

User Operations

1. User Operations Module

The User Operations Module is the module where the users of the programme are defined, module or programme authorisations are assigned for the defined users or user groups and security applications and parameters related to the defined users are specified.

2. Record

This is the module where the User Names and Passwords specific to every user can be defined, and where the authorisations for the Select, Insert, Update and Delete operations can be defined individually for every user.

2.1. User Group Records

In this Module, as it is possible to define the permissions for individually every user, it is also possible to gather users in groups and define permissions for the users collectively as a group. This facilitates the operation in that it allows for defining the permissions only for a related group instead of processing the definitions one by one for every user. Users acquire the permissions defined for the group in which they are included. For example, if the users in the Sales Department have the same permissions in the modules, then a single User Group Record can be defined for the Sales Department and all of the users in the Sales Department can be included in this group.

User Group Records

Group Member Users Group Permissions

Group Code: 01

Grp Descr: Purchase

Group Code	Grp Descr
>> 01	Purchase
02	Accounting
04	Support

Group Code

In this field, you should enter the code for the group you define. When adding the users to the groups you will use the code you indicate in this field.

Group Description

In this field, you can enter the explanation for the group code that you defined.

Group Member Users

In this field, you can view the users that are included in the related group.

Group Member Users

Group Code: 01

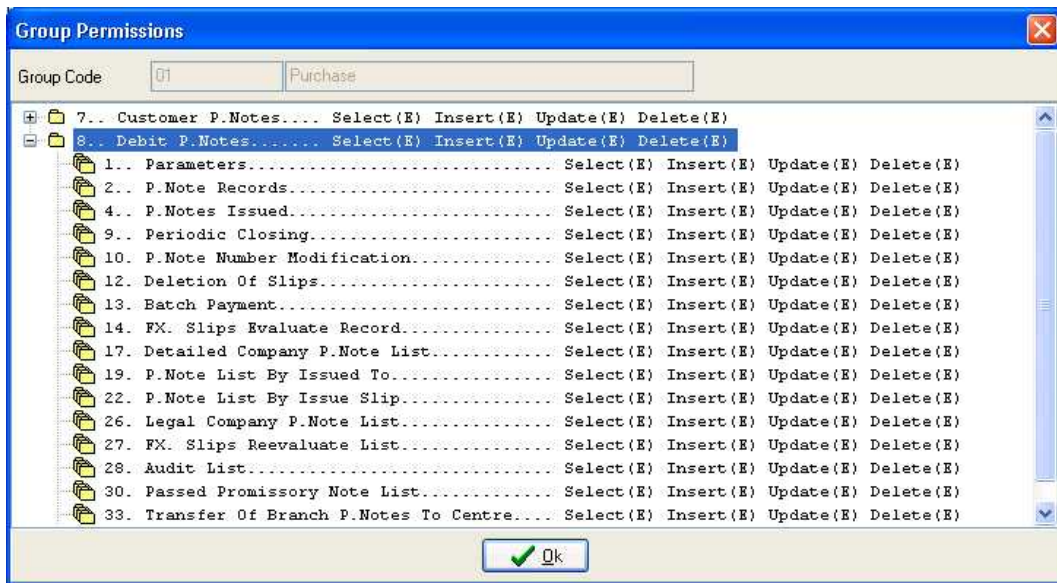
Grp Descr: Purchase

User Seq.No And Name	User Name	Name/Sur.
12	GÜLSEREN	GÜLSEREN SEREL
47	ARZU	ARZU YILDIZ

Ok

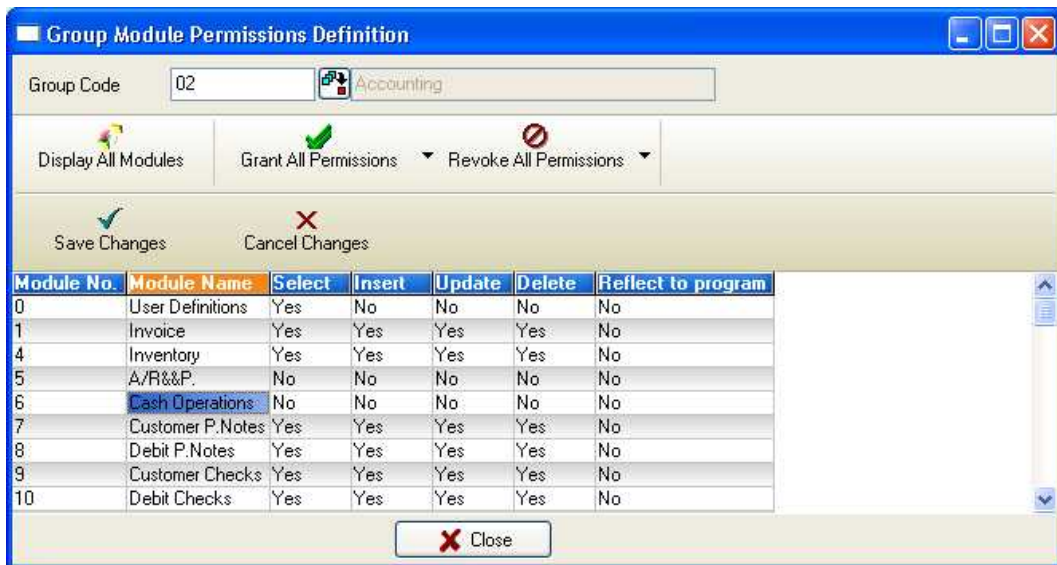
Group Permission

In this field, you can monitor the modules, the module menus and the permissions in the modules or menus that are defined for a certain group.



2.2. Group Module Permissions Definition

In this section, the permissions for the groups, which are defined in the User Group Records, can be specified individually according to modules.



Module No

In this field, you can view the number of the module for which you will define permissions.

Model Name

In this field, you can view the name of the module for which you will define permissions.

Select, Insert, Update, Delete

You can double-click in the related fields and choose between the *Yes* and *No* options. Choosing the *Yes* option indicates that the permission is given to the related user and choosing the *No* option indicates that the permission is taken from the related user.

Reflect to Program

After the permissions for the modules are defined, you should select the *Yes* option in the *Reflect to Program* field in order to apply the definition to all submenus of the programme, i.e. to the *Group Program Permission Definitions* menu.

Display All Modules

This field enables you to display all modules with a single key, instead of adding one by one every module for which the permissions will be defined.

Grant All Permissions

This field selects the *Yes* option for all four of the *Select, Insert, Update, Delete* fields, in other words, grants all permissions.

Revoke All Permissions

This field selects the *No* option for all of the *Select, Insert, Update, Delete* fields, in other words removes all permissions.

Save Changes

You should use this field to save the permissions definitions that you entered. If you do not use the Save key, the programme will not store the modifications that are processed in this section.

Cancel Changes

This field undoes the last definitions entered. When you use this key, all fields will be reversed to their previous state.

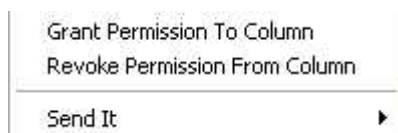
Close

This key closes the active window.

Function Keys

If you permission click when the cursor is on the *Module Name* field, the *Grant Permission to Column* and *Revoke Permissions from Column* options will be displayed. With these options, you can assign (grant) or remove (revoke) the *Select, Insert, Update* and *Delete* permissions as a whole for the active module.

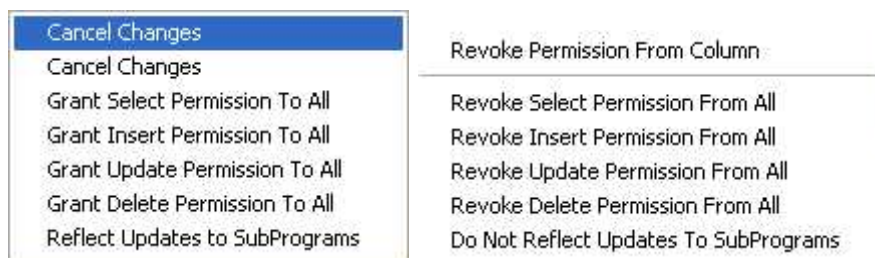
With the *Send It* option, you can transfer the information in the Grid window to the Excel, Word, Calculator, and Writer programmes. **For detailed information, please see [Introduction/Grid/Send It](#).**



If you permission click when the cursor is on the *Select, Insert, Update* and *Delete* columns, you can collectively give assign (Grant) or remove (revoke) permissions on column basis for all of the modules in the window. For example, if you permission-click when the cursor is on the Insert column, the window will change to the *Grant Permission to Column* and *Revoke Permissions from Column* window or if you permission-click when the cursor is on the Delete column, the window will change to the *Grant Delete Permission to All* and *Revoke Delete Permission from All* window. With the *Send It* option, you can transfer the information in the Grid window to the Excel, Word, Calculator, and Writer programmes. **For detailed information, please see [Introduction/Grid/Send It](#).**



With the options located to the permission of the *Grant All Permissions* and *Revoke All Permissions* fields, you can define permissions on both rows and columns basis. When you select the *Reflect Updates to Subprograms* and *Do not Reflect Updates to Subprograms* options, the permissions modifications you entered on rows or columns basis will be reflected to the submenus in the related modules.



2.3. Group Program Permissions Definition

In the *Group Module Permission Definition* menu, permissions were defined on basis of modules. This section enables further definitions of these permissions for the submenus of the related modules.

Group Program Permissions Definition

Group Code: 02 Accounting

Module No.: 12 General Ledger

Display All Programs Grant All Permissions Revoke All Permissions

Save Changes Cancel Changes

Program Number	Program Name	Select	Insert	Update	Delete
1	Parameters Entry	Yes	Yes	Yes	Yes
2	Account Plan	Yes	Yes	Yes	Yes
3	Group Code Records	Yes	Yes	Yes	Yes
4	Voucher Records	Yes	Yes	Yes	Yes
5	Voucher Explanations Records	Yes	Yes	Yes	Yes
6	Reference Code Records	Yes	Yes	Yes	Yes
7	Allocation Records	Yes	Yes	Yes	Yes
8	Voucher Number Modification	Yes	Yes	Yes	Yes

Close

Group Code

This is the field where you enter the code of the group for which you define permissions.

Module No

This is the field where you enter the number of the module which you will define permissions for its submenus.

The keys that are used for assigning permissions in the Group Module Permissions Definition menu serve for the same function also in the Group Program Permissions Definition menu. [For detailed information, please see User Definitions/Group Module Permissions Definition.](#)

2.4. User Records

This is the field where you can define the user names and passwords, and some further definitions.

User ID	User Name	Name/Sur.	Admin.?	Last Password C	Password Expira	E.Mail
1	NETSIS	Ayşe	E	05/02/2006	0	aliyilmaz@abc.com.tr
2	FATIH	Fatih	H	12/04/2004	0	

User ID

The user who is making the definitions must fill this field and assign this number for the users. A number, which is previously used for one user, cannot be later assigned to another user. A different number should be entered for every user.

User Name

You should enter the user name in this field. The name, which will be queried when logging into the related company, should be entered in this field. The same name cannot be used twice.

Name/Surname

This is the field where the Name and Surname of the defined user should be entered for information purposes.

Group Code

If the related user will be included in a certain group, then you should enter the related Group Code that is previously defined in the User Group Records in this field. A user can be defined in only one group or may not be included in any group.

When defining a group for a user, the program displays the query of *"This user has special permissions. Delete?"* If you confirm the deletion, all of the permissions that are previously defined for that user will be deleted and the user will have the permissions defined for the group of which he/she is a member. If the user is included in a group and special program permissions are additionally defined for the user, then priority will be given to the special permissions. For example, let us assume that you have defined a "LEDGER" group and this group has all of the permissions (*Select, Insert, Update, Delete*) to process the General Ledger Module. Let us further assume that user id 2 is defined in the "LEDGER" group. Additionally, user id 2 is given only the *Select* permission in the chart of accounts in the General Ledger

Module. In this case, user id 2 will be able to only monitor the chart of accounts records and will not be allowed to Update, Delete or Insert operations the chart of accounts (even though that user is included in the LEDGER group and has the permissions defined for the LEDGER group.)

Password

This field is for defining the user's password. The password, which will be queried when logging into the related company, should be entered in this field.

Last Password Change Date

In this field, you can view the date when a user has last changed his/her password. The programme inserts this information automatically.

Password Expiration Period (D)

Users are required to change their passwords at the end of this period. The period should be defined as days. For example, if you want that users work with the same password for 15 days and not be able to log in with the password after the 15th day, then you should enter 15 in this field.

E-mail Address

If the *E-Mail Application* is used in the programme, then some operations can be forwarded to the users via e-mails. In order to be able to send the information to the users, their e-mail addresses should be entered in this field.

Unlimited Internet User

Users, for which this parameter is selected, will be able to use e-mail operations for not only a single current account but will be able to receive (reporting) and send (give orders) information for all current accounts. Users, for which this parameter is not selected, will be able to use only the information send and receive functions for the specific current account that is enabled for them.

Admin?

When this box is checked, the programme understands that the related user is the *Admin*. The Admin user can work in every module regardless of permission and date limitations. Since Admins are granted all permissions in full, permissions definitions are not required in the User Module and User Program Permissions Definitions windows for such users. Additionally, an Admin user will not be included in the *Date Locking* system. The user named Netsis is always the Admin. This cannot be modified or deleted. Only the password for this user can be changed in order to prevent unauthorised usage. It is possible to also create other Admin users. Ro-based or field-based security applications will be applied as regularly done for other users.

Record Color

In this field, you can define colours for users. In this case, the information entered by every user in the programme will be displayed in the grid information in the colour that is assigned to the user in this section. For example, you will be able to identify by which user the related record was modified, by looking at the colour of the grid in the Current Account Transaction Records section. The upper permission field in the User Records

window allows you to attach images or documents as desired. [For details on attaching pictures-files, please see Introduction/Add Picture-File.](#)

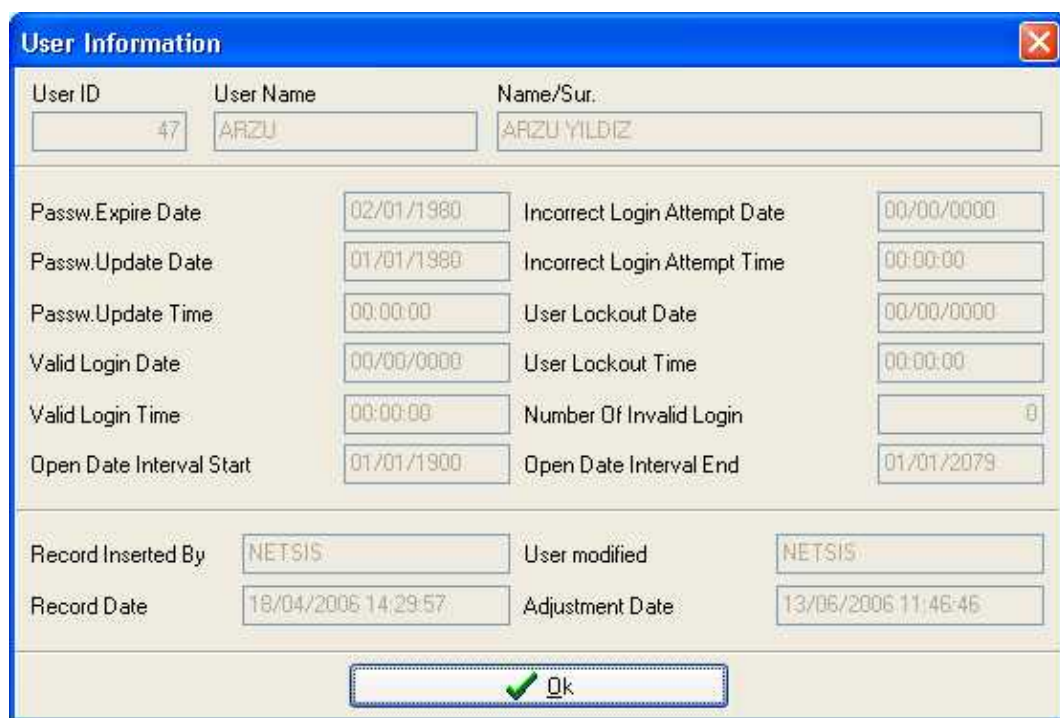
Shortcut Keys

In the upper part of the User Records window, there are some shortcut keys for monitoring several fields and processing several operations.



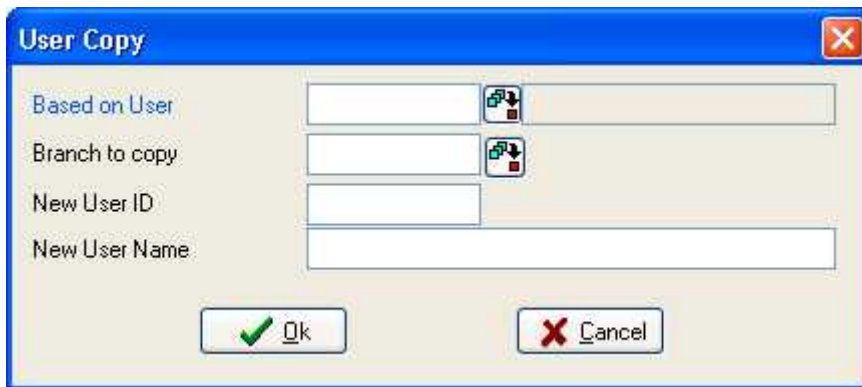
User Information

This is the section where you can monitor the fields and the user information that are defined in the User Parameters section.

A screenshot of a software window titled "User Information" with a blue title bar and a close button (X) in the top right corner. The window contains several input fields for user data. At the top, there are three fields: "User ID" with the value "47", "User Name" with "ARZU", and "Name/Sur." with "ARZU YILDIZ". Below these are two columns of date and time fields: "Passw.Expire Date" (02/01/1980), "Passw.Update Date" (01/01/1980), "Passw.Update Time" (00:00:00), "Valid Login Date" (00/00/0000), "Valid Login Time" (00:00:00), "Open Date Interval Start" (01/01/1900), "Incorrect Login Attempt Date" (00/00/0000), "Incorrect Login Attempt Time" (00:00:00), "User Lockout Date" (00/00/0000), "User Lockout Time" (00:00:00), "Number Of Invalid Login" (0), and "Open Date Interval End" (01/01/2079). At the bottom, there are four more fields: "Record Inserted By" (NETSIS), "User modified" (NETSIS), "Record Date" (18/04/2006 14:29:57), and "Adjustment Date" (13/06/2006 11:46:46). A large "Ok" button with a green checkmark icon is centered at the bottom of the window.

User Copy

By using this key, you can copy the permissions of a user to the file of a newly inserted user.



In the *Based on User* field, you should enter the user's number as defined in the User records menu. In the *New User ID and Name* fields, you should enter the information about the new user to which you wish to copy the source information. Thus, the programme will automatically insert a record for the new (undefined) user and copy to this new user the permissions that are previously assigned to the source user.



Unlock User

If you have defined a value in the Maximum Number of Incorrect Login Attempts in the User Parameters and a user has entered his/her password incorrectly more than the number of times indicated in this field, then the programme blocks that user for the period again defined in the parameters. The blocked (locked out) user can be enabled in this section by an authorised user.

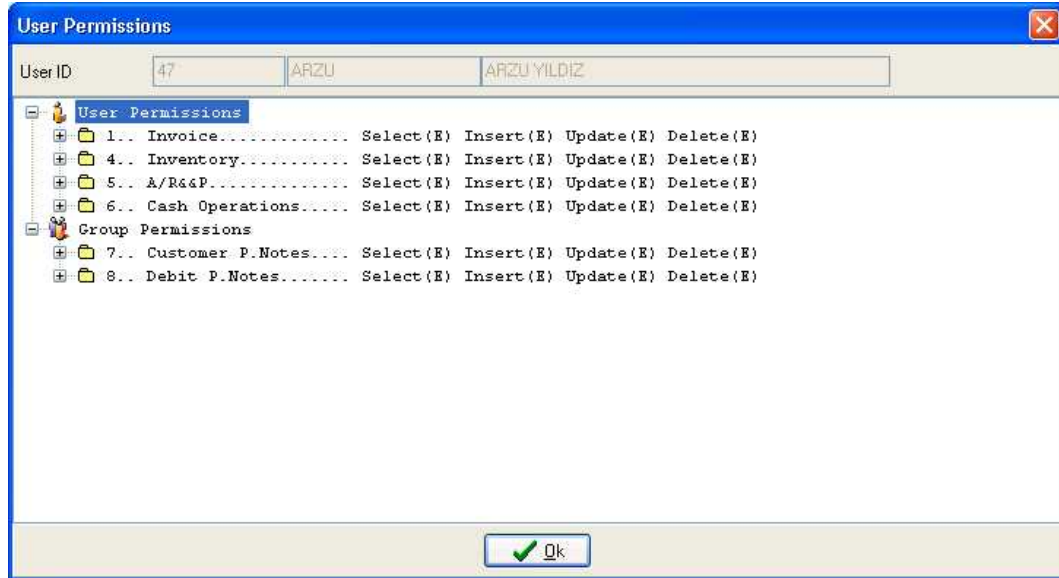


When you confirm this query with the *Yes* key, the programme will display the message of "User opened" remove the lockout and reactivate the related user's permissions.



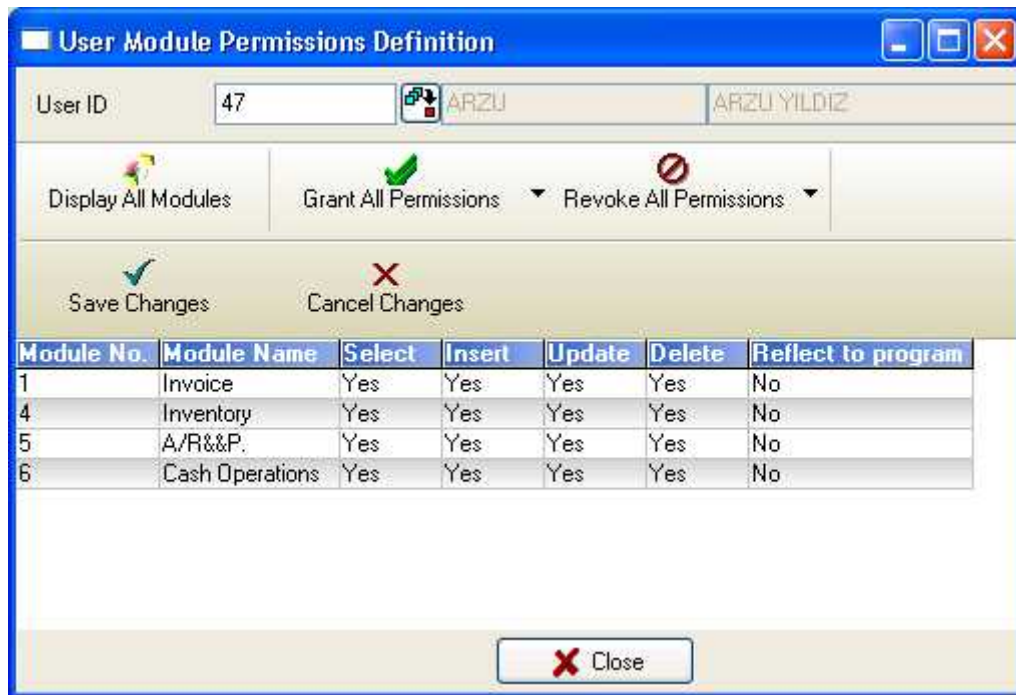
User Permissions

In this section, you can monitor the permissions assigned to a defined user.



2.5. User Module Permissions Definition

In this section, you can define module permissions for the users who are already defined in the User Records menu. The definition operations and the function keys are the same as those in the *Group Module Permissions Definitions* menu. [For details, please see User Defintions/Group Module Permissions Definitions section.](#)



2.6. User Program Permissions Definition

This is the section where the permissions defined in the *User Module Permissions Definitions* section can be further applied to the submenus. The definition operations and the function keys are the same as those in the *Group Module Permissions Definitions* menu. [For details, please see User Definitions/Group Module Permissions Definitions section.](#)

User Program Permissions Definition

User ID: 47 ARZU ARZU YILDIZ

Module No.: 1 Invoice

Display All Programs Grant All Permissions Revoke All Permissions

Save Changes Cancel Changes

Program Number	Program Name	Select	Insert	Update	Delete
1	Sale Invoice	Yes	Yes	Yes	Yes
2	Purchase Invoice	Yes	Yes	Yes	Yes
3	Sale Dispatch	Yes	Yes	Yes	Yes
4	Purchase Dispatch	Yes	Yes	Yes	Yes
5	Batch Invoicing Sales Dispatches	Yes	Yes	Yes	Yes
6	Batch Invoicing Purchase Dispatches	Yes	Yes	Yes	Yes
7	Sales Orders	Yes	Yes	Yes	Yes
8	Purchase Orders	Yes	Yes	Yes	Yes
9	Purchase Parameters	Yes	Yes	Yes	Yes
10	Sales Parameters	No	No	No	No
11	Branch Transfer	Yes	Yes	Yes	Yes

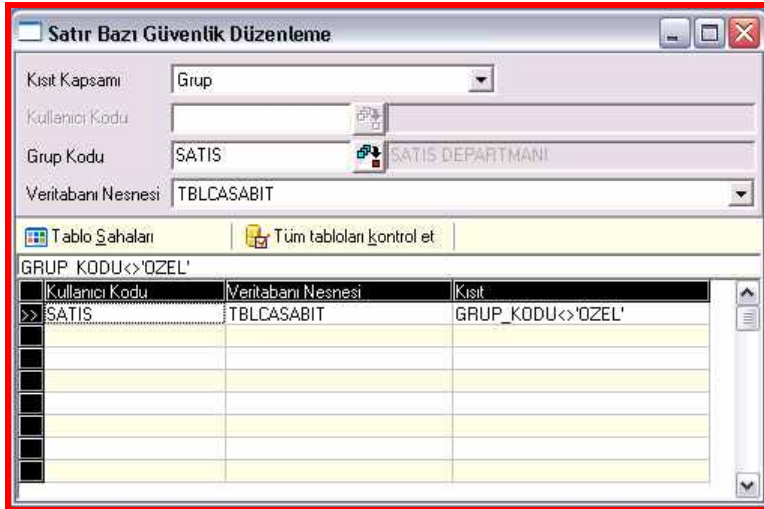
Close

2.7. Row-Based Security

In this section, you can define filters for *All Users*, for a *Group* or for a single *User*. With the Row-Based Security application, you can hence prevent that a user or user group enter irrelevant information that do not match the defined criteria.

With the Row-Based Security application, you can furthermore prevent that the restricted user or user group view the records defined in the range of the Filter.

The Row-Based Security application is available in the Fusion package and Oracle database.



Filter Range

This is the section where you can define the user or users to which the Row-Based Filter will be applied. This field displays the *All Users*, *Group* and *User* options.

All Users

When you select this option, the Row-Based Filter will be valid for all users who are defined in the programme.

Group

When you select this option, the Row-Based Filter will be valid for the group that you select among the groups that are defined in *User Group Records* field.

User

When you select this option, the Row-Based Filter will be valid for only a single user.

User ID

This field becomes active when you select the *User* option in the *Filter Range* field. You can use the User ID lookup in this field to select the user id to which the filter will be applied.

Group Code

This field becomes active when you select the *Group* option in the *Filter Range* field. You can use the Group Codes lookup in this field to select the User Group Code to which the filter will be applied.

Database Object

In this window, you can select the table to which the row-based filter will be applied. For example, if you are defining filters for a field in the Inventory Card Records menu, you should select the TBLSTSABIT option in this window.

In the window below the Database Object, you should write an SQL sentence about the field for which the filter will be defined. For example, if the row-based filter will be applied for a user group and for the Group Code field in the Current Account Records menu, the TBLCABIT option should be selected in

the Database Object. The definition of GROUP-CODE<>'SPECIAL' should be entered in the window below the Database Object. This means that the defined user group will not be able to view in the Current Account Records menu those Current Accounts that have the Group Code SPECIAL. Additionally, when entering a new Current Account definition or updating an existing Current Account definition, this user group will not be allowed to define the Group Code SPECIAL in the Group Code field of the related account. If any user in the related group attempts to process an operation contrary to the defined filter (for instance attempts to enter SPECIAL in the Group Code field when defining a Current Account), then the programme will display a warning message that says "Your entry does not match the row-based security filter," and will not allow for any records that contradicts the filter.

Keys



 Tablo Sahaları

Table Fields

In this section, you can monitor the fields of the table that are selected in the Database Object field. In other words, in this window you can view the field names of the table to which you will define the filter.

Saha Adı	Saha Tipi	Uzunluk	Precision	Zorunlu
KSMAS_KOD	VARCHAR2	0	0	Evet
KSMAS_NAME	VARCHAR2	0	0	Hayir
DOVIZLI	CHAR	0	0	Hayir
MUH_KOD	VARCHAR2	0	0	Hayir
KSSONDEV_D	DATE	0	0	Hayir
KSSONDEV_T	NUMBER	28	8	Hayir
KSMABUZ_BAS	CHAR	0	0	Hayir
KS_DEFBAS_TIP	CHAR	0	0	Hayir
DOVIZTIPI	NUMBER	3	0	Hayir
CEVRIMTIPI	NUMBER	3	0	Hayir
KURFARKIGELIRKODU	VARCHAR2	0	0	Hayir
KURFARKIGIDERKODU	VARCHAR2	0	0	Hayir
KSSONDEV_DOVIZ	NUMBER	28	8	Hayir
SUBE_KODU	NUMBER	5	0	Evet
YEDEK	VARCHAR2	0	0	Hayir
KAYITYAPANKUL	VARCHAR2	0	0	Hayir
KAYITTARIHI	DATE	0	0	Hayir
DUZELTMEYAPANKUL	VARCHAR2	0	0	Hayir
DUZELTMETARIHI	DATE	0	0	Hayir

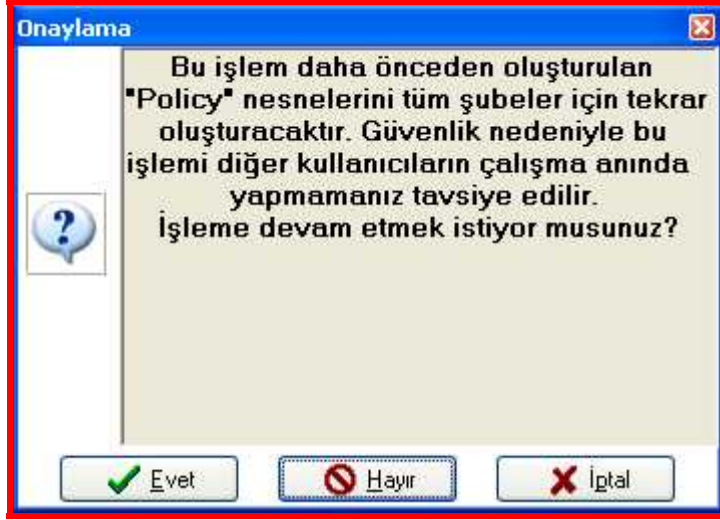


 Tüm tabloları kontrol et

Check All Tables

If any problems arise in objects that are created as a result of the filters defined in the Row-Based Security Application, this field enables you to recreate these objects. When you press this key, the programme will first display a warning window and start the operation when you confirm the

operation query. For security reasons, other users should quit the programme while this operation is in process.



2.8. Column-Based Data Validation Values

In this section, you can define filters for Users on Columns bases. When users enter any information that do not match the defined criteria, the programme will not allow for this entry and notify the user who is processing the information.

User Filter Definition Operations

Filter Range: Tum Kullanicilar

User ID:

Group Code:

Database Object: TBLSTSABIT Deletion Control

Process Name: kdv_ORANI Check Nulls

=18

Error Explan.: Vat Rate should be 18

User ID	Database Object	Process Name	Filter
ALL	TBLSTSABIT	DEPO_KODU	<>0
ALL	TBLSTSABIT	kdv_ORANI	=18

Filter Range

This is the section where you can define the user or users to which the Column-Based Filter will be applied. This field displays the *All Users*, *Group* and *User* options.

All Users

When you select this option, the Column-Based Filter will be valid for all users who are defined in the programme.

Group

When you select this option, the Column-Based Filter will be valid for the group that you select among the groups that are defined in *User Group Records* field.

User

When you select this option, the Column-Based Filter will be valid for only a single user.

User ID

This field becomes active when you select the *User* option in the *Filter Range* field. You can use the User ID lookup in this field to select the user id to which the filter will be applied.

Group Code

This field becomes active when you select the *Group* option in the *Filter Range* field. You can use the Group Codes lookup in this field to select the User Group Code to which the filter will be applied.

Database Object

In this window, you can select the table to which the column-based filter will be applied. For example, if you are defining filters for a field in the Inventory Transaction Records menu, you should select the TBLSTHAR option in this window.

Field Name

In this window, you can select the field for which the column-based filter will be defined. In the window below the Database Object, you should write an SQL sentence about the field for which the filter will be defined.

Deletion Control

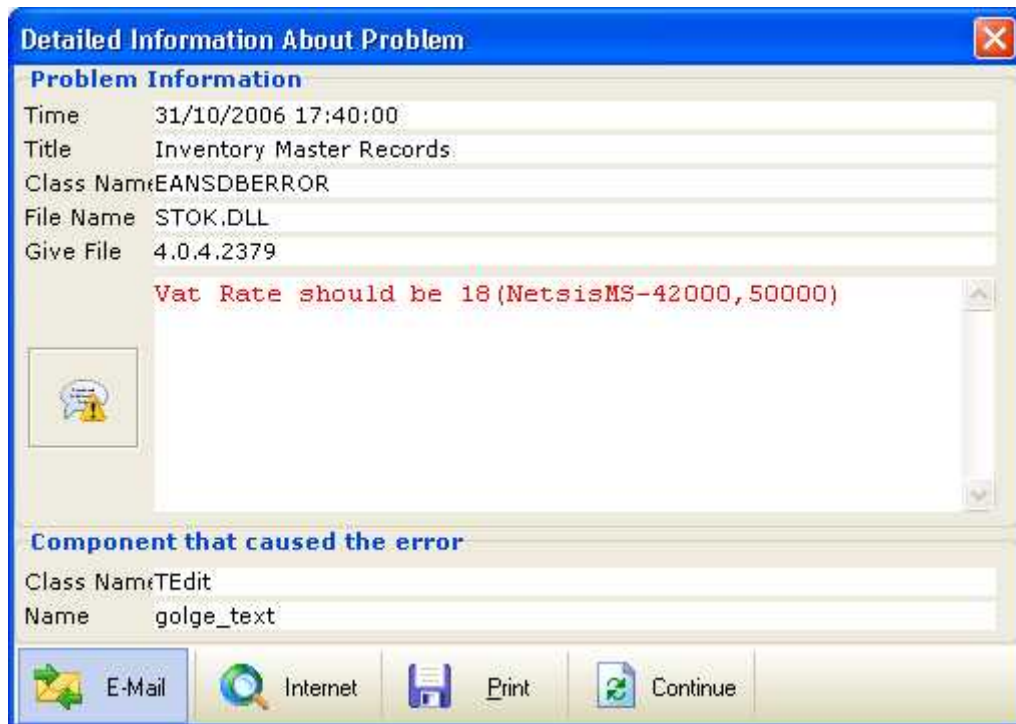
Selecting this field also prevents users from deleting the records that do not match the filters defined in the Column-Based data validation section. As the programme will not allow a user or user group to enter any records that do not match the defined filter, similarly when this field is selected, it will not allow users that fall in the range of the filter to delete any records that were previously inserted by users that fall out of the range of the filter.

Check Null

When this box is checked, the programme will also check the blank records for the defined filter. For example, when you define a filter to always enter 18 for the VAT Rate, the programme will display a warning message if a user leaves the VAT Rate field blank.

Error Explanation

In this field, you can enter an explanation for the warning message that you wish to be displayed when a user enters a record contrary to the defined filter. For example, let us assume that you want to define a filter for entering only 18 in the VAT Rate field in the inventory when inserting or updating a record. When you want to give such filters, you should make the following definitions. You should select the User option in the Filter Range field; define TBLSTSABIT in the Database Object field and VAT_RATE in the Field Name field. Additionally in the window in which the filter definition will be entered you should write =18. In the explanation for the warning window that will be displayed when users enter a record contrary to the defined filter, "VAT RATE SHOULD BE 18" can be written. Thus, when users enter the records, if they attempt to enter a VAT Rate other than 18, the programme will open a warning window and will not allow them to enter a record that does not match the defined filter.



2.9. User E-Mail Definitions

In this section, you can enter the definitions that will enable you to instantly inform the related users by e-mail about some of the operations that are processed in the company. With this section, some of the users will be informed about important developments at the moment they occur, nonetheless top executives in particular will be able to follow-up the developments in the company.

Operation	E-Mail	CC-Mail	Mobile Tel.
H- Cance	aliyilmaz@abc.com.tr		
I- Cancelli	aliyilmaz@abc.com.tr		

Operations

This is the section where you can select the operations about which the users will be informed. When users process the selected operation, this section will automatically send the e-mail/s.

E-Mail

In this field, you should enter the number of the user to which the e-mail will be sent. When you enter the related user id that is defined in the User Operations section and press the OK key, the e-mail address of the related user will be displayed in a window on the permission side. For the e-mail address of the related user to be displayed in the window, you should first have entered the user's e-mail address in the "E-Mail Address" field in the User Operations/User and Permissions Definitions sections. You can use the lookup key in the related field to view the user id lookup.

CC-Mail

If you want to send the e-mail to also to another user, then you should enter the second user's user id in this field. To be able to run this function, again you should first have entered the user's e-mail address in the "E-Mail Address" field in the User Operations/User and Permissions Definitions sections.

2.10. User Parameters

These are the default parameters for all users. In this section, you will enter the general definitions for the users.

Min. User Name Length	<input type="text" value="0"/>	Min. Password Length	<input type="text" value="0"/>
Password Expiration Period (Day)	<input type="text" value="0"/>	Number of Incorrect Login Attempts	<input type="text" value="0"/>
Detect Intruders	<input checked="" type="checkbox"/>	Length of Account Lockout (Minute)	<input type="text" value="0"/>
Retention Time (Minute) of Incorrect Logins	<input type="text" value="0"/>	Delete users automatically if not logged in	<input type="text" value="0"/> days <input type="checkbox"/>
Max User Count	<input type="text" value="0"/>	Control The Null Password On Program Entrance	<input type="checkbox"/>
Expiration period (days) of password given by admin	<input type="text" value="0"/>		

Minimum User Name Length

In this field, you should define the minimum length for the programme users' names. User names can be maximum 12 characters. When defining the users, the programme will not allow any entries shorter than the number of characters defined in this field. However, the programme will not consider a specific minimum limit if you leave this field as 0 (zero).

Minimum Password Length

The minimum length of users' passwords should be specified in this field. Passwords can be maximum 12 characters. When defining the users, the programme will not allow any password entries shorter than the number of characters defined in this field. However, the programme will not consider a specific minimum limit for passwords if you leave this field as 0 (zero).

Password Expiration Period (Day)

This is the time interval, in which users are required to change their passwords. This period should be defined as days. For example, if you want users to work with the same password for 10 days in succession, and then you want them to use different passwords after these ten days (as of the 11th day), you should enter 10 in this field. If you leave this field as 0 (zero), users will not be required to change their passwords at specific time intervals. This parameter is a measure against unauthorised usage of the programme by forcing programme users to change their passwords at certain intervals.

Detect Intruders

You should select this parameter if you wish to trace the incorrect login attempts of users by defining the maximum number of incorrect logins, the cancel time between two incorrect logins and the lockout time (Retention Time of Incorrect Login). The below-described filter parameters (Number of

Incorrect Login Attempts, Lockout Time, Retention Time of Incorrect Login) will not be enabled unless this parameter is selected.

Number of Incorrect Login Attempts

This field will be active when the "Detect Intruders" parameter is selected. The parameter specifies the number of times users are allowed to enter their passwords incorrectly after they enter their usernames. Users are allowed wrong entries as many times as indicated in this field. After the number of times allowed by this number, the programme will display a warning message that says "Too many incorrect entries. The programme is shutting down," and go to the company selection window. A certain time should pass before the same user can try to enter his/her password again and the user will be blocked during this time. The time the user will be blocked (Lockout) can be defined as a parameter.

Retention Time (Minute) of Incorrect Login

In cases where incorrect login attempts are recorded and users are blocked after a certain number of incorrect login attempts, this is the time required between two incorrect login attempts. For example, let us assume that you entered 1 in this parameter. When a user enters a wrong password, then attempts to login again, and once more enters the password wrong within the one minute after the first, the programme will count the second wrong password and verify this number with the value defined in the Number of Incorrect Login Attempts field. If, however, the same user makes the second login attempt after 1 minute, the programme will disregard (forget) the first attempt and consider the second incorrect attempt as the first. In this case, the number that the programme will verify with the value defined in the Number of Incorrect Login Attempts field will be 1.

The incorrect passwords, which the users enter, will be stored by the system according to the date and time starting with the very first attempt.

Length of Account Lockout (Minute)

When a user has entered his/her password incorrectly as many times as specified in the "Maximum Number of Incorrect Logins" field, the time during which that user will be blocked from logging in the programme will be defined in this field. The value in this field should be in minutes. The system will keep record of the days and hours during which the user is blocked. The last lockout date and the duration of the lockout for every user can be monitored in the User Information field of the User Definitions section.

Delete users automatically if not logged in __ days__

If users who are defined in the User Definitions section do not log in the programme during the time period specified in this field, then the system will automatically delete the names and all other defined information related to those users. To enable this function, you should enter a day value in the day field and select this parameter.

Maximum User Count

This parameter specifies the number of different computers to which a user can log in at the same time. If you want every user to log in one computer at once, you should enter 1 in this field. In this way, one user will be allowed to log into the programme only on one computer at a time. Hence, even if other users know the first user's name and password, they will not be able to log in

with the same identity. The value 0 (zero) indicates unlimited login permissions. In this case, the same user will be able to log into the programme with the same username and password simultaneously as many times as he/she wants.

Control the Null Password on Program Entrance

This option prevents entries without writing a password, i.e. prevents using null passwords. When this parameter is selected, if a user presses the enter key without writing a password, the system will display a warning message that says "You cannot enter without a password," even if a password is not defined for that user and will not allow the user to log in.

Expiration Period (Days) of Password Given by Admin

The Admin user is allowed to specify other users' passwords in the User Records window. In this field, you should enter the number of days this password defined by the Admin can be used. When the time (number of days) specified in this field is over, the system will require the user to change his/her password.

3. Operations

This section includes operations for updating user passwords and defining date locking and other related functions.

3.1. Change Password

This is the section where users can change their passwords. Passwords should be changed in this section on the day before the password expiration date defined as the company principle. For users who forget to change their passwords on the required day, the system will display a password change window at entry and allow them to change their passwords.

Old Password

This is the field where you should enter the password that will be changed.

New Password

This is the field where you should enter the new password that will replace the old.

Retype Password

In order to confirm the new password you should re-enter the new password in this field. The change operation will be completed when you enter the OK key.



A dialog box titled "Change Password" with a blue header and a close button (X) in the top right corner. It contains three text input fields: "Old P.word", "New P.word", and "Retype". Below the fields are two buttons: "Ok" with a green checkmark icon and "Cancel" with a red X icon.

3.2. Date Locking

While running the programme, when you have inserted all records (e.g. trial balance already created) and you do not want that any further operations are processed or any of the records are deleted up to a certain date for these records, this section enables you to prevent such operations. In multi-user operations, if there are several users who process the records, problems may arise due to modifications made by mistake on records that relate to periods for which the trial balance or the ledger is finalised. The programme therefore provides the opportunity to specify a certain time interval (on modules bases) in order to prevent modification of records that relate to the period.



A dialog box titled "Date Locking" with a blue header and a close button (X) in the top right corner. It contains a "Date Locking Password" text input field. Below it are two rows of radio buttons: the first row has "Lock Users One By One" and "Lock All Users"; the second row has "Group Based Lock" and "User based locking" (which is selected). Below the radio buttons are three text input fields: "Group Code" with a search icon, "User ID" with a search icon and the text "NETSIS", "Open Date Interval Start" with the value "01/01/1970", and "Open Date Interval End" with the value "31/12/2800".

Date Locking

The person who is processing the Date Locking should enter his/her password in this field. The password should not be known by anyone but the person in charge of processing this operation. The default for this password is "net1." Users can change this password as desired.

Lock Users One by One

You should select this field if you want to process the Date Locking operation for every user individually.

Lock All Users

You should select this field if you want to process the Date Locking operation for all users at once.

User ID

This field becomes active if you select the *Lock Users One by One* option. The user id for which the Date Locking operation will be processed should be indicated in this field.

Open Date Interval Start

In this field, you should enter the date as of which the Date Locking will not be valid, i.e., the start date of the period during which the operation will be open to users' access.

Open Date Interval End

In this field, you should enter the last date on which the Date Locking will not be valid, i.e., the end date of the period during which the operation will be open to users' access.

The programme will allow operations between the dates of the Open Date Interval Start and Open Date Interval End dates specified in the related fields, and will not allow record entry on dates that fall outside of this period.

3.3. Change Date Locking Password

This section can be used for changing the Date Locking Password used in the Date Locking window.



Old Password

This is the field where you should enter the password that will be changed.

New Password

This is the field where you should enter the new password that will replace the old.

Retype

In order to confirm the new password you should re-enter the new password in this field. The change operation will be completed when you enter the OK key.

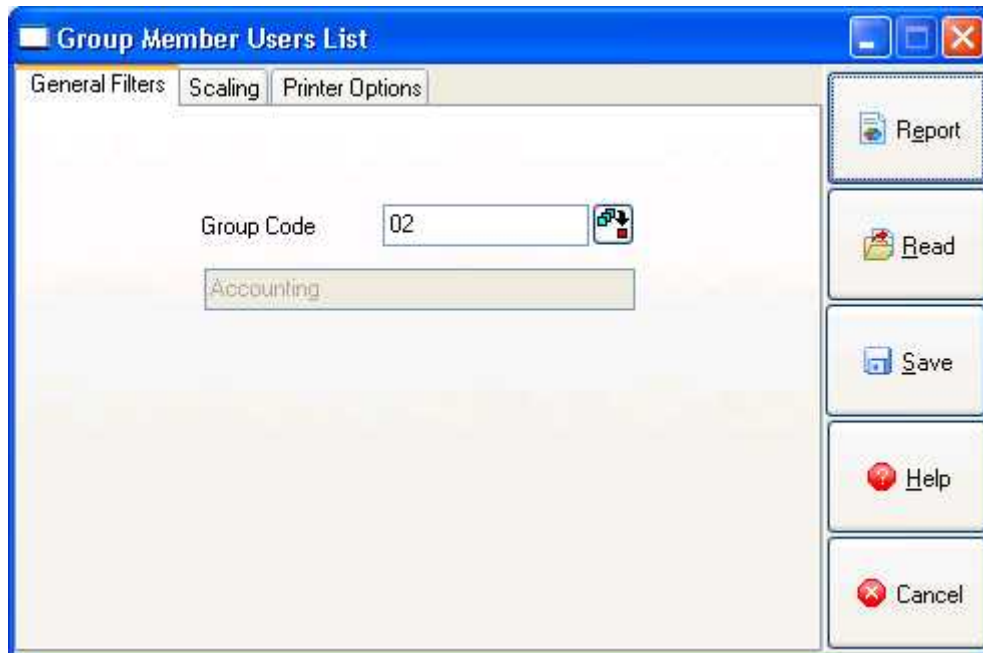
4. Reports

In this section, you can get reports related to the definitions processed in the Record section of the User Operations.

4.1. Group Member Users List

This report lists the groups and the related group members that are defined in the User Group Records.

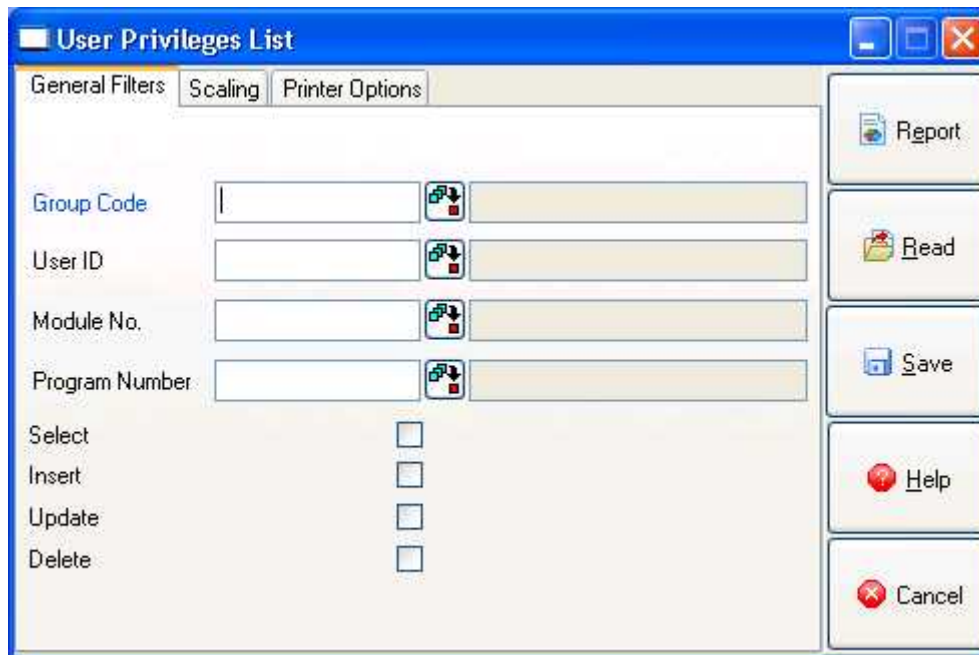
It is also possible to get the report of a single group by selecting the desired group by using the Group Code Lookup in the General Filters section.



[For details of the fields in the Scaling and Printer Options sections, and general usage of the reports, please see Introduction/Standard Report Usage.](#)

4.2. User Privileges List

This report lists the permissions defined to users in the User Records menu.



The report can be retrieved according to the filters defined in the General Filters section.

Group Code

If you wish to get the report for users defined in a specific group, then you should indicate the related Group Code in this field.

User ID

If you wish to get the report for only a single user, then you should indicate the related User ID in this field.

Module Number

If you wish to get the report of the user permissions that are defined for a single module, then you should indicate the related Module in this field.

Program Number

If you wish to get the report for a single menu option of a single module, then you should indicate the related submenu of the module in this field.

It is possible to get the list of the modules or submenus that have the *Select*, *Insert*, *Update* and *Delete* permissions by checking the boxes of the relevant permissions.

You can, for example, select the *Insert* box and get the list of the programme menus where a specific user has the permissions to process record operations.

For details of the fields in the Scaling and Printer Options sections, and general usage of the reports, please see Introduction/Standard Report Usage.

4.3. Group Permissions List

This report lists the permissions that are assigned to users in the groups that are defined in the User Group Records menu.

The screenshot shows a software window titled "Group Permissions List". At the top, there are three tabs: "General Filters", "Scaling", and "Printer Options". Below the tabs are three input fields: "Group Code", "Module No.", and "Program Number". Each input field has a small icon to its right. Below these fields are four checkboxes labeled "Select", "Insert", "Update", and "Delete". On the right side of the window, there is a vertical toolbar with five buttons: "Report", "Read", "Save", "Help", and "Cancel".

Group Code

If you wish to apply filter according to a group code, then you should enter the related Group Code in this field.

Module Number

If you wish to get the report of the user permissions that are defined for a single module, then you should indicate the related Module in this field.

Program Number

If you wish to get the report of the permissions that are defined for a single submenu option in a module, then you should indicate the related menu option in this field. For example, you may wish to list the permissions that are assigned for the Sales Invoices Menu in the Invoice Module.

It is possible to get the list of the modules or submenus that have the *Select*, *Insert*, *Update* and *Delete* permissions by checking the boxes of the relevant permissions.

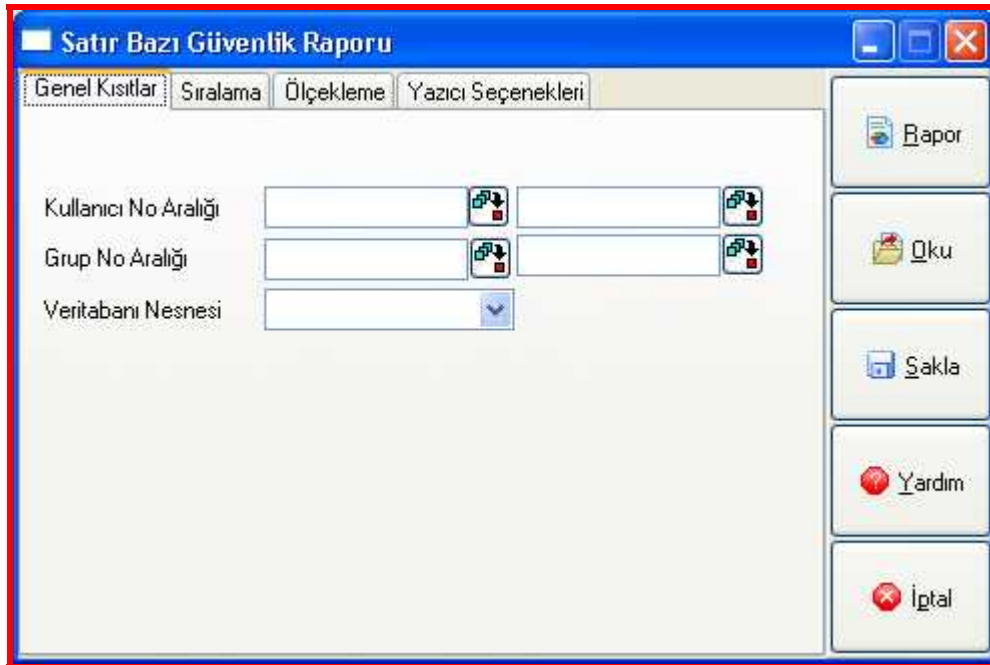
You can, for example, select the *Record* box and get the list of the programme menus where a specific user has the permissions to process record operations.

[For details of the fields in the Scaling and Printer Options sections, and general usage of the reports, please see Introduction/Standard Report Usage.](#)

4.4. Row-Based Security Report

In this section, you can get a report for the filters defined in the Row-Based Security Section. This report will be displayed in the Reports menu only if the

related database is Oracle and the "Row-Based Security System" or the "All" option is selected in the "Security Application" field in the Auxiliary/Company/Branch Parameter Definitions menu.



User ID Range

If you wish to get a report for a certain user range, then in this field you should enter the user id of the related users.

Group ID Range

If you wish to get a report for a certain user group range, then in this field you should enter the codes of the related groups.

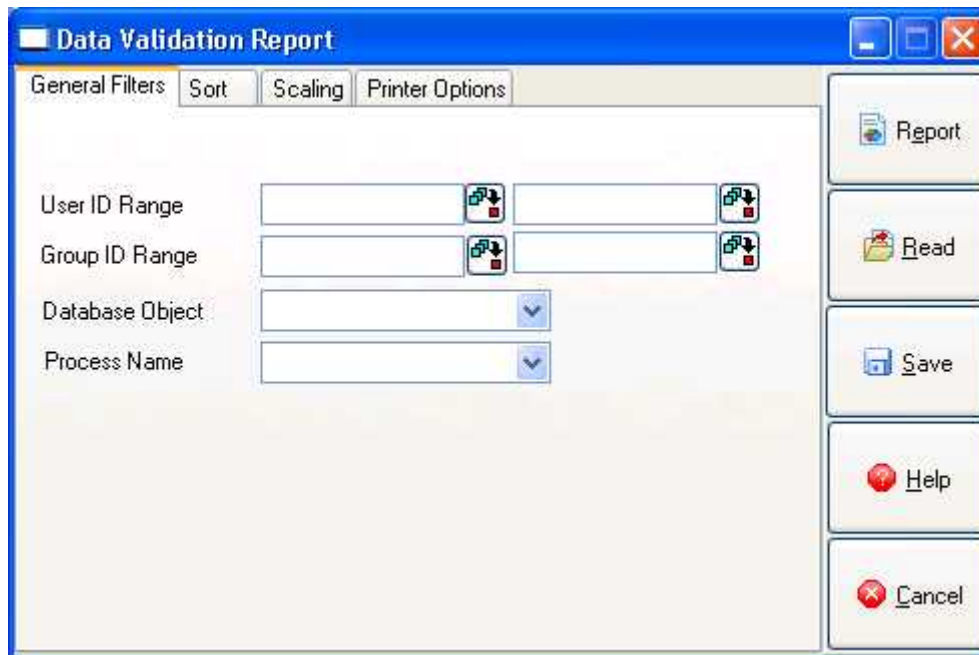
Database Object

You can select a Table name in this field and get a report of the filter definitions that are defined for the selected Table.

[For details of the fields in the Filter, Sort, Scaling and Printer Options sections, and general usage of the reports, please see Introduction/Standard Report Usage.](#)

4.5. Column-Based Data Validation Report

This is the section where the filters that are defined in the *Column-Based Validation Values* section can be listed. This report will be displayed in the Reports menu only if the "Column-Based Data Validation System" or the "All" option is selected in the "Security Application" field in the Auxiliary/Company/Branch Parameter Definitions menu.



User ID Range

If you wish to get a report for a certain user range, then in this field you should enter the user id of the related users.

Group ID Range

If you wish to get a report for a certain user group range, then in this field you should enter the codes of the related groups.

Database Object

In this field, you can select the name of the Table for which you wish to get the report of the defined filters.

Field Name

If you have selected a Table Name in the above-described field, in this field you should select the field of the table, for which you wish to get the filter report. E.g., the VAT-Rate field in the TBLSTSABIT Table.

[For details of the fields in the Filter, Sort, Scaling and Printer Options sections, and general usage of the reports, please see Introduction/Standard Report Usage.](#)