Operation Manual

DB Manager User Management

03.52.30

23.07.2021

Contents

1 Way4 users 5

1.1 Classification of Way4 users 5

1.2 User groups 6

2 Creating user workplaces 8

2.1 Window for working with user records 8

2.1.1 User group parameters ("Groups" area) 9

2.1.2 User account parameters ("Group Users" area) 10

2.1.3 Buttons 11

2.2 Adding, deleting and editing user groups 13

2.2.1 Adding a new user group 13

2.2.2 Modifying user groups 13

2.2.3 Deleting a user group 13

2.2.4 Updating user group privileges 13

2.2.5 Properties for working with Way4 Web 14

2.3 Editing the user list 15

2.3.1 Creating a user account 15

2.3.2 Changing user account parameters 16

2.3.3 Deleting a user from the list 16

2.3.4 Locking a Way4 user account 17

2.3.5 Unlocking a Way4 user account 17

2.3.6 Locking an Oracle DB user account 17

2.3.7 Unlocking an Oracle DB user account 17

2.3.8 Deleting an Oracle DB user account 18

2.3.9 Changing user passwords 18

2.4 Configuring additional privileges for DB objects for menu items 19

2.4.1 Configuring privilege packages 19

2.5 Initializing local constants 22

3 Logging 24

3.1 Process logging 24

3.2 Logging changes made in grid forms 24

3.3 Restoring deleted records 25
3.4 User login history 25
3.5 Locking inactive accounts 26
4 Privileges for Way4 directories 28
4.1 Standard Way4 directories 28
4.2 Privileges for standard Way4 directories 28
5 Limiting data access with user password encryption 30
6 Amendment Report 31

This manual covers the key concepts of administering Way4 users with DB Manager.

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

- "DB Manager Manual"
- "DB Manager. Menu Editor"
- "DB Manager. Form Builder"
- "WAY4™ PA-DSS Implementation Guide".

The following notation is used in the manual:

- Screen form field labels are shown in *italics*.
- Screen form button labels are shown in square brackets, such as [Approve].
- Sequences for selecting user 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".
- Key combinations in DB Manager are shown in angular brackets, for example <Ctrl>+<F3>.
- Variables that differ for each local instance, for example, directory and file names, as well as file paths, are shown in angular brackets; for example, <OWS_HOME>.

Warnings and information messages are indicated as follows:

⚠ Warnings about potentially hazardous situations or actions.

ⓘ 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.

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, Super 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 security administrator – "OWS_A";
- NetServer user– "OWS_N".

Administrators, operators and auditors (hereinafter referred to as Way4 users, to differentiate from administrative users) work with DB data using the DB Manager application (see the document "DB Manager Manual").

The schema owner (Owner) is the owner of all table and views (except custom views) and procedures. After system installation (execution of a procedure to switch to multi-user mode), access to the system via DB Manager is automatically denied for the schema owner.

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). The main function of a user with security administrator privileges is the creation of other Way4 users.

For the Super Security Administrator, Security Administrator, and Way4 system administrator to be able to work with objects from a granted user menu group in addition to their main functions of creating users and groups, forms, pipes, etc., their privileges must be updated ([Update User] button in the "DB Manager Users and Groups" window, see the section "Window for working with user records").

1.2 User groups

To facilitate administration, Way4 users are grouped. Each user group is provided with a user menu group (see the section "User menu" of the document "DB 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") a role is automatically created for each user group in the

DB. This role includes DB access privileges necessary and sufficient for working with this user menu group. The role is granted to users in the group.

2 Creating user workplaces

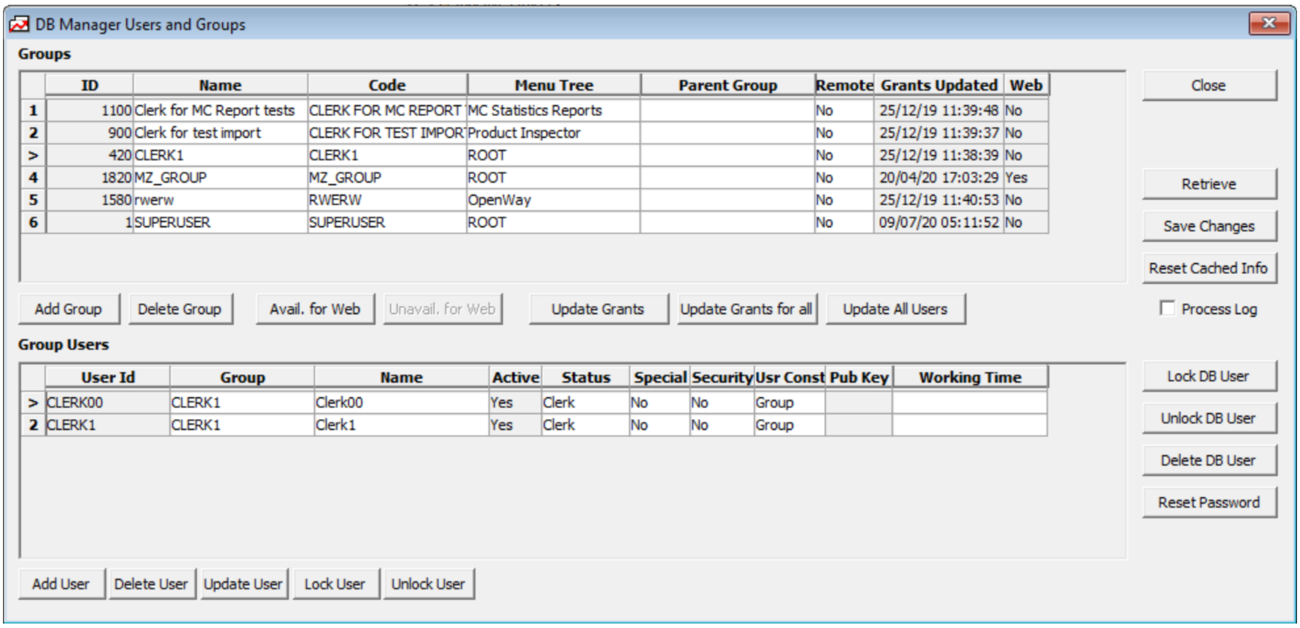
To create a Way4 user workplace, register a user account for the user in the appropriate group (see"User groups"). A predefined role (administrator, operator or auditor) is assigned at the user account level, and the security administrator administrator role can also be assigned. Access privileges for a user menu group are granted at the group level.

Distribution of access through the assignment of different user menu groups is performed using the following mechanisms:

- For each user group, creation of its own group-specific user menu group.
- Creating and editing copies of standard screen forms (see the document "DB Manager. Form Builder").
- Use of static and dynamic filters in screen forms (see the section "Form Editor window. "Fields" tab of the document "Form Editor") and definition of filter values (see the section "Initializing local constants").

2.1 Window for working with user records

User accounts are managed in the "DB Manager Users and Groups" dialog window, opened by selecting the menu item "Full → DB Administrator Utilities → Users & Grants → User Groups and Users – Edit".



Groups

	ID	Name	Code	Menu Tree	Parent Group	Remote	Grants Updated	Web
1	1100	Clerk for MC Report tests	CLERK FOR MC REPORT	MC Statistics Reports		No	25/12/19 11:39:48	No
2	900	Clerk for test import	CLERK FOR TEST IMPOR	Product Inspector		No	25/12/19 11:39:37	No
>	420	CLERK1	CLERK1	ROOT		No	25/12/19 11:38:39	No
4	1820	MZ_GROUP	MZ_GROUP	ROOT		No	20/04/20 17:03:29	Yes
5	1580	rwerw	RWERW	OpenWay		No	25/12/19 11:40:53	No
6	1	SUPERUSER	SUPERUSER	ROOT		No	09/07/20 05:11:52	No

Group Users

	User Id	Group	Name	Active	Status	Special	Security	Usr Const	Pub Key	Working Time
>	CLERK00	CLERK1	Clerk00	Yes	Clerk	No	No	Group		
2	CLERK1	CLERK1	Clerk1	Yes	Clerk	No	No	Group		

Window for managing access grants for users and user groups

The "Group Users" area shows the list of users for the group selected in the "Groups" area.

⚠ Any changes to user accounts and user groups that have not been confirmed by clicking [Save Changes], [Update Grants], [Update Grants for all], [Update All Users] or [Update User] will not be saved in the DB.

Any changes to the parameters of user accounts and groups are saved by successively clicking [Reset Cached Info] and [Save Changes]

Any changes made after the last time information was saved to the DB can be cancelled by restoring the information from the database. To do this, click [Retrieve].

The following subsections describe fields and control buttons in the "DB Manager Users and Groups" window.

2.1.1 User group parameters ("Groups" area)

- *ID* – group's unique identifier.
- *Name* – group name. This field can contain up to 50 characters, including spaces.
- Code – unique group code.
- *Menu Tree* – drop-down list for selecting the user group's root menu group.
- *Parent Group* – name of the parent group.
  If a value is specified in the field, this is a child group. The parent group's menu branch is used for child groups (the same privileges for DB objects), but for child groups, different values can specified local constants.
  Child groups are needed primarily to reduce the number of DB roles.
  The following rules should be followed when administering:

- After a parent group has been assigned to a group, access privileges must be updated ([Update Grants] button), and the child group's own roles, if any, will be deleted. It is also necessary to update privileges for all this group's users ([Update User] button).
- When a parent group is deleted, access privileges for the child group must be updated and its own roles will be created for it. It is also necessary to update privileges for all this group's users.
- After changes have been made to a menu branch, update access privileges for the parent group only.

- *Remote* – the ability to access Way4 remotely:

- "Yes" – the group's users can work with Way4 from a remote workstation, using the Way4 Remote Access application (see the document "Working with Way4™ Remote Access"). These users can't use DB Manager to work with the system and have more limited privileges than other users. Specifically, these users have the privilege to execute the SQL SELECT statement only from tables required for work, do not have privileges to execute the SQL UPDATE, INSERT, DELETE statements, but have the privilege to run special stored procedures that perform these operations with an additional security check.
- "No" – this group's users can't work with Way4 from a remote workstation. Work is only possible using DB Manager.

- "Web" – this group's users can only work with the system using Way4 Web. In this case Oracle DB user accounts are not created, and the [Add Group], [Delete Group], [Add User], [Delete User] buttons will be active for the group and users.

- *Grants Updated* – date of the last "Update Grants" activity for the group.
- *Web* – indicates whether the user group has access privileges for the Way4 Web application. Privileges can be granted by clicking [Avail. for Web].

2.1.2 User account parameters ("Group Users" area)

- *User Id* – unique identifier of the user for the connection with the Oracle DB. The value in this field must begin with a Latin letter and can contain digits, Latin letters and the underline character ("_"). If invalid characters are specified when creating the user account, the following message will be displayed: "User ID '<value>' is invalid. User ID should start with letter and contains only letters, digits or underscores".
- *Group* – drop-down list to specify the group to which the user belongs. The user's group can be changed by selecting a value in this field.
- *Name* – text field for specifying the user name; this field can contain up to 50 characters, including spaces.
- *Active* – indicates whether the user account is active; "Yes" – the account is active and the user can use DB manager to work with the system, "No" – the account is inactive (the user cannot use the client application to work with the system).
- *Status* – drop-down list to select the system user type (see the table in the section "Classification of Way4 users").
- *Special* – when set to "Yes", the user will have access to the "Special" system menu item (see the section "Using the System Menu" of the document "DB Manager Manual").
- *Security* – when set to "Yes", this user will have security administrator privileges.
- *Usr Const* – list to select the method for defining the values of local constants for this user:

- "Group" –use values that are set for the group to which this user belongs.
- "Individual" – use individual values for local constants.

- *Working Time* – time interval during which the user is allowed to access Way4 using DB Manager. This field must contain a string of 7 digits that are either "0" or "1", where the position of the digit indicates the day of the week (starting with Monday), and the value – whether the user is permitted to work with the system ("0" – prohibited", "1" – permitted). In addition, a time interval can be specified separating it from the mandatory string with a semicolon (";"). For example "1111100;09:00-13:00;14:00-20:00" means that the user can work any day of the week, except Saturday and Sunday, from 9:00-13:00 and from 14:00-20:00. If the user's working time is not specified, they can work with the system at any time.

ⓘ 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.

Instead of a character string, a "W" or "H" can be specified in the *Working Time* field. The "W" character indicates that this user can access the system only on days defined by the business calendar as working days (see the section "Business Calendar" of the document "Way4 Dictionaries"). The "H" character indicates that access is only possible on non-working days.

2.1.3 Buttons

The "DB Manager Users and Groups" dialog window contains the following buttons:

- [Close] – close the window.
- [Retrieve] – update information in the dialog window's fields by selecting current values from the DB.
- [Save Changes] – save changes to the DB.
- *Process Log* – when this checkbox is checked, a process that is recorded in the Process Log will be created for each DB Manager user session (see the section "DB Manager processes" of the document "DB Manager Manual"). Forms opened and procedures called by the user will be registered as separate system messages accompanying the open process.
- [Add Group] – add a new user group
- [Delete Group] – delete a selected user group
- [Avail. for Web] – set special properties for the selected user group to work with Way4 Web. Clicking the button opens the "WEB properties for officer group <officer_group_name>" form (for more information, see the section "Adding, deleting and editing user groups").
- [Unavail. for Web] – disable special properties for the selected group to work with Way4 Web.
- [Update Grants] – update access privileges for the selected user group.

  ⚠ For restrictions on performing this activity, see the section "Adding, deleting and editing user groups".

- [Update Grants for all] – update access privileges for all user groups.

  ⚠ For restrictions on performing this activity, see the section "Adding, deleting and editing user groups".

- [Reset Cached Info] – clear information about privileges required for access to DB objects from the DB Manager session cache.
- [Add User] – add a new user
- [Delete User] – delete the user

- [Update User] – create an Oracle DB user and grant them the necessary privileges for DB objects.

  > ⓘ This activity is only performed when copying a Way4 user's data to another DB.

  When creating a used for access to database objects through DB Manager, the following actions are performed in the system:

  - A record is deleted from the TD_CONS table if the user previously had access to Way4 Web, but the record wasn't deleted when "No" was set for the "Web" field.
  - The user is granted the appropriate Oracle roles.
  - The time of creation and user are set if data is absent (must be filled in when creating a user).

  When creating a user for access to database objects through DB Manager and Way4 Web, the following actions are performed in the system:

  - A record in the TD_CONS table and an authentication scheme are created, if access to Way4 Web is granted to a user group but they were not created, when "Yes" is set for the "Web" field.
  - The user is granted the appropriate Oracle roles.
  - The time of creation and user are set if data is absent (must be filled in when creating a user).

  When creating a user for access to database objects through Way4 Web, the following actions are performed in the system:

  - A record in the TD_CONS table and an authentication scheme are created, if they don't exist.
  - The time of creation and user are set if data is absent (must be filled in when creating a user).
- [Lock User] – lock a Way4 user account.
- [Unlock User] -unlock a Way4 user account.
- [Lock DB User] – lock the Oracle DB user account.
- [Unlock DB User] – unlock the Oracle DB user account.
- [Delete DB User] – delete the Oracle DB user account.
- [Reset Password] – change user password.

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, 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".

2.2 Adding, deleting and editing user groups

The actions described in this section are performed in the "DB Manager User and Groups" dialog window (see the section "Window for working with user records").

2.2.1 Adding a new user group

To add a new group, click [Add Group] in the "DB Manager User and Groups" window (see the section "Window for working with user records"). A new record will appear in the "Groups" window. In this window, fill in the *Name* and *Menu Tree* fields with the appropriate values and click [Reset Cached Info] and [Save Changes].

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 Tree* 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

Way4 allows editing group parameters such as group name (*Name* field), assigned menu group (*Menu Tree*field), system access type (*Remote* field), and parent group name (*Parent Group* field).

To save changes to a group's parameters, click [Reset Cached Info] and [Save Changes].

2.2.3 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 [Delete Group].

2.2.4 Updating user group privileges

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

- Modification of pipe parameters available from the menu branch.

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. Clicking [Update Grants for all] performs the "Update Grants" activity for all existing groups.

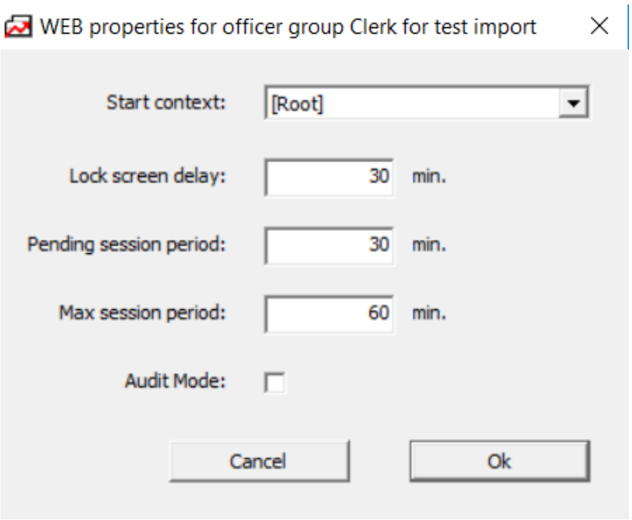
> ⚠ It is not recommended to update access privileges for all user groups (the [Update Grants] and [Update Grants for all] buttons) when there is a high load on the Oracle database server, such as when receiving and sending a large number of transaction messages online and or/running lengthy resource-intensive 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.
>
> If during the current DB Manager user session actions with menus or forms were performed that led to changes in privileges required to work with these menu items or forms, before the "Update Grants" activity, it is recommended to click [Reset Cached Info] to clear obsolete privileges cached in DB Manager.

2.2.5 Properties for working with Way4 Web

The "WEB properties for officer group <officer_group_name>" form is used to set special properties for a user group to work with Way4 Web.

The form contains the following fields:

- *Start context* – code of the context limiting the privileges of this group's users in Way4 Web. The "[Root]" value means that the selected user group is granted full access.
- *Lock screen delay* – number of minutes after which the web client screen will be blocked if a user from this group is inactive.
- *Pending session period* – session length 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 checked, user actions are audited.



WEB properties for officer group Clerk for test import

Start context: [Root]

Lock screen delay: 30 min.

Pending session period: 30 min.

Max session period: 60 min.

Audit Mode: □

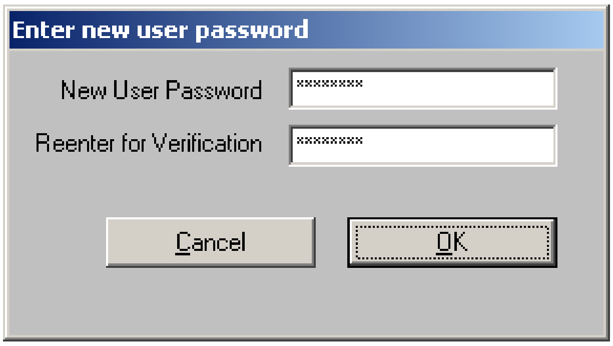
Form for setting special properties for working with Way4 Web

2.3 Editing the user list

The actions described in this section are performed in the "DB Manager User and Groups" dialog window (see the section "Window for working with user records").

2.3.1 Creating a user account

To create a new user account, in the "Groups" window of the "DB Manager User and Groups" dialog window, select the group to which the user will belong and click [Add User]. The "Enter New user password" dialog window will open with fields for entering the user's password (*New User Password*) and confirming it (*Reenter for Verification*).



Enter new user password

New User Password: *********

Reenter for Verification: *********

Dialog window for entering a user's password

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

When [OK] is clicked after entering the password and confirming it in the "Group Users" window, a new record will appear with empty *User Id*, *Name* and *Usr Const* fields.

The *User Id* field is mandatory. The value in this field must begin with a Latin letter and can contain digits, Latin letters and the underline character ("_"). If invalid characters are specified when creating the user account, the following message will be displayed: "User ID '<value>' is invalid. User ID should start with letter and contains only letters, digits or underscores". The other fields can be filled in later. For more information about the format and purpose of fields, see the section "Window for working with user records".

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. 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, sequentially click [Reset Cached Info] and [Save Changes] to save the changes to the DB.

An account for <User Id> will be created in the DB and will be assigned a role corresponding to the user group.

After this, the user will be able to connect to the DB (within the time interval allowed for work):

- With DB Manager if the user account's *Remote* field value is "No".
- With Way4 Remote Access if the *Remote* field value is "Yes".
- With Way4 Web (providing DB access using web services), if "Web" is specified in the *Remote* field.

2.3.2 Changing user account parameters

Any user account parameters can be edited, with the exception of the account's unique identifier (*User Id* field value).

To save changes to user account parameters, sequentially click [Reset Cached Info] and [Save Changes].

When the [Save Changes] command is executed, the following error may occur: "User IDs duplicated. Group: <user_group>, user id: <user_id>, group: <user_group>, user id: <user_id>".

2.3.3 Deleting a user from the list

To delete a user account, click [Delete User] and then [Save Changes].

> ⓘ Note that it may take a considerable amount of time to delete a user record.

2.3.4 Locking a Way4 user account

To lock a Way4 user account, select the user in the DB Manager Users and Groups" window and click [Lock User]. A confirmation window will be displayed with the prompt "Do you really want to lock the user (<User Id>)?". To unlock the user account, click [Yes]; to cancel, click [No].

After [Yes] has been clicked, the user account will be locked and "No" 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 inactive accounts").

2.3.5 Unlocking a Way4 user account

To unlock a Way4 user account, select the locked account in the "DB Manager User and Groups" window and click [Unlock User]. A confirmation window will be displayed with the prompt "Do you really want to unlock the user (<User Id>)?". To confirm, click [Yes]; to cancel, click [No].

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

2.3.6 Locking an Oracle DB user account

Before locking an Oracle DB user, lock the this user's Way4 account and click [Save Changes]. The value in the *Active* field will change to "No".

To lock an Oracle DB user account, in the "DB Manager User and Groups" window select a user with "No" in the *Active* field and click [Lock DB User]. A confirmation window will be displayed with the prompt "Do you really want to lock DB user (<User Id>)?". To confirm, click [Yes]; to cancel, click [No]. After clicking [Yes] the user account will be locked and a window with the message "DB User locked" will be displayed.

> ⚠ To be able to lock Oracle database users, the additional package "SYS.OWS_ADMINISTER_USER" must be installed in WAY4.

2.3.7 Unlocking an Oracle DB user account

Before unlocking an Oracle DB user, unlock this user's Way4 account and click [Save Changes]. The value in the *Active* field will change to "Yes".

To unlock an Oracle DB user account, in the "DB Manager User and Groups" window select a locked user with "Yes" in the *Active* field and click [Unlock DB User]. A confirmation window will be displayed with the prompt "Do you really want to unlock DB user (<User Id>)?". To unlock the user 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.

⚠ To be able to unlock Oracle database users, the additional package "SYS.OWS_ADMINISTER_USER" must be installed in WAY4.

2.3.8 Deleting an Oracle DB user account

Before deleting an Oracle DB user, lock the this user's Way4 account and click [Save Changes]. The value in the *Active* field will change to "No".

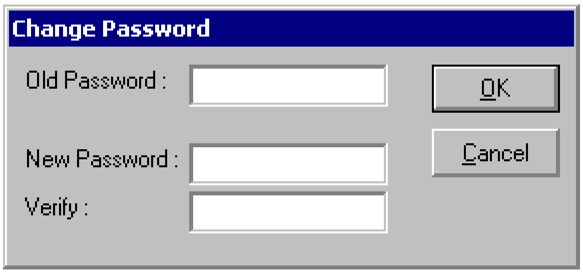
To delete an Oracle DB user account, in the "DB Manager User and Groups" window select a user with "No" in the *Active* field and click [Delete DB User]. A confirmation window will be displayed with the prompt "Do you really want to delete DB user (<User Id>)?". To confirm deletion of the account, click [Yes]; to cancel, click [No]. After clicking [Yes] the user account will be deleted and a window 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.

2.3.9 Changing user passwords

There are several ways to change a user's system access password in Way4:

- With the system menu item "Database => Change Password". This method is described in the section "Database Item" of the document "DB Manager Manual".
- With the user menu item "Full → DB Administrator Utilities → Users & Grants → Change Password". As a result, the "Change Password" window will open.

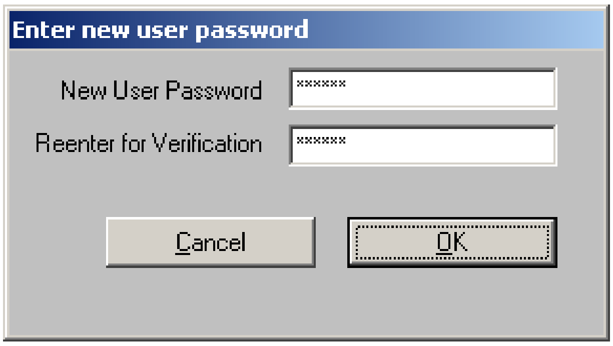


Window for entering a user's password

This window has three input fields:

- *Old Password*
- *New Password*
- *Verify* – reenter the new password. This value must match the value in the *New Password* field.

  After the appropriate values have been entered, click [OK] to change the password.
- In the "DB Manager User and Groups" window. Select the user and click [Reset Password]. This method is recommended if the user has forgotten their old password.
  A confirmation window will be displayed with the prompt "Do you really want to reset password (<User Id>)?". Click [Yes] to open the "Enter new user password" window.



Enter new user password

New User Password: ******

Reenter for Verification: ******

Changing a user's password

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

> ⚠ To use the [Reset Password] to change a password, the additional package "SYS.OWS_ADMINISTER_USER" must be installed in WAY4.

> ⓘ 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

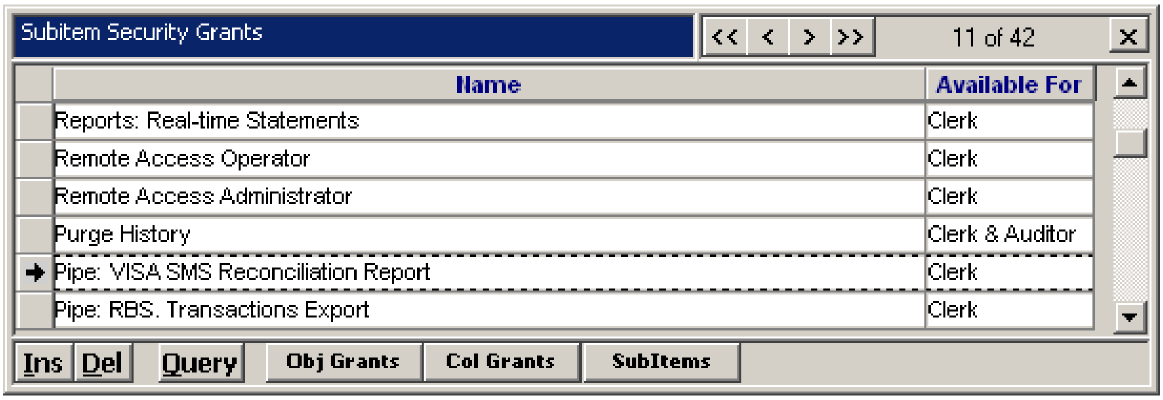
In some cases, for example, if menu items in the granted user menu group contain pipes or stored procedures requiring additional DB object privileges, it is necessary to grant additional privileges for these menu items.

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

> ⓘ When working with DB Manager, editing standard menu items from the standard delivery is prohibited. Only custom menu items or copies of standard menu items can be edited (see the document "DB 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

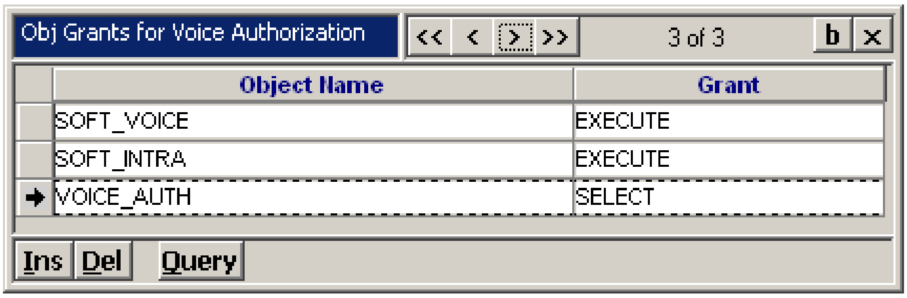
	Name	Available For
	Reports: Real-time Statements	Clerk
	Remote Access Operator	Clerk
	Remote Access Administrator	Clerk
	Purge History	Clerk & Auditor
➔	Pipe: VISA SMS Reconciliation Report	Clerk
	Pipe: RBS. Transactions Export	Clerk

Form for configuring menu subitem privilege packages

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]. The form contains two columns: *Object Name* specifying the DB object name, and *Grant*, which sets access rules for this object:

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

In the figure below, the package consists of privileges for three objects, two packages of stored procedures and one DB table.

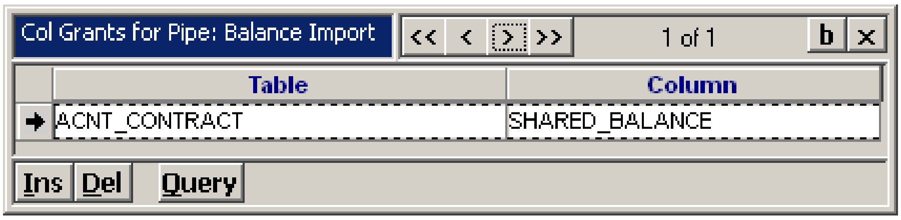


Obj Grants for Voice Authorization

	Object Name	Grant
	SOFT_VOICE	EXECUTE
	SOFT_INTRA	EXECUTE
➔	VOICE_AUTH	SELECT

Form to configure privileges for database objects

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

Form to configure privileges for specific DB table columns

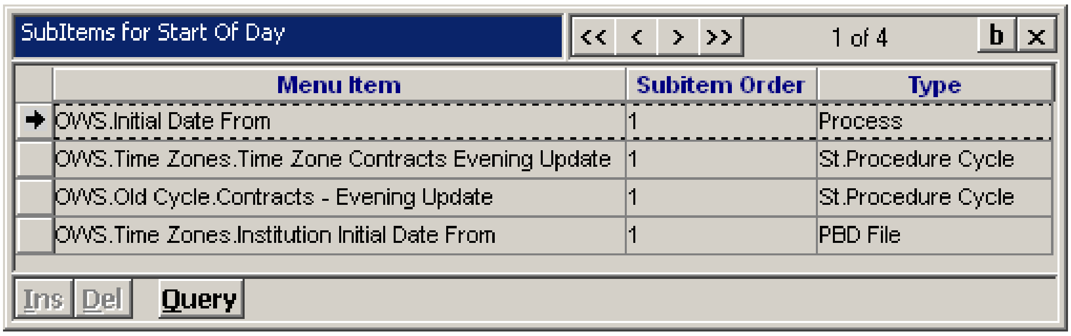
This form contains two columns:

- *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.

To view the list of menu subitems for which a privilege package is assigned, click [SubItems]. The "SubItems for <privilege package name>" form will open.



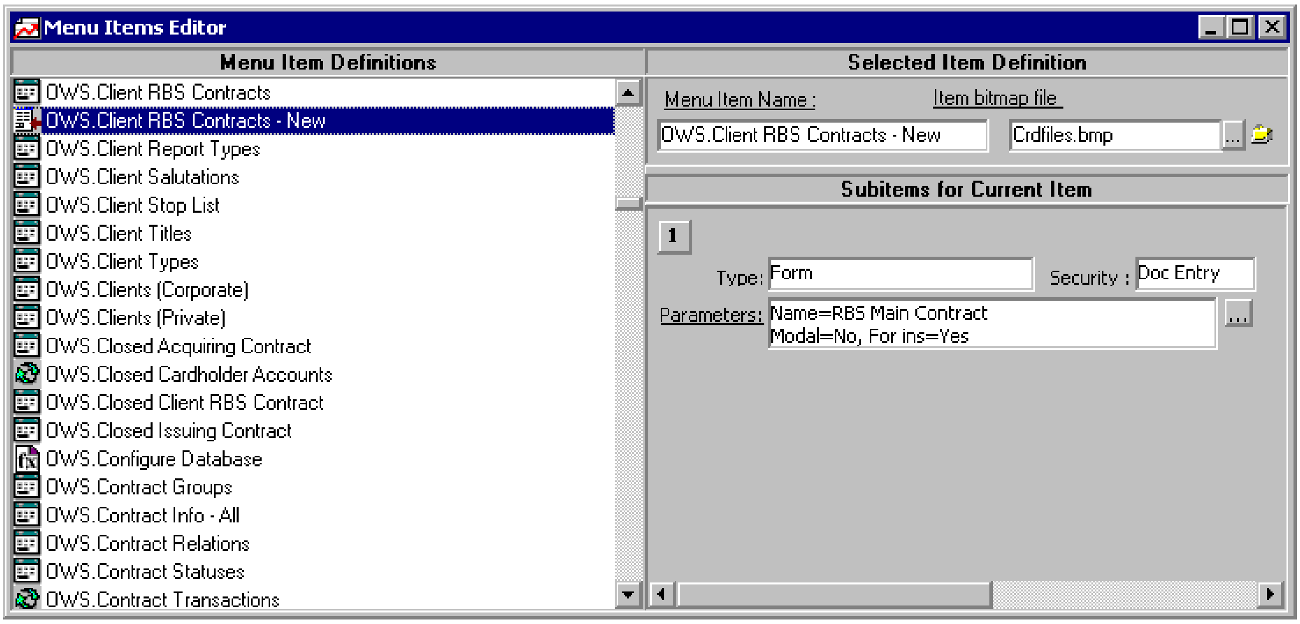
Menu Item	Subitem Order	Type
OWS.Initial Date From	1	Process
OWS.Time Zones.Time Zone Contracts Evening Update	1	St.Procedure Cycle
OWS.Old Cycle.Contracts - Evening Update	1	St.Procedure Cycle
OWS.Time Zones.Institution Initial Date From	1	PBD File

List of menu subitems for which a privilege packages is specified

Assigning a privilege package to a menu subitem

A privilege package is assigned to a menu item in the Menu Editor window (see the section "Menu Editor window" of the document "DB 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 document "DB Manager. Menu Editor".



Menu Item Definitions:

- OWS.Client RBS Contracts
- OWS.Client RBS Contracts - New
- OWS.Client Report Types
- OWS.Client Salutations
- OWS.Client Stop List
- OWS.Client Titles
- OWS.Client Types
- OWS.Clients (Corporate)
- OWS.Clients (Private)
- OWS.Closed Acquiring Contract
- OWS.Closed Cardholder Accounts
- OWS.Closed Client RBS Contract
- OWS.Closed Issuing Contract
- OWS.Configure Database
- OWS.Contract Groups
- OWS.Contract Info - All
- OWS.Contract Relations
- OWS.Contract Statuses
- OWS.Contract Transactions

Menu Item Name : OWS.Client RBS Contracts - New

Item bitmap file: Crdfiles.bmp

Type: Form

Security : Doc Entry

Parameters: Name=RBS Main Contract
Modal=No, For ins=Yes

Example of assigning a privilege package for a menu subitem

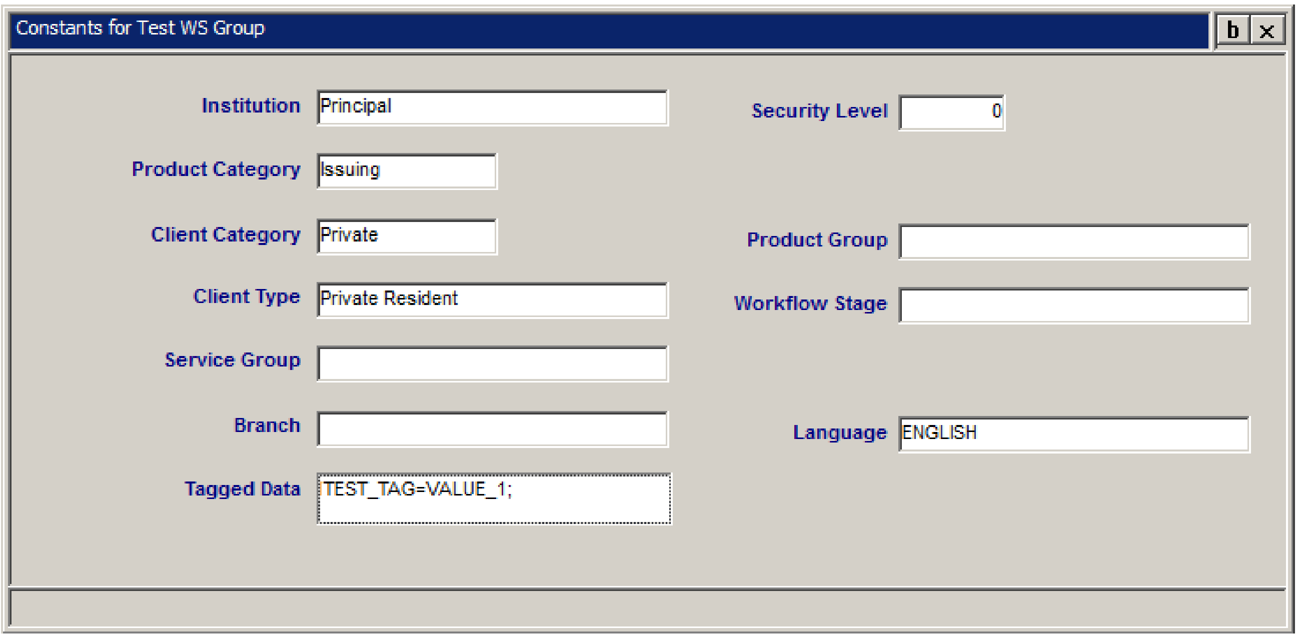
2.5 Initializing local constants

Local constants are used to filter data available while working with DB Manager forms.

Local constants are initialized when a user session is registered. Depending on the value of the *Usr Const* field in the "DB Manager User and Groups" field, either group or individual values of local constants will be used.

Values for initializing local constants are assigned in the following forms:

- Group local constants – "Constants for <user group name>" form. To open this form, click [Constants] in the form "User Groups and Users – View" (Full → DB Administrator Utilities → Users & Grants → User Groups and Users – View).



Constants for Test WS Group

Institution	Principal	Security Level	0
Product Category	Issuing		
Client Category	Private	Product Group	
Client Type	Private Resident	Workflow Stage	
Service Group			
Branch		Language	ENGLISH
Tagged Data	TEST_TAG=VALUE_1;		

Assigning values for initializing local constants for a user group

This form contains the following fields:

- *Institution* – name of financial institution.
- *Branch* – financial institution's branch.
- *Product Category* – Product category.
- *Client Category* – client category.
- *Client Type* – client type.
- *Service Group* – additional classification for clients.
- *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; this field value is used by the Advanced Applications R2 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 that can be generated in a local 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's value(s).
- Individual local constants – "Constants for <user name>" form. This form is opened by clicking [Constants] in the "Users for <user group name>" form, which is opened by clicking [Users] in the "User Groups and Users – View" form (Full → DB Administrator Utilities → Users & Grants → User Groups and Users – View).
  This form's fields are identical to the fields in the "Constants for <user group name>" form.

After initialization, the values of local constants can be redefined in special modal forms (for example, "Set Client Type", see the section "Clients and contracts" of the document "Issuing Module") or using "Assignment" menu item definition subitems (see the section ""Assignment" type of the document "DB Manager. Menu Editor").

3 Logging

This section describes principles of logging changes made to data by users while working with Way4, as well as principles for logging user sessions in 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.

For more information about process logging, see the section "DB Manager processes" of the document "DB Manager Manual".

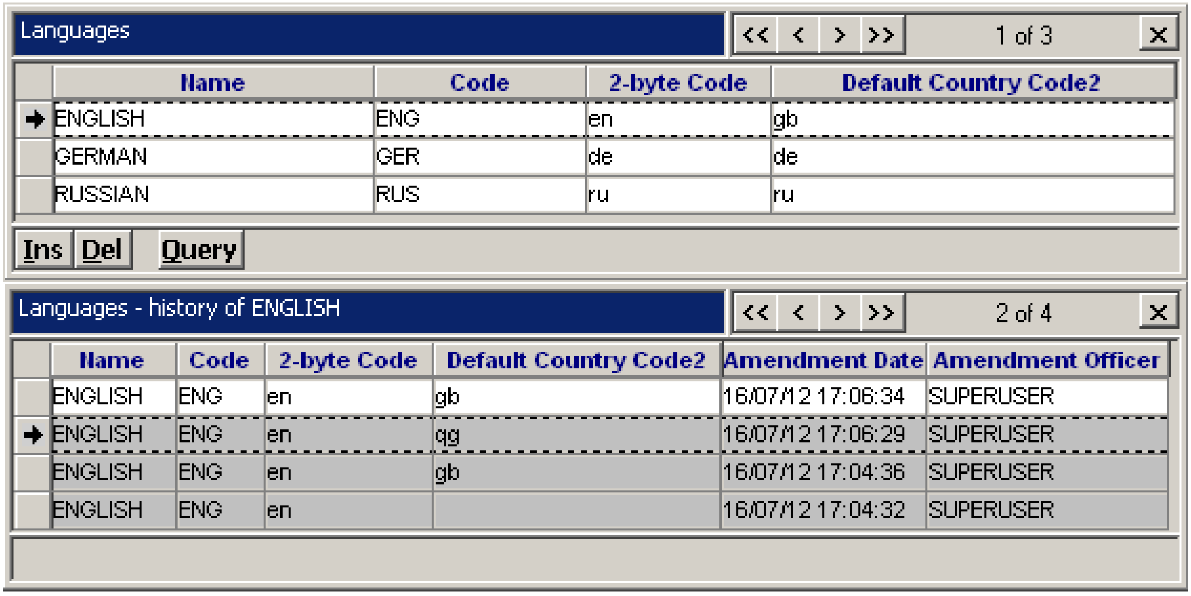
Logging changes made in grid forms

3.2 Logging changes 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.

To open the change history for a record, select the system menu item "Special => View History".

The additional form "<Grid form name> – history of ..." will open.



Languages

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

Languages - history of ENGLISH

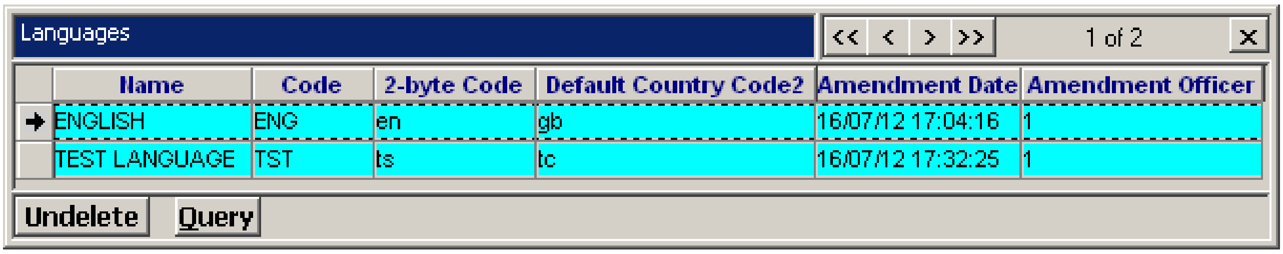
	Name	Code	2-byte Code	Default Country Code2	Amendment Date	Amendment Officer
	ENGLISH	ENG	en	gb	16/07/12 17:06:34	SUPERUSER
➔	ENGLISH	ENG	en	gg	16/07/12 17:06:29	SUPERUSER
	ENGLISH	ENG	en	gb	16/07/12 17:04:36	SUPERUSER
	ENGLISH	ENG	en		16/07/12 17:04:32	SUPERUSER

Example of a record's change history

In the 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 Restoring deleted records

To view records that were deleted from a grid form, use the menu item "Special => Deleted".



Name	Code	2-byte Code	Default Country Code2	Amendment Date	Amendment Officer
ENGLISH	ENG	en	gb	16/07/12 17:04:16	1
TEST LANGUAGE	TST	ts	tc	16/07/12 17:32:25	1

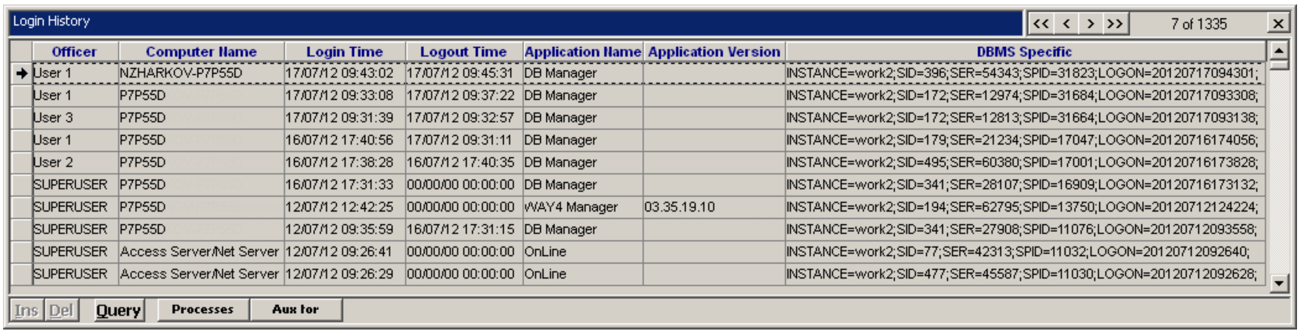
Example of viewing deleted records

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

3.4 User login history

When establishing a connection for a DB Manager user with the Way4 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 DB Manager is completed, the user logout date and time is also entered.

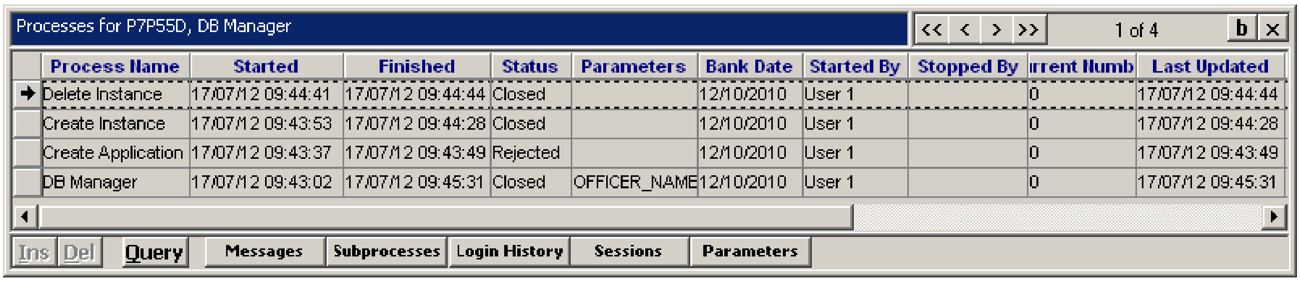
The log is accessed through the user menu item "Full → DB Administrator Utilities → Users & Grants → Login History". The "Login History" form will open.



Officer	Computer Name	Login Time	Logout Time	Application Name	Application Version	DBMS Specific
User 1	NZHARKOV-P7P55D	17/07/12 09:43:02	17/07/12 09:45:31	DB Manager		INSTANCE=work2;SID=396;SER=54343;SPID=31823;LOGON=20120717094301;
User 1	P7P55D	17/07/12 09:33:08	17/07/12 09:37:22	DB Manager		INSTANCE=work2;SID=172;SER=12974;SPID=31684;LOGON=20120717093308;
User 3	P7P55D	17/07/12 09:31:39	17/07/12 09:32:57	DB Manager		INSTANCE=work2;SID=172;SER=12813;SPID=31664;LOGON=20120717093138;
User 1	P7P55D	16/07/12 17:40:56	17/07/12 09:31:11	DB Manager		INSTANCE=work2;SID=179;SER=21234;SPID=17047;LOGON=20120716174056;
User 2	P7P55D	16/07/12 17:38:28	16/07/12 17:40:35	DB Manager		INSTANCE=work2;SID=495;SER=60380;SPID=17001;LOGON=20120716173828;
SUPERUSER	P7P55D	16/07/12 17:31:33	00/00/00 00:00:00	DB Manager		INSTANCE=work2;SID=341;SER=28107;SPID=16909;LOGON=20120716173132;
SUPERUSER	P7P55D	12/07/12 12:42:25	00/00/00 00:00:00	WAY4 Manager	03.35.19.10	INSTANCE=work2;SID=194;SER=62795;SPID=13750;LOGON=20120712124224;
SUPERUSER	P7P55D	12/07/12 09:35:59	16/07/12 17:31:15	DB Manager		INSTANCE=work2;SID=341;SER=27908;SPID=11076;LOGON=20120712093558;
SUPERUSER	Access Server/Net Server	12/07/12 09:26:41	00/00/00 00:00:00	OnLine		INSTANCE=work2;SID=77;SER=42313;SPID=11032;LOGON=20120712092640;
SUPERUSER	Access Server/Net Server	12/07/12 09:26:29	00/00/00 00:00:00	OnLine		INSTANCE=work2;SID=477;SER=45587;SPID=11030;LOGON=20120712092628;

Example of user login history

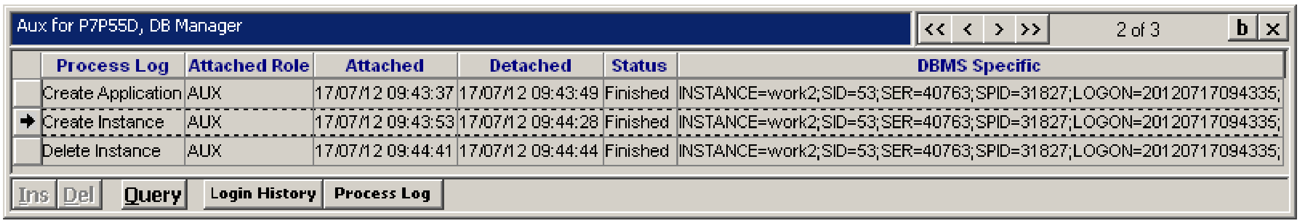
During one session when several processes are executed (starting pipes, deleting records, processing documents, etc.) several records are created in the "Login History" table, information on which is available in the form "Processes for <...>", opened by clicking [Processes] in the "Login History" form.



Process Name	Started	Finished	Status	Parameters	Bank Date	Started By	Stopped By	rrent Numb	Last Updated
Delete Instance	17/07/12 09:44:41	17/07/12 09:44:44	Closed		12/10/2010	User 1		0	17/07/12 09:44:44
Create Instance	17/07/12 09:43:53	17/07/12 09:44:28	Closed		12/10/2010	User 1		0	17/07/12 09:44:28
Create Application	17/07/12 09:43:37	17/07/12 09:43:49	Rejected		12/10/2010	User 1		0	17/07/12 09:43:49
DB Manager	17/07/12 09:43:02	17/07/12 09:45:31	Closed	OFFICER_NAME	12/10/2010	User 1		0	17/07/12 09:45:31

Processes started in one session

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



	Process Log	Attached Role	Attached	Detached	Status	DBMS Specific
	Create Application	AUX	17/07/12 09:43:37	17/07/12 09:43:49	Finished	INSTANCE=work2;SID=53;SER=40763;SPID=31827;LOGON=20120717094335;
➜	Create Instance	AUX	17/07/12 09:43:53	17/07/12 09:44:28	Finished	INSTANCE=work2;SID=53;SER=40763;SPID=31827;LOGON=20120717094335;
	Delete Instance	AUX	17/07/12 09:44:41	17/07/12 09:44:44	Finished	INSTANCE=work2;SID=53;SER=40763;SPID=31827;LOGON=20120717094335;

Processes that were created by other processes

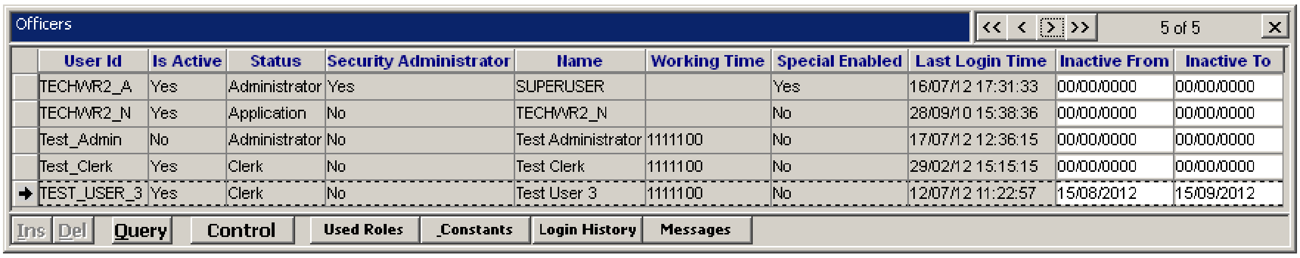
This form contains information about processes that were automatically created as a result of the execution of other processes.

> The Way4 Housekeeping module automatically clears the user login history and change log (see the document "Way4 Housekeeping").

3.5 Locking inactive accounts

Pursuant to PA-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".



	User Id	Is Active	Status	Security Administrator	Name	Working Time	Special Enabled	Last Login Time	Inactive From	Inactive To
	TECHWR2_A	Yes	Administrator	Yes	SUPERUSER		Yes	16/07/12 17:31:33	00/00/0000	00/00/0000
	TECHWR2_N	Yes	Application	No	TECHWR2_N		No	28/09/10 15:38:36	00/00/0000	00/00/0000
	Test_Admin	No	Administrator	No	Test Administrator	1111100	No	17/07/12 12:36:15	00/00/0000	00/00/0000
	Test_Clerk	Yes	Clerk	No	Test Clerk	1111100	No	29/02/12 15:15:15	00/00/0000	00/00/0000
➜	TEST_USER_3	Yes	Clerk	No	Test User 3	1111100	No	12/07/12 11:22:57	15/08/2012	15/09/2012

List of users who are registered in the system

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.

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

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). Pursuant PA-DSS requirements, the default value of this parameter is "90".

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 the system it is possible to lock (unlock) a specific 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. A "SUPERUSER" user for whom "1" is specified in the *ID* field of the "DB Manager User and Groups" window also 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.
- <OWS_TEMP> – stores temporary files created during DB Manager operation, and error log files (see the section "Temporary File Directory" of the document "DB Manager Manual"). This directory should be located on Way4 workstations.

<OWS_HOME> and <OWS_WORK> are public directories for all Way4 users and should be located on the file server.

The <OWS_TEMP> directory must be present on each workstation used to access Way4.

4.2 Privileges for standard Way4 directories

When setting up DB 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>).

All system users must have full privileges for the the (<OWS_TEMP>) temporary file directory.

Depending on the tasks performed by users, the latter can be divided into classes, each of which requires full privileges for access to standard Way4 system directories or their subdirectories.

System directory privileges required for various classes of users

User class	Responsibility	Directory
Administrators	WAY4 upgrade	<OWS_HOME>, <OWS_WORK>
	Creating and editing screen forms	<OWS_WORK>\Client\Shared
Operators	Card production	<OWS_WORK>\Data\Card_Prd
	Organization of interchange with international payment systems	<OWS_WORK>\Data\Interchange
	Organization of interchange with the RBS	<OWS_WORK>\Data\RBS
	Creation of reports	<OWS_WORK>\Data\Reports

5 Limiting data access with user password encryption

By default, a user's DB Manager password can also be used for access to DB data using an SQL expression editor or with any DB client application.

If required, a password obtained as the result of encrypting the DB 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 DB 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 DB Manager.

There are two ways of setting a password encryption key:

- Using the "PWD_ENCRYPTION" parameter in the [Client.DBM.Params] section of the "db.ini" file from the <OWS_WORK> directory.
- Using the "PWD_ENCRYPTION" parameter in the "Local Machine Parameters" window for configuring workstation parameter (see the section ""Database" item of the document "DB Manager Manual").

In both cases, this parameter's value is specified in the following format:

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

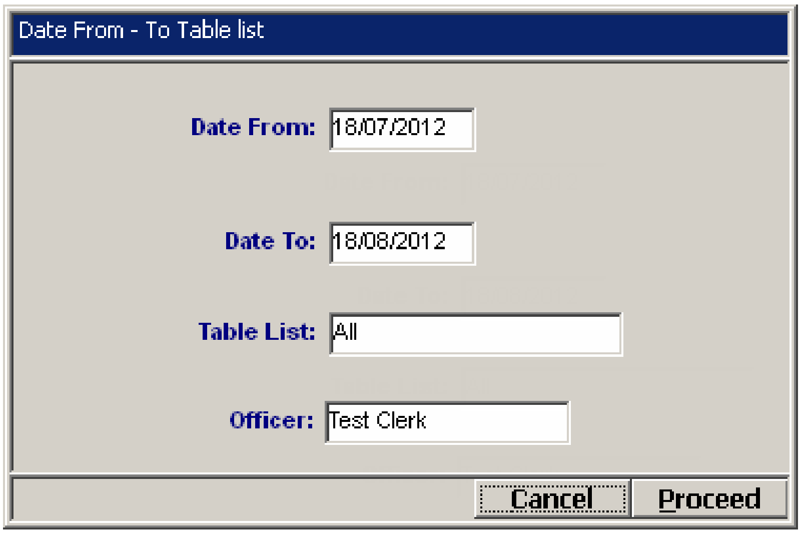
ASCII symbols with codes in the range from 33 to 127 can be used in the body of the encryption key. The key length can be up to 256 symbols.

> 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 password of the main security administrator ("OWS_A") is not encrypted even if "PWD_ENCRYPTION" is set. When the password of the main secuity administrator expires, the password must be changed through the database.

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 "Date From – To Table List" form will open.



Date From - To Table list

Date From:	18/07/2012
Date To:	18/08/2012
Table List:	All
Officer:	Test Clerk

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 in the form, click [Proceed]. 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.