Operation Manual

"WAY4™ User Management"

03.50.30

06/07/2020

Contents

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 notation is used in the document:

- Field labels in screen forms are shown in *italics.*
- Key combinations are shown in angular brackets, for example, <Ctrl>+<F3>.
- Names of screen form buttons and tabs are shown in square brackets, for example, [Approve].
- Sequences for selecting user menu items or context menu items are shown using arrows as follows: "Issuing → Contracts Input & Update".
- Sequences for selecting system menu items are shown using arrows as follows: Database => Change password.
- Variables that differ for each local instance, such as directory and file names, as well as file paths are shown in angular brackets, as in <OWS_HOME>.

Warnings and information are marked as follows:

⚠ Warnings about potentially hazardous situations or actions.

ⓘ Messages with information about important features, additional options, or the best use of certain system functions.

1. WAY4 Users

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

1.1 Classification of WAY4 users

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

Table Classification of WAY4 database users

User type (name)	Function	DB access privileges	Number
Schema owner "Owner", (Administrative user)	Creation of WAY4 DB objects	Full privileges for all schema objects (data and metadata)	1
Main security administrator (Administrative user)	Creation of users (including information security administrators) and user groups, granting access privileges to users and user groups	Full privileges to view, modify and delete WAY4 DB data	1
Information security administrator	Creation of users and user groups, granting access privileges to users and user groups	Partial privileges to view, modify and delete data in the WAY4 DB	Several
Administrator	Creation, modification and deletion of custom views, screen forms, pipes, modification of menu groups and user menu items	Partial privileges to view, edit and delete data	Several
Operator (Clerk)	Work with data in the provided menu group	Privileges to view, modify and delete data available from the provided user menu group	Unlimited

User type (name)	Function	DB access privileges	Number
Auditor	Viewing data available from the provided menu group	Privileges to view data available from the granted user menu group	Unlimited
NetServer user (Administrative user)	Online authorization	Privileges to execute several stored procedures	1

WAY4 administrative users usually have the following names:

- Schema owner – "OWS";
- Main information security administrator – "OWS_A";
- NetServer user– "OWS_N".

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

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

The main security administrator (Super Security Administrator) is created once when switching the system 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 assigned to users by granting them the corresponding privileges (see "Privileges"). The main function of a user with security administrator privileges is the creation of other WAY4 users.

1.2 User groups

To facilitate administration, WAY4 users are grouped. Each user group is provided with a user menu group (see the "User Menu" section of the document "WAY4 Manager Manual"). Access to other user menu groups is prohibited.

> ⓘ Each WAY4 user can belong to one user group only.

Each user group is also granted a set of DB access privileges. When the "Update Grants" activity is performed (see"Creating user workplaces") two roles are automatically created for each user group in the DB (in accordance with the granted access privileges), which include DB access privileges necessary and sufficient for working with this user menu group. These roles are granted to all users in the group.

2. Creating user workplaces

To create a WAY4 user workplace, register a user account for the user in the appropriate group (see"User groups"). In the user account, the user can be granted privileges that determine the user's role (administrator, operator, auditor or security administrator). Access privileges for a user menu group are granted at the user group level.

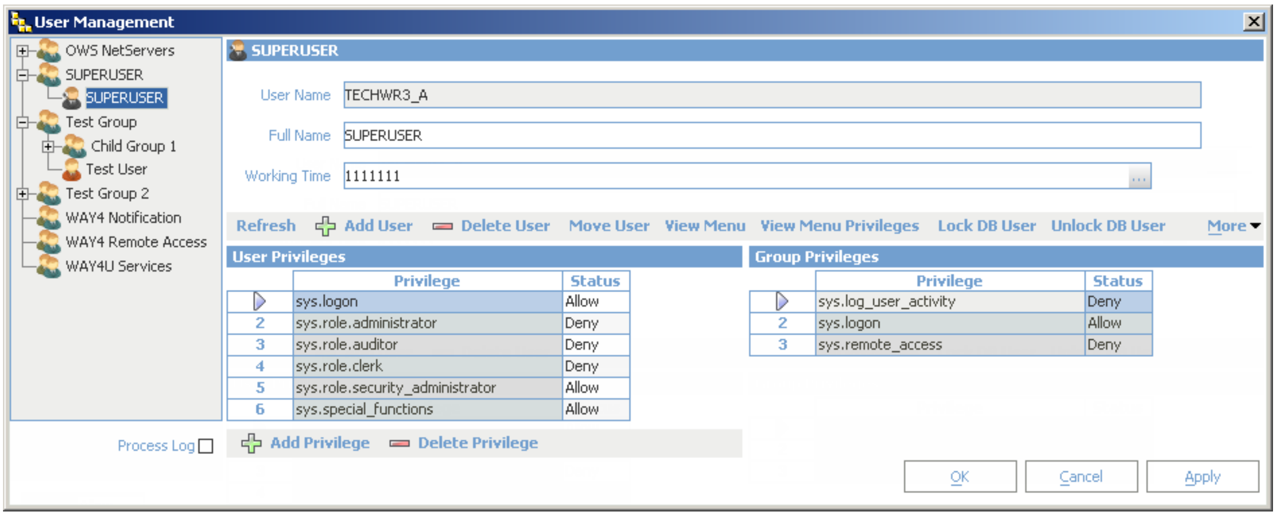
Access to user menu groups is granted using the following mechanisms:

- For each user group, creation of its own group-specific user menu group.
- Granting users and/or user groups privileges registered in WAY4, which are also set for the menu group (see the document "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 by redetermining these filter values (see the section "Initializing local constants").

2.1 Window for working with user records

User accounts are managed in the "User Management" window, opened from the menu item "Full → DB Administrator Utilities → Users & Grants → User Groups and Users - Edit".



User Name: TECHWR3_A

Full Name: SUPERUSER

Working Time: 1111111

User Privileges

	Privilege	Status
▷	sys.logon	Allow
2	sys.role.administrator	Deny
3	sys.role.auditor	Deny
4	sys.role.clerk	Deny
5	sys.role.security_administrator	Allow
6	sys.special_functions	Allow

Group Privileges

	Privilege	Status
▷	sys.log_user_activity	Deny
2	sys.logon	Allow
3	sys.remote_access	Deny

Fig. Window for administering users and user groups

In the left part of the window, a list of users and user groups is displayed in a hierarchical structure.

> Any changes to user accounts and user groups that have not been 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 accounts and groups are saved by clicking [Apply] and [OK].

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

2.1.1 User group parameters

The "Group" form of the "User Management" window (see the section "Window for working with user records") contains the following fields:

- *Name* – name of the group
- *Menu* – contains a drop-down list to specify the root menu group for this user group (the field cannot be edited for a child group).
- *Grants Update Time* – the date and time the "Update Grants" activity was last performed for this group (the field is read-only)
- *Additional Info* – field for entering additional information about the user group

> Note that the parent group's 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 needed primarily to reduce the number of DB roles.

The following rules should be followed when administering:

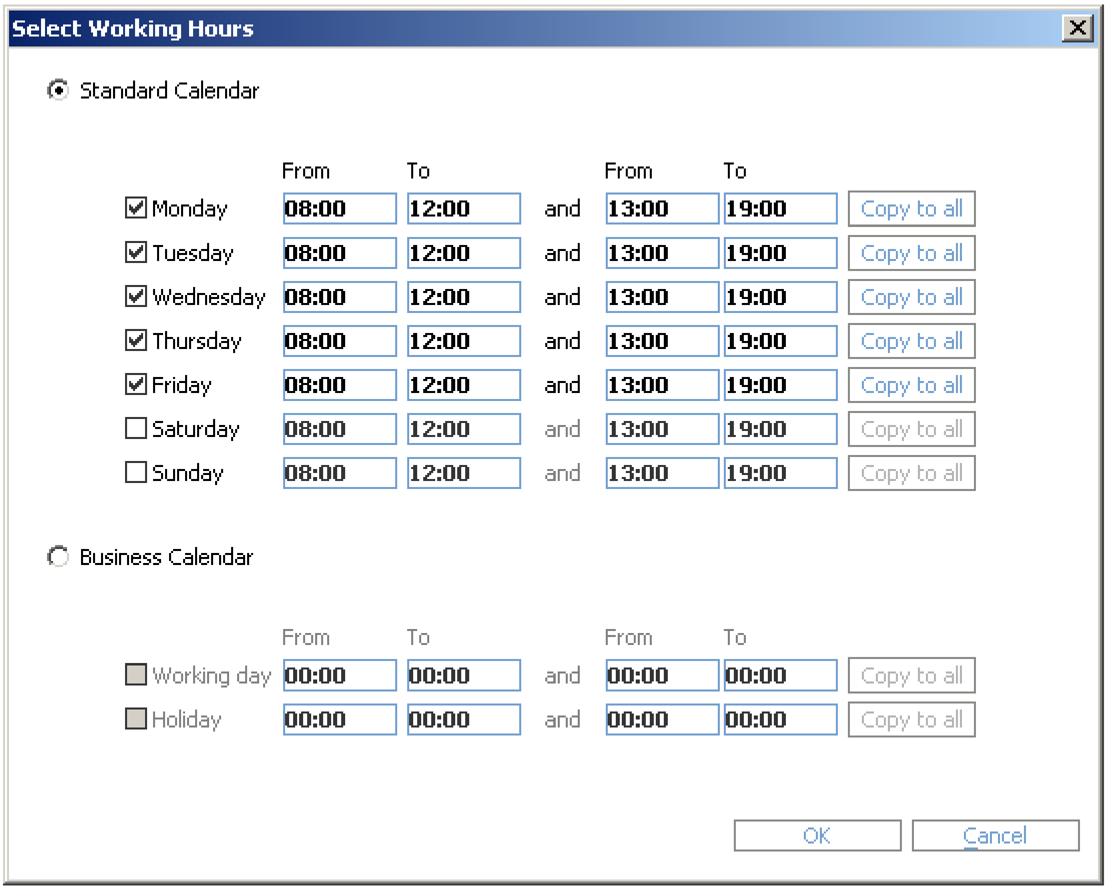
- After adding a child group, access privileges must be updated for the parent group (the [Update Grants] button).
- After making changes to a parent group menu branch, update access privileges for the parent group (the [Update Grants] button).

> For restrictions on performing the "Update Grants" activity, see the section "Updating user group privileges".

2.1.2 User account parameters

The "<user name>" form of the "User Management" window (see the section "Window for working with user records") contains the following fields:

- *User Name* – user ID for connection to the DB (this field is read-only).
- *Full Name* – user name.
- *Working Time* – time interval during which the user is allowed 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 to work with the system ("0" – denied, "1" – allowed). Clicking the ... button opens the "Select Working Hours" window.



Select Working Hours

● Standard Calendar

	From	To		From	To	
☑ Monday	08:00	12:00	and	13:00	19:00	Copy to all
☑ Tuesday	08:00	12:00	and	13:00	19:00	Copy to all
☑ Wednesday	08:00	12:00	and	13:00	19:00	Copy to all
☑ Thursday	08:00	12:00	and	13:00	19:00	Copy to all
☑ Friday	08:00	12:00	and	13:00	19:00	Copy to all
□ Saturday	08:00	12:00	and	13:00	19:00	Copy to all
□ Sunday	08:00	12:00	and	13:00	19:00	Copy to all

○ Business Calendar

	From	To		From	To	
□ Working day	00:00	00:00	and	00:00	00:00	Copy to all
□ Holiday	00:00	00:00	and	00:00	00:00	Copy to all

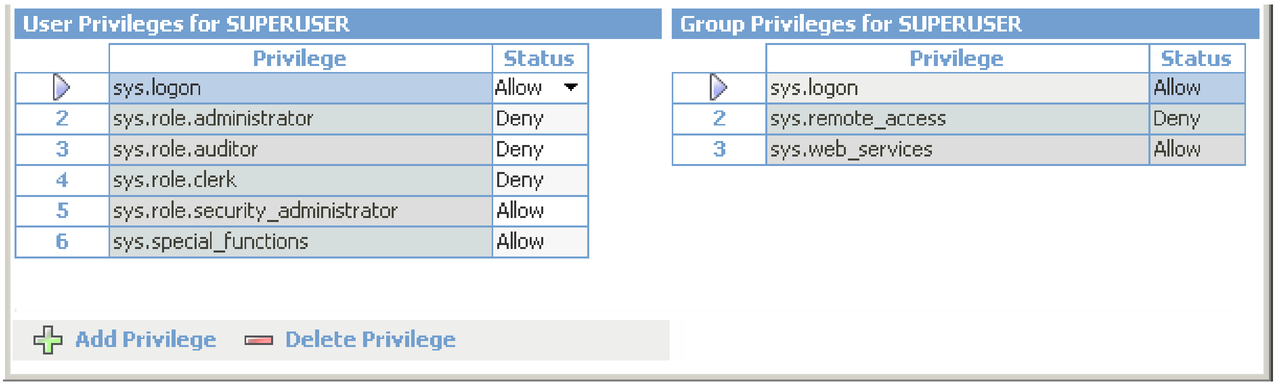
Fig. Setting an interval for system access

This window shows the interval for system access. The *Standard Calendar* and *Business Calendar* radio 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/holidays (see the section "Business Calendar" of the document "WAY4™ Dictionaries").

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

2.1.3 Privileges

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



User Privileges for SUPERUSER

	Privilege	Status
▷	sys.logon	Allow
2	sys.role.administrator	Deny
3	sys.role.auditor	Deny
4	sys.role.clerk	Deny
5	sys.role.security_administrator	Allow
6	sys.special_functions	Allow

Group Privileges for SUPERUSER

	Privilege	Status
▷	sys.logon	Allow
2	sys.remote_access	Deny
3	sys.web_services	Allow

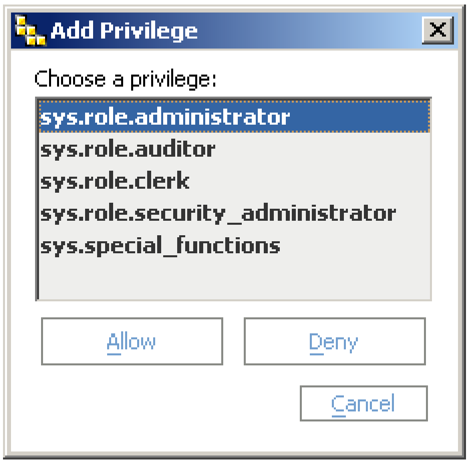
Fig. Access privileges for users and groups

The *Privilege* field indicates the name of the access privilege.

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

- "Allow" – permission to use the privilege
- "Deny" – use of the privilege is denied

To add privileges registered in WAY4, click the [Add Privilege] button. The "Add Privilege" form will be displayed.



Add Privilege

Choose a privilege:

sys.role.administrator
sys.role.auditor
sys.role.clerk
sys.role.security_administrator
sys.special_functions

Fig. Assigning access privileges

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

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

The following system privileges are registered in WAY4:

- "sys.client.way4manager" – privilege to work with the system using WAY4 Manager
- "sys.logon" – privilege to log into the system
- "sys.web_services" – privileges to work with WAY4 using a thin client that provides system access through 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 a SQL SELECT statement only from

tables required for work, they do not have the right to execute the SQL UPDATE, INSERT, DELETE statements, however, they have the right to run 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
- "sys.form_data_export" – privilege to print data and export information for an operator (Clerk). If the status of a user's or group's "sys.form_data_export" privilege is "Deny", printing and exporting are not allowed.

Note that the following priorities are used in WAY4 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 section "Window for working with user records") the following icons are used to designate users and user groups (the first icon 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, 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 applies to all users and all groups included in the 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.

2.1.4 Buttons

The "User Management" window (see the section "Window for working with user records") contains the following buttons:

- For user groups:

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

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

  - [View Menu Privileges] – display a window with the list of privileges necessary for access to the root menu group.
  - [Update Grants] – update access privileges for the selected user group
  - [Update Grants For All] – update access privileges for all user groups who are granted the privilege to work with the system using WAY4 Manager ("sys.client.way4manager" privileges are assigned)

> ⚠ For restrictions on updating access privileges, see the section "Updating user group privileges".

  - [Show Grants] – display a window with information about privileges for access to DB objects of the root menu group (packages of stored procedures, tables, etc.)

- For users:
  - [Refresh] – refresh data in the "User Management" window
  - [Add User] – add a new user
  - [Delete User] – delete the user
  - [Move User] – move the user to a different group
  - [View Menu] – display a window with the user's root menu group
  - [View Menu Privileges] – display a window with the list of privileges necessary for access to the root menu 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
  - [Lock Officer] – lock a WAY4 user account

- [Unlock Officer] -unlock a WAY4 user account

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, run the following command in the console:

```
<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 schema owner name.

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".

> The *Process Log* checkbox controls logging of user actions to the process log. If the checkbox is selected, all user actions will be logged in the process log. If the checkbox is not selected, all security related actions will be logged in the process log. All administrator actions are considered security related and are logged regardless of whether the checkbox is selected.

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

2.2 Editing user groups

2.2.1 Adding a new user group

To add a new group or a child group, select any group in the "User Management" window (see the section "Window for working with user records") and click the [Add Group] or [Add Child Group] button. As a result, a new record will appear in the window's "Group" form. Fill in the appropriate fields (see "User group parameters") and click the [Apply] button.

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 DB object privileges, additional privileges must be granted for these menu items (see "Configuring additional privileges for DB objects for menu items").

2.2.2 Modifying user groups

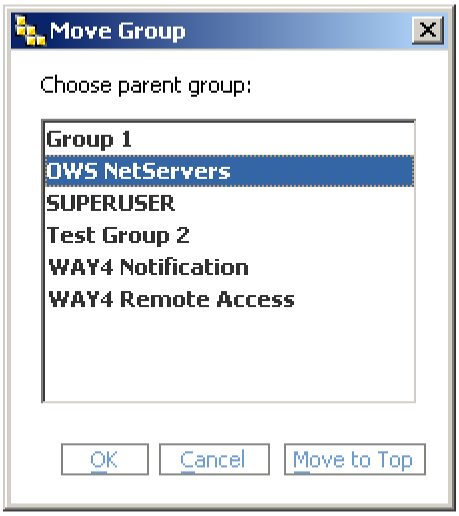
It is possible to modify the parameters of created groups, such as group name (the *Name* field), the assigned menu group (the *Menu* field) and additional information about the group (the *Additional Info* field).

Changes to a group's parameters are saved by clicking the [Apply] button in the "User Management" window (see the section "Window for working with user records").

2.2.3 Assigning a higher group to a user group

A group that doesn't have a parent group can be assigned a higher-ranking group, and a child group can be reassigned to a different parent group.

To do so, select the required group in the "User Management" window (see the section "Window for working with user records") and click the [Move Group] button. The "Move Group" window with a list of user groups will open.



Move Group

Choose parent group:

Group 1
OWS NetServers
SUPERUSER
Test Group 2
WAY4 Notification
WAY4 Remote Access

Fig. Assigning a parent group to a group

To assign a parent group to a group, select the parent group in the "Choose parent group" field and click [OK]; to cancel the activity, click [Cancel].

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

2.2.4 Deleting a user group

A user group can only be deleted if there aren't any user accounts in it.

To delete a user group, click the [Delete Group] button in the "User Management" window (see the section "Window for working with user records"). A confirmation window with the prompt "Do you really want to remove the group <group name>?" will be displayed. To confirm, click [Yes]; to cancel, click [No].

2.2.5 Menu root group

To view the menu root group assigned to a user group, select the user group in the "User Management" window (see the section "Window for working with user records") and click [View Menu].

The "Menu" window will open.

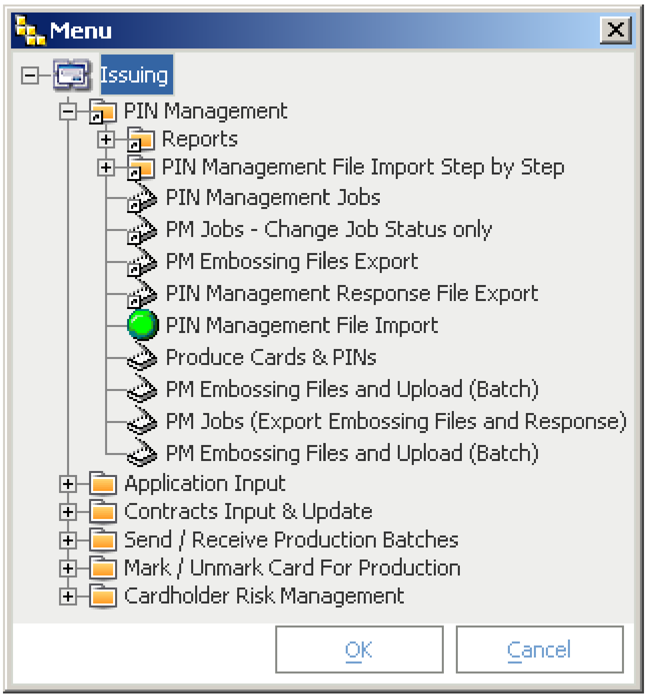

Menu
Issuing
PIN Management
Reports
PIN Management File Import Step by Step
PIN Management Jobs
PM Jobs - Change Job Status only
PM Embossing Files Export
PIN Management Response File Export
PIN Management File Import
Produce Cards & PINs
PM Embossing Files and Upload (Batch)
PM Jobs (Export Embossing Files and Response)
PM Embossing Files and Upload (Batch)
Application Input
Contracts Input & Update
Send / Receive Production Batches
Mark / Unmark Card For Production
Cardholder Risk Management
OK
Cancel

Fig. Information about the menu root group

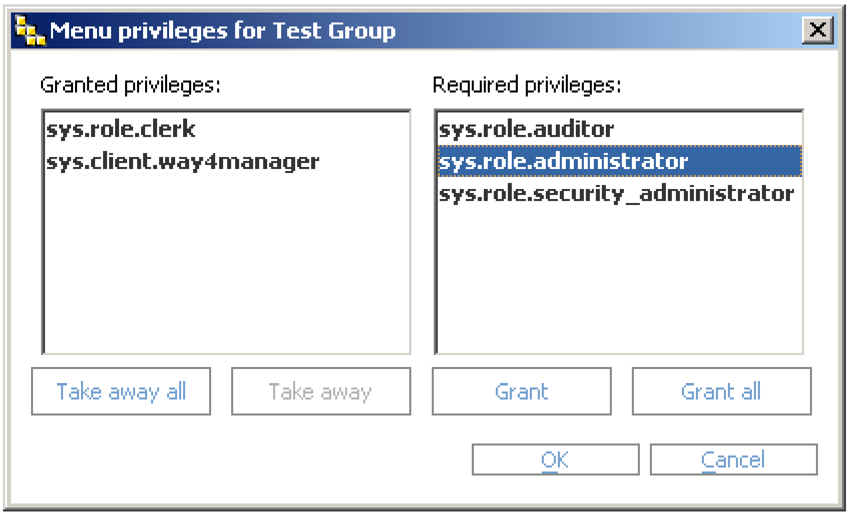
This window contains information about menu groups and items in the menu root group for this user group.

2.2.6 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" window (see the section "Window for working with user records") and click [View Menu Privileges].

The "Menu privileges for <user group name>" window will open.



Granted privileges: sys.role.clerk, sys.client.way4manager

Required privileges: sys.role.auditor, sys.role.administrator, sys.role.security_administrator

Fig. Menu root group privileges

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

To grant a user group privileges that are required for a menu 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 section "Privileges") will contain the value "Deny" for the corresponding privileges.

2.2.7 Updating user group privileges

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

- Addition of new items to 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.

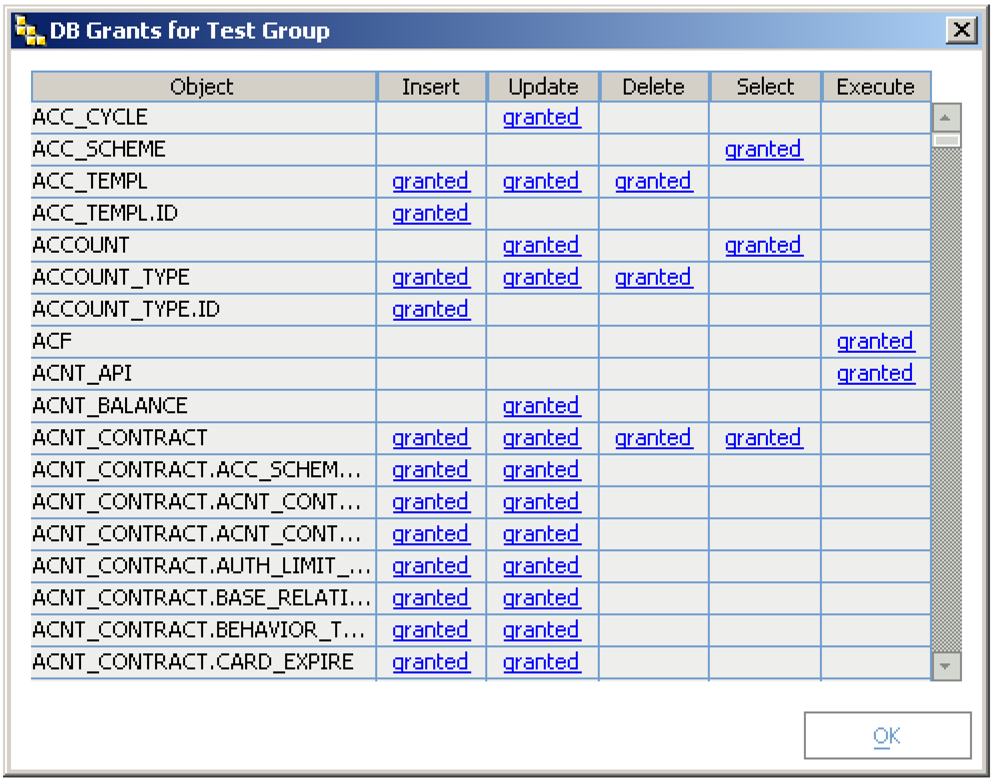
After performing any of these activities, the "Update Grants" activity must be performed for all user groups whose menu groups were affected by the changes. For each user group, this activity is performed by clicking [Update Grants] in the "User Management" window (see the section "Window for working with user records"). Clicking [Update Grants For All] performs the "Update Grants" activity 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/running lengthy resource-intensive procedures (opening the business day, processing documents, generating reports, etc.). Otherwise, due to Oracle software limits, transaction message exchange timeouts are possible and as a result, transactions may be declined.

2.2.8 Privileges required to open menu root group objects

It is possible to view information about privileges for a menu root group's DB objects (stored procedure packages, tables, etc.). To do so, in the"User Management" window (see the section "Window for working with user records") select a user group and click [Show Grants].

The window "DB Grants for <user group name>" will open.



Object	Insert	Update	Delete	Select	Execute
ACC_CYCLE		granted			
ACC_SCHEME				granted	
ACC_TEMPL	granted	granted	granted		
ACC_TEMPL.ID	granted				
ACCOUNT		granted		granted	
ACCOUNT_TYPE	granted	granted	granted		
ACCOUNT_TYPE.ID	granted				
ACF					granted
ACNT_API					granted
ACNT_BALANCE		granted			
ACNT_CONTRACT	granted	granted	granted	granted	
ACNT_CONTRACT.ACC_SCHEM...	granted	granted			
ACNT_CONTRACT.ACNT_CONT...	granted	granted			
ACNT_CONTRACT.ACNT_CONT...	granted	granted			
ACNT_CONTRACT.AUTH_LIMIT_...	granted	granted			
ACNT_CONTRACT.BASE_RELATI...	granted	granted			
ACNT_CONTRACT.BEHAVIOR_T...	granted	granted			
ACNT_CONTRACT.CARD_EXPIRE	granted	granted			

Fig. Privileges for DB objects

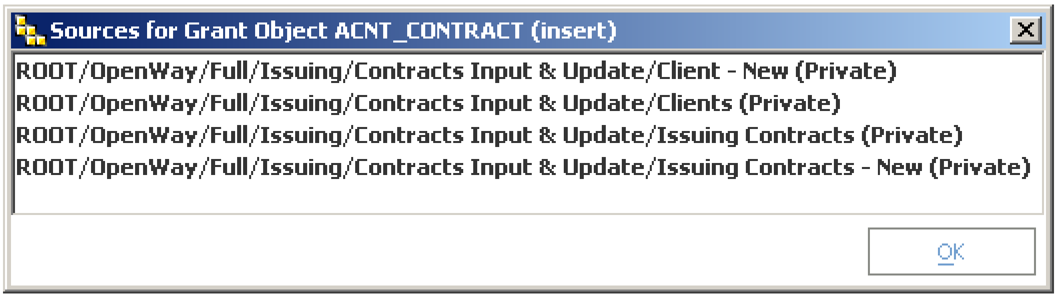
This window contains the following fields:

- *Object* – name of the DB object
- *Insert* – privilege to add records
- *Update* – privilege to modify
- *Delete* – privilege to delete records
- *Select* – privilege to select records
- *Execute* – privilege 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 run forms, processes, pipes, etc. In order for all users in the group to receive these privileges, perform the "Update Grants" activity (see "Updating user group privileges").

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



Sources for Grant Object ACNT_CONTRACT (insert)

ROOT/OpenWay/Full/Issuing/Contracts Input & Update/Client - New (Private)
ROOT/OpenWay/Full/Issuing/Contracts Input & Update/Clients (Private)
ROOT/OpenWay/Full/Issuing/Contracts Input & Update/Issuing Contracts (Private)
ROOT/OpenWay/Full/Issuing/Contracts Input & Update/Issuing Contracts - New (Private)

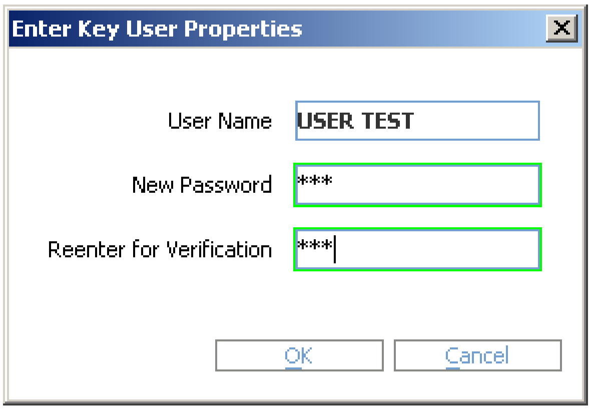
Menu items requiring privileges for an object

The form shows menu items that require DB object privileges.

2.3 Editing the user list

2.3.1 Creating a user account

To create a new user account, in the "User Management" window (see the section ""Window for working with user records"), 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" window will open with fields to enter the user name (*User Name*), user password (*New Password*) and password verification (*Reenter for Verification*).



Enter Key User Properties

User Name: USER TEST
New Password: ***
Reenter for Verification: ***

Fig. Window for entering user name and password

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

After filling in the fields and clicking [OK], a new record will 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 user account in the *Working Time* field (see "User account parameters"). Accordingly, it is recommended to specify time parameters when creating an account.

ⓘ Note that by default, the *Working Time* field contains the value "0000000", which denies the user access to the system at all times.

To finish creating the user account, click the [Apply] button in the "User Management" window to save the changes to the DB.

A user account will be created in the DB and will be assigned a role corresponding to the user group.

This user can now connect to the DB during the allowed time interval, using the WAY4 Manager application if the user has "sys.logon" and "sys.client.way4manager" privileges, or using a remote access application if the user has "sys.logon" and "sys.remote_access" privileges.

2.3.2 Changing user account parameters

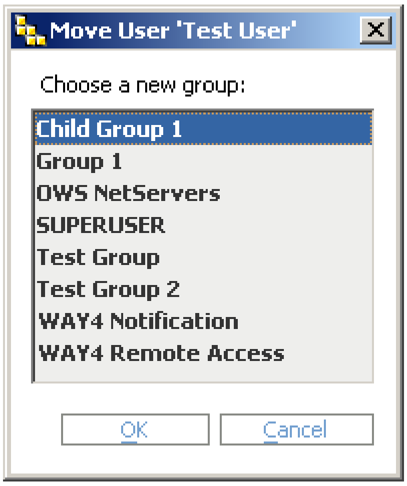
It is possible to change any user account parameters except for the account's unique ID, contained in the *User Name* field of the "<user name>" form of the "User Management" window (see the section "Window for working with user records").

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

2.3.3 Assigning a new user group to a user

A new user group can be assigned to a user.

In the "User Management" window (see the section "Window for working with user records") select the user and click [Move User]. The "Move User <user name>" window will open.



Move User 'Test User'

Choose a new group:

- Child Group 1
- Group 1
- OWS NetServers
- SUPERUSER
- Test Group
- Test Group 2
- WAY4 Notification
- WAY4 Remote Access

Fig. Assigning a new user group to a user

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.

2.3.4 Deleting a user from the list

To delete a user account from the list, in the "User Management" window (see the section "Window for working with user records") select the user and click [Delete User].

2.3.5 Locking a WAY4 user account

To lock a WAY4 user account, in the "User Management" window (see the section "Window for working with user records") , select the user and click the [Lock Officer] button. A confirmation window will be displayed with the question "Do you really want to perform Lock Officer?". To confirm, click the [Yes] button; to cancel, click [No].

After the [Yes] button has been clicked, the user account will be locked.

A specific user's account can be locked (unlocked) automatically (see the section "Locking inactive accounts").

2.3.6 Unlocking a WAY4 user account

To unlock a WAY4 user account, in the "User Management" window (see the section "Window for working with user records"), select the user and click the [Unlock Officer] button. A confirmation window will be displayed with the question "Do you really want to perform Unlock Officer?". To unlock the user account, click the [Yes] button; to cancel, click [No].

2.3.7 Locking an Oracle DB user account

ⓘ Before locking an Oracle DB user, lock the selected user's WAY user account (see the section "Locking a WAY4 user account").

To lock an Oracle DB user account, in the "User Management" window (see the section "Window for working with user records") select the user and click [Lock DB User]. A confirmation window with the prompt "Do you really want to perform Lock DB User?" will be displayed. To confirm, click the [Yes] button; to cancel, click [No]. After clicking [Yes] the user account will be locked and a window with the message "User locked" will be displayed.

⚠ Before locking a user account, this user's privileges to log into the system should be locked. For the privilege "sys.logon", specify "Deny" in the *Status* field of the "User Privileges" form (see the section "Privileges"). To be able to lock Oracle database users, the additional package "SYS.OWS_ADMINISTER_USER" must be installed in WAY4 (see the section "Buttons").

2.3.8 Unlocking an Oracle DB user account

ⓘ Before unlocking an Oracle DB user, unlock the selected user's WAY user account (see the section "Unlocking a WAY4 user account").

To unlock an Oracle DB user account, in the "User Management" window (see the section "Window for working with user records"), select the user and click [Unlock DB User]. A confirmation window with the prompt "Do you really want to perform Unlock DB User?" will be displayed. To unlock the user account, click the [Yes] button; to cancel, click [No]. After clicking [Yes] the user account will be unlocked and a window with the message "User unlocked" will be displayed.

⚠ Before unlocking a user account, the user should be granted privileges to log into the system. For the privilege "sys.logon", specify "Allow" in the *Status* field of the "User Privileges" form (see the section "Privileges"). To be able to unlock Oracle database users, the additional package "SYS.OWS_ADMINISTER_USER" must be installed in WAY4 (see the section "Buttons").

2.3.9 Deleting an Oracle DB user account

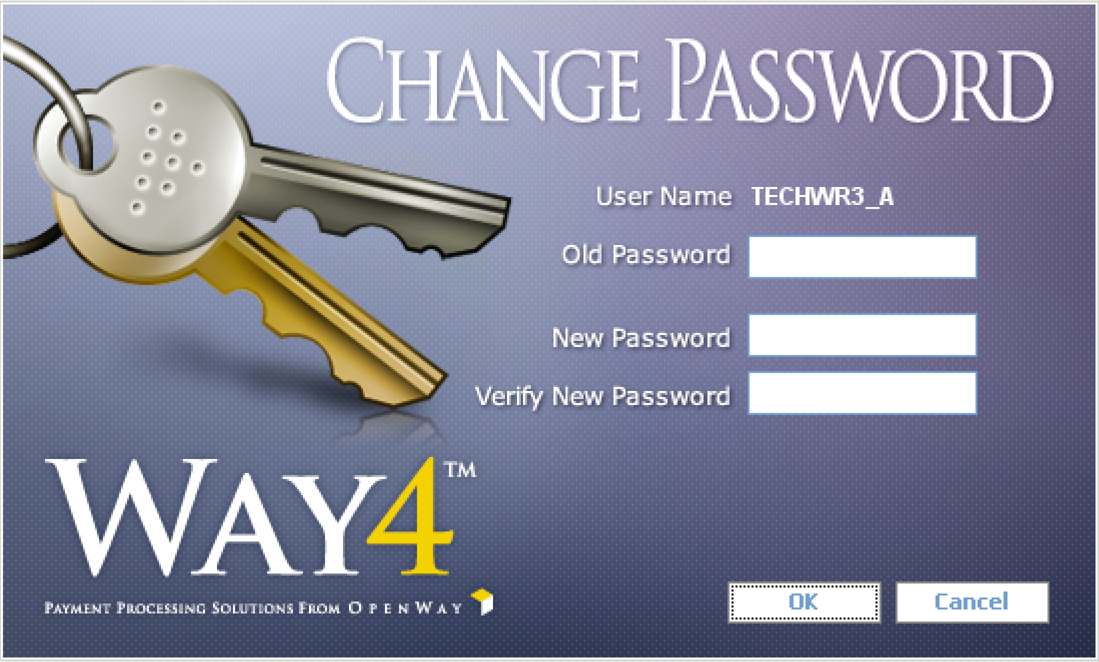
To delete an Oracle DB user account, in the "User Management" window (see the section "Window for working with user records") select the user and click [Drop DB User]. A confirmation window with the prompt "Do you really want to perform Drop DB User?" will be displayed. To confirm deletion of the account, 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 deleted".

To be able to delete Oracle database users, the additional package "SYS.OWS_ADMINISTER_USER" must be installed in WAY4 (see the section "Buttons").

2.3.10 Changing user passwords

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 document "WAY4 Manager Manual".
- With the user menu item "Full → DB Administrator Utilities → Users & Grants → Change Password". As a result, the "Change Password" window will open.



CHANGE PASSWORD

User Name TECHWR3_A

Fig. Window for changing a user's password

This window has three input fields:

- *Old Password* – old password
- *New Password* – new password
- *Verify New Password* – confirm the new password by re-entering the value from the *New Password* field.After filling in these fields, click [OK] to change the password.

- In the "User Management" window (see the section "Window for working with user records"); select the user and click [Reset Password]. This method is recommended if the user has forgotten their old password.

A confirmation window with the prompt "Do you really want to perform Reset Password?" will be displayed. Click [Yes] to open the "Enter New User Password" window.

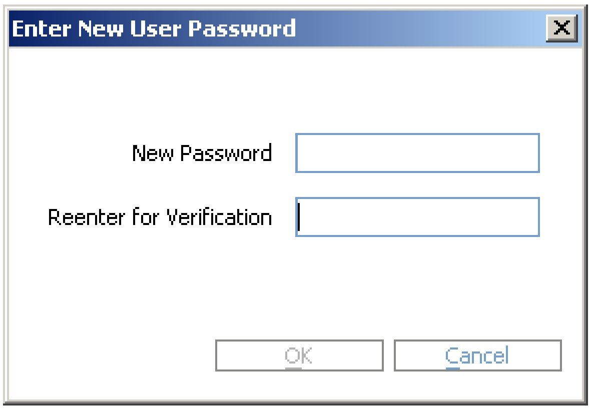


Fig. Changing a user's password

To change the password, enter the new password in the *New Password* field, re-enter it in the *Reenter for Verification* field and click [OK].

> 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".
> Note that the security administrator cannot change the passwords of existing users. This restriction is due to Oracle DBMS security requirements.

2.4 Configuring additional privileges for DB objects for menu items

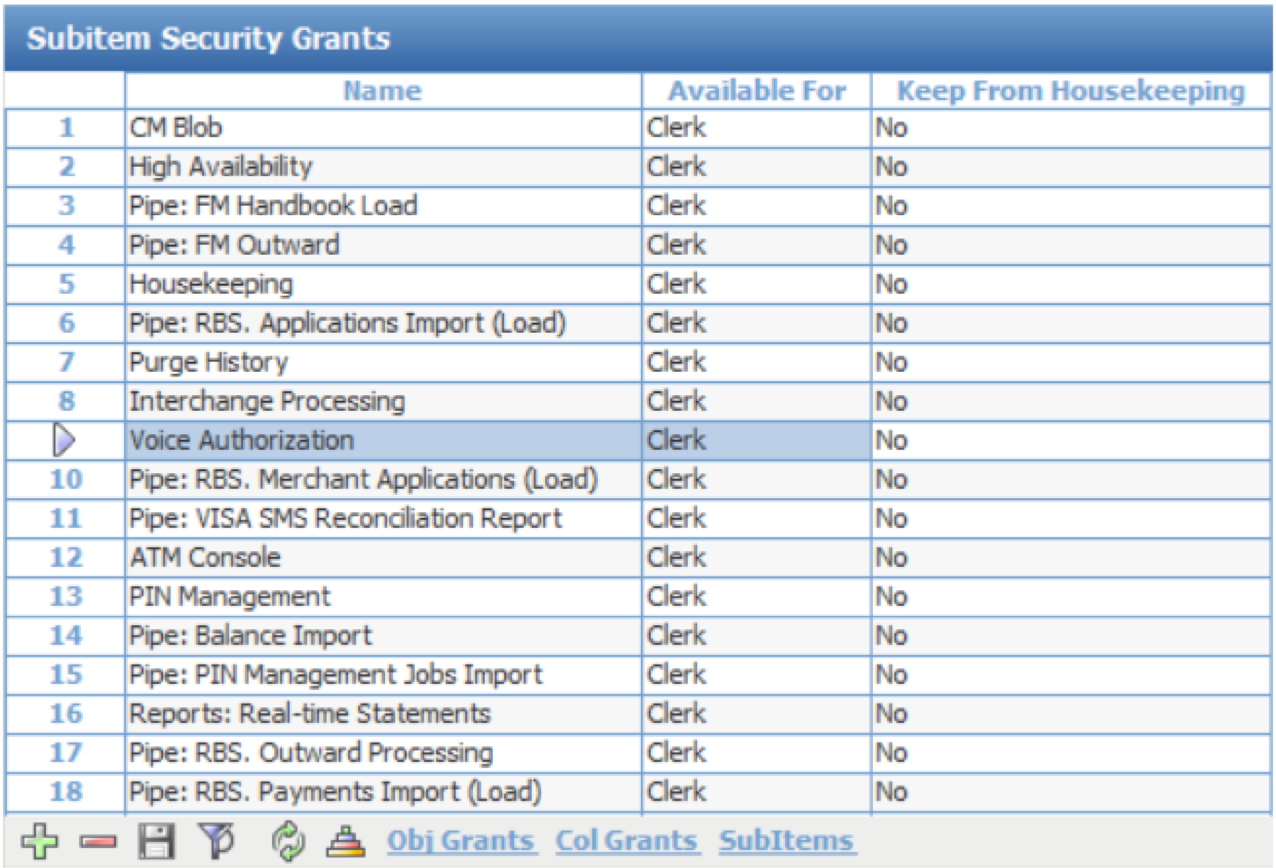
In some cases, for example, if menu items in the granted user menu group contain pipes or stored procedures requiring additional DB object privileges, it is necessary to grant additional privileges for these menu items.

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

> When working with WAY Manager, edit standard menu items supplied with the standard system is prohibited. Only custom menu items or copies of standard menu items can be edited (see the document "WAY4 Manager Menu Editor").

2.4.1 Configuring privilege packages

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



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
▷	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

Fig. Configuring menu subitem privilege packages

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

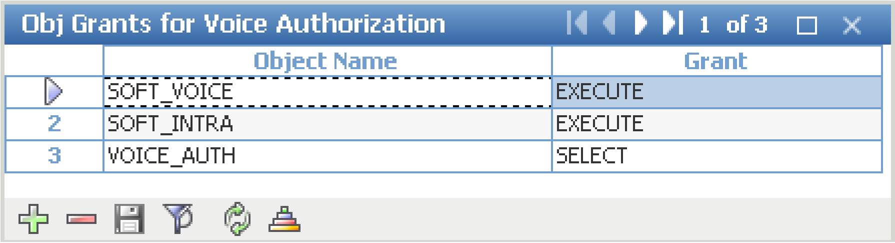
The roles of users who can use these privileges are specified in the *Available For* field:

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

To disable deletion of records for privilege packages that are more than one year old, select "Y" in the *Keep From Housekeeping* field. By default, this field's value is "N".

> The WAY4 Housekeeping module automatically clears the user registration log and change log (see the document "WAY4 Housekeeping™").

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



Obj Grants for Voice Authorization

	Object Name	Grant
▷	SOFT_VOICE	EXECUTE
2	SOFT_INTRA	EXECUTE
3	VOICE_AUTH	SELECT

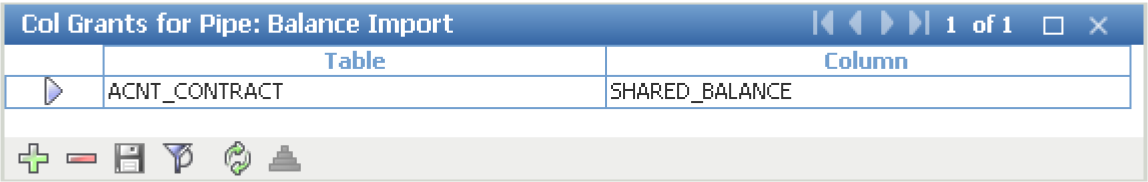
Fig. Form to configure privileges for database objects

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 privileges for access to the object:

- "UPDATE" – modify
- "INSERT" – add records
- "DELETE" – delete
- "EXECUTE" – execute
- "SELECT" – select

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

Privileges can be granted for certain columns of a table and not for the table in its entirety. This is done in the "Col Grants for <privilege package name>" form opened by clicking [Col Grants] in the "Subitem Security Grants" form.



Col Grants for Pipe: Balance Import

	Table	Column
▷	ACNT_CONTRACT	SHARED_BALANCE

Fig. Form to configure privileges for specific DB table columns

This form contains the following fields:

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

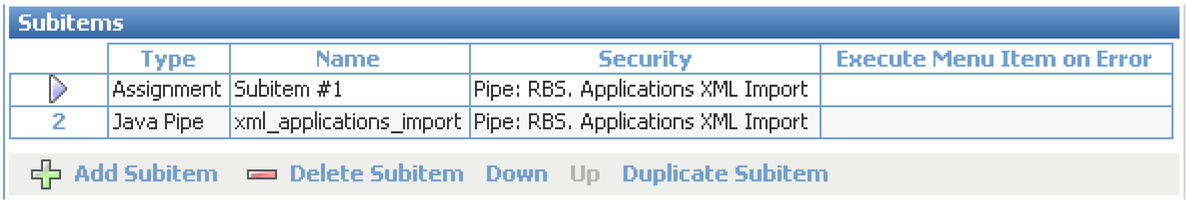
> ⓘ If the "Col Grants for <privilege package name>" form contains at least one record for the table, privileges defined in the "Obj Grants for <privilege package name>" form will be granted only for the specified columns.

2.4.2 Assigning a privilege package to a menu subitem

Assigning a privilege package to a menu subitem

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

A privilege package is selected from the list in the *Security* field for the menu item definition's subitem. For more information, see the section "Editing Menu Subitems" of the document "WAY4 Manager Menu Editor".



Subitems

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

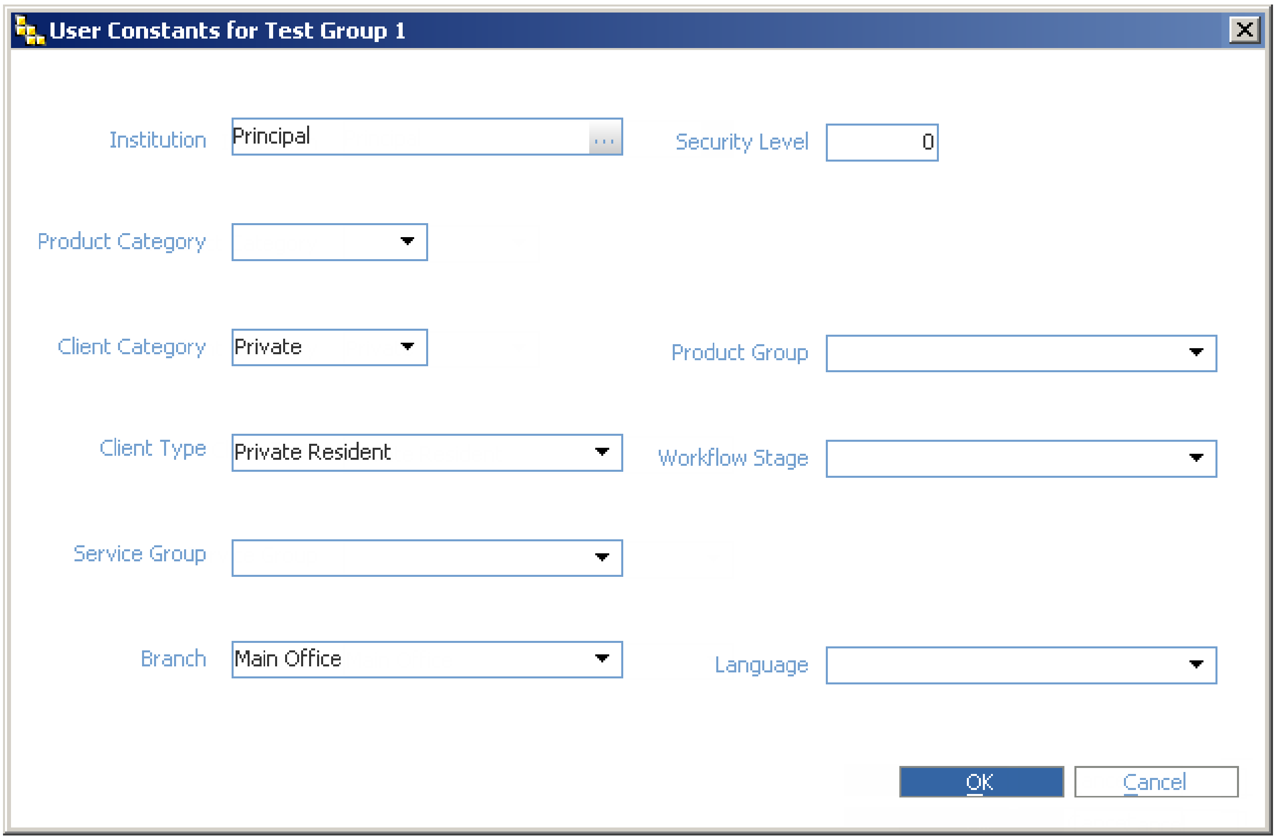
Fig. Example of assigning a privilege package for a menu subitem

2.5 Initializing 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").

Local constants are initialized when registering a user work session. 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 <user group name>", opened by clicking [Edit User Constants] in the "User Management" window (see the section "Window for working with user records").



User Constants for Test Group 1

Institution: Principal
Security Level: 0
Product Category:
Client Category: Private
Product Group:
Client Type: Private Resident
Workflow Stage:
Service Group:
Branch: Main Office
Language:

Fig. Initializing local constants for a user group

This form contains the following fields:

- *Institution* – name of financial institution
- *Product Category* – product category
- *Client Category* – client category
- *Client Type* – client type.
- *Service Group* – additional classification for clients.
- *Branch* – financial institution's 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 application workflow step type; the value of this field is used by the Advanced Applications module
- *Language* – language for reports supporting generation in the local language

After initialization, 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 document "Issuing Module User Manual"), as well as "Assignment" menu item definition subitems (see the section "Type "Assignment"" of the document "WAY4 Manager Menu Editor").

3. Logging

This section describes principles of logging changes made to data by users while working with the system, as well as principles of logging user login to the system.

3.1 Process logging

Processes in WAY4 are registered in the process log. For each process, startup parameters, current banking date, the user who started the process, start and end date and time are logged; and also, if termination of the process was forced, the user who did this.

Process logging is described in more detail in the section "WAY4 Manager Processes" of the document "WAY4 Manager Manual".

Logging changes to records made in grid forms

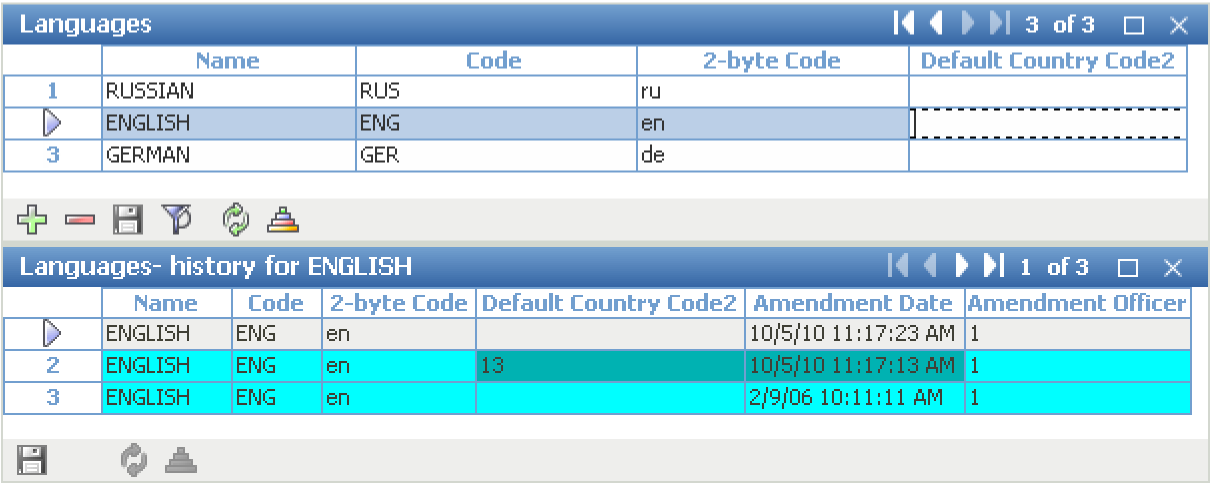
3.2 Logging changes to records made in grid forms

Logging changes to records made in grid forms

Each 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 "<grid form name> - history for <...>" will appear on the screen.



Languages

3 of 3

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

Languages- history for ENGLISH

1 of 3

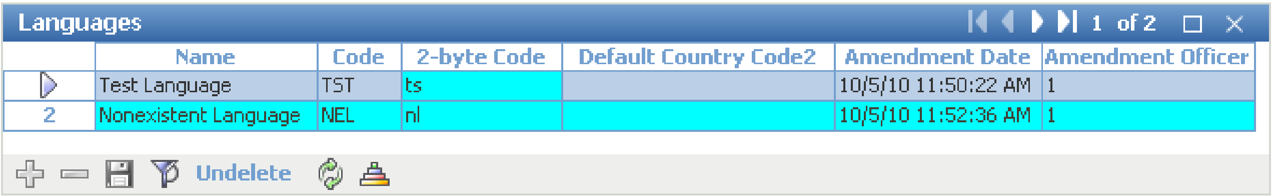
	Name	Code	2-byte Code	Default Country Code2	Amendment Date	Amendment Officer
▷	ENGLISH	ENG	en		10/5/10 11:17:23 AM	1
2	ENGLISH	ENG	en	13	10/5/10 11:17:13 AM	1
3	ENGLISH	ENG	en		2/9/06 10:11:11 AM	1

Fig. Example of the history of changes to a record

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

3.3 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>.



	Name	Code	2-byte Code	Default Country Code2	Amendment Date	Amendment Officer
▷	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

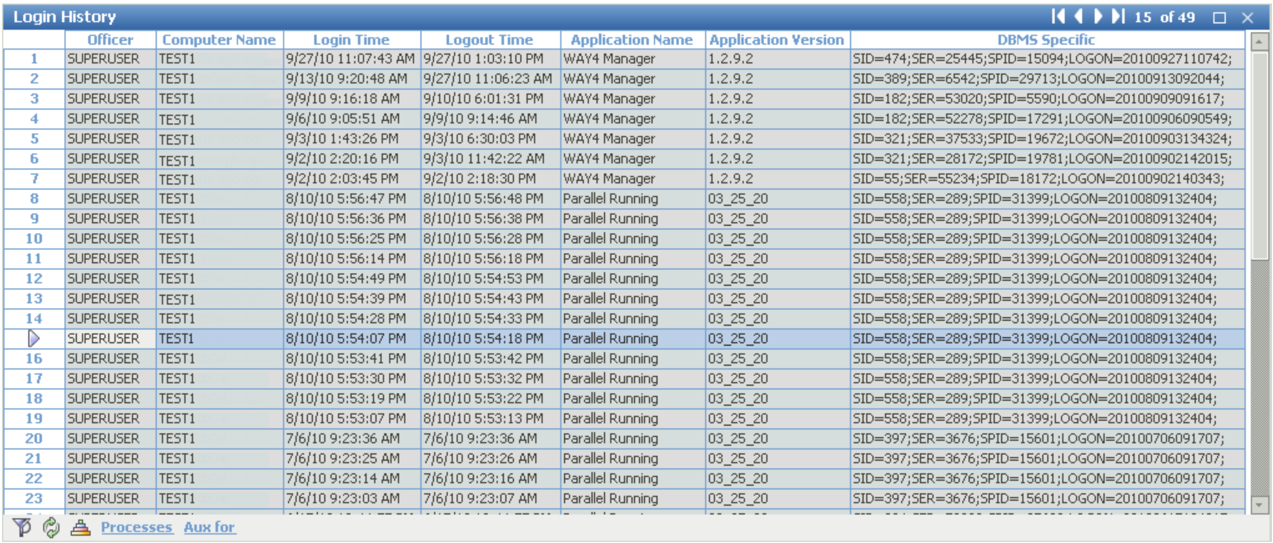
Fig. Example of viewing deleted records

A deleted record is recovered by selecting it from the list and clicking [Undelete].

3.4 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.

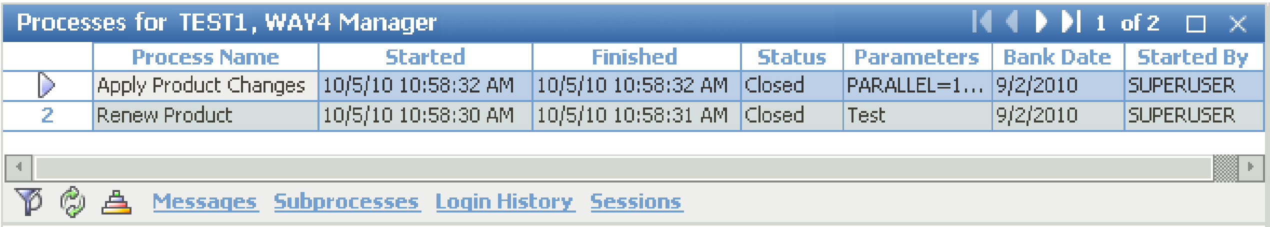
The log is accessed through the user menu item "Full → DB Administrator Utilities → Users & Grants → Login History".



	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;
▷	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. Example of user login history

During one session when several 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 <...>", opened by clicking [Processes] in the "Login History" form.

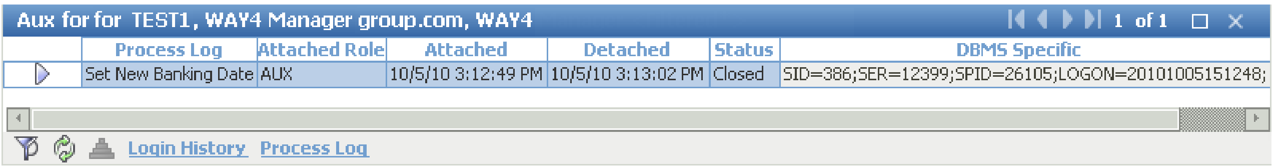


Processes for TEST1, WAY4 Manager

	Process Name	Started	Finished	Status	Parameters	Bank Date	Started By
▷	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. Processes started in one session

Clicking [Aux for] in the "Login History" form opens the "Aux for <...>" form.



Aux for for TEST1, WAY4 Manager group.com, WAY4

	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. Processes that were created by other processes

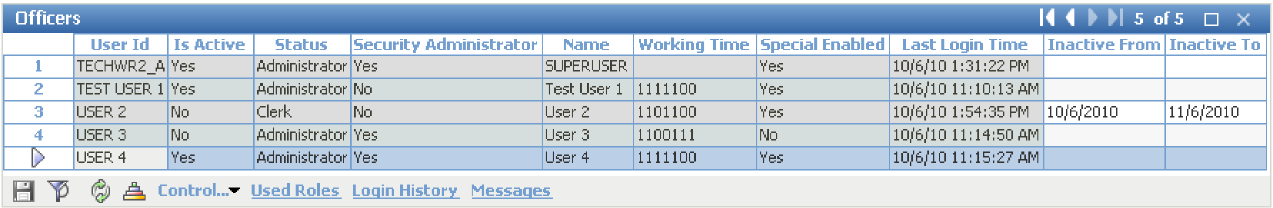
This form contains information about processes that were automatically created as a result of the execution of other processes.

The WAY4 Housekeeping module automatically clears the user registration log and change log (see the document "WAY4 Housekeeping™").

3.5 Locking inactive accounts

Pursuant to PCI DSS requirements, 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 available in the "Officers" form, opened through the menu item "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Officers".



Officers

	User Id	Is Active	Status	Security Administrator	Name	Working Time	Special Enabled	Last Login Time	Inactive From	Inactive To
1	TECHWR2_A	Yes	Administrator	Yes	SUPERUSER		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		
▷	USER 4	Yes	Administrator	Yes	User 4	1111100	Yes	10/6/10 11:15:27 AM		

Fig. List of users registered in WAY4

The fields *Inactive From* and *Inactive To* are used to specify the time interval for locking a user account.

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 each registered user's last login, and if more than the permissible number of days have passed since then, 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 the document "WAY4 Global Parameters"). By default, the value of this parameter is "90" in accordance with PCI DSS 8.5.5 requirements.

A process that is started by selecting the menu item "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Start Inactive Officers Monitor" automates the daily launch 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) a specifc user's account. To do so, in the "Officers" form, select the user, click [Control] 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 "Application" in the *Status* field (accounts used for applications, for example, NetServer and Scheduler) cannot be locked. Also, a user with the "SUPERUSER" name cannot be locked.

4. Privileges for WAY4 directories

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

4.1 Standard WAY4 directories

WAY4 has the following standard directories:

- <OWS_HOME> – the main system directory, containing the standard 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 operation; this directory should be located on the WAY4 file server.

> ⓘ Changes to the contents of the <OWS_HOME> directory are only permissible during a system upgrade.

- <OWS_WORK> is a system directory containing a structure partially 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" of the document "WAY4 Manager Manual").

<OWS_HOME> and <OWS_WORK> are public directories for all WAY4 users and should be located on the file server.

4.2 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.

Table System directory privileges required for various classes of users

User class	Responsibility	Directory
Administrators	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
Operators	Card production	<OWS_WORK>\Data\Card_Prd
	Organization of interchange 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 a virtual disk (RAM disk) instead of these directories. The use of non-volatile media for these purposes is prohibited. Each time a virtual disk is initialized, for example, after a computer reboot, it is necessary to restore the directory structure on this disk.

To redirect export, the path to the corresponding directory on the encrypted media 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.

To restrict "Operator Clerk" user access to the error stack trace, set "no" for the parameter "SHOW_ERROR_STACK_TRACE" in the section [Client.DBM.Params] of the file "<OWS_WORK>\db.ini".

5. 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 Manger.

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.

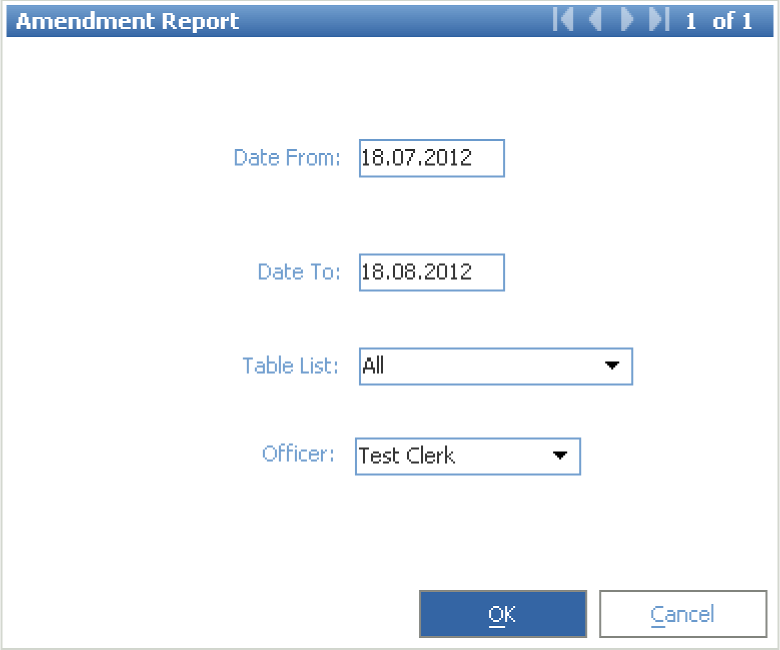
The encryption key can also be specified in the WAY4 Manager launch parameter:

```
<OWS_HOME>\client\way4manager\dbmanager\way4manager.exe PWD_ENCRYPTION=<encryption
key>
```

6. 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 "Amendment Report" form will be displayed.



Amendment Report

Date From:	18.07.2012
Date To:	18.08.2012
Table List:	All
Officer:	Test Clerk

Fig. Setting report parameters

This form contains the following fields:

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

After filling the form, click [OK]. 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.