DB Manager User Management

Contents

Introduction

This document describes the principal concepts of administering WAY4™ users using the DB Manager client application.

While working with this document, it is recommended that users refer to the following reference material from OpenWay's documentation series:

- DB Manager Manual

- Menu Editor

- Form Builder

- WAY4™ PA-DSS Implementation Guide

The following notation is used in this document:

- Field labels in screen forms are shown in *italics*.

- Button labels in screen forms are shown in square brackets, such as [Approve].

- Menu selection sequences are shown with arrows, such as "Issuing → Contracts Input & Update".

- Sequences for selecting system menu items are shown with different arrows, such as "Database => Change password".

- Key combinations used while working with DB Manager are shown in angular brackets such as <Ctrl>+<F3>.

- The names of directories and/or files that vary for each local instance of the program are also displayed in angular brackets, like <OWS_HOME>.

- Warnings about potentially hazardous situations or actions are marked with the ⚠sign.

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

Chapter 1. WAY4 System Users

This chapter deals with the classification of WAY4 users and their access privileges in relation to WAY4 database.

Classification of WAY4 Users

The classification of WAY4 users, according to their functions, and the access privileges granted to each user class are shown in Table 1.

Table 1. Classification of WAY4 database users

User type/name	Function	Database access privileges	Number
Scheme Owner, "Owner" (a service user)	Creating WAY4 database objects	Full access privileges to all scheme objects (data and metadata)	1
Main data security administrator Super Security Administrator (a service user)	Creating users, including data security administrators and user groups; granting access privileges to users and user groups	Full privileges to view, modify and delete WAY4 database data	1
Data security administrator	Creating users, and user groups granting access privileges to users and user groups	Restricted privileges to view, modify and delete WAY4 database data	Several
Administrator	Creating, editing and deleting user views, screen forms and pipes; editing user menu groups and items	Restricted privileges to view, modify and delete data	Several
Operator (Clerk)	Working with data in the menu group provided	Privileges to view, modify and delete data accessible in the provided user menu group	Unlimited
Auditor	Viewing data accessible in the provided user menu group	Privileges to view data accessible in the provided user menu group	Unlimited
NetServer user (a service user)	Online authorisation	Privilege to execute some stored procedures	1

Normally, WAY4 users have the following names:

- Scheme Owner – OWS

- Super Security Administrator – OWS_A

- NetServer user – OWS_N

Administrators, operators and auditors, hereinafter referred to as WAY4 users as opposed to service users (see Table 1.), use the DB Manager application (see the DB Manager Manual) to work with data in the WAY4 database.

The Scheme Owner owns all tables, views, excluding custom views, and procedures. After the system is installed (switched to multi-user mode), the Scheme Owner is automatically forbidden to enter the system through DB Manager.

The Super Security Administrator is created once when the system is first run in the multi-user mode. The principal function of the Super Security Administrator is creating WAY4 users, including data security administrators.

WAY4 users, administrators and operators may be assigned data security administrator functions. The principal function of a user with data security administrator privileges is creating other WAY4 users.

In order for the main data security administrator (Super Security Administrator), security administrator and WAY4 system administrators to, in addition to their main functions (creation of users and groups, forms, pipes, etc.), work with objects from the user menu group provided, it is necessary to update privileges for these users ([Update User] button of the dialog window, see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window").

User Groups

In order to make administering the system convenient, WAY4 users are aggregated in groups. Each user group is assigned a user menu group (see the "User Menu" section in the DB Manager Administrator Manual). A user group assigned a certain user menu group has no access to other user menu groups.

Each WAY4 user may belong to only one user group.

Each user group is assigned a package of privileges for accessing the database. While performing the "Update Grants" operation (see the section "Creating Workplaces"), each user group is automatically assigned a role that includes database access privileges necessary and sufficient for working with the given user menu group. The role is shared by all users included in the group.

Chapter 2. Creating Workplaces

In order to create a workplace for a WAY4 user, the user's account must be registered in the corresponding group (see the section "User Groups"). A predefined user role is assigned at the account level (administrator, operator or auditor), including data security administrator. Access privileges to a user menu group are granted at the user group level.

The distribution of access privileges by granting user groups access to certain menu groups is done in the following ways:

- For each user group, creating a user group menu specific to that group.

- Creating copies of or editing standard screen forms (see the document "Form Builder").

- Using static and dynamic filters in screen forms (see the section "Form Builder Window: the "Fields" Tab" section in the "Form Builder") and parallel preconfiguration of filter values (see the "Initialising Local Constants" section).

DB Manager Users and Groups Dialogue Window

User accounts are created, deleted and modified in a special dialogue window "DB Manager Users and Groups" (see Fig. 1) opened by selecting the "Full → DB Administrator Utilities → Users & Grants → User Groups and Users - Edit" menu item

Fig. 1. Dialogue window for administering user and user group access privileges

In the "Group Users" area, the list of the members of the user group selected in the "Groups" area is displayed.

⚠ No modifications of user accounts and user groups are saved in the database unless confirmed by clicking the [Save Changes], [Update Grants], [Update Grants for all], [Update All Users] or [Update User] buttons.

Any changes in the parameters of user accounts or groups are saved by sequentially clicking the [Reset Cached Info] and [Save Changes] buttons.

Any changes replacing or altering the last saved information may be cancelled before they are saved and the previous information retrieved from the database and restored by clicking the [Retrieve] button.

The following sections describe the fields and buttons of the "DB Manager Users and Groups" dialogue window (see Fig. 1).

User Group Parameters: "Groups" Area

- *ID* – unique group ID.

- *Name* – name of a group. This field may contain up to 50 symbols, including spaces.

- *Menu Tree* – field for selecting a root menu group for a certain user group.

- *Parent Group* – name of parent group.

  If a value is specified in this field, this is a child group. For child groups, the menu folder of their parent group is used (that is, the same privileges for database objects); however, other values of local constants can be specified for them.

  Child groups are in the first place necessary to cut the number of database roles.

  During administration, follow these rules:

  - After assigning a parent group to a group, update its access privileges (the [Update Grants] button). This will delete the group's own roles, if present. Also, update privileges of all users in the group (the [Update User] button).

  - After deleting a parent group, update access privileges of its child group. This will create its own roles for the group. Also, update privileges of all users in the group.

  - After modifying a menu folder, update access privileges of the parent group only.

- *Remote* – possibility of remote access to WAY4:

  - "Yes" users of this group may work with WAY4 from a remote workplace, using the WAY4 Remote Access client application (see the document "Working with WAY4™ Remote Access". These users may not work with WAY4 using DB Manager and their access privileges are restricted as compared with others. They may execute the SELECT SQL operator only from the tables they use in their work and they may not execute the UPDATE, INSERT and DELETE operators. However, they may start stored procedures that execute these operators for additional security checks.

  - "No" – users of this group can only work with WAY4 using DB Manager; they cannot work with WAY4 from a remote workplace.

  - "Web" – users of this group can only work with WAY4 using a thin client. In this case, Oracle database user accounts are not created and the [Add

Group], [Delete Group], [Add User], [Delete User] buttons will be active for groups and users.

- *Grants Updated* is the date of the latest "Update Grants" operation performed for a particular group.

Account Parameters: "Group Users" Area

- *User Id* – a unique user ID for connecting to the Oracle database. The value in this field must begin with a Latin letter and may contain digits, Latin letters and the underline character ("_"). If when creating a user account, invalid symbols are specified in this field, a window will be displayed with the message "User ID '<value>' is invalid. User ID should start with letter and contains only letters, digits or underscores".

- *Group* – drop-down list to select the group to which this user belongs. It is possible to change a user's user group by selecting a value in this field.

- *Name* – text field containing the name of a user, which may consist of up to 50 symbols including spaces.

- *Active* – marker indicating whether the user record is active: "Yes" – the record is active and the user can work with WAY4 using DB Manager, "No" – the user record is inactive the user cannot work with WAY4 using the client application.

- *Status* – drop-down list that indicates the type of a system user (see Table 1. in the section "Classification of WAY4 Users").

- *Special* – when this flag is set (the "Yes" value), a user will have access to the "Special" system menu item (see the section "Using the System menu" section of the document "DB Manager Administrator Manual").

- *Security* – when this flag is set (the "Yes" value), the user will be granted data security administrator privileges.

- *Usr Const* – drop-down list to specify how local constant values will be specified for this user:

  - "Group" – values set for groups to which this user belongs are used.

  - "Individual" – individual values of local constants are used.

- *Working Time* – field determining the time period in which a particular user is allowed access to the WAY4 database through DB Manager. This field must contain a string of 7 digits, either 1 or 0. The position of a digit corresponds to a day of the week, 1 meaning access allowed and 0 meaning access denied. The time of day period may also be indicated. It must be separated from the mandatory string with a semicolon ";". For example, "1111100;09:00-13:00;14:00-20:00" means that a user may work any day of the week except Saturday and Sunday, from 9:00 to 13:00 and from 14:00 to 20:00. If no time of day is indicated, the user may work with WAY4 at any time.

  Note that when a user account is created, the default value of this field is 0000000. This is why a period when access to the database is allowed should be indicated at the time an account is created.

Besides, in the *Working Time* field, either "W" or "H" may be indicated instead of a string of symbols. "W" means that the user may access the system only on business days, while "H" means that access is granted only on non-working days as defined in the business calendar (see the "Business Calendar" section in the WAY4™ Dictionaries Administrator Manual).

Buttons

The "DB Manager Users and Groups" dialogue window (see Fig. 1) contains the following buttons:

- [Close] – close the window

- [Retrieve] – replace the information entered in the fields with the values currently stored in the database

- [Save Changes] – save the changes in the database

- *Process Log* – when this flag is set, for each DB Manager user session a process will be generated that is registered in the Process Log (see the chapter "DB Manager Processes" of the document "DB Manager Manual"). Opening forms and calling procedures by the user will be registered as separate system messages accompanying an open process.

- [Add Group] – add a new user group

- [Delete Group] – remove the selected user group

- [Avail. For Web] – for the selected user group, set special properties for working with WAY4 Web. Clicking the button opens the "WEB properties for officer group <officer_group_name>" form (for more information, see the section "Properties for Working with WAY4 Web")

- [Unavail. For Web] – for the selected user group, disable special properties that were set for working with WAY4 Web

- [Update Grants] – renew the access privileges of the selected user group

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

- [Update Grants for all] – renew the access privileges of all user groups

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

- [Update All Users] – create Oracle database users and assign all the necessary access privileges to them

  ⓘ This is done only when copying WAY4 users' data to another database.

- [Reset Cached Info] – clear a DB Manager session's cached data on privileges required for access to database objects.

- [Add User] – add a new user

- [Delete User] – delete the specified user

- [Update User] – create and assign all the necessary access privileges to a new Oracle database user

     This is done only when copying WAY4 users' data to another database.

- [Lock User] – lock a WAY4 user account.

- [Unlock User] – unlock a WAY4 user account.

- [Lock DB User] – lock an Oracle user account.

- [Unlock DB User] – unlock an Oracle user account.

- [Delete DB User] – delete an Oracle user account.

- [Reset Password] – change user password.

 In order for functionality provided by the [Lock DB User], [Unlock DB User], [Delete 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".

Adding, Removing and Modifying User Groups

The actions described in this section are performed in the "DB Manager User and Groups" dialogue window (see Fig. 1 in the "DB Manager Users and Groups Dialogue Window" section hereof).

Adding User Group

To add a new user group, click the [Add Group] button in the "DB Manager User and Groups" dialogue window (see Fig. 1 in the "DB Manager Users and Groups Dialogue Window" section). A new record will appear in the "Groups" sub-window. In this window, the *Name* and *Menu Tree* fields must be filled in with appropriate values (see the "DB Manager Users and Groups Dialogue Window" section). After that is done, click the [Reset Cached Info] and [Save Changes] buttons.

This will result in the creation, in the database, of a role consisting of database access privileges necessary and sufficient to work with the menu group indicated in the *Menu Tree* field.

⚠ In certain cases, like when the indicated user menu contains, as menu items, pipes or stored procedures requiring additional database access privileges, such additional database access privileges must be granted so that such menu items may be used (see the "Granting Additional Privileges of Access to Database Menu Items" section hereof).

Modifying User Groups

WAY4 allows for modifying such parameters of newly created groups as *Name*, the assigned menu group – *Menu Tree* and the type of access to the system as determined by the *Remote* field, as well as the name of the parent group (*Parent Group* field).

The altered parameters of a group are saved by clicking the [Reset Cached Info] and [Save Changes] buttons.

Removing User Groups

A user group may be removed only if it contains no user accounts.

Groups are removed by clicking the [Delete Group] button.

Updating User Group Privileges

There is a number of operations when modifying a workplace that require access privileges to objects necessary for working with a user menu group to be updated for users belonging to this group. These operations are as follows:

- Adding new menu items to the menu group assigned to a user group

- Removing menu items from the assigned menu group

- Modifying screen forms accessible directly or indirectly, that is, through other forms, from the assigned menu group

- Modifying the configurations of the pipes accessible through a certain menu branch

After any of the above operations has been performed, the "Update Grants" operation must be performed for all the user groups whose menus have been affected by the changes. The access privileges of a single user group may be updated by clicking the [Update Grants] button. Clicking the [Update Grants for all] button will result in resetting the access privileges of all existing user 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.

⚠ If, during the current DB Manager user session, any manipulations of menus or forms altering the access privileges needed to work with these menu items or forms have been performed, then, before executing the "Update Grants"

operation, cash memory should be reset by clicking the [Reset Cached Info] button to remove the no longer actual grants info.

Properties for Working with WAY4 Web

The "WEB properties for officer group <officer_group_name>" form is used to set special properties for working with the WAY4 Web web application for a selected group (see Fig. 2).

The following fields are available in the form:

- *Start context* – code of the context that restricts the privileges of this group's users in WAY4 Web. The "[Root]" value indicates full access is granted for the selected user group.

- *Lock screen delay* – number of minutes after which the web client screen will be locked when a user from this group is inactive.

- *Pending session period* – length of a session when a user from this group is inactive (in minutes).

- *Max session period* – maximum session length for a user from this group (in minutes.

- *Audit mode* – when this checkbox is selected, the mode for auditing user actions is enabled.
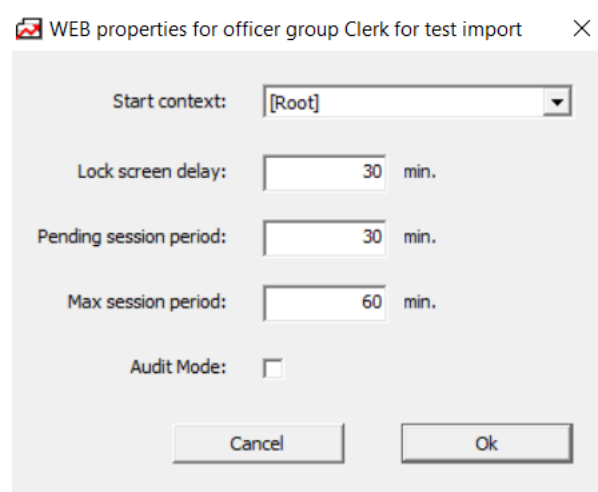
Fig. 2 Form to set special properties for working with WAY4 Web

Editing User Lists

The actions described in this section are performed in the "DB Manager User and Groups" dialogue window (see Fig. 1 in the "DB Manager Users and Groups Dialogue Window" section).

Creating a User Account

To create a new user account, select the group the new user will belong to – in the "Groups" sub-window of the "DB Manager User and Groups" dialogue window (see Fig. 1 in the "DB Manager Users and Groups Dialogue Window" section). This will result in appearing of the "Enter New user password" dialogue

window (see Fig. 3) containing fields for entering (*New User Password*) and verifying (*Reenter for Verification*) the passwords.
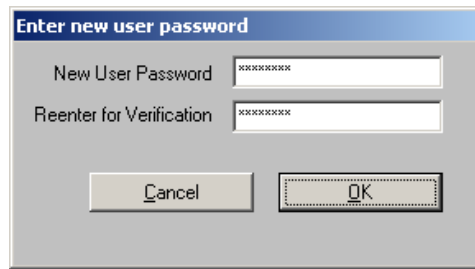

Fig. 3. Dialogue window for entering user passwords

⚠ It should be kept in mind that by default, a user password used to register a DB Manager session can also be used to access data in the Oracle database through an SQL editor. If necessary, this function can be switched off to prevent unauthorised access (see the section "Data Access Restriction through User Password Encryption").

When the [OK] button is clicked after the password has been entered and verified, a new user account with blank *User Id, Name* and *Usr Const* fields appears in the "Group Users" sub-window.

The *User Id* field is mandatory. The value in this field must begin with a Latin letter and may contain digits, Latin letters and the underline ("_") character. If invalid characters are specified in this field when creating a user account, a window will appear with the message "User ID '<value>' is invalid. User ID should start with letter and contains only letters, digits or underscores". The other fields may be filled in at a later time. For more information on field formats and functions, see the section "Account Parameters: "Group Users" Area" section.

According to WAY4 data security principles, each user may access the system within the hours set by the user's time parameters, which must be defined for every account in the *Working Time* field (see "Account Parameters: "Group Users" Area"). It is recommended that the time parameters be set at the time an account is created.

ⓘ It should be kept in mind that the value that appears in the *Working Time* field by default is "0000000", which means that the user has no access to the system at any time.

To complete the creation of a user account, click the [Reset Cached Info] and [Save Changes] buttons sequentially – to save the changes in the database.

This will result in the creation, in the database, of a <User Id>, which will be assigned a role according to the user group it belongs to.

After this, the user can connect to the database (during the permitted time period):

- With DB Manager if the user account's *Remote* field value is "No".

- With the WAY4 Remote Access, if the "Yes" value specified in the *Remote* field.

- With thin client (providing access to the database using Web services), if the "Web" value is specified in the *Remote* field.

Reconfiguring User Accounts

WAY4 allows altering any user account parameters with the exception of the unique User ID (the value of the *User Id* field).

After any parameters have been altered, the changes must be saved in the database by clicking the [Reset Cached Info] and [Save Changes] buttons sequentially.

Removing Users from List

To remove a user account, click the [Delete User] button, and then click the [Save Changes] button.

Note that it may take a considerable amount of time to delete a user account.

Locking a WAY4 User Account

To lock a WAY4 user account, in the "DB Manager Users and Groups" dialogue window (see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window"), select the account and click the [Lock User] button. As a result, a dialogue window will be displayed with the question "Do you really want to lock the user (<User Id>)?". To confirm locking the account, click [Yes]; to cancel, click [No].

After clicking [Yes], the user account will be locked, and the "No" value will be specified in the *Active* field of the "DB Manager User and Groups" window.

A specific user's account can be locked (unlocked) automatically (see the section "Locking Unused User Accounts").

Unlocking a WAY4 User Account

To unlock a WAY4 user account, in the "DB Manager User and Groups" dialogue window (see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window"), select the locked account and click the [Unlock User] button. As a result, a dialogue window will be displayed with the question "Do you really want to unlock the user (<User Id>)?". To confirm unlocking the account, click [Yes]; to cancel, click [No].

After clicking [Yes], the user account will be unlocked, and the "Yes" value will be specified in the *Active* field of the "DB Manager User and Groups" window.

Locking an Oracle Database User Account

Before locking an Oracle database user, lock this user's WAY4 account (see the section "Locking a WAY4 User Account") and click the [Save Changes] button. The value in the *Active* field will change to "Yes".

To lock the Oracle database user account, in the "DB Manager Users and Groups" dialogue window (see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window"), select a user with the "No" value in the *Active* field, and click the [Lock DB User] button. A dialogue window will be displayed with the question "Do you really want to lock DB user (<User Id>)?". To confirm locking the account, click [Yes]; to cancel, click [No]. After clicking [Yes], the user account will be blocked and a window with the message "DB User locked" will be displayed.

⚠ 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 Database User Account

ⓘ Before unlocking an Oracle database user, unlock this user's WAY4 account (see the section "Unlocking a WAY4 User Account") and click the [Save Changes] button. The value in the *Active* field will change to "Yes".

To unlock an Oracle database user account, in the "DB Manager Users and Groups" dialogue window (see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window"), select a locked user with the "Yes" value in the *Active* field, and click the [Unlock DB User] button. A dialogue window will be displayed with the question "Do you really want to unlock DB user (<User Id>)?". To confirm unlocking the account, click [Yes]; to cancel, click [No]. After clicking [Yes], the user account will be unlocked and a window with the message "DB User unlocked" will be displayed.

⚠ 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 Database User Account

ⓘ Before deleting an Oracle database user, lock this user's WAY4 account (see the section "Locking a WAY4 User Account") and click the [Save Changes] button. The value in the *Active* field will change to "No".

To delete an Oracle database user account, in the "DB Manager Users and Groups" dialogue window (see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window"), select a user with the "No" value in the *Active* field, and click the [Delete DB User] button. A dialogue window will be displayed with the question "Do you really want to delete DB user (<User Id>)?". To confirm deletion of the account, click [Yes]; to cancel, click [No]. After clicking [Yes], the user account will be deleted and a window with the message "User deleted" will be displayed.

⚠ 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 Passwords

In WAY4, user passwords are changed in the following ways.

- Using the "Database => Change Password" system menu item. This method described in the "'Database Item" section of the document "DB Manager Manual".

- Using the "DB Administrator Utilities → Users & Grants → Change Password" user menu item, which opens the "Change Password" dialogue window (see Fig. 4).
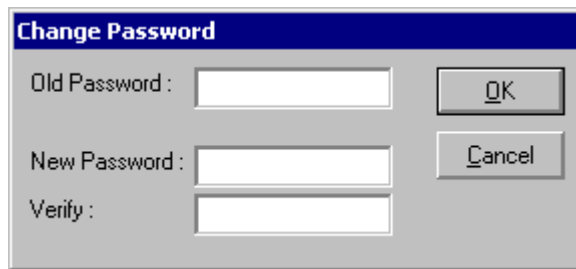
Fig. 4. Dialogue window for changing user passwords

This dialogue window has three fields:

▪ *Old Password*

▪ *New Password*

▪ *Verify* – reenter the new password.

After the appropriate values have been entered, click the [OK] button to change the password.

• In the "DB Manager User and Groups" dialogue window (see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window"). Select the user and click the [Reset Password] button. It is recommended to use this method if the user has forgotten his/her password.

As a result, a dialogue window will be displayed with the question "Do you really want to reset password (<User Id>)?". Clicking [Yes] opens the "Enter new user password" window (see Fig. 5).
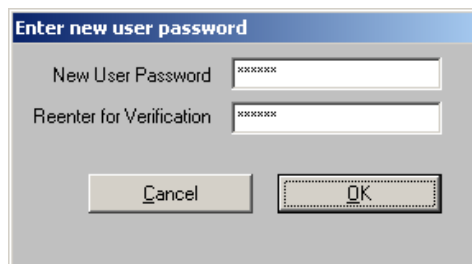
Fig. 5. Changing a user password

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

⚠️ For a password to be changed using the [Reset Password] button, the additional package "SYS.OWS_ADMINISTER_USER" must be installed in WAY4 (see the section "Buttons").

ℹ️ Note that according to DBMS Oracle security requirements, data security administrators cannot change existing users' passwords.

Granting Additional Privileges of Access to Database Menu Items
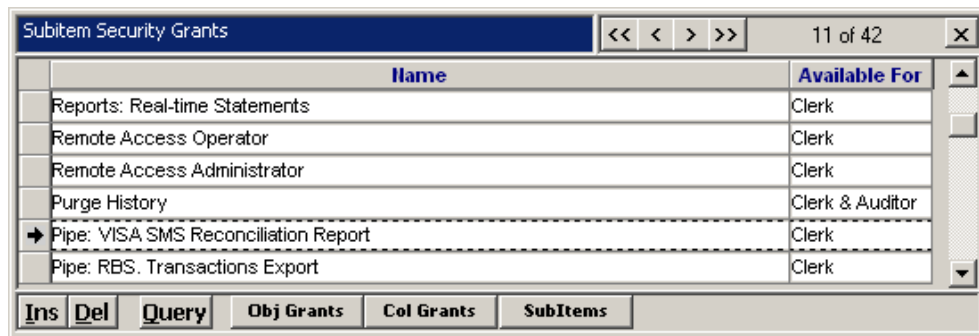
When pipes or stored procedures requiring additional database access privileges are present in the assigned menu group as user menu items, such additional privileges must be granted to the involved users.

Such privilege packages are granted for each individual menu definition sub-item (see the "Editing the User Menu" section in the Menu Editor Administrator Manual).

ⓘ While working with DB Manager, the editing of supplied standard menu items is prohibited. Only user-created menu items or copies of standard menu items may be edited (see the document "Menu Editor").

Configuring Privilege Packages

Privilege packages are viewed, deleted, updated, or created through the " Full → DB Administrator Utilities → Users & Grants → Subitem Security Grants" menu item. When this item is selected, the "Subitem Security Grants" form comes up on the screen (see Fig. 6).

Fig. 6. Form for configuring additional access privilege packages for accessing menu sub-items.

The privileges of access to database objects such as stored procedure packages, or tables are configured with the use of "Obj Grants for <name of package of access privileges>" form (see Fig. 7). The form is brought to the screen by clicking the [Obj Grants] button. There are two columns in the form. In the left column (*Object Name*), the name of a database object must be specified. The access privileges for the selected object are selected in the column on the right (*Grant*). They are as follows:

- "UPDATE" – the privilege to modify records.
- "INSERT" – the privilege to add records
- "DELETE" – the privilege to delete records
- "EXECUTE" – the privilege to execute procedures
- "SELECT" – the privilege to execute the SELECT operator

ⓘ In the example shown in Fig. 7, the package consists of access privileges to three objects: two stored procedure packages and one database table.

Fig. 7. Form for configuring access privileges to database objects

The system allows granting privileges for certain columns instead of for the whole table. This is done in the "Col Grants for <the name of a privilege package>" form (see Fig. 8). This form is opened by clicking the [Col Grants] button in the "Subitem Security Grants" form (see Fig. 6).

Fig. 8. Form for configuring access privileges for individual columns of a database table

There are two columns in this form:

- *Table* – containing the name of a database table

- *Column* – containing the name of a column in that table

If there is even just one entry in the "Col Grants for <name of privilege package>" form, the privileges granted in the "Obj Grants for <name of package of access privileges>" form (see Fig. 7) will be good only for the indicated column or columns.

The list of menu sub-items associated with a configured access privilege package is reviewed by clicking the [SubItems] button, which brings up the "SubItems for <name of privilege package>" form (see Fig. 9).

Fig. 9. List of menu sub-items associated with a privilege package

Granting Additional Privilege Packages for Menu Items

Additional privilege packages for menu items are granted in the Form Editor window (see the "Menu Editor Window" section in the Menu Editor Administrator Manual).

A package of additional access privileges is selected from the list opening in the *Security* field for a sub-item definition (see Fig. 10). For more details, please refer to the Menu Editor Administrator Manual section.
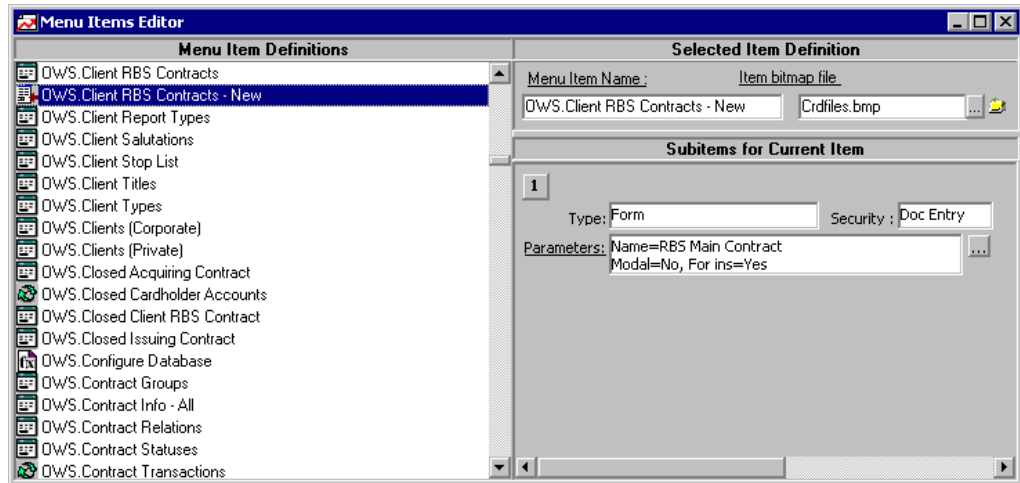
Fig. 10. Example of granting an additional privilege package for a menu sub-item

Initialising Local Constants

Local constants are used to filter data available while working with DB Manager forms (see the "Form Builder Window: the "Fields" Tab" section in the Form Builder Administrator Manual).

Local constants are initialised when a user session is registered. Depending on the value of the *Usr Const* field of the "DB Manager Users and Groups" form (see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window", either group or individual values of local constants will be used.

Values for initialising local constants initialisation are assigned in the following forms:

* Group local constants – the "Constants for <user group name>" form (see Fig. 11). It is accessed by clicking the [Constants] button in the "User Groups and Users – View" form ("Full → DB Administrator Utilities → Users & Grants → User Groups and Users - View").

Fig. 11. Assigning values for local constants initialisation to a user group

This form contains the following fields:

▪ *Institution* – name of financial institution.

- ▪ *Branch* – financial institution branch.

- ▪ *Product Category* – Product type.

- ▪ *Client Category* – client category.

- ▪ *Client Type* – client type.

- ▪ *Service Group* – additional client classification.

- ▪ *Security Level* – access level; this value is used to filter command types sent to an ATM from the console that must be available to the user.

- ▪ *Product Group* – product group; this field value is used by the Advanced Applications R2 module.

- ▪ *Workflow Stage* – registered type of application processing stage; this field value is used by the Advanced Applications R2 module.

- ▪ *Language* – language used in reports that can be generated in a national language.

- ▪ *Tagged Data* – system field for storing and setting tags used to filter data. Tags in the field are set in the format "<Tag_Name>=<Value>;", where <Tag_Name> is the tag name and <Value> is the tag value(s).

- • Individual local constants – the "Constants for <user name>" form. This form is opened by clicking the [Constants] button in the "Users for <user group name>" form that is opened by clicking the [Users] button in the "User Groups and Users – View" form (Full → DB Administrator Utilities → Users & Grants → User Groups and Users - View).

  The forms of this field are identical to the fields of the "Constants for <user group name>" form (see Fig. 11).

After initialisation, local constants may be redefined through special modal forms (e.g. "Set Client Type" – see the "Clients and Contracts" section in the Issuing Module User Manual) and menu item definition sub-items of the "Assignment" type (see the "Assignment Type" section in the Menu Editor" Administrator Manual).

Chapter 3. Logging

This section describes the principles of logging changes made in records by WAY4 users while working in the system and the principles of logging system user registrations.

Process Logging

In WAY4, instances of process execution are entered in the Process Log. Registered for each process are starting parameters, the current banking date, the user who starts the process, the start and completion dates and times and, if a process is terminated forcibly, the name of the user who terminates it.

For more details on process logging, please refer to the "DB Manager Processes" section chapter in the DB Manager Administrator Manual.

Logging Changes in Grid Form Records

Any change made by a user in any editable field of a WAY4 grid form is registered in the History Log. Information as to the history of changes remains available for every record whatever the grid form.

Access to the History Log concerning a specific record is gained through the "Special => View History" system menu item.

When this menu item is selected, "<name of table form> - history of …" additional form will open (see Fig. 12).

Fig. 12. Example of the history of changes in a record

The additional form contains a list of the versions of the selected record, and information about change dates and the user who made the change.

Restoring Removed Records

The deleted records of a table form may be viewed by selecting the "Special =>
Deleted" system menu item (see Fig. 13).

Fig. 13. Example of viewing deleted records

Deleted records are restored by first selecting a record on the list and then
clicking the [Undelete] button.

User Login History

When a WAY4 user establishes connection with the database, a record to that
effect is created in the Login History log. The record includes the name of the
workstation the user used for connecting to the database and the date and time
of connection. After the user closes the connection, the closing date and time are
added to the record.

Access to the Login History log is gained through the "Full → DB Administrator
Utilities → Users & Grants → Login History" user menu item. This item opens
the "Login History" form (see Fig. 14).

Fig. 14. Example of the WAY4 Login History log

When several process are executed during one session (starting pipes, deleting
records, processing documents, etc.), several records are created in the "Login
History" table. Information about these records is accessible in the "Processes
for <…>" form (see Fig. 15) opened by clicking the [Processes] button in the
"Login History" form.

Fig. 15. Processes started during one session

Clicking the [Aux for] button in the "Login History" form opens the "Aux for
<…> form (see Fig. 16).

Fig. 16. Auxiliary processes

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

In WAY4, the Login History log and/or the history of changes are purged automatically by the WAY4 Housekeeping module (see the document "WAY4™ Housekeeping").

Locking Unused User Accounts

According to PA-DSS, user accounts that have not logged in the system for a long period of time (over 90 days) must be locked. Moreover, in WAY4 it is possible to temporarily lock user accounts.

The list of registered WAY4 users is accessible in the "Officers" form (see Fig. 17) opened by selecting the menu item "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Officers".

Fig. 17. List of registered WAY4 users

In the *Inactive From* and *Inactive To* fields, the interval during which the user account will be locked can be specified.

To lock user accounts, use the "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Lock Inactive Officers" menu item. Selecting this menu item executes a stored procedure that checks the last login date of all registered users and, if it is more than the allowed number of days ago, revokes all database object access privileges and sets the *Is Active* field to "No".

The *Last Login Time* field is used to register the time and date of the last system login.

To specify the number of days after the last login when a user account must be locked, use the "OFFICER_MAX_INACTIVITY_DAYS" global parameter. This parameter is specified in the "Additional Global Parameters" form (Full → Configuration Setup → Main Tables → Additional Global Parameters). The default parameter value is "90" according to PA-DSS.

To automatically execute the "Lock Inactive Officers" menu item every day, use the process started through the "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Start Inactive Officers Monitor" menu item. The process execution is logged in the process log. To stop the process, select the

"Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Stop Inactive Officers Monitor" menu item.

In WAY4 it is possible to lock (unlock) the account of a specifc user. To do so, in the "Officers" form (see Fig. 17), 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 for whom the value "1" is specified in the *ID* field of the "DB Manager Users and Groups" form (see Fig. 1 in the section "DB Manager Users and Groups Dialogue Window") cannot be locked, either.

Chapter 4. Privileges of Access to WAY4 Directories

This chapter describes standard WAY4 directories and the privileges of access to these directories assigned to various system users.

Standard WAY4 Directories

The following standard directories exist in WAY4:

- <OWS_HOME> is the principal directory of the system. It contains the standard subdirectory and file structure, which is the same for all the basic directories that belong to the same version of the system. The structure of this directory must never be altered. It must be always located on the file server of the WAY4 system.

  The contents of the<OWS_HOME> directory may be altered only while the system is being upgraded.

- <OWS_WORK> is a system directory whose structure is partially analogous to that of the <OWS_HOME> directory. It contains various configuration files, data files specific to the particular WAY4 configuration, files containing user-created screen forms, menu items, and reports, etc. It is recommended that this directory be located on the file server of the WAY4 system.

- <OWS_TEMP> is a directory used to store temporary files created by the DB Manager application and Error Log files (see the "Temporary Files Directory" section in the DB Manager Administrator Manual). This directory should be present on WAY4 workstations.

The <OWS_HOME> and <OWS_WORK> directories are accessible to all WAY4 users and must be located on the file server of the WAY4 system.

The <OWS_TEMP> directory must be present on each workstation used to access WAY4.

Privileges of Access to Standard WAY4 Directories

When the DB Manager application is installed on the WAY4 file server, every system user must be granted access privileges allowing them to read the files located in the <OWS_HOME> principal system directory and the <OWS_WORK> work directory.

All system users must have full privileges of access to the <OWS_TEMP> temporary files directory.

Depending on their functions, system users fall into classes, each granted its own package of privileges of access to WAY4 directories and subdirectories (see Table 2).

Table 2. Access privileges granted to WAY4 users depending on the classes they belong to

User Class	Functions	Directory

Administrators	Upgrading WAY4	<OWS_HOME>, <OWS_WORK>
	Creating and editing screen forms	<OWS_WORK>\Client\Shared
Operators	Issuing cards	<OWS_WORK>\Data\Card_Prd
	Effecting interaction with international payment systems	<OWS_WORK>\Data\Interchange
	Effecting interaction with the RBS	<OWS_WORK>\Data\RBS
	Generation of reports	<OWS_WORK>\Data\Reports
	Housekeeping	<OWS_WORK>\Data\Archive

Appendix 1. Data Access Restriction through User Password Encryption

By default, a user password used to register a DB Manager session can also be used to access data in the database through an SQL editor or using another client application.

If necessary, data in the database can be accessed through a password created by encrypting a DB Manager login password with an encryption value (key). In this case, the database can only be accessed through DB Manager as access to the database requires using not the password entered by the user when starting DB Manager but an encrypted value unknown to the user.

A password encryption key can be specified in one of two ways:

- Through the "PWD_ENCRYPTION" parameter in the [Client.DBM.Params] section of the "db.ini" file located in the <OWS_WORK> directory

- Through the "PWD_ENCRYPTION" parameter in the "Local Machine Parameters" window used to configure workstation parameters (see the section "Database" Item" in the document "DB Manager Manual").

In both cases, values of this parameter are specified in the following format:

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

In encryption key bodies, ASCII characters with codes ranging between 33 and 127 may be used. Keys may be up to 256 characters long.

It should be kept in mind that the database access password is not encrypted if no encryption key value is specified (or an empty line is specified).

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. 18).
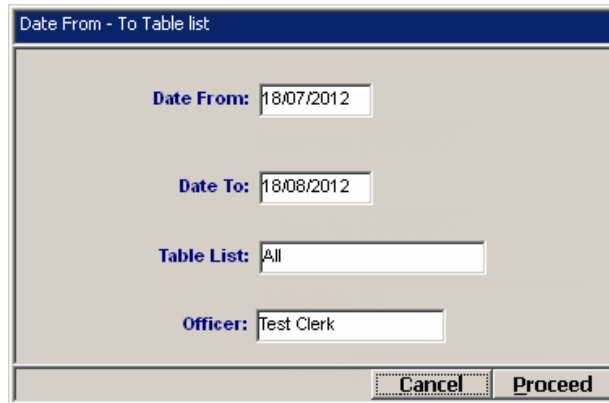

Fig. 18. Setting report parameters

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.