



Operation Manual

Администрирование пользователей в системе WAY4

03.51.30

30.07.2020

СОДЕРЖАНИЕ

1	Пользователи системы WAY4	5
1.1	Классификация пользователей системы WAY4	5
1.2	Группы пользователей	7
2	Технология создания рабочих мест	8
2.1	Диалоговое окно для работы с учетными записями	8
2.1.1	Параметры пользовательских групп	9
2.1.2	Параметры учетных записей пользователей	10
2.1.3	Права доступа (Privileges)	11
2.1.4	Кнопки	13
2.2	Редактирование групп пользователей	15
2.2.1	Добавление новой группы пользователей	15
2.2.2	Модификация группы пользователей	16
2.2.3	Назначение группе пользователей вышестоящей группы	16
2.2.4	Удаление группы пользователей	16
2.2.5	Корневая группа меню	17
2.2.6	Список прав, необходимых для доступа к корневой группе меню	17
2.2.7	Обновление прав пользовательских групп	18
2.2.8	Права доступа, необходимые для запуска объектов корневой группы меню	19
2.3	Редактирование списка пользователей	20
2.3.1	Создание учетной записи пользователя	20
2.3.2	Изменение параметров учетной записи пользователя	22
2.3.3	Назначение пользователю новой пользовательской группы	22
2.3.4	Удаление пользователя из списка	22
2.3.5	Блокирование учетной записи пользователя системы WAY4	22
2.3.6	Разблокирование учетной записи пользователя системы WAY4	23
2.3.7	Блокирование учетной записи пользователя БД Oracle	23
2.3.8	Разблокирование учетной записи пользователя БД Oracle	23
2.3.9	Удаление учетной записи пользователя БД Oracle	24
2.3.10	Изменение пароля пользователя	24
2.4	Настройка дополнительных прав доступа к объектам БД для пунктов меню	26
2.4.1	Настройка пакетов прав	26

2.4.2	Назначение пакета дополнительных прав подпункту меню	28
2.5	Инициализация локальных переменных	29
3	Протоколирование	31
3.1	Протоколирование работы процессов	31
3.2	Протоколирование изменений, произведенных в табличных формах	31
3.3	Восстановление удаленных записей	32
3.4	Журнал регистрации пользователей в системе	32
3.5	Блокирование неиспользуемых учетных записей	34
4	Права доступа к каталогам системы WAY4	36
4.1	Стандартные каталоги системы WAY4	36
4.2	Права доступа к стандартным каталогам системы WAY4	36
5	Ограничение доступа к данным при использовании шифрования пароля пользователя	38
6	Отчет "Amendment Report"	39

В документе приведены основные концепции администрирования пользователей в системе WAY4™.

При работе с данным документом рекомендуется пользоваться следующими источниками из комплекта документации OpenWay:

- "Работа с WAY4 Manager"
- "Редактор меню WAY4 Manager";
- "Редактор форм WAY4 Manager";
- "Рекомендации по обеспечению безопасности в системе WAY4™ согласно стандарту PCI DSS";
- "Работа с WAY4 Remote Access";
- "Глобальные параметры системы WAY4™".

В документации используются следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- комбинации клавиш приводятся в угловых скобках, например, <Ctrl>+<F3>;
- названия кнопок экранных форм и вкладок приводятся в квадратных скобках, например, [Approve];
- последовательность выбора пункта в меню пользователя или контекстном меню отображается с помощью стрелок следующим образом: "Issuing → Contracts Input & Update";
- последовательность выбора пункта в системном меню отображается с помощью стрелок следующим образом: Database => Change password;
- различные переменные значения, например, имена каталогов и файлов, а также пути к файлам, варьируемые для каждой локальной машины, приводятся в угловых скобках, например, <OWS_HOME>.

Предостережения и информационные сообщения размечаются следующим образом:



Предостережения в связи с возможностью совершения неправильных действий.



Сообщения, содержащие информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

1 Пользователи системы WAY4

В данном разделе приведена классификация пользователей системы WAY4, а также описаны права их доступа к объектам базы данных (БД).

1.1 Классификация пользователей системы WAY4

Классификация пользователей системы WAY4 по функциональному назначению, а также необходимые для каждого класса пользователей права доступа к БД представлены в Таблице.

Табл. Классификация пользователей базы данных системы WAY4

Тип (наименование) пользователя	Функции	Права доступа к БД	Кол-во
Владелец схемы "Owner", (Служебный пользователь)	Создание объектов БД системы WAY4	Полные права на все объекты схемы (данные и метаданные)	1
Главный администратор информационной безопасности (Служебный пользователь)	Создание пользователей (в том числе администраторов информационной безопасности) и пользовательских групп, предоставление прав доступа пользователям и пользовательским группам	Полные права на просмотр, модификацию и удаление данных БД системы WAY4	1
Администратор информационной безопасности	Создание пользователей и пользовательских групп, предоставление прав доступа пользователям и пользовательским группам	Частичные права на просмотр, модификацию и удаление данных БД системы WAY4	несколько

Тип (наименование) пользователя	Функции	Права доступа к БД	Кол-во
Администратор	Создание, редактирование и удаление пользовательских представлений, экранных форм, пайпов, редактирование групп меню и пунктов меню пользователя	Частичные права на просмотр, модификацию и удаление данных	несколько
Оператор (Clerk)	Работа с данными в предоставленной группе меню	Права на просмотр, модификацию и удаление данных, доступных из предоставленной группы меню пользователя	Не ограничено
Аудитор	Просмотр данных, доступных из предоставленной группы меню	Права на просмотр данных, доступных из предоставленной группы меню пользователя	Не ограничено
Пользователь для NetServer (Служебный пользователь)	Online-авторизация	Права на исполнение нескольких хранимых процедур	1

Обычно служебные пользователи системы WAY4 имеют следующие наименования:

- Владелец схемы – "OWS";
- Главный администратор информационной безопасности – "OWS_A";
- Пользователь для NetServer – "OWS_N".

Работа администраторов, операторов и аудиторов (далее просто пользователей системы WAY4 в отличие от служебных пользователей) с данными БД системы WAY4 осуществляется при помощи приложения WAY4 Manager (см. документ "Работа с WAY4 Manager").

Владелец схемы (Owner) является владельцем всех таблиц, пользовательских представлений и процедур. После установки системы (выполнения процедуры переключения в многопользовательский режим) доступ в систему при помощи приложения WAY4 Manager для владельца схемы автоматически запрещен.

Главный администратор информационной безопасности (Super Security Administrator) создается один раз при переводе системы в многопользовательский режим. Основной функцией главного администратора информационной безопасности является создание пользователей системы WAY4, в том числе администраторов информационной безопасности.

Роль администратора информационной безопасности (Security Administrator) назначается пользователям системы WAY4 (администраторам и операторам). Назначение пользователям определенных ролей осуществляется посредством добавления пользователям соответствующих прав доступа (Privilege) (см. "[Права доступа \(Privileges\)](#)"). Основной функцией пользователя с правами администратора информационной безопасности является создание других пользователей системы WAY4.

1.2 Группы пользователей

Для удобства администрирования пользователи системы WAY4 объединяются в группы. Каждой группе пользователей предоставляется для работы группа меню пользователя (см. раздел "Меню пользователя" документа "Работа с WAY4 Manager"). При этом доступ к другим группам меню пользователя запрещен.



Каждый пользователь системы WAY4 может принадлежать только к одной группе пользователей.

Каждой группе пользователей также предоставляется набор прав доступа к БД. При выполнении операции "Update Grants" (см. "[Технология создания рабочих мест](#)") для каждой группы пользователей в БД автоматически создаются две роли (в соответствии с предоставленными правами доступа), включающие в себя права доступа к БД, необходимые и достаточные для работы с данной группой меню пользователя. Эти роли предоставляется всем пользователям, входящим в данную группу.

2 Технология создания рабочих мест

Для создания рабочего места (Workplace) пользователя системы WAY4 необходимо зарегистрировать учетную запись данного пользователя в соответствующей группе (см. "[Группы пользователей](#)"). При этом на уровне учетной записи пользователю могут быть назначены права доступа (Privilege), определяющие роль пользователя (администратор, оператор, аудитор или администратор информационной безопасности). Права доступа к группе меню пользователя предоставляются на уровне группы пользователей.

Распределение доступа к группам меню пользователя производится с помощью следующих механизмов:

- создание для каждой группы пользователей своей, специфичной именно для нее, группы меню пользователя;
- назначение пользователям и/или группам пользователей зарегистрированных в системе прав доступа (Privilege), которые заданы также для группы меню (см. документа "Редактор меню WAY4 Manager").

Распределение доступа к данным, доступным пользователям при работе с формами WAY4 Manager, осуществляется с помощью статических и динамических фильтров (см. раздел "Окно редактора форм. Вкладка "Fields" документа "Редактор форм WAY4 Manager"), а также переопределения значений этих фильтров (см. раздел "[Инициализация локальных переменных](#)").

2.1 Диалоговое окно для работы с учетными записями

Работа с учетными записями пользователей осуществляется в специально предназначенном для этого диалоговом окне "User Management", доступном при выполнении пункта меню "Full → DB Administrator Utilities → Users & Grants → User Groups and Users – Edit".

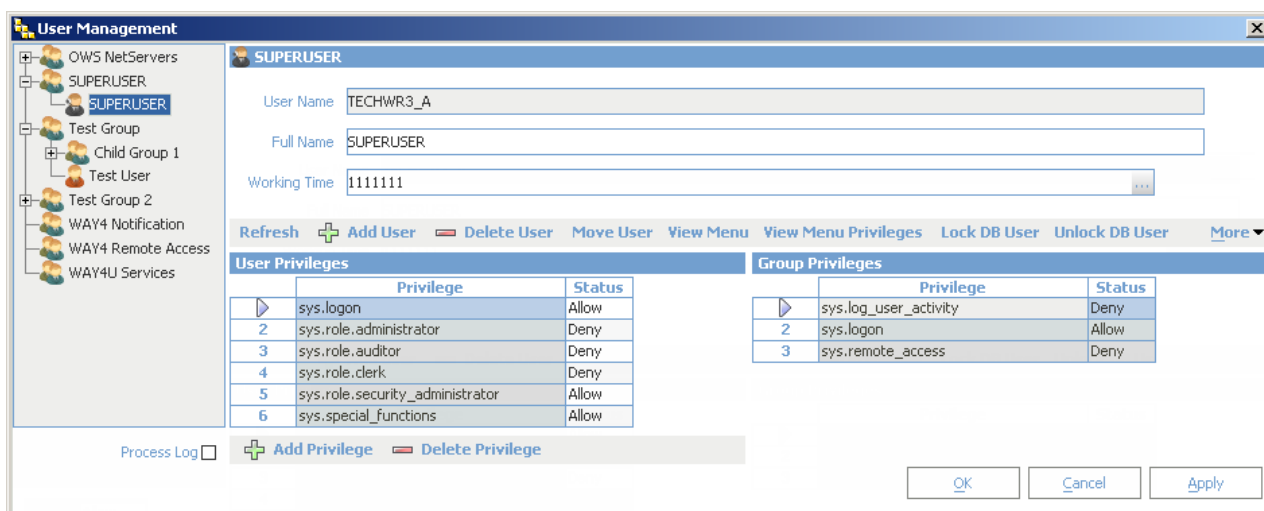


Рис. Окно администрирования пользователей и пользовательских групп

В левой части окна в виде иерархической структуры отображается список пользователей и пользовательских групп.



Любые изменения учетных записей пользователей и пользовательских групп, которые не были подтверждены с помощью нажатия на кнопки [Apply], [OK], либо на кнопки [Update Grants], [Update Grants for All], не сохраняются в БД.

Сохранение любых изменений параметров учетных записей пользователей и групп выполняется при помощи нажатия на кнопку [Apply] и [OK].

В следующих подразделах описываются поля и кнопки управления окна "User Management".

2.1.1 Параметры пользовательских групп

Форма "Group" окна "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") содержит следующие поля:

- *Name* – наименование группы;
- *Menu* – поле с выбором из списка для указания группы меню, являющейся корневой для данной группы пользователей (для дочерней группы данное поле недоступно для редактирования);
- *Grants Update Time* – дата и время последнего проведения операции "Update Grants" для данной группы (поле недоступно для редактирования);
- *Additional Info* – поле для ввода дополнительной информации о пользовательской группе;
- *Security model* – модель безопасности;
- *Available for Web* – признак наличия у группы пользователей прав доступа к веб-приложению WAY4 Web;
- *Code* – код группы.



Следует иметь в виду, что для дочерних групп используется ветка меню родительской группы (те же права на объекты базы данных), но для дочерних групп можно определять другие значения для локальных переменных. При этом в поле *Derived Menu* дочерней группы будет содержаться наименование ветки меню родительской группы.

Дочерние группы необходимы в первую очередь для уменьшения количества ролей базы данных.

При администрировании следует руководствоваться следующими правилами:


- После добавления дочерней группы необходимо выполнить обновление прав доступа для родительской группы (кнопка [Update Grants]).
- При внесении изменений в ветку меню родительской группы следует выполнять обновление прав доступа для родительской группы (кнопка [Update Grants]).

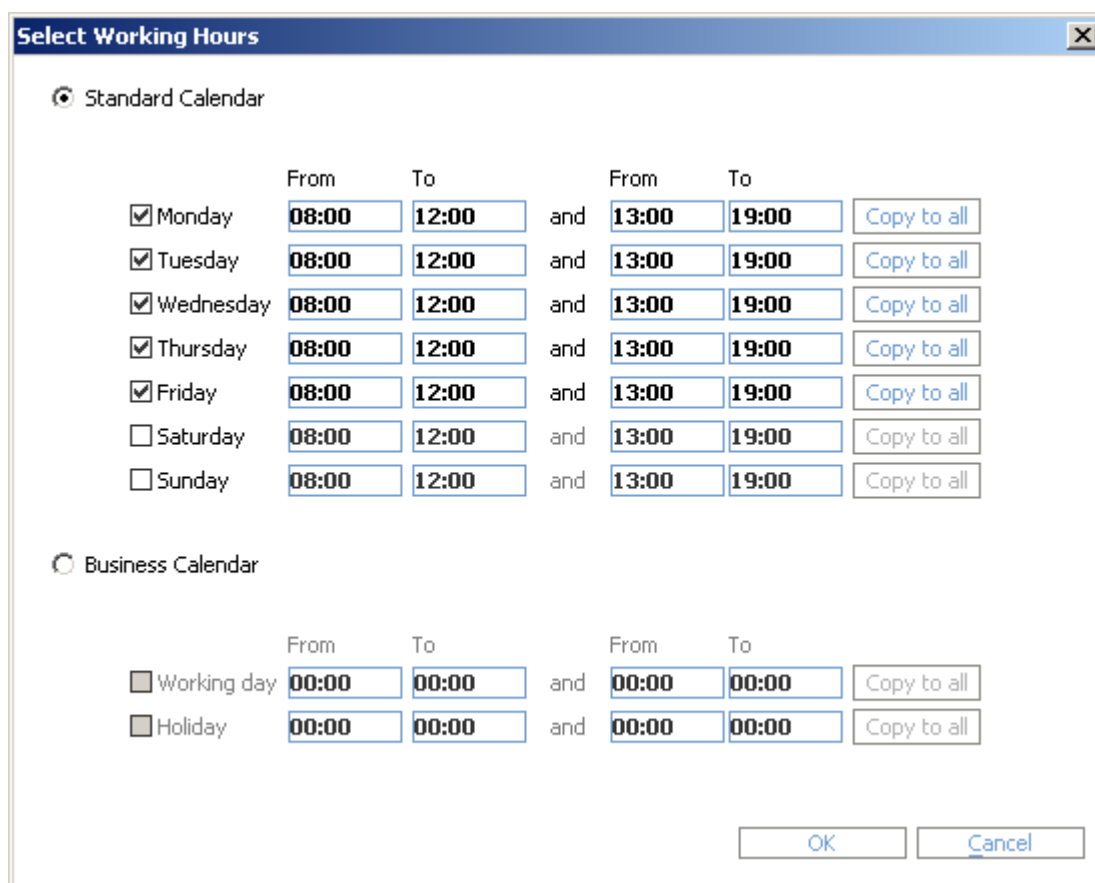


Об ограничениях на выполнение операции "Update Grants" см. в разделе "[Обновление прав пользовательских групп](#)".

2.1.2 Параметры учетных записей пользователей

Форма "<Имя пользователя>" окна "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") содержит следующие поля:

- *User Name* – идентификатор пользователя, используемый для соединения с БД (поле недоступно для редактирования);
- *Full Name* – текстовое поле для указания имени пользователя;
- *Working Time* – поле для указания временного интервала, в течение которого данному пользователю разрешено получать доступ в систему WAY4 с помощью приложения WAY4 Manager. В данном поле обязательно должна присутствовать строка из семи цифр, состоящая из "0" либо "1", где позиция цифры означает день недели (начиная с понедельника), а значение – разрешена либо нет работа пользователя с системой ("0" – запрещена, "1" – разрешена). При нажатии на кнопку  на экране будет представлено окно "Select Working Hours".



Select Working Hours

☒ Standard Calendar

	From	To		From	To	
<input checked="" type="checkbox"/> Monday	08:00	12:00	and	13:00	19:00	Copy to all
<input checked="" type="checkbox"/> Tuesday	08:00	12:00	and	13:00	19:00	Copy to all
<input checked="" type="checkbox"/> Wednesday	08:00	12:00	and	13:00	19:00	Copy to all
<input checked="" type="checkbox"/> Thursday	08:00	12:00	and	13:00	19:00	Copy to all
<input checked="" type="checkbox"/> Friday	08:00	12:00	and	13:00	19:00	Copy to all
<input type="checkbox"/> Saturday	08:00	12:00	and	13:00	19:00	Copy to all
<input type="checkbox"/> Sunday	08:00	12:00	and	13:00	19:00	Copy to all

☐ Business Calendar

	From	To		From	To	
<input type="checkbox"/> Working day	00:00	00:00	and	00:00	00:00	Copy to all
<input type="checkbox"/> Holiday	00:00	00:00	and	00:00	00:00	Copy to all

[OK](#) [Cancel](#)

Рис. Определение интервала доступа в систему

Данное окно предназначено для указания временного интервала доступа в систему. Группа переключателей *Standard Calendar* и *Business Calendar* позволяет задавать временной интервал

для каждого дня недели либо по дням недели, определенным с помощью бизнес-календаря как рабочие или выходные (см. раздел "Бизнес-календарь" документа "Общие перечни системы WAY4™").



Следует иметь в виду, что по умолчанию при создании учетной записи пользователя в поле *Working Time* присутствует значение "00000000", что полностью запрещает работу пользователя с системой. Поэтому при создании учетной записи пользователя рекомендуется указывать какой-либо разрешенный для работы с системой временной интервал.

2.1.3 Права доступа (Privileges)

Права доступа (Privileges) пользователей и групп пользователей назначаются соответственно в формах "User Privileges" и "Group Privileges" окна "User Management" (см. раздел "Диалоговое окно для работы с учетными записями"). С помощью прав доступа (Privileges) пользователям и групп пользователей могут быть назначены определенные роли, а также даны права доступа к веткам меню, к системному меню, права на запуск клиентского приложения и т.д.

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



 Add Privilege
  Delete Privilege

Рис. Права доступа для пользователей и групп

В поле *Privilege* указано наименование прав доступа (Privilege).

Поле *Status* может содержать одно из следующих значений:

- "Allow" – разрешение на использование прав доступа;
- "Deny" – запрет на использование прав доступа.

Для добавления зарегистрированных в системе прав доступа (Privileges) необходимо нажать на кнопку [Add Privilege]. При этом на экране будет представлена форма "Add Privilege".

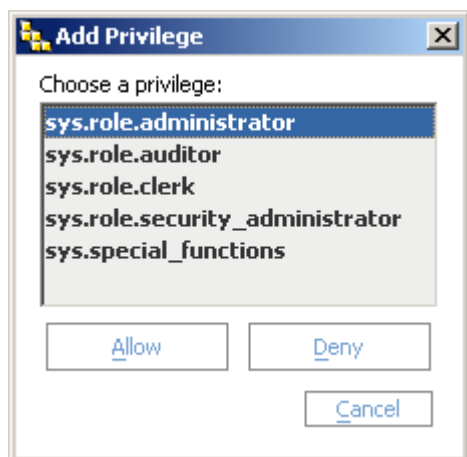


Рис. Назначение прав доступа

В данной форме необходимо выбрать права доступа (Privilege), после чего нажать на кнопку [Allow] (разрешить использование прав доступа) или [Deny] (запретить использование). Для отмены назначения прав доступа необходимо нажать на кнопку [Cancel].

Для удаления прав доступа из формы "User Privileges" или "Group Privileges" следует нажать на кнопку [Delete Privilege].

В системе зарегистрированы следующие системные права доступа (Privileges):

- "sys.client.way4manager" – права на работу с системой с помощью WAY4 Manager;
- "sys.login" – права на вход в систему;
- "sys.web_services" – права на работу с системой с помощью тонкого клиента, представляющего доступ к системе посредством веб-сервисов.
- "sys.remote_access" – права на работу с системой WAY4 с удаленного рабочего места (см. документ "Работа с WAY4 Remote Access"); пользователи, имеющие право удаленной работы с системой, имеют более ограниченные права по сравнению с другими пользователями, а именно: имеют право на выполнение SQL-оператора SELECT только из необходимых для работы таблиц, не имеют права на выполнение SQL-операторов UPDATE, INSERT, DELETE, однако имеют право на выполнение специальных хранимых процедур, которые выполняют эти операции с дополнительной проверкой безопасности;
- "sys.special_functions" – права доступа к пункту системного меню "Special";
- "sys.role.security_administrator" – роль администратора информационной безопасности;
- "sys.role.administrator" – роль администратора;
- "sys.role.clerk" – роль оператора (Clerk);
- "sys.role.auditor" – роль аудитора;
- "sys.form_data_export" – права на вывод данных на печать и экспорт информации для оператора (Clerk). Если у пользователя или группы пользователей привилегия "sys.form_data_export" в статусе "Deny", то печать и экспорт запрещены.













Следует иметь в виду, для ролей пользователей и групп пользователей в системе используются следующие приоритеты:

- Главный администратор информационной безопасности;
- Администратор информационной безопасности;
- Администратор;

- Оператор (Clerk);
- Аудитор.

При этом наивысшим приоритетом обладает администратор информационной безопасности.

В окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") для обозначения пользователей и пользовательских групп используются следующие пиктограммы (первая пиктограмма – в случае если редактирование разрешено, вторая – при невозможности редактирования):

-  ,  – группа меню;
-  ,  – главный администратор информационной безопасности;
-  ,  – администратор информационной безопасности;
-  ,  – администратор;
-  ,  – оператор (Clerk);
-  ,  – аудитор.

При назначении прав доступа необходимо руководствоваться следующими правилами:

- Если группе пользователей и пользователям, принадлежащим данной группе, назначены различные роли, то используется роль с наивысшим приоритетом.
- Если установлен запрет на использование прав доступа для группы пользователей, данный запрет распространяется на всех пользователей и все группы, включенные в данную группу.
- Если группе пользователей назначены права доступа, а для пользователя данной группы установлен запрет на использование тех же прав доступа, то пользователь не будет иметь назначенных группе прав доступа. Таким образом, запрет на использование прав доступа имеет более высокий приоритет.

2.1.4 Кнопки

Диалоговое окно "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") содержит следующие кнопки:

- Для групп пользователей:
 - [Refresh] – обновить данные в окне "User Management";
 - [Add Group] – добавить новую группу пользователей;
 - [Add Child Group] – добавить подчиненную группу пользователей;
 - [Add User] – добавить нового пользователя;
 - [Delete Group] – удалить выбранную группу пользователей;
 - [Move Group] – назначить группе пользователей вышестоящую группу;
 - [Edit User Constants] – инициализировать локальные переменные для выбранной группы;
 - [View Menu] – вывести на экран окно с группой меню, являющейся корневой для выбранной группы пользователей; данная группа меню будет доступна при входе в систему всем пользователям выбранной группы.



В зависимости от дополнительных прав доступа (Privilege), назначенных пользователям выбранной группы, корневая группа меню может содержать различные элементы.

- [View Menu Privileges] – вывести на экран окно со списком прав доступа (Privilege), необходимых для доступа к корневой группе меню;
- [Update Grants] – произвести обновление прав доступа для выбранной группы пользователей.
- [Update Grants For All] – произвести обновление прав доступа для всех групп пользователей, которым предоставлены права на работу с системой с помощью WAY4 Manager (назначены права доступа "sys.client.way4manager").



Об ограничениях на выполнение обновления прав доступа см. в разделе "[Обновление прав пользовательских групп](#)".

- [Show Grants] – вывести на экран окно с информацией о правах доступа к объектам БД корневой группы меню (пакетам хранимых процедур, таблицам и т. д.);
- Для пользователей:
 - [Refresh] – обновить данные в окне "User Management";
 - [Add User] – добавить нового пользователя;
 - [Delete User] – удалить указанного пользователя;
 - [Move User] – переместить пользователя в другую группу;
 - [View Menu] – вывести на экран окно с группой меню, являющейся корневой для данного пользователя;
 - [View Menu Privileges] – вывести на экран окно со списком прав доступа (Privilege), необходимых для доступа к корневой группе меню;
 - [Lock DB User] – заблокировать учетную запись пользователя БД Oracle;
 - [Unlock DB User] – разблокировать учетную запись пользователя БД Oracle;
 - [Drop DB User] – удалить учетную запись пользователя БД Oracle;
 - [Reset Password] – изменить пароль пользователя;
 - [Lock Officer] – заблокировать учетную запись пользователя системы WAY4;
 - [Unlock Officer] – разблокировать учетную запись пользователя системы WAY4.

Для того чтобы функциональность, реализуемая с помощью кнопок [Lock DB User], [Unlock DB User], [Drop DB User] и [Reset Password], была доступна, необходимо в системе установить дополнительный пакет "SYS.OWS_ADMINISTER_USER". Для этого необходимо выполнить в консоли следующую команду:

```
<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>
```

где: <SYSPassword> – пароль пользователя sys; <Host>:<Port>:<SID> – имя сервера, порт (по умолчанию "1521") и "SID" базы данных; <LogFilePath> – полный путь и имя файла журнала; <OWS_Owner> – имя владельца схемы.

В случае если не выполнить установку данного пакета, после нажатия на кнопку на экране будет представлено окно с сообщением об ошибке "SYS.OWS_ADMINISTER_USER not found: cannot perform action".



Флажок *Process Log* управляет регистрацией в журнале выполнения процессов (Process Log) действий пользователей. Если флажок установлен, то в журнале выполнения процессов регистрируются все действия пользователей. Если флажок не установлен, то регистрируются все действия, связанные с безопасностью. Все действия администратора считаются связанными с безопасностью и регистрируются независимо от установки флажка.

Кнопка [Apply] окна "User Management" предназначена для утверждения изменений, кнопка [Cancel] – для отмены совершенных изменений. При нажатии на кнопку [OK] происходит утверждение изменений и закрытие окна "User Management".

2.2 Редактирование групп пользователей

2.2.1 Добавление новой группы пользователей

Для добавления новой группы или дочерней группы необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать любую группу, после чего нажать соответственно на кнопку [Add Group] или [Add Child Group]. В результате в форме "Group" данного окна появится новая запись, в которой необходимо заполнить соответствующие поля (см. "[Параметры пользовательских групп](#)"), после чего нажать на кнопку [Apply].

В результате в БД будет создана роль, включающая в себя права доступа к базе, необходимые и достаточные для работы с указанной в поле *Меню* группой меню.



В некоторых случаях, например, если в качестве пунктов меню в предоставленной группе меню пользователя содержатся пайпы либо хранимые процедуры, требующие дополнительных прав доступа к объектам БД, для данных пунктов меню требуется предоставление дополнительных прав доступа (см. "[Настройка дополнительных прав доступа к объектам БД для пунктов меню](#)").

2.2.2 Модификация группы пользователей

В системе существует возможность модифицировать параметры созданных групп.

Сохранение изменений параметров группы выполняется при помощи нажатия на кнопку [Apply] в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)").

2.2.3 Назначение группе пользователей вышестоящей группы

В системе существует возможность назначать группе, не имеющей вышестоящей группы, вышестоящую группу, а также переназначать подчиненной группе другую вышестоящую группу.

Для этого необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выделить требуемую группу и нажать на кнопку [Move Group]. В результате на экране будет представлено окно "Move Group", содержащее список групп пользователей.

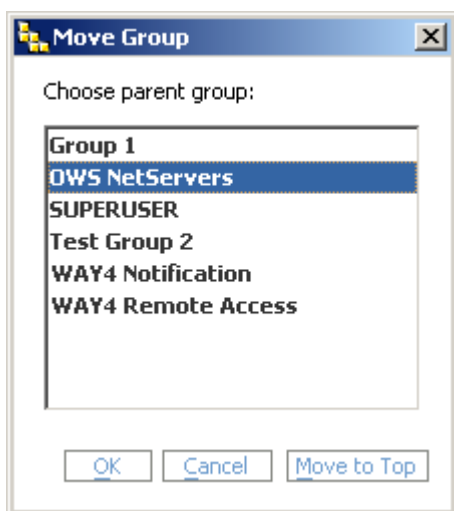


Рис. Назначение группе вышестоящей группы

Для назначения группе вышестоящей группы необходимо в поле "Choose parent group" выбрать группу, после чего нажать на кнопку [OK], для отмены назначения вышестоящей группы – на кнопку [Cancel].

При нажатии на кнопку [Move to Top] группа пользователей станет группой корневого уровня, т.е. не будет являться подчиненной.

2.2.4 Удаление группы пользователей

Удаление группы пользователей возможно только при отсутствии в ней учетных записей пользователей.

Для удаления группы пользователей необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") нажать на кнопку [Delete Group]. В результате на экране будет представлено диалоговое окно с вопросом "Do you really want to

remove the group <наименование группы>". Для подтверждения удаления необходимо нажать на кнопку [Yes], для отмены – на кнопку [No].

2.2.5 Корневая группа меню

Для просмотра группы меню, назначенной группе пользователей в качестве корневой, необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать группу, после чего затем нажать на кнопку [View Menu].

В результате на экране будет представлено окно "Menu".

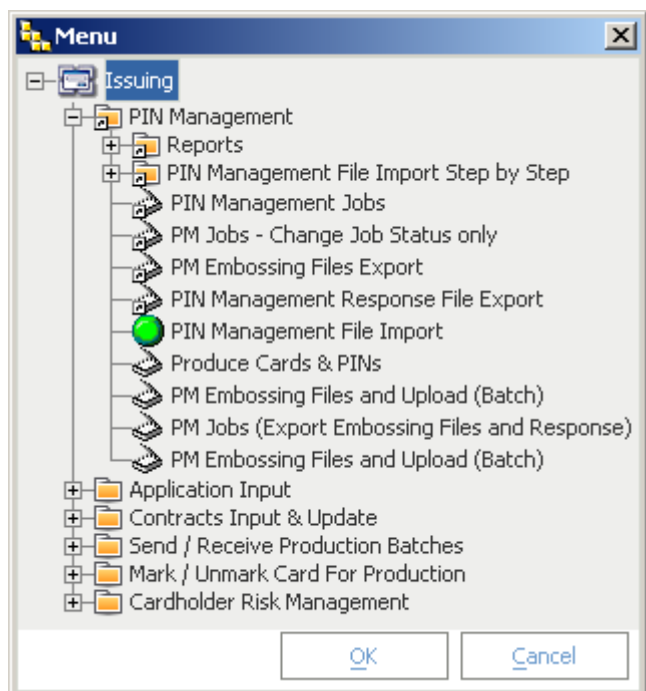


Рис. Информация о корневой группе меню

Данное окно содержит информацию о группах и пунктах меню, находящихся в корневой для данной группы пользователей группе меню.

2.2.6 Список прав, необходимых для доступа к корневой группе меню

В системе существует возможность просматривать список прав (Privilege), необходимых для доступа к корневой группе меню, а также предоставлять требуемые права доступа группе пользователей.

Для этого необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать группу, после чего нажать на кнопку [View Menu Privileges].

В результате на экране будет представлено окно "Menu privileges for <наименование пользовательской группы>".

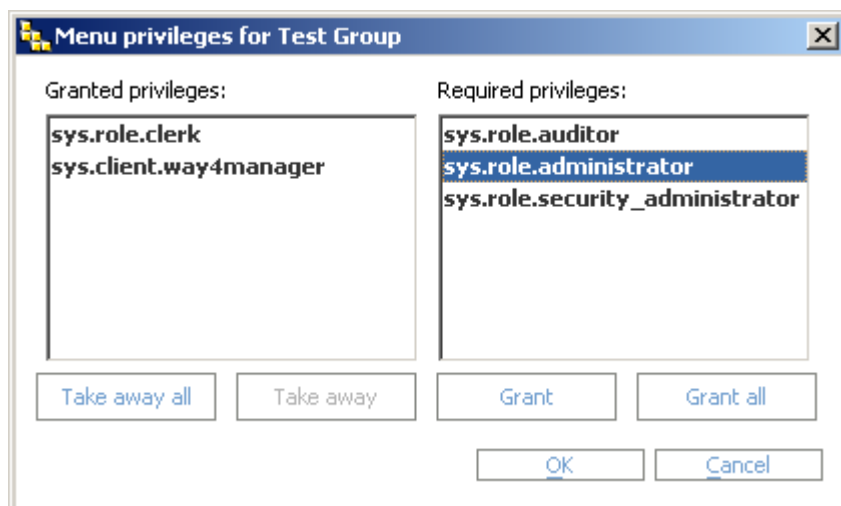


Рис. Права доступа (Privileges) для корневой группы меню

В поле *Granted Privileges* содержится список прав доступа, предоставленных группе пользователей, а в поле *Required privileges* – список прав доступа, необходимых (но не назначенных группе пользователей) для работы с корневой группой меню.

Для предоставления группе пользователей требуемых для работы с группой меню прав доступа следует в поле *Required privileges* выбрать права доступа и нажать на кнопку [Grant], для предоставления всех прав доступа – на кнопку [Grant all].

Для того чтобы запретить использование предоставленных группе пользователей прав доступа, следует в поле *Granted Privileges* выбрать права доступа и нажать на кнопку [Take away], для запрета всех предоставленных прав доступа – на кнопку [Take away all]. При этом для соответствующих прав доступа в поле *Status* формы "Group Privileges" (см. раздел "[Права доступа \(Privileges\)](#)") будет содержаться значение "Deny".

2.2.7 Обновление прав пользовательских групп

Существует ряд операций при модификации рабочего места, при которых необходимо обновление прав доступа к объектам, используемым при работе с предоставленной группой меню пользователя, для пользователей, принадлежащих данной группе пользователей. К таким операциям относятся:

- добавление новых пунктов в предоставленную группу меню;
- удаление пунктов меню из предоставленной группы меню;
- модификация экранных форм, доступных прямо или косвенно (через другую форму) из предоставленной группы меню.

После выполнения любой из вышеперечисленных операций по модификации необходимо выполнить операцию "Update Grants" для всех групп пользователей, группы меню которых были затронуты данными изменениями. Для отдельной, предварительно выбранной группы пользователей, данная операция выполняется с помощью нажатия на кнопку [Update Grants] в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)"). Нажатие на кнопку [Update Grants For All] приводит к выполнению операции "Update Grants" для всех существующих групп.

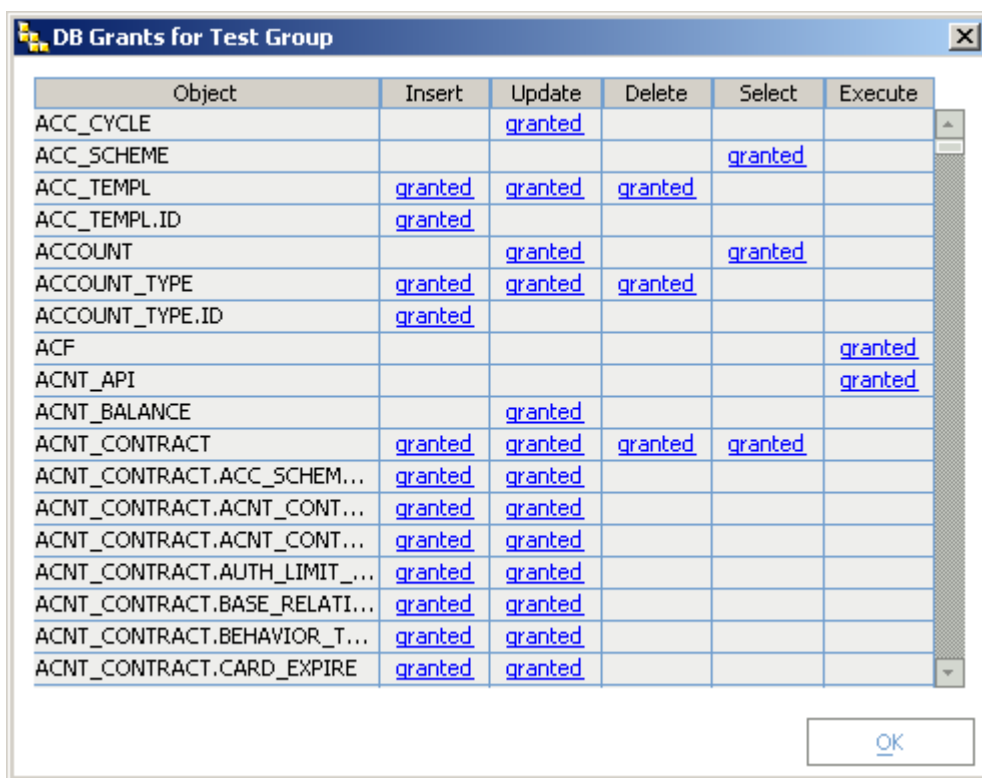


Не рекомендуется выполнять обновление прав доступа для всех групп пользователей (кнопки [Update Grants] и [Update Grants for all]) при высокой нагрузке на сервер БД Oracle, т.е. при получении и отправке большого количества транзакционных сообщений в режиме онлайн и/или выполнении длительных ресурсоемких процедур (открытие операционного дня, обработка документов, генерация отчетов и т. п.). В противном случае из-за ограничений программного обеспечения Oracle возможно получение тайм-аутов при обмене транзакционными сообщениями, и, как следствие, отказ в проведении операций.

2.2.8 Права доступа, необходимые для запуска объектов корневой группы меню

В системе существует возможность просматривать информацию о правах доступа к объектам БД (пакетам хранимых процедур, таблицам и т.д.) корневой группы меню. Для этого необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать пользовательскую группу, после чего нажать на кнопку [Show Grants].

В результате на экране будет представлено окно "DB Grants for <наименование пользовательской группы>".



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

Рис. Права доступа к объектам БД

Данное окно содержит следующие поля:

- *Object* – наименование объекта БД;
- *Insert* – права на добавление записей;
- *Update* – права на модификацию;
- *Delete* – права на удаление записей;

- *Select* – права на выборку записей;
- *Execute* – права на исполнение.

Если объекту БД предоставлены права доступа, в соответствующем поле данного окна будет содержаться значение "granted", в противном случае поле будет не заполнено.



Следует иметь в виду, что данная форма содержит список объектов и прав доступа, которые требуются для запуска форм, процессов, пайпов и т. д. Для того чтобы данные права получили все пользователи, входящие в группу, необходимо выполнить операцию "Update Grants" (см. "[Обновление прав пользовательских групп](#)").

При нажатии на ссылку "granted" в поле формы "DB Grants for <наименование пользовательской группы>" на экране будет представлена форма "Sources for Grant Object <наименование объекта БД и предоставленных прав>".

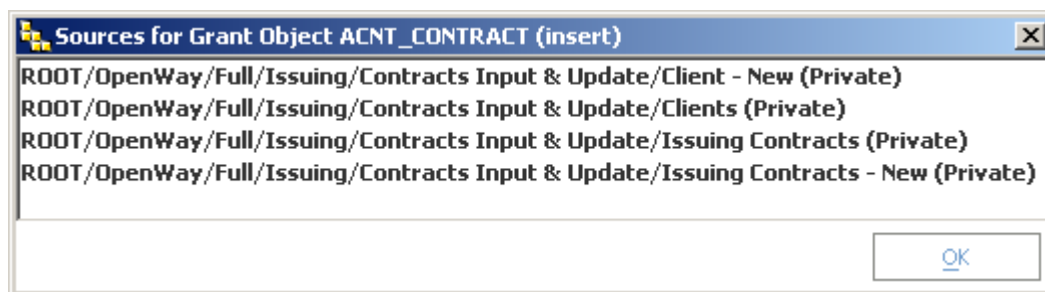


Рис. Пункты меню, которым требуются права доступа к объекту

В форме представлены пункты меню, которым требуются данные права доступа к объекту БД.

2.3 Редактирование списка пользователей

2.3.1 Создание учетной записи пользователя

Для создания новой учетной записи пользователя необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать группу или пользователя из группы, к которой новый пользователь будет принадлежать, после чего нажать на кнопку [Add User]. В результате на экране будет представлено диалоговое окно "Enter Key User Properties" с полями для ввода имени пользователя (*User Name*), пароля пользователя (*New Password*) и подтверждения пароля (*Reenter for Verification*).

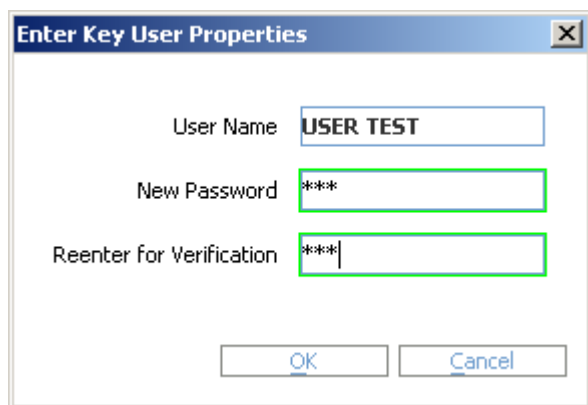


Рис. Диалоговое окно для ввода имени и пароля пользователя



Следует иметь в виду, что по умолчанию пароль, используемый пользователем для регистрации сеанса в WAY4 Manager, может также быть использован для доступа к данным с помощью любого клиентского приложения для БД. Для предотвращения получения несанкционированного доступа при необходимости данную возможность можно отключить (см. раздел "[Ограничение доступа к данным при использовании шифрования пароля пользователя](#)").

При нажатии на кнопку [OK] после заполнения полей в группе пользователей появится новая запись.

Согласно принципам обеспечения безопасности данных системы каждому пользователю предоставляется доступ в систему в соответствии с установленными для него временными параметрами, которые необходимо указывать для каждой учетной записи в поле *Working Time* (см. "[Параметры учетных записей пользователей](#)"). Таким образом, для учетной записи рекомендуется указывать временные параметры доступа при ее создании.



Следует обратить внимание, что по умолчанию в значении поля *Working Time* содержится значение "0000000", что запрещает доступ пользователя в систему в любое время.

Для завершения операции создания учетной записи пользователя необходимо нажать на кнопку [Apply] окна "User Management", чтобы сохранить изменения в БД.

В результате в БД будет создана учетная запись пользователя, которой будет назначена роль в соответствии с группой пользователя.

После этого данный пользователь сможет подключаться к БД в пределах разрешенного для работы временного интервала, используя приложение WAY4 Manager, в случае если ему предоставлены права доступа "sys.logon" и "sys.client.way4manager", либо приложение для удаленного доступа, если ему предоставлены права доступа "sys.logon" и "sys.remote_access".

2.3.2 Изменение параметров учетной записи пользователя

Система позволяет изменять любые параметры учетной записи пользователя за исключением ее уникального идентификатора, содержащегося в поле *User Name* формы "<Имя пользователя>" окна "User Management" (см. раздел ["Диалоговое окно для работы с учетными записями"](#)).

Сохранение изменений параметров учетной записи пользователя выполняется при помощи нажатия на кнопку [Apply] окна "User Management".

2.3.3 Назначение пользователю новой пользовательской группы

В системе существует возможность назначать пользователю новую пользовательскую группу.

Для этого необходимо в диалоговом окне "User Management" (см. раздел ["Диалоговое окно для работы с учетными записями"](#)) выбрать пользователя и нажать на кнопку [Move User]. В результате на экране будет представлено окно "Move User <имя пользователя>".

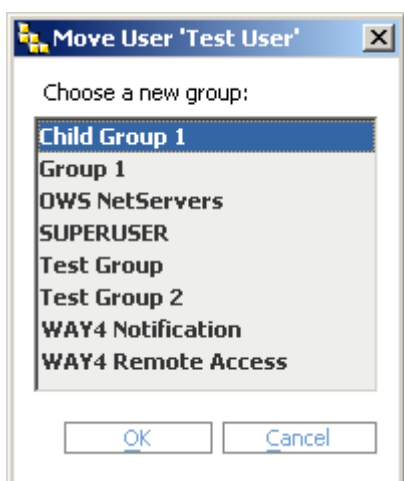


Рис. Назначение пользователю новой пользовательской группы

Для назначения пользователю пользовательской группы необходимо в поле "Choose a new group" выбрать группу, после чего нажать на кнопку [OK], для отмены назначения группы – на кнопку [Cancel].

2.3.4 Удаление пользователя из списка

Для удаления учетной записи пользователя из списка необходимо в диалоговом окне "User Management" (см. раздел ["Диалоговое окно для работы с учетными записями"](#)) выбрать пользователя, после чего нажать на кнопку [Delete User].

2.3.5 Блокирование учетной записи пользователя системы WAY4

Для того чтобы заблокировать учетную запись пользователя системы WAY4, необходимо в диалоговом окне "User Management" (см. раздел ["Диалоговое окно для работы с учетными записями"](#)) выбрать пользователя, после чего нажать на кнопку [Lock Officer]. В результате на экране будет представлено диалоговое окно с вопросом "Do you really want to perform Lock

Officer?". Для подтверждения блокирования учетной записи необходимо нажать на кнопку [Yes], для отмены – на кнопку [No].

После нажатия на кнопку [Yes] учетная запись пользователя будет заблокирована.

В системе существует возможность автоматического блокирования (разблокирования) учетной записи определенного пользователя (см. раздел "[Блокирование неиспользуемых учетных записей](#)").

2.3.6 Разблокирование учетной записи пользователя системы WAY4

Для того чтобы разблокировать учетную запись пользователя системы WAY4, необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать пользователя, после чего нажать на кнопку [Unlock Officer]. В результате на экране будет представлено диалоговое окно с вопросом "Do you really want to perform Unlock Officer?". Для подтверждения разблокирования учетной записи необходимо нажать на кнопку [Yes], для отмены – на кнопку [No].

2.3.7 Блокирование учетной записи пользователя БД Oracle



Перед блокированием пользователя БД Oracle следует заблокировать учетную запись выбранного пользователя системы WAY4 (см. раздел "[Блокирование учетной записи пользователя системы WAY4](#)").

Для того чтобы заблокировать учетную запись пользователя БД Oracle, необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать пользователя, после чего нажать на кнопку [Lock DB User]. В результате на экране будет представлено диалоговое окно с вопросом "Do you really want to perform Lock DB User?". Для подтверждения блокирования учетной записи необходимо нажать на кнопку [Yes], для отмены – на кнопку [No]. После нажатия на кнопку [Yes] учетная запись пользователя будет заблокирована, а на экране будет представлено окно с сообщением "User locked".



Перед блокированием учетной записи пользователя следует заблокировать данному пользователю права на вход в систему, т.е. для прав доступа "sys.logon" в поле Status формы "User Privileges" (см. раздел "[Права доступа \(Privileges\)](#)") необходимо указать значение "Deny". Для того чтобы функциональность блокирования пользователей БД Oracle была доступна, необходимо в системе установить дополнительный пакет "SYS.OWS_ADMINISTER_USER" (см. раздел "[Кнопки](#)").

2.3.8 Разблокирование учетной записи пользователя БД Oracle



Перед разблокированием пользователя БД Oracle следует разблокировать учетную запись выбранного пользователя системы WAY4 (см. раздел "[Разблокирование учетной записи пользователя системы WAY4](#)").

Для того чтобы разблокировать учетную запись пользователя БД Oracle, необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать пользователя, после чего нажать на кнопку [Unlock DB User]. В результате на экране будет представлено диалоговое окно с вопросом "Do you really want to perform Unlock DB User?". Для подтверждения разблокирования учетной записи необходимо нажать на кнопку [Yes], для отмены – на кнопку [No]. После нажатия на кнопку [Yes] учетная запись пользователя будет разблокирована, а на экране будет представлено окно с сообщением "User unlocked".



Перед разблокированием учетной записи пользователя следует предоставить данному пользователю права на вход в систему, т.е. для прав доступа "sys.logon" в поле Status формы "User Privileges" (см. раздел "[Права доступа \(Privileges\)](#)") необходимо указать значение "Allow". Для того чтобы функциональность разблокирования пользователей БД Oracle была доступна, необходимо в системе установить дополнительный пакет "SYS.OWS_ADMINISTER_USER" (см. раздел "[Кнопки](#)").

2.3.9 Удаление учетной записи пользователя БД Oracle

Для того чтобы удалить учетную запись пользователя БД Oracle, необходимо в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)") выбрать пользователя, после чего нажать на кнопку [Drop DB User]. В результате на экране будет представлено диалоговое окно с вопросом "Do you really want to perform Drop DB User?". Для подтверждения удаления учетной записи необходимо нажать на кнопку [Yes], для отмены – на кнопку [No]. После нажатия на кнопку [Yes] учетная запись пользователя будет удалена, а на экране будет представлено окно с сообщением "User deleted".



Для того чтобы функциональность удаления пользователей БД Oracle была доступна, необходимо в системе установить дополнительный пакет "SYS.OWS_ADMINISTER_USER" (см. раздел "[Кнопки](#)").

2.3.10 Изменение пароля пользователя

Для изменения пароля доступа пользователя к системе существует три способа:

- С помощью пункта системного меню "Database => Change Password". Данный способ описан в разделе "Пункт "Database" документа "Работа с WAY4 Manager".
- С помощью пункта меню пользователя "Full → DB Administrator Utilities → Users & Grants → Change Password". В результате на экране будет представлено диалоговое окно "Change Password".



Рис. Диалоговое окно для смены пароля пользователя

Данное диалоговое окно содержит три поля для ввода:

- *Old Password* – старый пароль;
 - *New Password* – новый пароль;
 - *Verify New Password* – подтверждение нового пароля, значение которого должно соответствовать значению поля *New Password*. После заполнения указанных полей соответствующими значениями и нажатия на кнопку [OK] пароль будет изменен.
- С помощью диалогового окна "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)"), в котором необходимо выбрать пользователя, после чего нажать на кнопку [Reset Password]. Данный способ рекомендуется использовать в случае, когда пользователь забыл старый пароль.

В результате на экране будет представлено диалоговое окно с вопросом "Do you really want to perform Reset Password?". При нажатии на кнопку [Yes] на экране будет представлено окно "Enter New User Password".

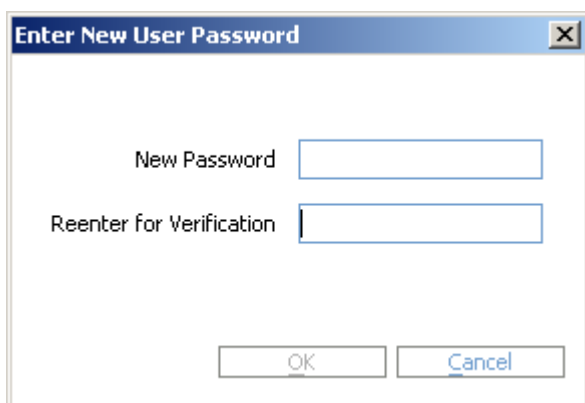



Рис. Изменение пароля пользователя

Для смены пароля следует в указанном окне ввести новый пароль в поле *New Password* и подтвердить новый пароль в поле *Reenter for Verification*, после чего нажать на кнопку [OK].


 Для параметра "FAILED_LOGIN_ATTEMPTS" СУБД Oracle рекомендуется указать значение "4" или более для ограничения количества вводов неверного пароля. Следует иметь в виду, что по требованиям стандарта PCI DSS значение данного параметра не должно превышать значения "6". Описание правил использования параметра см. в документации Oracle "Oracle® Database Security Guide" в разделе "Configuring Authentication".

Необходимо иметь в виду, что администратор информационной безопасности не может изменять пароли существующим пользователям. Данное ограничение связано с требованиями по безопасности СУБД Oracle.

2.4 Настройка дополнительных прав доступа к объектам БД для пунктов меню

В некоторых случаях, например, если в качестве пунктов меню в предоставленной группе меню пользователя содержатся пайпы либо хранимые процедуры, требующие дополнительных прав доступа к объектам БД, для данных пунктов меню требуется предоставление дополнительных прав доступа.

Данные права предоставляются для каждого отдельного подпункта определения пункта меню (см. раздел "Работа с редактором определений пунктов меню" документа "Редактор меню WAY4 Manager") в виде пакетов прав.

 При работе с приложением WAY Manager редактирование стандартных пунктов меню эталонной поставки запрещено. Редактированию подлежат только созданные пользователем пункты меню либо копии стандартных пунктов меню (см. документ "Редактор меню WAY4 Manager").

2.4.1 Настройка пакетов прав

Для просмотра, удаления, редактирования и создания пакетов прав необходимо вызвать пункт меню "Full → DB Administrator Utilities → Users & Grants → Subitem Security Grants". В результате на экране будет представлена форма "Subitem Security Grants".

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













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

Рис. Настройка пакетов дополнительных прав доступа к подпунктам меню

В поле *Name* данной формы указано наименование пакета прав.

В поле *Available For* – роли пользователей, которым предоставлены права на использование данных прав доступа:

- "Clerk" – операторам;
- "Clerk & Auditor" – операторам и аудиторам.

Для отключения очистки записей о пакетах прав, которым больше года, следует в поле *Keep From Housekeeping* выбрать значение "Y". По умолчанию значение данного поля "N".



Очистка журнала регистрации пользователей в системе и/или истории изменений осуществляется автоматически средствами модуля WAY4 Housekeeping (см. документ "Housekeeping в системе WAY4™").

Для настройки прав доступа к объектам БД (пакетам хранимых процедур, таблицам и т.д.) предназначена форма "Obj Grants for <наименование пакета прав>", которая вызывается при нажатии на кнопку [Obj Grants].

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

Рис. Форма для настройки прав на объекты базы данных

В поле *Object Name* данной формы путем выбора из списка указывается название объекта БД, а в поле *Grant* – права доступа к данному объекту:

- "UPDATE" – модификация;
- "INSERT" – добавление записей;
- "DELETE" – удаление;
- "EXECUTE" – исполнение;
- "SELECT" – выборка.



На вышеприведенном Рисунке примере пакет состоит из прав на три объекта – два пакета хранимых процедур и одна таблица БД.

В системе существует возможность выдавать права не на всю таблицу целиком, а только на определенные столбцы. Для этого используется форма "Col Grants for <наименование пакета прав>", которая может быть вызвана с помощью нажатия на кнопку [Col Grants] формы "Subitem Security Grants".

Col Grants for Pipe: Balance Import			1 of 1		
	Table	Column			
▶	ACNT_CONTRACT	SHARED_BALANCE			

Рис. Форма для настройки прав доступа к отдельным столбцам таблиц БД

Данная форма содержит следующие поля:

- *Table* – имя таблицы БД;
- *Column* – наименование столбца соответствующей таблицы.



В случае если в форме "Col Grants for <наименование пакета прав>" для таблицы присутствует хотя бы одна запись, права, определяемые с помощью формы "Obj Grants for <наименование пакета прав>", будут выданы только на указанные столбцы.

2.4.2 Назначение пакета дополнительных прав подпункту меню

Назначение пакета дополнительных прав подпункту меню

Назначение пакета дополнительных прав подпункту определения пункта меню производится в форме "Subitems" окна редактора определений пунктов меню (см. раздел "Работа с редактором определений пунктов меню" документа "Редактор меню WAY4 Manager").

Пакет дополнительных прав доступа выбирается из списка в поле *Security* для подпункта определения пункта меню. Подробнее см. раздел "Редактирование подпунктов меню" документа "Редактор меню WAY4 Manager".

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



 **Add Subitem**
 **Delete Subitem**
Down **Up** **Duplicate Subitem**

Рис. Пример назначения пакета дополнительных прав доступа для подпункта меню

2.5 Инициализация локальных переменных

Значения локальных переменных (Local Constants) используются для фильтрации данных, доступных при работе в формах WAY4 Manager (см. раздел "Окно редактора форм. Вкладка "Fields"" документа "Редактор форм WAY4 Manager").

Инициализация локальных переменных выполняется при регистрации сеанса работы пользователя. При этом используются значения, заданные для группы, к которой принадлежит данный пользователь.

Присвоение значений для инициализации локальных переменных осуществляется в форме "User Constants for <наименование группы пользователей>", доступной при нажатии на кнопку [Edit User Constants] в диалоговом окне "User Management" (см. раздел "[Диалоговое окно для работы с учетными записями](#)").

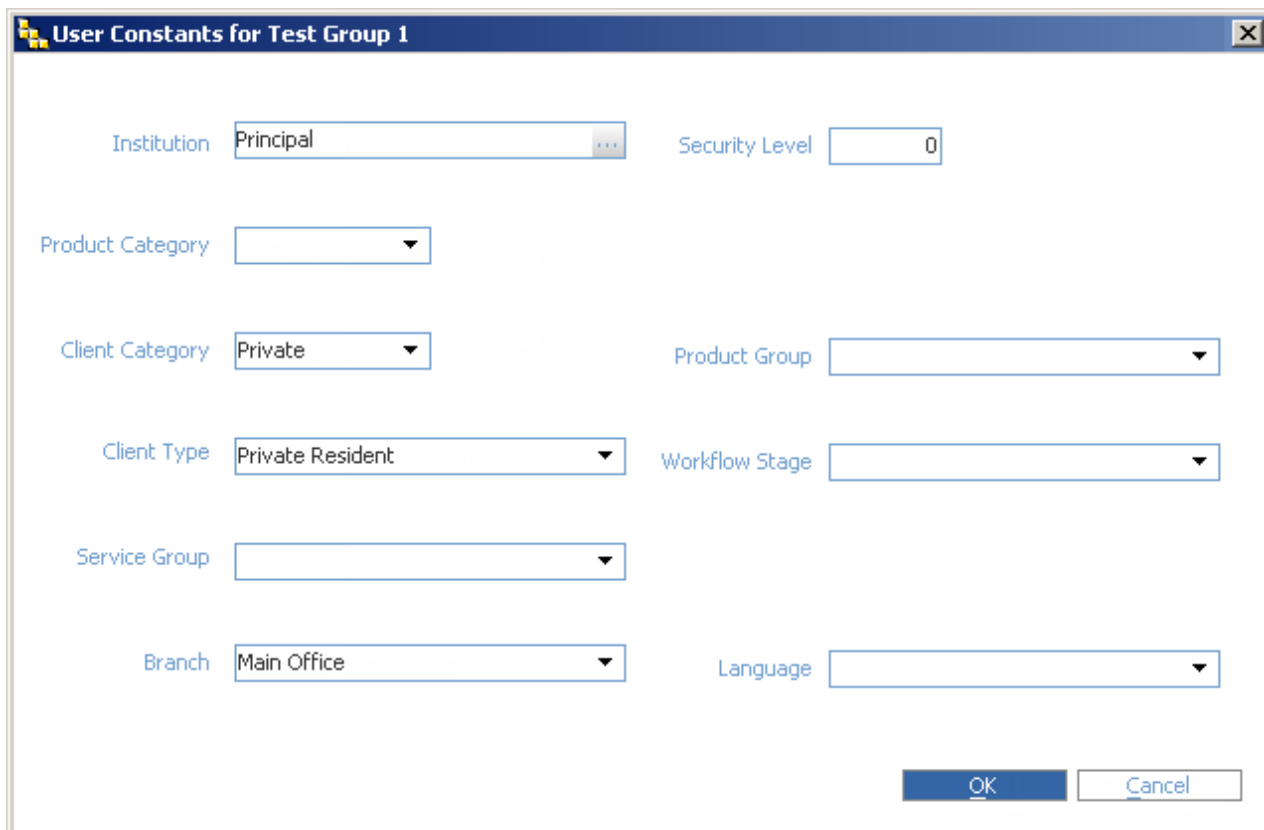


Рис. Инициализации локальных переменных для группы пользователей

В данной форме доступны следующие поля:

- *Institution* – наименование финансового института;
- *Product Category* – тип Продукта;
- *Client Category* – категория клиента;
- *Client Type* – тип клиента;
- *Service Group* – дополнительная классификация клиентов;
- *Branch* – подразделение (филиал) финансового института;
- *Security Level* – уровень допуска; данное значение используется при фильтрации доступных пользователю типов команд, посылаемых на банкомат с помощью консоли;
- *Product Group* – группа продукта; значение данного поля используется расширенным модулем загрузки заявлений;
- *Workflow Stage* – зарегистрированный тип этапа обработки заявлений; значение данного поля используется расширенным модулем загрузки заявлений (Advanced Applications);
- *Language* – язык для отчетов, поддерживающих формирование на национальном языке.

После инициализации значения локальных переменных могут быть переопределены с помощью специальных модальных форм, а также подпунктов определений пунктов меню типа "Assignment" (см. раздел "Тип "Assignment" документа "Редактор меню WAY4 Manager").

3 Протоколирование

В данном разделе описаны принципы протоколирования изменений, вносимых в данные пользователями при работе с системой, а также принципы протоколирования регистрации пользователей в системе.

3.1 Протоколирование работы процессов

Выполнение процессов в системе WAY4 регистрируется в журнале выполнения процессов (Process Log). Для каждого процесса регистрируются параметры запуска, текущая банковская дата, пользователь, запустивший процесс, дата и время запуска и завершения процесса, а также, в случае если процесс был принудительно завершен, пользователь, прервавший выполнение процесса.

Подробнее протоколирование работы процессов описано в разделе главе "Процессы в WAY4 Manager" документа "Работа с WAY4 Manager".

Протоколирование изменений, произведенных в табличных формах

3.2 Протоколирование изменений, произведенных в табличных формах

Протоколирование изменений, произведенных в табличных формах

Каждое изменение, вносимое пользователем в разрешенные для редактирования поля табличной форм, регистрируется в системе WAY4 в журнале изменений записей. Для любой табличной формы можно по каждой записи получить информацию об истории ее изменений.

Для доступа к журналу истории изменений следует для требуемой записи выбрать пункт системного меню "Special => View Record History" или нажать комбинацию клавиш <Ctrl>+<Shift>+<H>.

В результате на экране будет представлена дополнительная форма "<Наименование табличной формы> – history for <...>".

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

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

Рис. Пример истории изменения записи

В дополнительной форме будут представлены список "версий" выбранной записи и информация о дате изменения и пользователе, внесшем данное изменение.

3.3 Восстановление удаленных записей

Для просмотра удаленных записей табличной формы используется пункт системного меню "Special => View Deleted" или комбинация клавиш <Ctrl>+<Shift>+<D>.

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

Рис. Пример просмотра удаленных записей

Восстановление удаленной записи производится при помощи предварительного выбора нужной удаленной записи из списка с последующим нажатием на кнопку [Undelete].

3.4 Журнал регистрации пользователей в системе

При установке соединения для пользователя WAY4 Manager с БД системы создается запись в таблице "Login History" журнала регистрации пользователей, включающая имя рабочей станции, с которой устанавливалось соединение, а также дату и время установки соединения. При завершении работы с WAY4 Manager в данную запись заносится также дата и время завершения работы.

Доступ к журналу осуществляется с помощью выбора пункта меню пользователя "Full → DB Administrator Utilities → Users & Grants → Login History".

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

Рис. Пример журнала регистрации пользователей в системе

Во время одного сеанса работы при выполнении некоторых процессов (запуск пайпов, удаление записей, обработка документов и т. д.) в таблице "Login History" создаются несколько записей, информации о которых доступна в форме "Processes for <...>", открывающейся при нажатии на кнопку [Processes] в форме "Login History".

Processes for TEST1, WAY4 Manager							
	Process Name	Started	Finished	Status	Parameters	Bank Date	Started By
1	Apply Product Changes	10/5/10 10:58:32 AM	10/5/10 10:58:32 AM	Closed	PARALLEL=1...	9/2/2010	SUPERUSER
2	Renew Product	10/5/10 10:58:30 AM	10/5/10 10:58:31 AM	Closed	Test	9/2/2010	SUPERUSER

Рис. Процессы, стартовавшие за время одного сеанса работы

При нажатии на кнопку [Aux for] в форме "Login History" на экране будет представлена форма "Aux for <...>".

Aux for for TEST1, WAY4 Manager group.com, WAY4						
	Process Log	Attached Role	Attached	Detached	Status	DBMS Specific
1	Set New Banking Date AUX		10/5/10 3:12:49 PM	10/5/10 3:13:02 PM	Closed	SID=386;SER=12399;SPID=26105;LOGON=20101005151248;

Рис. Процессы, порожденные другими процессами

Данная форма содержит информацию о процессах, которые были автоматически созданы в результате выполнения других процессов.



Очистка журнала регистрации пользователей в системе и/или истории изменений осуществляется автоматически средствами модуля WAY4 Housekeeping (см. документ "Housekeeping в системе WAY4™").

3.5 Блокирование неиспользуемых учетных записей

Согласно стандарту PCI DSS необходимо блокировать учетные записи пользователей, которые длительное время (более 90 дней) не регистрировались в системе. Кроме того, в системе существует возможность временно блокировать учетные записи пользователей.

Список зарегистрированных в системе пользователей доступен в форме "Officers", вызываемой на экран при выборе пункта меню "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Officers".

Officers										
	User Id	Is Active	Status	Security Administrator	Name	Working Time	Special Enabled	Last Login Time	Inactive From	Inactive To
1	TECHWR2_A	Yes	Administrator	Yes	SUPERUSER		Yes	10/6/10 1:31:22 PM		
2	TEST USER 1	Yes	Administrator	No	Test User 1	1111100	Yes	10/6/10 11:10:13 AM		
3	USER 2	No	Clerk	No	User 2	1101100	Yes	10/6/10 1:54:35 PM	10/6/2010	11/6/2010
4	USER 3	No	Administrator	Yes	User 3	1100111	No	10/6/10 11:14:50 AM		
	USER 4	Yes	Administrator	Yes	User 4	1111100	Yes	10/6/10 11:15:27 AM		

Рис. Список зарегистрированных в системе пользователей

В полях *Inactive From* и *Inactive To* можно указать временной интервал блокирования учетной записи пользователя.

Для выполнения блокирования учетных записей используется пункт меню "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Lock Inactive Officers". При выборе данного пункта меню вызывается хранимая процедура, которая проверяет дату последней регистрации в системе каждого зарегистрированного пользователя, и если с этого момента прошло больше допустимого количества дней, для данной учетной записи отменяются все права доступа к объектам базы данных, а также указывается значение "No" в поле *Is Active*. С помощью данной хранимой процедуры будут также заблокированы те учетные записи, которые не являются заблокированными и для которых текущая системная дата попадает в интервал, заданный в полях *Inactive From* и *Inactive To*. Кроме того, будут разблокированы учетные записи, для которых текущая системная дата превышает дату, указанную в поле *Inactive To*.

Для фиксирования даты и времени последней регистрации в системе служит поле *Last Login Time*.

В поле *Special Enabled* указано предоставлен ли пользователю доступ (значение "Yes") к пункту системного меню "Special" (см. раздел "Использование системного меню" документа "Работа с DB Manager").

Для указания количества дней, по прошествии которых с момента последней регистрации пользователя в системе следует заблокировать данную учетную запись, используется глобальный параметр "OFFICER_MAX_INACTIVITY_DAYS" (см. раздел "OFFICER_MAX_INACTIVITY_DAYS" документа "Глобальные параметры системы WAY4"). По умолчанию для данного параметра указано значение "90" согласно рекомендации 8.5.5 стандарта PCI DSS.

Для автоматизации ежедневного запуска пункта меню "Lock Inactive Officers", служит процесс, который запускается на выполнение при выборе пункта меню "Full → DB Administrator Utilities →

Users & Grants → Inactive Officers → Start Inactive Officers Monitor". Информация о выполнении данного процесса отражается в журнале выполнения процессов. Остановку данного процесса можно осуществить с помощью выбора пункта меню "Full → DB Administrator Utilities → Users & Grants → Inactive Officers → Stop Inactive Officers Monitor".

В системе существует возможность блокирования (разблокирования) учетной записи определенного пользователя. Для этого необходимо в форме "Officers" выбрать пользователя, после чего нажать на кнопку [Control] и в контекстном меню выбрать пункт "Lock" ("Unlock"). В результате учетная запись пользователя будет заблокирована (разблокирована), а в поле *Is Active* будет указано значение "No" ("Yes").



В случае если пользователь был разблокирован, в поле *Last Login Time* будут указаны дата и время разблокирования.

Кроме того, существует возможность одновременно с блокированием (разблокированием) учетной записи пользователей системы WAY4 блокировать учетные записи пользователей БД Oracle. Для этого необходимо в форме "Additional Global Parameters" (Full → Configuration Setup → Main Tables → Additional Global Parameters) добавить глобальный параметр "SY_OFFICER_USE_DB_RIGHTS" и указать для данного параметра значение "Y".



Следует иметь в виду, что пользователи, у которых в поле *Status* указано значение "Application" (учетные записи, используемые для приложений, например, NetServer, Планировщик), не могут быть заблокированы. Также не может быть заблокирован пользователь с именем "SUPERUSER".

4 Права доступа к каталогам системы WAY4

В данном разделе приведено описание стандартных каталогов системы WAY4, а также права доступа к данным каталогам различных пользователей системы.

4.1 Стандартные каталоги системы WAY4

В системе WAY4 существуют следующие стандартные каталоги:

- <OWS_HOME> – основной каталог системы, содержащий эталонную структуру подкаталогов и файлов, одинаковую для всех основных каталогов системы одной и той же версии; структура данного каталога не подлежит изменению в процессе работы системы; данный каталог следует размещать на файловом сервере системы WAY4;



Изменение содержимого каталога <OWS_HOME> допустимо только при проведении модернизации системы (upgrade).

- <OWS_WORK> – каталог системы, содержащий структуру, частично аналогичную структуре каталога <OWS_HOME>, включающую в себя различные настроечные файлы, файлы данных, специфичные для конкретной конфигурации системы WAY4, файлы экранных форм, пунктов меню и отчетов, созданных пользователем, и т. д.; данный каталог следует размещать на файловом сервере системы WAY4;
- "<...>\Documents and Settings\<имя пользователя>\.OWS\<наименование БД>" – каталог системы, предназначенный для хранения временных файлов, создаваемых в процессе работы приложения WAY4 Manager, а также файлов журнала ошибок (см. раздел "Каталог временных файлов" документа "Работа с WAY4 Manager").

Каталоги <OWS_HOME> и <OWS_WORK> являются общедоступными для всех пользователей системы WAY4 и должны быть расположены на файловом сервере.

4.2 Права доступа к стандартным каталогам системы WAY4

При установке приложения WAY4 Manager на файловом сервере всем пользователям системы должны быть предоставлены права на чтение файлов основного каталога системы (<OWS_HOME>), а также права на чтение файлов рабочего каталога (<OWS_WORK>).

В зависимости от задач, выполняемых пользователями, последние могут быть разбиты на классы, каждому из которых требуются полные права на доступ к стандартным каталогам системы WAY4 либо к их подкаталогам.

Табл. Права доступа к каталогам системы, необходимые для пользователей различных классов

Класс пользователей	Обязанности	Каталог
Администраторы	Модернизация (upgrade) системы WAY4	<OWS_HOME>, <OWS_WORK>
	Создание и редактирование экранных форм, пунктов меню, определений пунктов меню и пользовательских представлений	<OWS_WORK>\Client\WAY4Manager\components\dbm.module
Операторы	Выпуск карт	<OWS_WORK>\Data\Card_Prd
	Организация взаимодействия с международными платежными системами	<OWS_WORK>\Data\Interchange
	Обеспечение взаимодействия с банковскими системами	<OWS_WORK>\Data\RBS
	Создание отчетов	<OWS_WORK>\Data\Reports



Следует иметь в виду, что каталоги "<OWS_WORK>\Data\Interchange" и "<OWS_WORK>\Data\RBS" используются для выгрузки с последующей передачей (trasit) файлов при взаимодействии с платежными и банковскими системами. Настоятельно рекомендуется использовать вместо данных каталогов, каталоги на виртуальном диске (RAM disk); использование энергонезависимых носителей в данных целях запрещено. При каждой инициализации виртуального диска, выполняемой, например, после перезагрузки компьютера, необходимо восстанавливать структуру каталогов на данном диске.

Для перенаправления выгрузки необходимо указать в параметрах "INTERCHANGE_PATH" и "RBS_INTERCHANGE_DIR" секции [Client.DBM.Params] файла "<OWS_WORK>\db.ini" путь к соответствующему каталогу на шифрованном носителе.

Для ограничения доступа к трассировке стека ошибок пользователям типа "Оператор (Clerk)" следует для параметра "SHOW_ERROR_STACK_TRACE" секции [Client.DBM.Params] файла "<OWS_WORK>\db.ini" задать значение "no".

5 Ограничение доступа к данным при использовании шифрования пароля пользователя

По умолчанию пароль, используемый пользователем для регистрации сеанса в WAY4 Manager, может также быть использован для доступа к данным с помощью любого клиентского приложения для БД.

При необходимости для доступа к данным БД может быть использован пароль, полученный в результате шифрования пароля для регистрации сеанса в WAY4 Manager с помощью криптографической величины (ключа). Таким образом, доступ к БД с использованием известного пользователю пароля возможен только через WAY4 Manager, поскольку для доступа к БД фактически используется не то значение пароля, которое пользователь вводит при запуске WAY4 Manager, а зашифрованное, которое неизвестно пользователю.

Ключ шифрования пароля может быть определен с помощью параметра "PWD_ENCRYPTION" или "PASSWORD_ENCRYPTION" (при работе с системой WAY4 с удаленного рабочего места, используя приложение WAY4 Remote Access) секции [Client.DBM.Params] файла "db.ini", расположенного в каталоге <OWS_WORK>; параметр необходимо указывать в следующем виде:

```
PWD_ENCRYPTION=<ключ шифрования>
```

или при работе с удаленного рабочего места (WAY4 Remote Access):

```
PASSWORD_ENCRYPTION=<ключ шифрования>
```

В теле ключа шифрования могут использоваться ASCII-символы с кодами из диапазона от 33 до 127. Длина ключей может быть до 256 символов.



Если значение ключа шифрования не указано (или указана пустая строка), шифрование пароля для доступа к БД не осуществляется. Пароль главного администратора безопасности ("OWS_A") не шифруется даже при заданном параметре "PWD_ENCRYPTION". По истечении срока действия пароля главного администратора безопасности смену пароля нужно осуществлять через БД.

Ключ шифрования также можно указывать в параметре запуска приложения WAY4 Manager:

```
<OWS_HOME>\client\way4manager\dbmanager\way4manager.exe PWD_ENCRYPTION=<ключ шифрования>
```

6 Отчет "Amendment Report"

Отчет "Amendment Report" используется для мониторинга изменений, которые вносил пользователь в таблицы БД. Данный отчет содержит информацию об изменениях в таблицах, внесенных выбранным пользователем за определенный промежуток времени.

Для формирования отчета необходимо выбрать в меню пользователя пункт "Full → DB Administrator Utilities → Users & Grants → Amendment Report". В результате на экране будет представлена форма "Amendment Report".

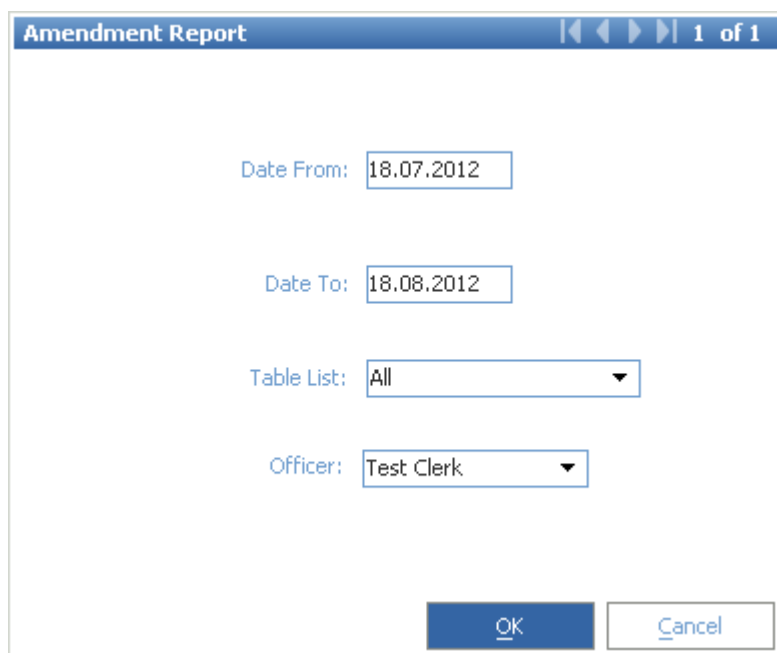


Рис. Задание параметров отчета

Данная форма содержит следующие поля:

- *Date From* – дата начала периода формирования отчета;
- *Date To* – дата окончания периода формирования отчета;
- *Table List* – поле с выбором из списка для указания таблицы (таблиц), для которой будет формироваться отчет;
- *Officer* – поле с выбором из списка для указания пользователя, для которого будет формироваться отчет.

После заполнения полей формы необходимо нажать на кнопку [OK]. В результате будет запущен процесс формирования отчета, по окончании которого сформированный отчет будет представлен в браузере.



Следует иметь в виду, что формирование отчета может занимать длительное время.

В первой строке сформированного отчета будет указано наименование отчета, во второй – информация об отчетном периоде, пользователе и списке таблиц, для которых создан отчет. Далее в отчете идут разделы, содержащие информацию об изменениях в таблицах. Каждый раздел содержит заголовок "Table name: <наименование таблицы>" и таблицу, включающую следующие поля:

- *Id* – идентификатор записи в таблице, для которой были сделаны изменения;
- *Officer* – пользователь, внесший изменения;
- *Date* – дата внесения изменений;
- *Action* – действие (например, "Add" – добавление нового значения, "Del" – удаление значения);
- *Column* – наименование поля таблицы БД;
- *Old value* – старое значения поля таблицы БД;
- *New value* – новое значение поля таблицы БД.