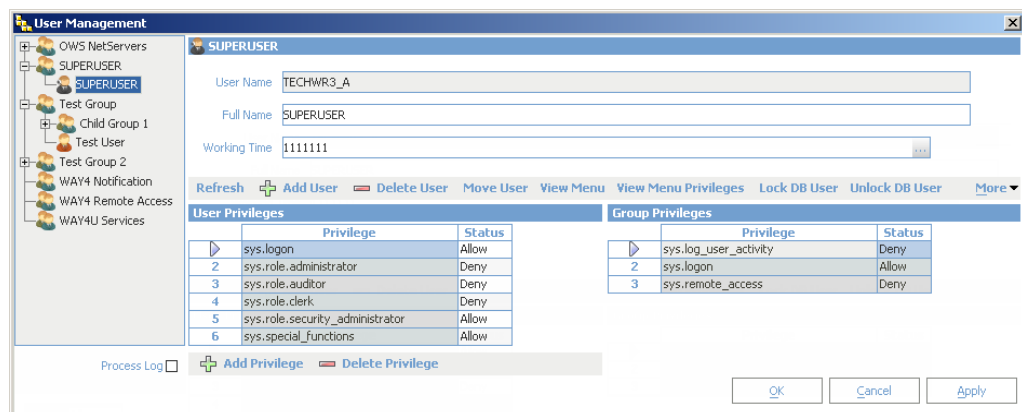



Fig. 1. Window for managing users and user groups

The left portion of the window shows a list of users and user groups as a hierarchical structure.

 Any changes to user and user group accounts not confirmed by clicking [Apply], [OK], or [Update Grants], [Update Grants for All], will not be saved in the DB.


Any changes to the parameters of user and user group accounts are saved by clicking [Apply] and [OK].

The following subsections describe fields and buttons in the "User Management" window.

## User group parameters

The "Group" form of the "User Management" window (see the figure Fig. 1 of the section "User Management" Window") contains the following fields:


- *Name* – name of the group
- *Menu* – field with selection from a drop-down list to specify the root menu group for the given user group (this field cannot be edited for a child group)
- *Grants Update Time* – the date and time of the last execution of the "Update Grants" operation for the given group (this field cannot be edited)
- *Additional Info* – field for additional information about the user group

 Note that the parent group menu branch is used for child groups (the same privileges for DB objects), but for child groups different values can be specified for local constants. In this case, the *Derived Menu* field of the child group will contain the name of the parent group menu branch.

Child groups are mostly necessary to decrease the number of DB roles.


The following rules should be observed for administration:

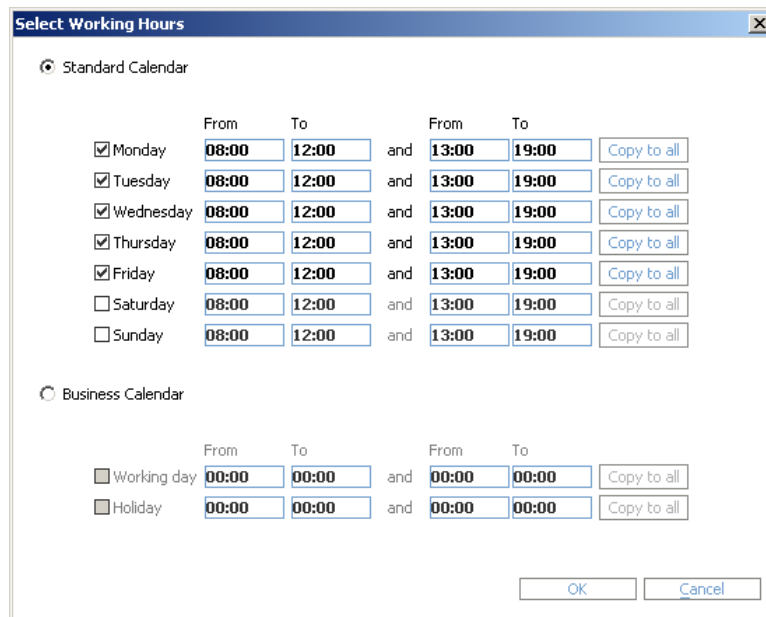
- After adding a child group it is necessary to update access privileges for the parent group (the [Update Grants] button).
- After making changes to a parent group menu branch, access privileges for the parent group should be updated (the [Update Grants] button).

 See the section "Updating User Group Privileges" for information on limitations to performing the "Update Grants" operation.

## User account parameters

The "<User name>" form of the "User Management" window (see the figure Fig. 1 of the section "User Management" Window") contains the following fields:

- *User Name* – user ID used for connection to the DB (this field cannot be edited)
- *Full Name* – a text field to specify the name of the user
- *Working Time* – a field to specify the interval within which the given user is permitted to access WAY4 using WAY4 Manager. This field must contain a string consisting of seven "0" and/or "1" numbers, where the position of each number corresponds to a day of the week (beginning with Monday), and the value indicates if the user is allowed access to the system ("0" – denied, "1" – permitted). Clicking the  button opens the "Select Working Hours" window (see Fig. 2).



The "Select Working Hours" dialog box has two main sections: "Standard Calendar" and "Business Calendar".

**Standard Calendar:** This section is selected with a radio button. It lists days of the week from Monday to Sunday. Each day has a "From" and "To" time field. For Monday through Friday, the times are 08:00 to 12:00 and 13:00 to 19:00. For Saturday and Sunday, the times are 08:00 to 12:00. There is an "and" label between the two time ranges for each day. To the right of each "To" field is a "Copy to all" button.

**Business Calendar:** This section is not selected. It has two sub-sections: "Working day" and "Holiday". Each has a "From" and "To" time field, both set to 00:00. There is an "and" label between the two time ranges. To the right of each "To" field is a "Copy to all" button.

At the bottom right are "OK" and "Cancel" buttons.

Fig. 2. Setting the interval for system access

This window shows the interval for access to the system. The *Standard Calendar* and *Business Calendar* toggle button groups allow the interval to be set for each day of the week or for days of the week determined by the business calendar as working days or weekends (see the "Business Calendar" section of the "WAY4™ Dictionaries" document).

**i** Note that when a user account is created, the *Working Time* field contains the value "0000000" by default, which fully prohibits the user from working with the system. Therefore, when creating a user account, it is recommended to specify an interval when work with the system is permitted.

## Privileges

User and user group privileges are assigned in the "User Privileges" and "Group Privileges" forms of the "User Management" window (see the figure Fig. 1 of the section "User Management" Window"). Privileges are used to assign users and user groups specific roles, to grant access to menu branches, to the system menu, the right to start the client application, etc.

User Privileges for SUPERUSER			Group Privileges for SUPERUSER		
	Privilege	Status		Privilege	Status
	sys.logon	Allow		sys.logon	Allow
2	sys.role.administrator	Deny	2	sys.remote_access	Deny
3	sys.role.auditor	Deny	3	sys.web_services	Allow
4	sys.role.clerk	Deny			
5	sys.role.security_administrator	Allow			
6	sys.special_functions	Allow			

+ Add Privilege
 - Delete Privilege

Fig. 3. Privileges for users and user groups

The *Privilege* field shows the name of privilege.

The *Status* field can contain one of the following values:

- "Allow" – permission to use the privilege



- "Deny" – use of the privilege is denied

Click [Add Privilege] to add privileges registered in the system. The "Add Privilege" form will appear on the screen (see Fig. 4).

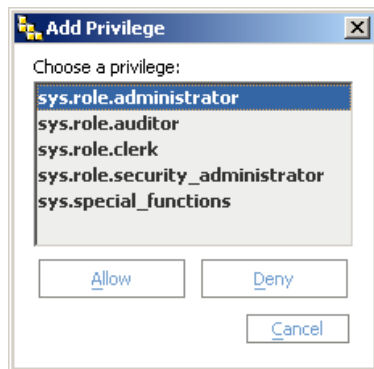



Fig. 4. Assigning privileges

Select the privilege in this form and click [Allow] (permit use of the privilege) or [Deny] (prohibit use). To cancel assignment of privileges, click [Cancel].

To delete privileges from the "User Privileges" or "Group Privileges" form, click [Delete Privilege].

The following system privileges are registered in the system:

- "sys.client.way4manager" – privilege to work with the system using WAY4 Manager
- "sys.logon" – privilege to log onto the system
- "sys.web\_services" – privileges to work with WAY4 using a thin client providing system access by Web services
- "sys.remote\_access" – privilege to work with WAY4 from a remote workplace (see the document "Working with WAY4™ Remote Access"); the privileges of users with remote access to WAY4 are more limited than those of other users: they can execute the SQL-operator SELECT only from tables required for work, they do not have the right to execute the SQL-operators UPDATE, INSERT, DELETE, however, they have the right to execute special stored procedures that execute these operations with additional security checks.
- "sys.special\_functions" – privilege for the "Special" system menu item
- "sys.role.security\_administrator" – security administrator role
- "sys.role.administrator" – administrator role
- "sys.role.clerk" – operator role (Clerk)
- "sys.role.auditor" – auditor role








 Note that the following priorities are used in the system for user and group roles:

- Main security administrator
- Security administrator

- Administrator
- Operator (Clerk)
- Auditor

The security administrator has the highest priority.

In the "User Management" window (see the figure Fig. 1 of the section "User Management" Window") the following pictograms are used to designate users and user groups (the first pictogram is used when editing is allowed; the second, when editing is prohibited):

- ,  – menu group
- ,  – main security administrator
- ,  – security administrator
- ,  – administrator
- ,  – operator (Clerk)
- ,  – auditor

When assigning privileges, it is necessary to observe the following rules:

- If a user group and users belonging to this group are assigned different roles, the role with the highest priority is used.
- If the use of privileges is denied for a user group, this prohibition extends to all users and all groups included in this group.
- If a user group is assigned privileges, and a user from this group is denied use of these privileges, the user will not have the privileges assigned to the group. Therefore, the denial of privileges has a higher priority.

## Buttons

The "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") contains the following buttons:

- For user groups:
  - [Refresh] – refresh data in the "User Management" window
  - [Add Group] – add a new group of users
  - [Add Child Group] – add a child group of users
  - [Add User] – add a new user
  - [Delete Group] – delete a selected group of users
  - [Move Group] – assign the group of users a higher-ranking group
  - [Edit User Constants] – initialize local constants for a selected group
  - [View Menu] – display a window with the menu root group for the selected user group; this menu group will be available to all users of the selected group when they log onto the system.



Depending on additional privileges assigned to users of a selected group, the menu root group can contain various elements.

- [View Menu Privileges] – display a window with the list of privileges necessary for access to the menu root group.
- [Update Grants] – update access privileges for the selected group of users



See the section "Updating User Group Privileges" for information on limitations to performing this operation.

- [Update Grants For All] – update access privileges for all groups of users who are granted the privilege to work with the system using WAY4 Manager ("sys.client.way4manager" privileges are assigned)



See the section "Updating User Group Privileges" for information on limitations to performing this operation.

- [Show Grants] – display a window with information about privileges for access to DB objects of the menu root group (stored procedure packages, tables, etc.)
- For users:
  - [Refresh] – refresh data in the "User Management" window
  - [Add User] – add a new user
  - [Delete User] – delete a selected user
  - [Move User] – move a user to a different group
  - [View Menu] – display a window with the menu root group for the given user
  - [View Menu Privileges] – display a window with the list of privileges required for access to the menu root group
  - [Lock DB User] – lock the Oracle DB user account
  - [Unlock DB User] – unlock the Oracle DB user account
  - [Drop DB User] – delete the Oracle DB user account
  - [Reset Password] – change user password



In order for functionality provided by the [Lock DB User], [Unlock DB User], [Drop DB User] and [Reset Password] buttons to be available, the additional package "SYS.OWS\_ADMINISTER\_USER" must be installed in WAY4. To do so, execute the following console command:

```
<OWS_Home>\db\ssp.bat connect=sys/<SYSPassword>@<Host>:<Port>:<SID>  
log=<LogFilePath>  
<OWS_Home>\db\scripts\oracle\install\sys\additional\ows_administer_user.ssp  
<OWS_Owner>
```

Where: <SYSPassword> is the sys user password; <Host>:<Port>:<SID> is the server name, port (by default "1521") and "SID" of the database; <LogFilePath> is the full path and name of the log file; <OWS\_Owner> is the name of the scheme owner.

If this package is not installed, after clicking the button, a window will be displayed with the error message "SYS.OWS\_ADMINISTER\_USER not found: cannot perform action".

Moreover, the "User Management" window contains the *Process Log* flag. When this flag is set, a process will be generated and registered in the Process Log for each work session of a user with WAY4 Manager (see the "**WAY4 Manager Processes**" section of the "WAY4 Manager Manual"). In this case, the opening of a form by a user and starting of a procedure will be registered as separate system messages accompanying these processes.


The [Apply] button of the "User Management" window is used to confirm changes; the [Cancel] button is used to cancel changes made. Clicking [OK] confirms changes and closes the "User Management" window.

## Editing user groups

### Adding a new user group

To add a new group or a child group, select any group in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") and click the [Add Group] or [Add Child Group] button. As a result, a new account will appear in the window's "Group" form. Fill in the appropriate fields (see "User group parameters"), and click [Apply].

In the DB a role will be created that includes DB access privileges that are necessary and sufficient for work with the menu group specified in the *Menu* field.

 In some cases, for example, if menu items in the granted user menu group contain pipes or stored procedures requiring additional privileges for access to DB objects, it is necessary to grant additional access privileges for such menu items (see "Configuring additional privileges for menu item").

### Modifying user groups

It is possible to modify the parameters of created groups such as group name (the *Name* field), the assigned menu group (the *Menu* field) and additional information about the group (the *Additional Info* field).

Changes to a group's parameters are saved by clicking [Apply] in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window").

### Assigning a user group to a higher-ranking group

It is possible to assign a group that doesn't have a higher-ranking group to a higher-ranking group, as well as reassign a child group to a different higher-ranking group.

To do so, select the required group in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") and click [Move Group]. The "Move Group" window will appear on the screen (see Fig. 5), containing a list of user groups.

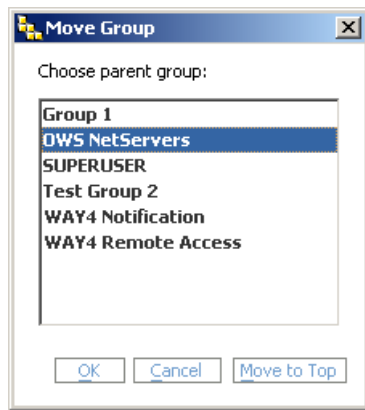


Fig. 5. Assigning a higher-ranking group to a group

To assign a higher-ranking group to a group, select the group in the *Choose parent group* field and click [OK]; to cancel the assignment of a higher-ranking group, click [Cancel].

If [Move to Top] is clicked, the user group becomes the root level group, meaning it will not be a child group.

## Deleting a user group

It is possible to delete a user group only if it has no user accounts.

To delete a group of users, in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") click the [Delete Group] button. A dialog window with the question "Do you really want to remove the group <name of group>?" will appear on the screen. To confirm deletion, click [Yes]; to cancel, click [No].

## Menu root group

To view the menu root group assigned to a user group, select the user group in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") and click [View Menu].

The "Menu" window will appear on the screen (see Fig. 6).

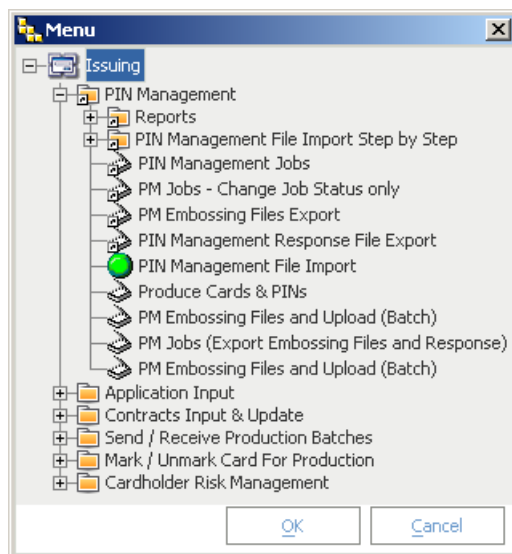


Fig. 6. Information about the menu root group

This window contains information about menu groups and items in the menu root group for this user group.

## List of privileges required for access to the menu root group

It is possible to view the list of privileges required for access to the menu root group, as well as to grant the required privileges to a user group.

To do so, select a group in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") and click [View Menu Privileges].

The "Menu privileges for <name of user group>" window will appear on the screen (see Fig. 7).

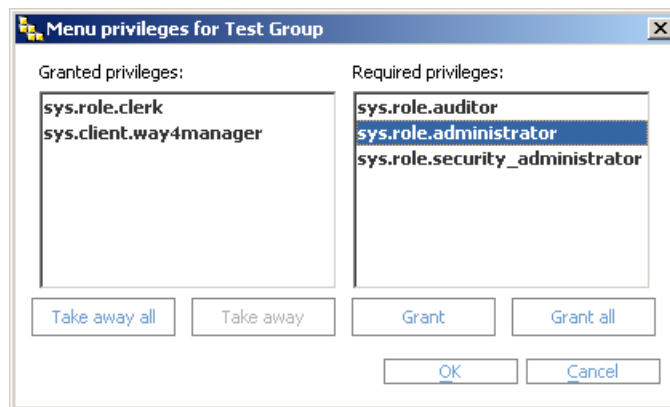


Fig. 7. Privileges for the menu root group

The *Granted Privileges* field contains a list of privileges granted to a user group, and the *Required privileges* field contains a list of privileges necessary (but not assigned to the user group) to work with the menu root group.

To grant privileges required for a menu group to a user group, select the privileges in the *Required privileges* field and click [Grant]; to grant all privileges, click [Grant all].


To deny the use of privileges granted to the user group, select the privileges in the *Granted Privileges* field and click [Take away]; to deny all granted privileges, click [Take away all]. The *Status* field of the "Group Privileges" form (see the figure Fig. 3 of the section Privileges) will contain the value "Deny" for the corresponding privileges.

## Updating user group privileges

When modifying a workplace, there are a number of operations in which it is necessary to update privileges for objects used in working with the assigned user menu group, for users belonging to the given user group. These operations are:

- Addition of new items in the assigned menu group
- Deletion of menu items from the assigned menu group
- Modification of screen forms accessible directly or indirectly (through a different form) from the assigned menu group.

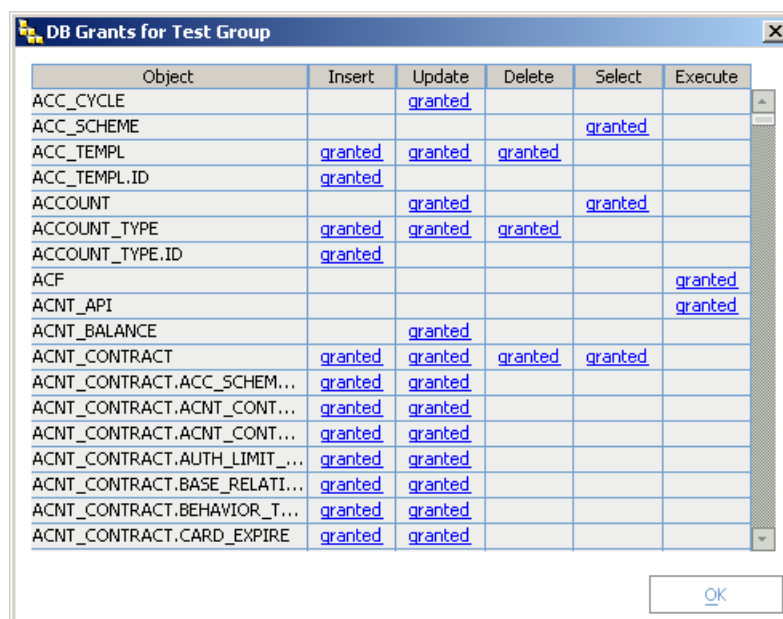
After executing any of the abovementioned modification operations, it is necessary to execute the "Update Grants" operation for all user groups, whose menu groups were affected by the given changes. For a particular, selected user group, this operation is executed by clicking [Update Grants] in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window"). Clicking [Update Grants For All] executes the "Update Grants" operation for all existing groups.

 It is not recommended to update access privileges for all user groups (the [Update Grants] and [Update Grants for all] buttons) when there is a high load on the Oracle database server, such as when receiving and sending a large number of transaction messages online and or/executing lengthy resource-intensive procedures (opening the operational day, processing documents, generating reports, etc.). Otherwise, due to Oracle software limits, transaction message exchange timeouts are possible and as a result, operations may be declined.

### Privileges required to open menu root group objects

It is possible to view information about privileges for menu root group DB objects (stored procedure packages, tables, etc.). To do so, in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") select the user group and click [Show Grants].

The window "DB Grants for <name of user group>" will appear on the screen (see Fig. 8).



Object	Insert	Update	Delete	Select	Execute
ACC_CYCLE		<a href="#">granted</a>			
ACC_SCHEME				<a href="#">granted</a>	
ACC_TEMPL	<a href="#">granted</a>	<a href="#">granted</a>	<a href="#">granted</a>		
ACC_TEMPL.ID	<a href="#">granted</a>				
ACCOUNT		<a href="#">granted</a>		<a href="#">granted</a>	
ACCOUNT_TYPE	<a href="#">granted</a>	<a href="#">granted</a>	<a href="#">granted</a>		
ACCOUNT_TYPE.ID	<a href="#">granted</a>				
ACF					<a href="#">granted</a>
ACNT_API					<a href="#">granted</a>
ACNT_BALANCE		<a href="#">granted</a>			
ACNT_CONTRACT	<a href="#">granted</a>	<a href="#">granted</a>	<a href="#">granted</a>	<a href="#">granted</a>	
ACNT_CONTRACT.ACC_SCHEM...	<a href="#">granted</a>	<a href="#">granted</a>			
ACNT_CONTRACT.ACNT_CONT...	<a href="#">granted</a>	<a href="#">granted</a>			
ACNT_CONTRACT.ACNT_CONT...	<a href="#">granted</a>	<a href="#">granted</a>			
ACNT_CONTRACT.AUTH_LIMIT...	<a href="#">granted</a>	<a href="#">granted</a>			
ACNT_CONTRACT.BASE_RELATI...	<a href="#">granted</a>	<a href="#">granted</a>			
ACNT_CONTRACT.BEHAVIOR_T...	<a href="#">granted</a>	<a href="#">granted</a>			
ACNT_CONTRACT.CARD_EXPIRE	<a href="#">granted</a>	<a href="#">granted</a>			

Fig. 8. DB object privileges


This window contains the following fields:

- *Object* – name of the DB object
- *Insert* – right to add records
- *Update* – right to modify
- *Delete* – right to delete records



- *Select* – right to select records
- *Execute* – right to execute

If DB object privileges are granted, the corresponding field of this window will contain the value "granted"; otherwise the field will not be filled in.

 Note that this form contains a list of objects and privileges that are required to open forms, processes, pipes, etc. In order for all users in the group to receive these privileges, it is necessary to execute the "Update Grants" operation (see "Updating user group privileges").

Clicking the "granted" link in a field of the "DB Grants for <name of user group>" form opens the "Sources for Grant Object <name of DB object and granted privileges>" form (see Fig. 9).

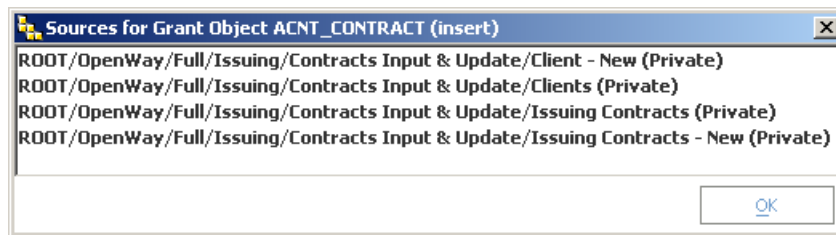


Fig. 9. Menu items requiring privileges for an object

The form shows menu items which require DB object privileges.

## Editing the user list

### Creating a user account

To create a new user account, in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") select the group or a user from the group to which the new user will belong and click [Add User]. The "Enter Key User Properties" dialog window will appear on the screen (see Fig. 10) with fields to enter the user name (*User Name*), user password (*New Password*) and password verification (*Reenter for Verification*).

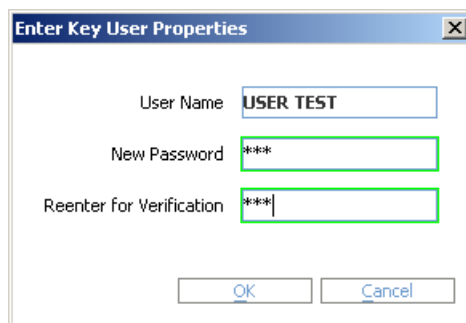




Fig. 10. Dialog window to enter user name and password

 Note that by default, a user's password to log onto WAY4 Manager can also be used to access data using any DB client application. To prevent unauthorised access, this functionality can be turned off, if necessary (see the section "Limiting data access with user password encryption").



After filling in the fields, click [OK] for a new account to appear in the user group.

According to data security principles, each user is granted access to the system in accordance with time parameters set for the user. These parameters are set for each account in the *Working Time* field (see "User account parameters"). Therefore, it is recommended to specify time parameters for an account when it is created.

 Note that by default, the *Working Time* field contains the value "00000000", which denies the user access to the system at all times.

To finish creating a user account, click [Apply] in the "User Management" window in order for the changes to be saved in the DB.

As a result, in the DB a user account will be created which will be assigned a role corresponding to the user group.

The given user can now connect to the DB during the permitted time interval, using the WAY4 Manager application if the user is granted the privileges "sys.logon" and "sys.client.way4manager", or using a remote access application, if the user is granted the privileges "sys.logon" and "sys.remote\_access".

## Changing user account parameters

It is possible to change any user account parameters except for the account's unique ID, contained in the *User Name* field of the "<User name>" form of the "User Management" window (see the figure Fig. 1 of the section "User Management" Window").

Changes to user account parameters are saved by clicking [Apply] in the "User Management" window.

## Assigning a user to a new user group

It is possible to assign a user to a new user group.

In the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") select the user and click [Move User]. The "Move User <user name>" will be displayed on the screen (see Fig. 11).



Fig. 11. Assigning a user to a new user group

To assign a user to a user group, in the "Choose a new group" field, select the group and click [OK]; click [Cancel] to cancel the assignment of a group.

## Deleting a user from the list

To delete a user account from a list, in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") select the user and click [Delete User].

## Locking an Oracle DB user account

To lock an Oracle DB user account, in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") select the user and click [Lock DB User]. The question "Do you really want to perform Lock DB User?" will be displayed on the screen. To confirm account locking, click [Yes]; to cancel, click [No]. After clicking [Yes] the user account will be locked and a window with the message "User locked" will appear on the screen.



Before locking a user account, this user's privileges to log onto the system should be locked. For the privilege "sys.logon" it is necessary to specify the value "Deny" in the *Status* field of the "User Privileges" form (see the figure Fig. 3 of the section "Privileges").



For Oracle database user locking functionality to be available, the additional package "SYS.OWS\_ADMINISTER\_USER" must be installed in WAY4 (see the section "Buttons").

## Unlocking an Oracle DB user account

To unblock an Oracle DB user account, in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window"), select the user and click [Unlock DB User]. A dialog window with the question "Do you really want to perform Unlock DB User?" will appear on the screen. To confirm account unlocking, click [Yes], to cancel, click [No]. After clicking [Yes] the user account will be unlocked and a window with the message "User unlocked" will appear on the screen.




Before unlocking a user account, the user should be granted privileges to log onto the system. For the privilege "sys.logon" it is necessary to specify the value "Allow" in the *Status* field of the "User Privileges" form (see the figure Fig. 3 of the section "Privileges").



For Oracle database user unlocking functionality to be available, the additional package "SYS.OWS\_ADMINISTER\_USER" must be installed in WAY4 (see the section "Buttons").

## Deleting an Oracle DB user account

To delete an Oracle DB user account, in the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window") select the user and click [Drop DB User]. A dialog window with the message "Do you really want to perform Drop DB User?" will appear on the screen. To confirm deletion of the account, click [Yes]; to cancel, click [No]. After clicking [Yes] the user account will be deleted and a window will appear on the screen with the message "User locked".

 For Oracle database user deleting functionality to be available, the additional package "SYS.OWS\_ADMINISTER\_USER" must be installed in WAY4 (see the section "Buttons").

## Changing user password

There are three ways to change a user's system access password:

- With the system menu item "Database => Change Password". This method is described in the section "Database Item" of the "WAY4 Manager Manual".
- With the user menu item "Full → DB Administrator Utilities → Users & Grants → Change Password". As a result, the dialog window "Change Password" will appear on the screen (see Fig. 12).



Fig. 12. Password change dialog window

This dialog window has three fields for entry:

- *Old Password* – old password
- *New Password* – new password
- *Verify New Password* – verify the new password; the value must correspond to the value of the *New Password* field.

After filling in these fields with the appropriate values, click [OK] to change the password.

- Through the "User Management" dialog window (see the figure Fig. 1 of the section "User Management" Window"); select the user and click [Reset Password]. It is recommended to use this method if the user has forgotten his/her old password.

As a result, a dialog window with the question "Do you really want to perform Reset Password?" will appear on the screen. When [Yes] is clicked, the "Enter New User Password" window will appear (see Fig. 13).

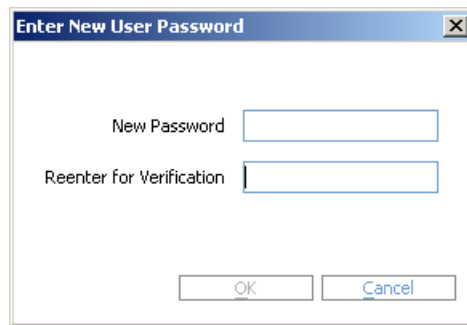


Fig. 13. Changing user password

To change a password, enter the new password in the *New Password* field of this window and confirm the new password in the *Reenter for Verification*, then click [OK].

**i** It is recommended to specify "4" or more for the Oracle DMBS parameter "FAILED\_LOGIN\_ATTEMPTS" to limit the number of failed attempts to enter the correct password. Note that according to PCI DSS, the value of this parameter may not exceed "6". Rules for using the parameter are described in Oracle documentation in the "Configuring Authentication" section of the "Oracle® Database Security Guide".

**i** It is important to note that due to Oracle DBMS security requirements, the security administrator cannot change passwords of existing users.

## Configuring additional privileges for menu item DB objects

In some cases, for example, if menu items in the granted user menu group contain pipes or stored procedures requiring additional DB object privileges, it is necessary to grant additional privileges for these menu items.

These privileges are granted for each separate menu item definition subitems (see the section "[Working with Menu Item Definition Editor](#)" of "WAY4 Manager Menu Editor") as privilege packages.

**i** When working with WAY Manager, it is forbidden to edit standard menu items supplied with the system. Only menu items created by users or copies of standard menu items can be edited (see "[WAY4 Manager Menu Editor](#)").

## Configuring privilege packages

To view, delete, edit and create privilege packages, open the menu item "Full → DB Administrator Utilities → Users & Grants → Subitem Security Grants". The form "Subitem Security Grants" will appear on the screen (see Fig. 14).

Subitem Security Grants			
	Name	Available For	Keep From Housekeeping
1	CM Blob	Clerk	No
2	High Availability	Clerk	No
3	Pipe: FM Handbook Load	Clerk	No
4	Pipe: FM Outward	Clerk	No
5	Housekeeping	Clerk	No
6	Pipe: RBS. Applications Import (Load)	Clerk	No
7	Purge History	Clerk	No
8	Interchange Processing	Clerk	No
9	Voice Authorization	Clerk	No
10	Pipe: RBS. Merchant Applications (Load)	Clerk	No
11	Pipe: VISA SMS Reconciliation Report	Clerk	No
12	ATM Console	Clerk	No
13	PIN Management	Clerk	No
14	Pipe: Balance Import	Clerk	No
15	Pipe: PIN Management Jobs Import	Clerk	No
16	Reports: Real-time Statements	Clerk	No
17	Pipe: RBS. Outward Processing	Clerk	No
18	Pipe: RBS. Payments Import (Load)	Clerk	No

[Obj Grants](#) [Col Grants](#) [SubItems](#)

Fig. 14. Configuring packages of additional privileges for menu subitems

In the *Name* field of this form, the name of the privilege package is specified.

, The roles of users who are granted the right to use these privileges are specified in the *Available For* field:

- "Clerk" – operators
- "Clerk & Auditor" – operators and auditors

To keep privilege packages over a year old from being cleared, set "Y" in the *Keep From Housekeeping* field. By default, the value of this field is "N".

The log of user registration in WAY4 and/or the history of changes are automatically cleared with WAY4 Housekeeping tools (see the document "WAY4™ Housekeeping").

The form "Obj Grants for <name of package of privileges>" is used to configure DB object privileges (stored procedure packages, tables, etc.). This form is opened by clicking [Obj Grants] (see Fig. 15).


Obj Grants for Voice Authorization			1 of 3	□	×
	Object Name	Grant			
1	SOFT_VOICE	EXECUTE			
2	SOFT_INTRA	EXECUTE			
3	VOICE_AUTH	SELECT			

Fig. 15. Form for configuring DB object privileges

In the *Object Name* field of this form, specify the name of the DB object by selecting it from a list, and in the *Grant* field, specify the object privileges:

- "UPDATE" – modify
- "INSERT" – add records
- "DELETE" – delete

- "EXECUTE" – execute
- "SELECT" – select

 In the example shown in the figure above Fig. 15, the package consists of privileges for three objects, two packages of stored procedures and one DB table.

It is possible to grant privileges for particular columns of a table and not for the table in its entirety. The form "Col Grants for <name of package of privileges>" is used to do so (see Fig. 16). The form can be opened by clicking [Col Grants] in the "Subitem Security Grants" form (see Fig. 14).

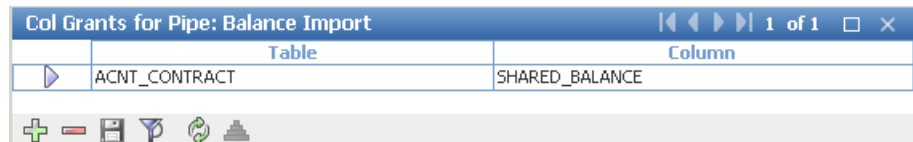



Table	Column
ACNT_CONTRACT	SHARED_BALANCE

Fig. 16. Form for configuring privileges for particular DB table columns

This form contains the following fields:

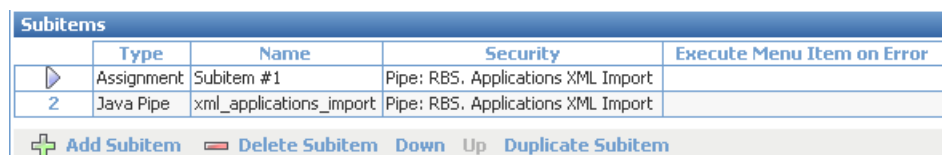
- *Table* – name of DB table
- *Column* – column name of corresponding table

 If the "Col Grants for <name of package of privileges>" form contains at least one record for the table, privileges determined by the "Obj Grants for <name of package of privileges>" form (see Fig. 15) will be granted only for the specified columns.

## Assigning a package of additional privileges to a menu subitem

A package of additional privileges is assigned to a menu item definition subitem in the "Subitems" form of the menu item editor window (see the section "[Working with Menu Item Definition Editor](#)" of "WAY4 Manager Menu Editor").

A package of additional privileges is selected from a list in the *Security* field for the menu item definition subitem (see Fig. 17). For more information see the section "Editing Menu Subitems" of "WAY4 Manager Menu Editor".



Type	Name	Security	Execute Menu Item on Error
Assignment	Subitem #1	Pipe: RBS. Applications XML Import	
Java Pipe	xml_applications_import	Pipe: RBS. Applications XML Import	

Fig. 17. Example of assigning a package of additional privileges for a menu subitem

## Initialization of local constants

The values of local constants are used to filter data available when working with WAY4 Manager forms (see the section "[Form Editor Window. 'Fields' Tab](#)" of "WAY4 Manager Form Editor").

Initialization of local constants is performed when registering a user work session. In doing so, values are used that are set for the group to which the given user belongs.

Values for initialization of local constants are assigned in the form "User Constants for <name of user group>" (see Fig. 18), opened by clicking [Edit User Constants] in the "User Management" dialog window ((see the figure Fig. 1 of the section "User Management" Window)).

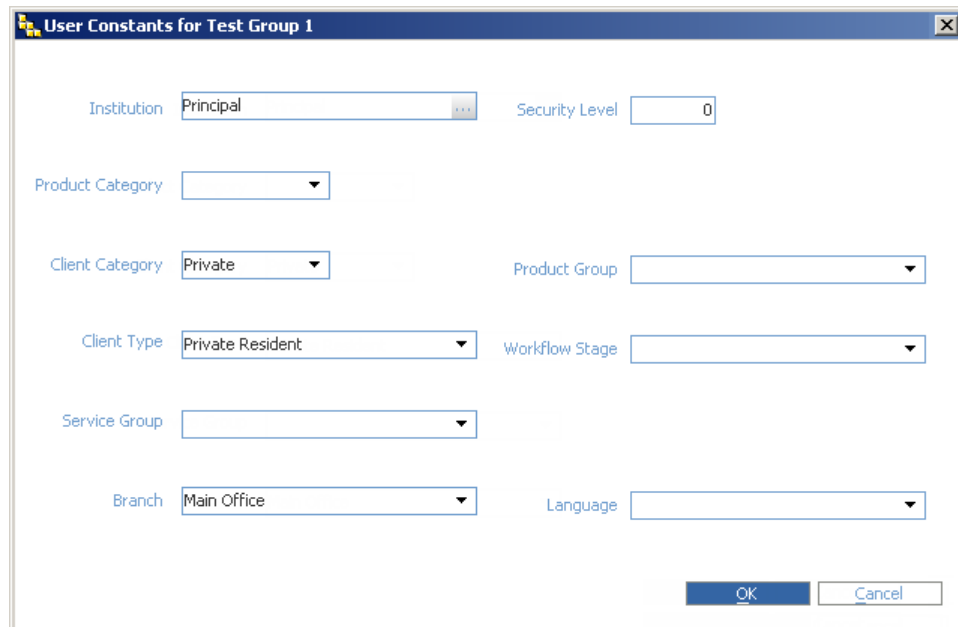


Fig. 18. Initialization of user constants for a user group

The following fields are available in this form:

- *Institution* – name of financial institution
- *Product Category* – product category
- *Client Category* – client category
- *Client Type* – client type
- *Service Group* – additional client classification
- *Branch* – financial institution branch
- *Security Level* – access level; this value is used to filter the types of commands available to a user that are sent to ATMs using a console
- *Product Group* – product group; the value of this field is used by the Advanced Applications module
- *Workflow Stage* – the registered type of application workflow stage; the value of this field is used by the Advanced Applications module
- *Language* – language for reports supporting generation in the local language

After initializing, the values of local constants can be redefined using special modal forms (for example, the "Set Client Type" form – see the section "Manual Data Input" of the "Issuing Module User Manual"), as well as

"Assignment" type menu item subitems (see the section "Type "Assignment"" of "WAY4 Manager Menu Editor").



## Chapter 3. Logging

This section describes principles of logging changes made to data by users during work with the system, as well as principles of logging user registration in the system.

### Process logging

Processes in WAY4 are registered in the process log. For each process, start parameters, current banking date, the user starting the process, process start and end date and time are registered; and also, if execution of the process was stopped, the user who interrupted its execution.

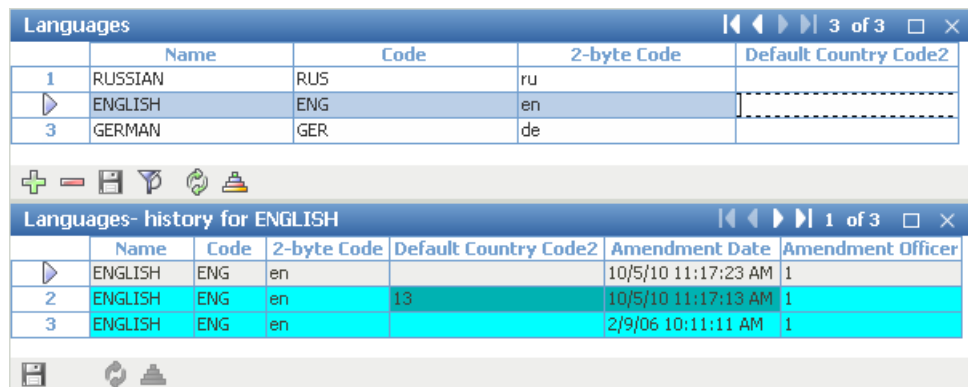
Process logging is described in more detail in the section "[WAY4 Manager Processes](#)" of "WAY4 Manager Manual".

### Logging changes to records made in grid forms

Every change made by a user in an editable field of a grid form is registered in WAY4 in the record change log. It is possible to receive information on the history of changes to any record in any grid form.

For access to the record change log, select the system menu item "Special => View Record History" or press the key combination <Ctrl>+<Shift>+<H>.

An additional form "<Name of grid form> - history for <...>" will appear on the screen (see Fig. 19).



	Name	Code	2-byte Code	Default Country Code2
1	RUSSIAN	RUS	ru	
2	ENGLISH	ENG	en	
3	GERMAN	GER	de	

	Name	Code	2-byte Code	Default Country Code2	Amendment Date	Amendment Officer
1	ENGLISH	ENG	en		10/5/10 11:17:23 AM	1
2	ENGLISH	ENG	en	13	10/5/10 11:17:13 AM	1
3	ENGLISH	ENG	en		2/9/06 10:11:11 AM	1

Fig. 19. Example of record change log

In an additional form, a list of "versions" of the selected record will be shown and information about the date of a change and the user who made the given change.

### Recovering deleted records

To view a grid form's deleted records, select the system menu item "Special => View Deleted" or the key combination <Ctrl>+<Shift>+<D> (see Fig. 20).

	Name	Code	2-byte Code	Default Country Code2	Amendment Date	Amendment Officer
1	Test Language	TST	ts		10/5/10 11:50:22 AM	1
2	Nonexistent Language	NEL	nl		10/5/10 11:52:36 AM	1

Fig. 20. Example of viewing deleted records

Deleted records are recovered by selecting the required deleted record from a list and clicking [Undelete].

## User login history

When establishing a connection for a WAY4 Manager user with the system DB, a record is created in the "Login History" table of the user registration log, including the name of the workstation from which the connection was established, as well as the date and time the connection was made. When work with WAY4 Manager is completed, the user logout date and time is also entered.

The log is accessed by selecting the user menu item "Full → DB Administrator Utilities → Users & Grants → Login History" (see Fig. 21).

	Officer	Computer Name	Login Time	Logout Time	Application Name	Application Version	DBMS Specific
1	SUPERUSER	TEST1	9/27/10 11:07:43 AM	9/27/10 1:03:10 PM	WAY4 Manager	1.2.9.2	SID=474;SER=25445;SPID=15094;LOGON=20100927110742;
2	SUPERUSER	TEST1	9/13/10 9:20:48 AM	9/27/10 11:06:23 AM	WAY4 Manager	1.2.9.2	SID=389;SER=6542;SPID=29713;LOGON=20100913092044;
3	SUPERUSER	TEST1	9/9/10 9:16:18 AM	9/10/10 6:01:31 PM	WAY4 Manager	1.2.9.2	SID=182;SER=53020;SPID=5590;LOGON=20100909091617;
4	SUPERUSER	TEST1	9/6/10 9:05:51 AM	9/9/10 9:14:46 AM	WAY4 Manager	1.2.9.2	SID=182;SER=52278;SPID=17291;LOGON=20100906090549;
5	SUPERUSER	TEST1	9/3/10 1:43:26 PM	9/3/10 6:30:03 PM	WAY4 Manager	1.2.9.2	SID=321;SER=37533;SPID=19672;LOGON=20100903134324;
6	SUPERUSER	TEST1	9/2/10 2:20:16 PM	9/3/10 11:42:22 AM	WAY4 Manager	1.2.9.2	SID=321;SER=28172;SPID=19781;LOGON=20100902142015;
7	SUPERUSER	TEST1	9/2/10 2:03:45 PM	9/2/10 2:18:30 PM	WAY4 Manager	1.2.9.2	SID=55;SER=55234;SPID=18172;LOGON=20100902140343;
8	SUPERUSER	TEST1	8/10/10 5:56:47 PM	8/10/10 5:56:48 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
9	SUPERUSER	TEST1	8/10/10 5:56:36 PM	8/10/10 5:56:38 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
10	SUPERUSER	TEST1	8/10/10 5:56:25 PM	8/10/10 5:56:28 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
11	SUPERUSER	TEST1	8/10/10 5:56:14 PM	8/10/10 5:56:18 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
12	SUPERUSER	TEST1	8/10/10 5:54:49 PM	8/10/10 5:54:53 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
13	SUPERUSER	TEST1	8/10/10 5:54:39 PM	8/10/10 5:54:43 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
14	SUPERUSER	TEST1	8/10/10 5:54:28 PM	8/10/10 5:54:33 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
15	SUPERUSER	TEST1	8/10/10 5:54:07 PM	8/10/10 5:54:18 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
16	SUPERUSER	TEST1	8/10/10 5:53:41 PM	8/10/10 5:53:42 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
17	SUPERUSER	TEST1	8/10/10 5:53:30 PM	8/10/10 5:53:32 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
18	SUPERUSER	TEST1	8/10/10 5:53:19 PM	8/10/10 5:53:22 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
19	SUPERUSER	TEST1	8/10/10 5:53:07 PM	8/10/10 5:53:13 PM	Parallel Running	03_25_20	SID=558;SER=289;SPID=31399;LOGON=20100809132404;
20	SUPERUSER	TEST1	7/6/10 9:23:36 AM	7/6/10 9:23:36 AM	Parallel Running	03_25_20	SID=397;SER=3676;SPID=15601;LOGON=20100706091707;
21	SUPERUSER	TEST1	7/6/10 9:23:25 AM	7/6/10 9:23:26 AM	Parallel Running	03_25_20	SID=397;SER=3676;SPID=15601;LOGON=20100706091707;
22	SUPERUSER	TEST1	7/6/10 9:23:14 AM	7/6/10 9:23:16 AM	Parallel Running	03_25_20	SID=397;SER=3676;SPID=15601;LOGON=20100706091707;
23	SUPERUSER	TEST1	7/6/10 9:23:03 AM	7/6/10 9:23:07 AM	Parallel Running	03_25_20	SID=397;SER=3676;SPID=15601;LOGON=20100706091707;

Fig. 21. Example of the user registration log

During one work session when some processes are executed (starting pipes, deleting records, processing documents, etc.) several records are created in the "Login History" table, information on which is available in the form "Processes for <...>" (see Fig. 22), opened by clicking [Processes] in the "Login History" form.

	Process Name	Started	Finished	Status	Parameters	Bank Date	Started By
1	Apply Product Changes	10/5/10 10:58:32 AM	10/5/10 10:58:32 AM	Closed	PARALLEL=1...	9/2/2010	SUPERUSER
2	Renew Product	10/5/10 10:58:30 AM	10/5/10 10:58:31 AM	Closed	Test	9/2/2010	SUPERUSER


Fig. 22. Processes started during one work session

Clicking the [Aux for] button in the "Login History" form opens the "Aux for <...>" form (see Fig. 23).

Process Log	Attached Role	Attached	Detached	Status	DBMS Specific
Set New Banking Date	AUX	10/5/10 3:12:49 PM	10/5/10 3:13:02 PM	Closed	SID=386;SER=12399;SPID=26105;LOGON=20101005151248;

Fig. 23. Processes generated by other processes

This form contains information about processes that were automatically created as a result of the execution of other processes.

 The WAY4 Housekeeping module automatically cleans the user registration log and change record log (see "WAY4 Housekeeping").

## Locking inactive accounts

According to PCI DSS standards, it is necessary to lock the accounts of users who have not logged into the system for a significant time (more than 90 days). Moreover, it is possible to temporarily lock user accounts.

The list of users registered in the system is accessible in the "Officers" form (see Fig. 24), opened by selecting the menu item "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Officers".

Officers

1

TECHWR2\_A

Yes

Administrator

Yes

SUPERUSER

1111100

Yes

10/6/10 1:31:22 PM

2

TEST USER 1

Yes

Administrator

No

Test User 1

1111100

Yes

10/6/10 11:10:13 AM

3

USER 2

No

Clerk

No

User 2

1101100

Yes

10/6/10 1:54:35 PM

10/6/2010

11/6/2010

4

USER 3

No

Administrator

Yes

User 3

1100111

No

10/6/10 11:14:50 AM

5

USER 4

Yes

Administrator

Yes

User 4

1111100

Yes

10/6/10 11:15:27 AM

Control...

Used Roles

Login History

Messages

Fig. 24. List of users registered in the system

The fields *Inactive From* and *Inactive To* are used to specify the temporary interval in which a user account is locked.

To lock user accounts, select the menu item "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Lock Inactive Officers". When this menu item is selected, a stored procedure is opened which checks the date of the last login of each registered user, if the permissible number of days since this date has been exceeded, all DB object privileges are denied for this account and the value "No" is specified in the *Is Active* field. This stored procedure also locks those accounts which are not locked whose current system date falls in the interval set in the fields *Inactive From* and *Inactive To*. Moreover, accounts whose current system date exceeds the date specified in the *Inactive To* field will be unlocked.

The *Last Login Time* field shows the date and time of the last log into the system.

The *Special Enabled* field specifies whether a user has access ("Yes") to the "Special" system menu item (see the section "Using the System Menu" of the document "DB Manager Manual").

To specify the number of days from a user's last log into the system after which this account will be locked, the global parameter "OFFICER\_MAX\_INACTIVITY\_DAYS" is used (see the section "OFFICER\_MAX\_INACTIVITY\_DAYS" of "WAY4 Global Parameters").

By default, the value of this parameter is "90" in accordance with PCI DSS 8.5.5. standards.

A process started by selecting the menu item "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Start Inactive Officers Monitor" automates the daily start of the menu item "Lock Inactive Officers". Information about the execution of this process is reflected in the process journal. This process can be stopped by selecting the menu item "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Stop Inactive Officers Monitor".

In WAY4 it is possible to lock (unlock) the account of a specific user. To do so, in the "Officers" form (see Fig. 24), select the user, click the [Control] button and select the context menu item "Lock" ("Unlock"). As a result, the user account will be locked (unlocked) and the "No" ("Yes") value will be specified in the *Is Active* field.



If the user was unlocked, the date and time of unlocking will be specified in the *Last Login Time* field.

Moreover, simultaneously with locking (unlocking) a WAY4 user account, it is possible to lock Oracle database user accounts. To do so, in the "Additional Global Parameters" form (Full → Configuration Setup → Main Tables → Additional Global Parameters), add the global parameter "SY\_OFFICER\_USE\_DB\_RIGHTS" and specify the "Y" value for this parameter.



Note that users with the "Application" value in the *Status* field (accounts used for applications, for example, NetServer and Schedule) cannot be locked. Also, a user with the "SUPERUSER" name cannot be locked, either.

## Chapter 4. Privileges for WAY4 directories

This section describes standard WAY4 directories as well as the privileges of various system users for these directories.

### Standard WAY4 directories

WAY4 has the following standard directories:

- <OWS\_HOME> – the main system directory, containing the supplied structure of subdirectories and files which is the same for all main system directories of the same version; the structure of this directory cannot be changed during system work; this directory should be located on the WAY4 file server.



Changes to the contents of the <OWS\_HOME> directory are only permissible in a system upgrade.

- <OWS\_WORK> is a system directory containing a structure partially the similar to that of the <OWS\_HOME> directory structure, including various configuration files, data files specific to a particular WAY4 configuration, screen form, menu and report files created by users, etc. This directory should be located on the WAY4 file server.
- "<...>\Documents and Settings\<user name>\.OWS\<name of database>" is a system directory for storage of temporary files created during WAY4 Manager operation, as well as error log files (see the section "Temporary File Directory" in "WAY4 Manager Manual").

<OWS\_HOME> and <OWS\_WORK> are public directories for all WAY4 users and should be located on the file server.


### Privileges for standard WAY4 directories

When setting up WAY4 Manager on the file server, all users should be granted the privilege to read files in the main system directory (<OWS\_HOME>), as well as privileges to read files in the working directory (<OWS\_WORK>).

Depending on the tasks performed by users, the latter can be divided into classes, each of which requires full privileges for access to standard WAY system directories or their subdirectories (see Table 2).

Table 2. System directory privileges required for various classes of users

User class	Responsibility	Directory
<b>Administrators</b>	WAY4 upgrade	<OWS_HOME>, <OWS_WORK>
	Creation and modification of screen forms, menu items, menu item definitions and user views	<OWS_WORK>\Client\WAY4Manager\components\dbm.module
<b>Operators</b>	Card issue	<OWS_WORK>\Data\Card_Prd
	Organization of interaction with international payment systems	<OWS_WORK>\Data\Interchange
	Ensuring interaction with bank systems	<OWS_WORK>\Data\RBS
	Creation of reports	<OWS_WORK>\Data\Reports

 Note that the directories "<OWS\_WORK>\Data\Interchange" and "<OWS\_WORK>\Data\RBS" are used for file transit when interacting with payment and banking systems. It is highly recommended to use directories on the RAM disk instead of these directories. The use of nonvolatile carriers for these purposes is prohibited. In every initialization of the RAM disk executed, for example, after resetting the computer, it is necessary to reconstruct the directory structure on this disk.

To redirect export, the path to the corresponding directory on the encrypted carrier must be specified in the parameters "INTERCHANGE\_PATH" and "RBS\_INTERCHANGE\_DIR" of the [Client.DBM.Params] section of the "<OWS\_WORK>\db.ini" file.

## Appendix 1. Limiting data access with user password encryption

By default, a user's WAY4 Manager password can also be used for access to data through any DB client application.

If required, a password obtained as the result of encrypting the WAY4 Manager password with a cryptographic variable (key) can be used for access to DB data. Therefore, access to the DB with a password known to the user is only possible through WAY4 Manager, since for DB access an encrypted value, unknown to the user, is used and not the value of the password entered by the user when starting WAY4 Manager.

The password encryption key can be defined using the parameter "PWD\_ENCRYPTION" or "PASSWORD\_ENCRYPTION" (when working remotely with WAY4 using WAY4 Remote Access) of the [Client.DBM.Params] section of the "db.ini" file, located in the <OWS\_WORK> directory; the parameter must be specified in the following form:

```
PWD_ENCRYPTION=<encryption key>
```

or when working remotely (WAY4 Remote Access):

```
PASSWORD_ENCRYPTION=<encryption key>
```

ASCII symbols with codes in the range from 33 to 127 can be used in the body of the encryption key. The key length can be up to 256 symbols.



Note that if the value of the encryption key is not specified (or an empty string is specified), the password is not encrypted for DB access.

## Appendix 2. Amendment Report

The report "Amendment Report" is used to monitor changes made in the database by a user. This report contains information about changes made in tables by a selected user for a certain time interval.

To generate a report, select the user menu item "Full → DB Administrator Utilities → Users & Grants → Amendment Report". The "Date From – To Table List" form will be displayed (see Fig. 25).

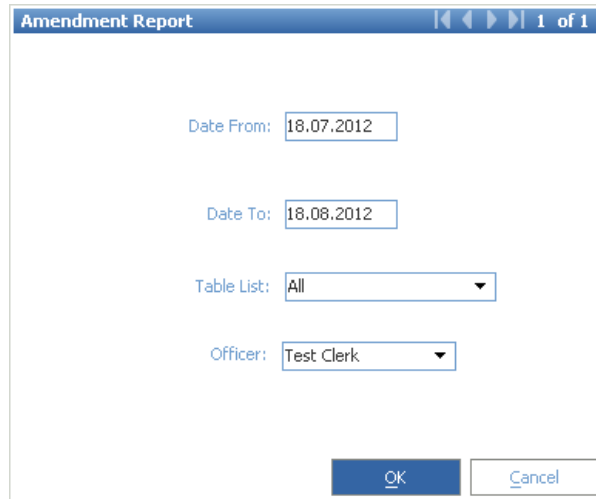


Fig. 25. Setting report parameters

This form contains the following fields:

- *Date From* – start date of report generation.
- *Date To* – end date of report generation.
- *Table List* – drop-down list to specify the table (tables) for which the report will be generated.
- *Officer* – drop-down list to specify the user for whom the report will be generated.

After filling in the form fields, click the [Proceed] button. The report generating process will be started, at the end of which the generated report will be displayed in a browser.



Note that report generation may take a significant amount of time.

The report name will be specified in the first row of the generated report; in the second row, information about the reporting period, user and list of tables for which the report was created. Next are sections containing information about changes in tables. Each section contains the header "Table name: <table name>" and a table including the following fields:

- *Id* – identifier of the table record for which changes were made.
- *Officer* – user who made the changes.
- *Date* – date of changes.



- *Action* – action (for example, "Add" – add a new value; "Del" – delete a value).
- *Column* – database table field name.
- *Old value* – old value of the database table field.
- *New value* – new value of the database table field.