Security Management System
Oracle FLEXCUBE Corporate Lending 12.1.0.0.0
[April] [2016]

Part No. E74823-01

ORACLE
FINANCIAL SERVICES

ORACLE

Security Management System
[April] [2016]
Version 12.1.0.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax:+91 22 6718 3001
www.oracle.com/financialservices/

Table of Contents

1. About this Manual

1.1 Introduction

This Manual is designed to help you to quickly get familiar with the Security Management System (SMS) module of Oracle FLEXCUBE.

It provides an overview of the module and takes you through the various stages in setting- up and using the security features that Oracle FLEXCUBE offers.

Besides this User Manual, you can find answers to specific features and procedures in the Online Help, which can be invoked, by choosing Help Contents from the *Help* Menu of the software. You can further obtain information specific to a particular field by placing the cursor on the relevant field and striking <F1> on the keyboard.

1.2 Audience

This Manual is intended for the following User/User Roles:

Role	Function
Oracle FLEXCUBE Implementers	To set up the initial start up parameters in the individual client workstations. To set up security management parameters for the Bank.
SMS Administrator for the Bank	To set the SMS bank parameters. To identify the Branch level SMS Administrators.
SMS Administrator for the Branch	To create User and Role profiles for the branches of your bank. Will also grant access to the various functions to the Users.
An Oracle FLEXCUBE user	Any user of Oracle FLEXCUBE whose activities are traced by the SMS module.

1.3 Organization

This Manual is organized into the following chapters:

Chapter 1	*About this Manual* - Gives information on the intended audience. It also lists the various chapters covered in this User Manual.
Chapter 2	*Security Management* — Explains the multi-pronged approach employed in Oracle FLEXCUBE to ensure high security standards.
Chapter 3	*Associated Functions* — This chapter deals with the associated functions that you will need to perform in maintaining System Security, like resetting passwords, clearing users from the system.
Chapter 4	*Information Retrieval* — Deals with the various reports that can be

	generated for the module.

1.4 Related documents

The Procedures User Manual

2. Security Management

2.1 Introduction

Controlled access to the system is a basic parameter that determines the robustness of the security in banking software. In Oracle FLEXCUBE, we have employed a multi-pronged approach to ensure that this parameter is in place.

2.1.1 Only Authorized Users Access the System

First, only authorized users can access the system with the help of a unique User ID and a password. Secondly, a user should have access rights to execute a function. Any activity involving movement of funds and addition or modification of information should be authorized by a user other than the one who initiated the activity. Thus, at least two people will be involved in all activities that require authorization.

2.1.2 User Profiles

The user profile of a user contains the User ID, the password and the functions to which the user has access. The user profile can be created or modified only when two people, called Control Clerks in the system, log in using their passwords. Thus, the key to controlling access to the system is always with two people. Once the Control Clerks have created the user profile and the user logs in, a change of the password can be forced. This is to ensure that even the Control Clerks do not know the password of a user.

2.1.3 Encryption of the Password

While capturing the password the system encrypts the password in the 128-bit algorithm. Similarly when you choose to change the password the same algorithm is used for password encryption.

Subsequently, whenever you login using the password the 128-bit encryption algorithm is used and is validated against the password, which is stored in your name.

Only those passwords that are encrypted using 128 –bit algorithm are transmitted over the network to the server.

2.1.4 Restricted Number of Unsuccessful Attempts

You can define the maximum number of unsuccessful attempts after which a User ID should be disabled. When a User ID has been disabled, the Control Clerks should enable it. The password of a user can be made applicable only for a fixed period. This forces the user to change the password at regular intervals thus reducing security risks. Further, you can define passwords that could be commonly used by a user as Restrictive Passwords at the user, user role and bank level. A user cannot use any password that is listed as a Restrictive Password at any of these levels.

If you entered wrong password more than ‘n’ successive times, User status will be disabled and a message will be displayed stating that user will be logged off.

2.1.5 Restricted Access to Branches

You can indicate the branches from where a user can operate. Click on  in the Restricted Access screen to define the branches from where a user can operate.

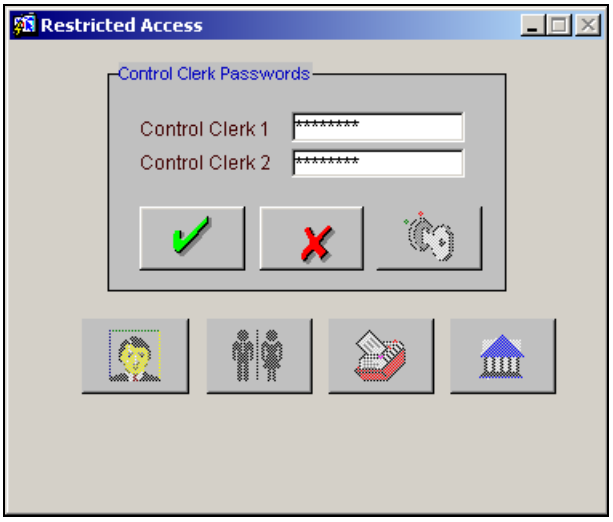
2.1.6 All Activities Tracked

Extensive log is kept of all the activities on the system. You can generate reports on the usage of the system anytime. These reports give details of unsuccessful attempts at accessing the system along with the nature of these attempts. It could be an unauthorized user attempting to use the system, an authorized user trying to run a function without proper access rights, etc.

2.1.7 Logging-in as a Control Clerk

All activities related to system security like creating and modifying user profiles, generating audit trails, etc. can be performed only when two users (designated as Control Clerks in the system) log in to the system.

From the Application Browser invoke the Control Clerk Passwords screen. It is available under the module Security Maintenance as Restricted Access.



2.1.8 Changing Control Clerk Passwords

After the two Control Clerks have entered their passwords, click on  to change the passwords. The Control Clerk Password Change screen will be displayed. You can change the passwords for Control Clerk 1 and Control Clerk 2 by entering the old and new passwords.

2.1.9 Setting-up Parameters at the Bank Level

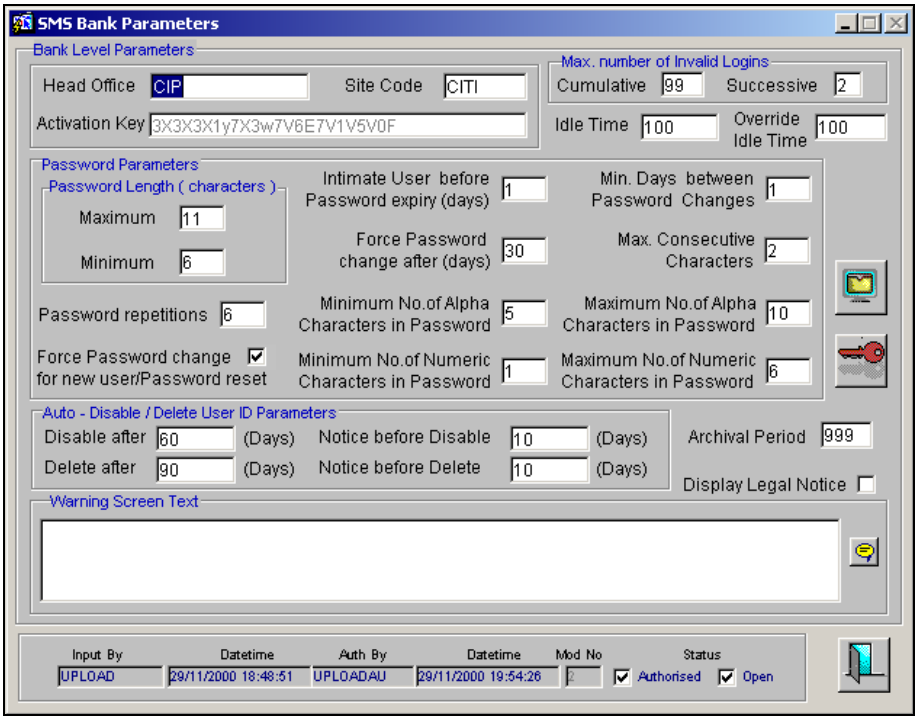
Certain parameters related to security management should be defined at the bank level. These parameters will apply to all the users of the system. Examples of such parameters are the number of invalid login attempts after which a user-id should be disabled, the maximum and minimum length for a password, the number of previous passwords that should not be used, the interval at which the password should be changed by every user, etc.

2.1.10 Automatic Disabling and Deletion of User IDs

As part of defining the bank level parameters you can indicate the number of days after which User IDs ought to be automatically disabled by the system. Similarly, you can specify the number of days after which an intimation notice should be sent to users informing them that their ID was disabled due to inactivity.

When a User ID has not been used for a long time you can choose to delete it permanently from the system by specifying the number of days after which it is to be deleted. In addition you can indicate the number of days after which an intimation notice should be sent to users informing them that their ID will be deleted due to inactivity.

To define Bank Level Parameters, click on  at the Control Clerk Login screen, after both the control clerk passwords have been given and you have confirmed the login by clicking on  .



2.1.10.1 Defining Restrictive Passwords for the Bank

You can define a list of passwords that cannot be used by any user of the system in the bank. This list, called the Restrictive Passwords list can be defined at three levels:

- At the bank level (applicable to all the users of the system).
- At the user role level (applicable for all the users doing a similar kind of role).
- At the user level (applicable for the user).

The list of Restrictive Passwords should typically contain those passwords the users are most likely to use: the name of your bank, city, country, etc. For a user role, it could contain names, or terms, that are commonly used in the department. At the user level, it could contain the names of loved ones, etc. By disallowing users from using such common passwords, you can reduce the risk of somebody other than the user knowing the password.

Click  to define Restrictive Passwords to define passwords that should not be used by any user of the bank. At the Restrictive Passwords screen, click on  after you have entered the password list.

2.1.10.2 Capturing the Text that is to be Displayed in the Warning Screen

At your bank, you may require a warning message to be displayed to all users who log into Oracle FLEXCUBE. Typically, such log-in messages contain legal and security policy statements. You can capture the content of such a message in the Warning Screen Text field.

This message will be displayed soon after a user clicks on the Oracle FLEXCUBE login icon. The user will be allowed to continue with the login process only after he clicks on the OK button on the message window.

You can modify the contents of the message only during the transaction input stage. The changes will come into effect during the next login by a user. The maximum size of the warning message is '1000' characters.

 You will be allowed to specify the contents of the warning message only if the 'Display Legal Notice' option is enabled.

2.1.10.3 Restricting the Length of User Passwords

You are allowed to place restrictions on the number of alpha and numeric characters that can be specified for a user password.

Specifying the Minimum and Maximum Number of Alpha Characters in a Password

You can specify the minimum and maximum number of alphabetical characters that a user can specify while setting a password. The system validates these specifications only when a user chooses to change the password.

If you do not specify the limits, the following default values will be used:

- Minimum No of Alpha Characters = 0
- Maximum No of Alpha Characters = Maximum Password Length

Specifying the Minimum and Maximum Number of Numeric Characters in a Password

Likewise, you can also specify the minimum and maximum number of numeric characters allowed in a password. The system validates the password only when a user chooses to change the password.

If you do not specify the limits, the following default values will be used:

- Minimum No of Numeric Characters = 0
- Maximum No of Numeric Characters = Maximum Password Length

 You can specify any number between 0 and 11 in each of these fields. However, you must ensure that the sum total of the minimum number of alpha characters and the maximum number of numeric characters is less than or equal to the 'Maximum Password Length'. Similarly, the sum total of the maximum number of alpha characters and the minimum number of numeric characters should be less than or equal to the 'Maximum Password Length'.

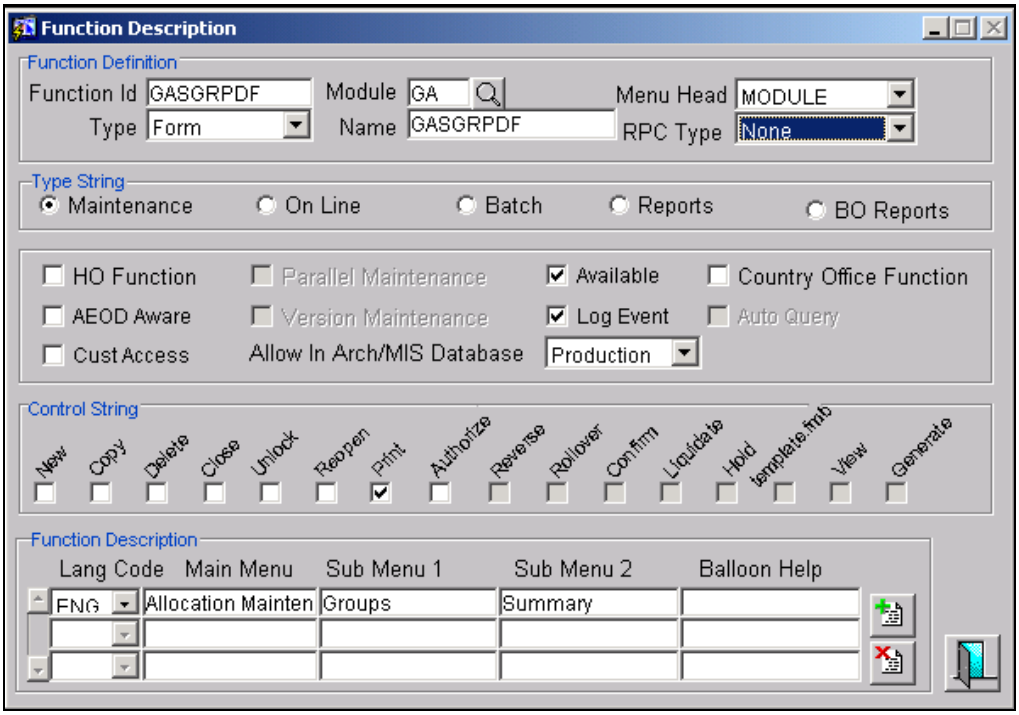
Specifying the Maximum Number of Consecutive characters in a password

You also have to specify the maximum number of times an alpha or a numeric character can appear in a password. If a user captures a password which exceeds the maximum number that you have specified the user will be asked to change the password.

2.1.11 Defining Functions

Any function that is a part of the system should be defined through the Function Definition screen before it is available for execution. Mostly, our professionals at i-flex solutions Limited carry out this activity. In the event of a function being added at your bank, you should define it through this screen.

In the Application Browser, the Function Description screen is available under the System Administration module under Function Description.



Indicating Whether Parallel Maintenance is Required

You have the option to indicate whether you want to record capture the modification or addition of new details in parallel. After you have specified your preference, the data will be available in parallel for processing only after authorization.

You can have a parallel data structures for all the following maintenances:

- Customer Maintenance details
- Customer Address details
- Liability Maintenance
- Interest & Charges Special Conditions
- Customer A/c Maintenance
- GL's Maintenance
- Local Holiday details
- Currency Holiday details
- MIS Class Maintenance

Parallel Maintenance option is available only for the above mentioned functions.

Specifying Whether the Function ID Should be Available in the Archival Database

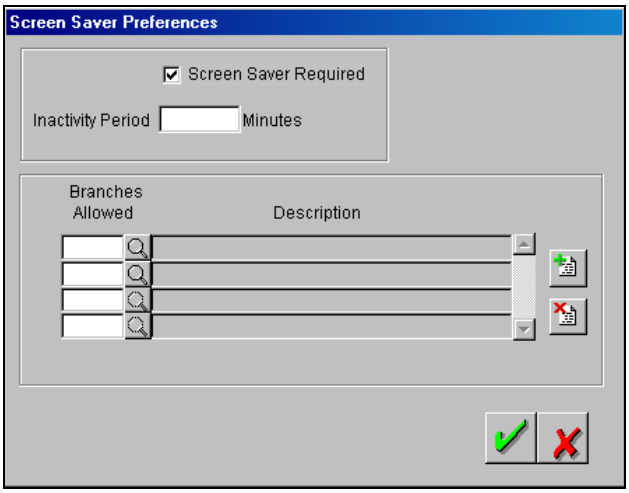
The archival database contains the soft purged data. In this database, you can view only those functions ids that are allowed on the Archival Database. To make the function ids (screens, in other words) available for viewing, you have to select the 'Allow In Archival Database' option when you define a function.

You can exercise this option for FX and MM modules only.

For more information on archiving and purging of data, refer the 'EOC Operations for FX and MM' chapter of the Operations User Manual.

2.1.11.1 Setting the Auto-lock Preferences for your Bank

For your bank, you can specify the inactivity period in Oracle FLEXCUBE after which the system should activate the password protected screen saver. Invoke the Screen Saver Preferences screen by clicking on the button in the SMS Bank Parameters screen.

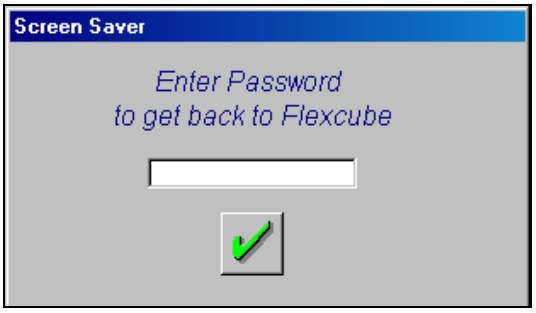


You can indicate that the system should automatically lock the workstations of user's after a specified time of inactivity. Also, specify the period after which the system should activate the screen saver if the system is inactive. The inactivity period is specified in minutes. As a result, each time a user in Oracle FLEXCUBE leaves the system inactive for the specified period, the system will activate the screen saver.

These preferences are maintained for your bank at the Head Office level. Since the auto-lock or screen saver preferences that you specify will have to be made applicable to all Oracle FLEXCUBE users whose sign-on branch is included in the Branches Allowed section of this screen you have to identify the branches of your bank in which you would like to enforce this preference.

The screen saver will be activated only if the Operating System is Windows/NT. Also note that it will not be activated if the modal window is active. For instance it will not be activated if the Error or Override message windows are open.

You have to enter your password to re-log into Oracle FLEXCUBE.



If you entered wrong password more than ‘n’ successive times, User status will be disabled and a message will be displayed stating that user will be logged off.

After you have indicated your preferences, the system will display the data as per the last authorized records. Only if you indicate this preference, the ‘Last authorized Record’ option in all the above mentioned maintenance forms will be enabled. Subsequently if you choose this option and execute a query, the system will fetch the data, which is the last authorized record. However, you cannot create, copy, close, reopen, or modify the record.

2.1.12 Defining a User Role

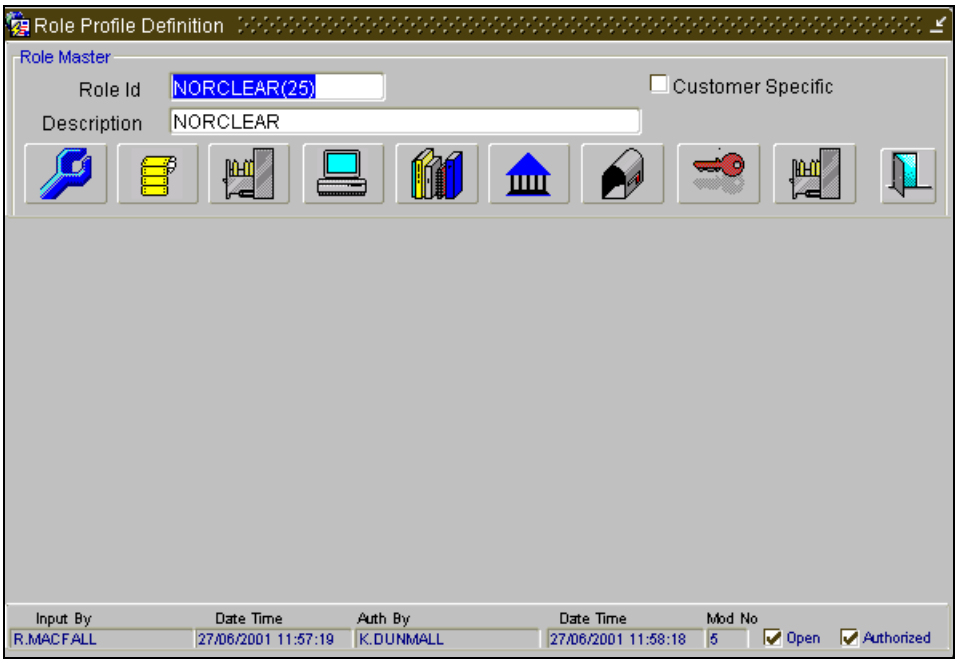
It is likely that users working in the same department at the same level of hierarchy need to have similar user profiles. In such cases, you can define a Role Profile, which includes access rights to the functions that are common to a group of users. A user can be linked to a Role Profile by which you give the user access rights to all the functions in the Role Profile.

2.1.13 Classifying a Role Profile

By default, a Role Profile you define will be for the users who are employees of your bank. You can indicate that the profile is for customers who might login from remote terminals to inquire on their transactions and balances.

2.1.14 The Procedure for Defining Role Profiles

Role profiles are defined in the Role Master screen. In the Control Clerk login screen, click on  button.



2.1.15 Defining Functions for a Role Profile

After you have defined the basic attributes of a role profile (the Role ID, Description, Branch and whether it is customer- specific) you should define the functions to which the role profile has access. The various functions in the system fall under four categories.

The categories and the icon in the Role Master screen that takes you to the respective function definition screen are as follows:

Category	Description	Icon
Maintenance	Functions relating to the maintenance of static tables.	
Batch	Functions relating to the automated operations (like automatic liquidation of contract, interest, etc.)	
Reports	Functions relating to the generation of reports in the various modules.	
On-line	Functions relating to contract processing.	

When the Role Functions screen is displayed, the following is the procedure for defining the functions.

To add a function, click on  . At Function ID, you should select the function for which you want to give rights. Click on the  button for a list of Function IDs belonging to the category along with their descriptions. From this list you can pick up the function for which you want to give access rights by double clicking on it when it is highlighted. You can then specify the rights to the different actions for the functions by checking against the action. These actions can be:

2.1.15.1 Static Tables

- New (Define a new record).
- Copy (Copy details of an existing record).
- Delete (Delete an existing record).
- Close (Close an existing record).
- Unlock (to amend an existing record).
- Reopen (Reopen an existing record).
- Print (Print the details of selected records).
- Authorize (Authorize any maintenance activity on a record).

2.1.15.2 Reports

- Generate (to generate reports)
- View (view the reports)
- Print (print the reports)

To delete the access rights given for a function, select the Function ID and click on  .

2.1.15.3 Batch

- Generate (to generate reports)
- View (view the reports)
- Print (print the reports)

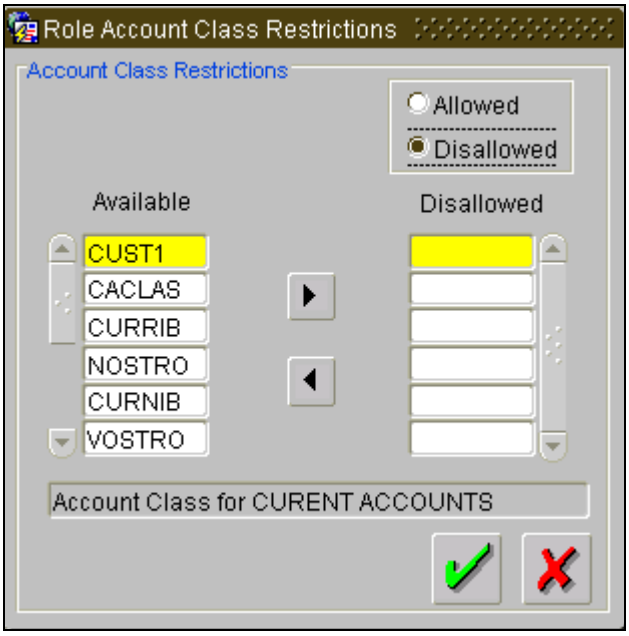
2.1.15.4 Contracts and On-Line Transaction Processing

- New (Define a new record).
- Copy (Copy details of an existing record).
- Delete (Delete an existing record).
- Close (Close an existing record).
- Unlock (to amend an existing record).
- Reopen (Reopen an existing record).
- Print (Print the details of selected records).
- Authorize (Authorize any maintenance activity on a record).
- Reverse (reverse an authorized contract).
- Rollover (to manually roll over an existing contract into a new contract).
- Confirm (to indicate the counterparty or broker confirmation of a contract).
- Liquidate (to manually liquidate a contract).
- Hold (to put a contract on hold).

- Template (to save a contract as a template).
- View (to see the details of the contract).

2.1.16 Restricting Account Class for a Role Profile

You can restrict a role from accessing certain Account Classes maintained, using 'Role Account Class Restrictions' screen. You can invoke this screen by clicking on  in 'Role Profile Definition' screen.



You can allow or disallow a role from accessing certain Account Classes.

Account Class Restrictions

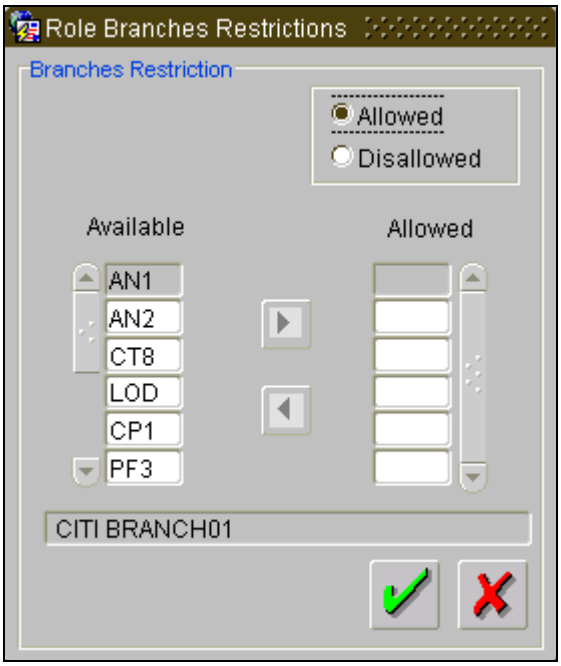
Select an option to restrict an Account Class from the following options:

- Allowed – if you need to allow a role to access certain Account Class.
- Disallowed – if you need to disallow a role to handle certain Account Class.

The system displays Account Classes maintained at your bank. Select the product and click on  . Based on your selection, the system will either allow/disallow the user from using the specified products.

2.1.17 Restricting Branch for a Role Profile

You can restrict a role from accessing certain Branch maintained, using 'Role Branches Restrictions' screen. You can invoke this screen by clicking on  in 'Role Profile Definition' screen.



You can allow or disallow a role from accessing certain Branch.

Account Class Restrictions

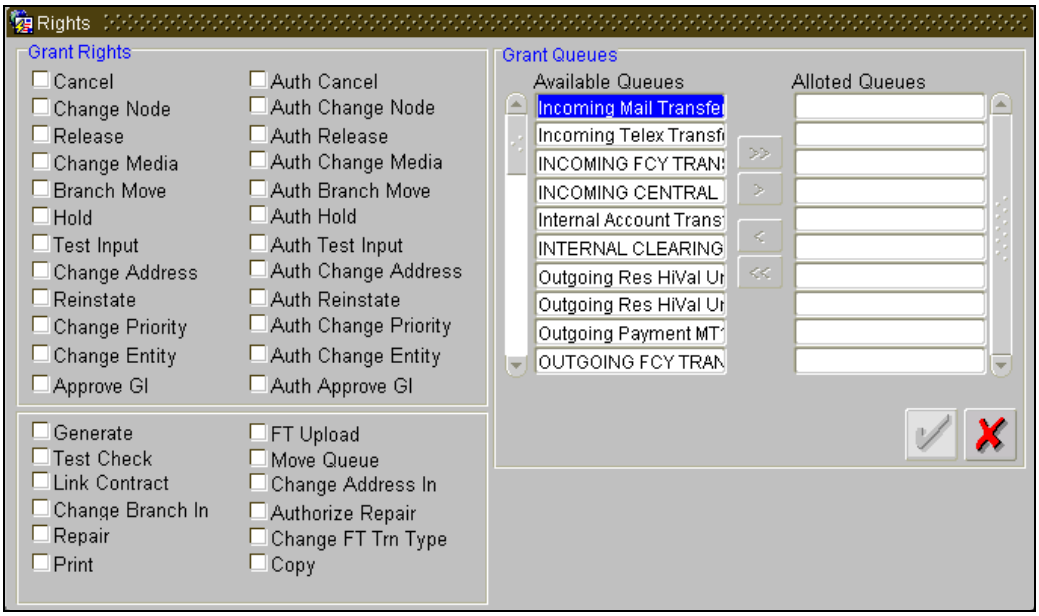
Select an option to restrict a Branch from the following options:

- Allowed – if you need to allow a role to access certain Branch.
- Disallowed – if you need to disallow a role to handle certain Branch.

The system displays branches maintained for your bank. Select the product and click on  . Based on your selection, the system will either allow/disallow the user from using the specified products

2.1.18 Providing Rights for a Role Profile

You can provide certain rights to a role, using 'Rights' screen. You can invoke this screen by clicking on  in 'Role Profile Definition' screen.



Grant Rights

Select the rights you need to grant by checking the box adjoining the following rights:

- Cancel
- Change Node
- Release
- Change Media
- Branch Move
- Hold
- Test Input
- Change Address
- Reinstate
- Change Priority
- Change Entity
- Approve GI
- Generate
- Test Check
- Link Contract
- Change Branch In
- Repair
- Print

- Auth Cancel
- Auth Change Node
- Auth Release
- Auth Change Media
- Auth Branch Move
- Auth Hold
- Auth Test Input
- Auth Change Address
- Auth Reinstate
- Auth Change Priority
- Auth Change Entity
- Auth Approve GI
- FT Upload
- Move Queue
- Change Address In
- Authorize Repair
- Change FT Trn Type
- Copy

Grant Queues

Select a queue and click on  . Based on your selection, the system will either allow/disallow the user from using the specified products. The system displays all available queues.

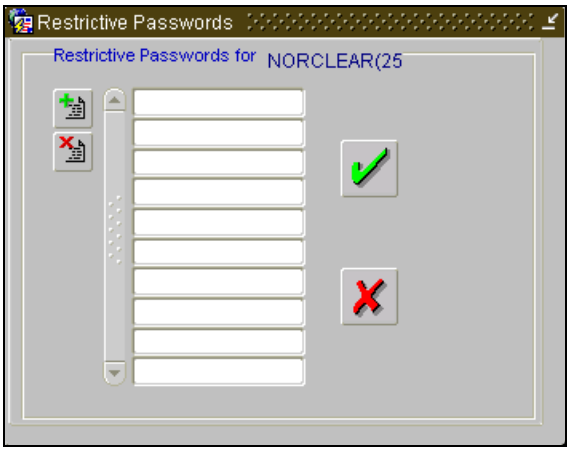
2.1.19 Defining Restrictive Passwords for a Role

You can define a list of passwords that cannot be used by a user. This list, called the Restrictive Passwords list can be defined at three levels:

- At the bank level (applicable to all the users of the system).
- At the user role level (applicable for all the users doing a similar kind of role).
- At the user level (applicable for the user).

The list of Restrictive Passwords should contain those passwords that the users are most likely to use: the name of your bank, city, country, etc. For a user role, it could contain names, or terms, that are commonly used in the department. At the user level, it could contain the names of loved ones, etc. By disallowing users from using such common passwords, you can reduce the risk of somebody other than the user knowing the password.

Click on key icon to define the list of Restrictive Passwords for the role profile you are defining.

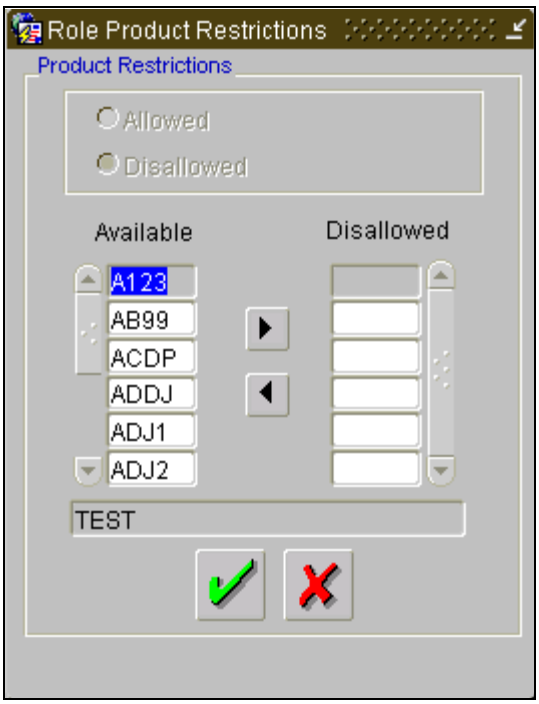


Any user, who is attached to the role, cannot use a password in this list.

You can define only the functions that are applicable for the role and the list of Restrictive Passwords for a role. All the other attributes of a user profile should be defined when the user profile is being created.

2.1.20 Restricting Products for a Role Profile

You can restrict a role from using certain products maintained, using 'Role Product Restrictions' screen. You can invoke this screen by clicking on in 'Role Profile Definition' screen.



You can allow or disallow a role from using certain products.

Product Restrictions

Select an option to restrict a product from the following options:

- Allowed – if you need to allow a role to handle certain products.
- Disallowed – if you need to disallow a role to handle certain products.

The system displays LS, LD and SLT products maintained at your bank. Select the product and click on  . Based on your selection, the system will either allow/disallow the user from using the specified products.

2.1.21 Copying the Role Profile of an Existing Role

Often, you may have to create a Role Profile that closely resembles an existing one. In such a case, you can copy the existing profile on to the new one.

Choose Copy from the Action menu. A list of existing role profiles will be displayed. Click on the one you want to copy. All the details of the profile except the Role ID will be copied and displayed. Enter a unique Role ID. You can change any of the details of the profile before saving it.

2.1.22 Deleting a Role Profile

A Role Profile should be deleted only if there are no users linked to it. Thus, before deleting a role profile, you should modify each user profile attached to it and delete the link to the role.

Select Delete from the Action menu to delete an existing role profile. If the role is linked to any user, a warning message will be displayed. This message will bring your attention to the fact that the user profile to which the role is linked will not be the same if the role profile is deleted.

You will be prompted to confirm the deletion. The Role Profile will be deleted only if you confirm the deletion.

2.1.23 Defining a User Profile

A User Profile defines the activities that a user can carry out on the system. It also contains the user ID, the name through which the user will access the system and the password.

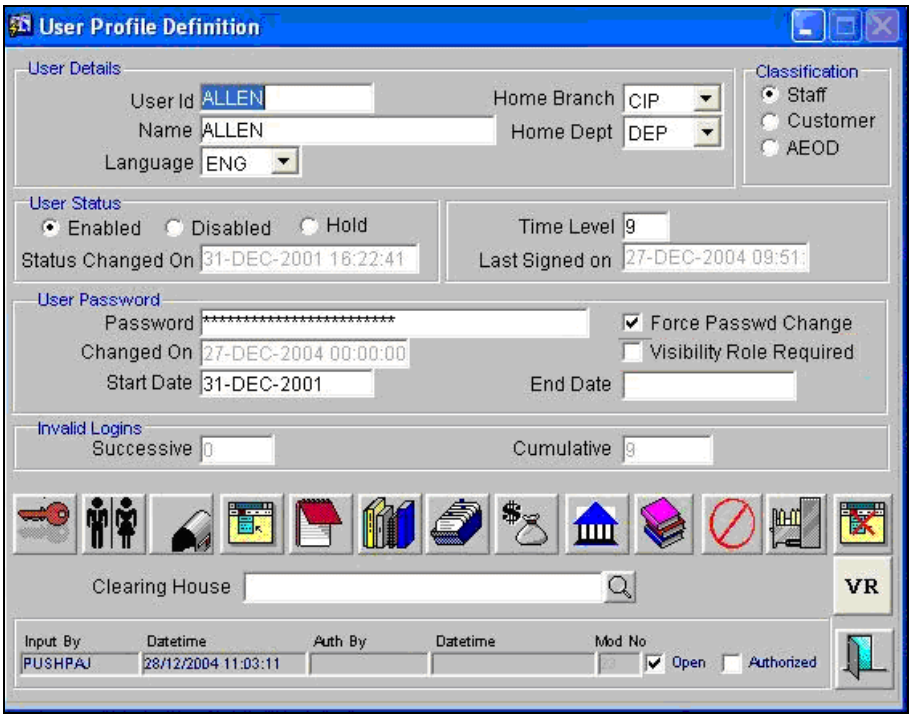
You can create User Profiles only when two Control Clerks have logged in. Click on  in the Control Clerk log on screen to invoke the function for user profile definition. After you have entered all the details in the first screen, click on the appropriate icon in the group of icons displayed at the bottom of the screen.

2.1.24 Classifying a User

You can classify a user as belonging to one of the following categories:

Staff	A user of the system who is an employee of your bank. You can include any of the functions available in the system in the user profile. Ideally, you should not include functions that are part of End of Cycle operations in the profile of a Staff user.
Customer	A customer who would want to log into the system from a remote terminal. You can include only those functions through which the customer can inquire into balances and transactions.
AEOD	A user at the bank who is responsible for running the automated End of Day operations. You can include any of the functions available in the system in the user profile. Ideally, you should include only functions that are part of End of Cycle operations in the profile of a AEOD user.

You can indicate this through the Classification field in the User Profile Definition screen. To invoke this screen, choose User Administration and then Detailed under it.



2.1.25 Allowing a User to Operate from Different Branches

When you create a User Profile, it will be attached to the branch where it is created. This means that the user can execute the functions defined for the profile from this branch. For a user profile, you can indicate that the user can access other branches also. The kind of functions a user can perform in a branch other than the one where the user profile is created depends on the category of the user.

2.1.25.1 User Belonging to the Staff Category

In each branch, you should create a user profile called the Guest. The functions defined for this branch will be applicable for a user of a different branch. Typically, this profile should have access to functions like inquiry into balances, etc. If this Guest profile is not created in a branch, a user not belonging to that branch will not be allowed to change branch to it.

The branch where the user profile is created is called the Home branch and the other branches are called Host branches.

2.1.25.2 User Belonging to the AEOD Category

For such a user, the functions defined for the user profile where the profile created (the Home branch) will be applicable in every branch (Host branch).

2.1.25.3 User Belonging to the Customer Category

A user of this category can log on only to the branch where the profile is created.

2.1.25.4 Auto Authorize

If automatic authorization has been enabled for a function, branch and user profile, and such a user has rights for both input and authorize operations, any record maintained by such a user in the corresponding function (maintenance or online) screens will be automatically authorized when the Save operation is performed.

Check this field to indicate that a user is allowed to perform automatic authorization.

For the maintenance to be authorized, the field, ‘Auto Authorize’ should be checked at both ‘User Profile Definition’ and ‘Function Description’ screens.

2.1.25.5 Visibility Role Required

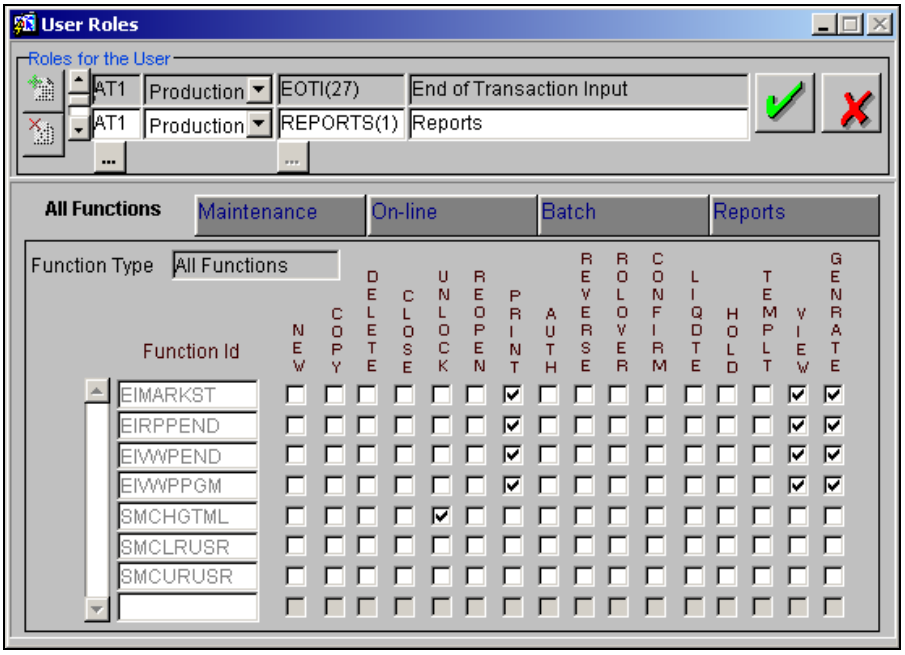
You can filter the data visible to the user based on expense code of the customer.

Check this field to indicate that data viewing is filtered for the user based on the expense code of the customer.

For more details on Visibility Roles refer to the section entitled ‘Maintaining Visibility Roles’ in this chapter.

2.1.26 Roles for the User

Through the User Roles Definition screen you can define branch specific user roles for each User Profile. Click on  in the User Profile Definition screen. The User Roles Definition screen will be displayed.



To attach a role to the user profile within a specific branch, click on  . Next, click on  and identify the Branch in which you would like to define the role. Subsequently, select from the list and choose the role which is to be associated with the User Profile by double clicking it.

For a user, you can define roles individually for the production database and for the archival database, if you have chosen to maintain the purge history tables in a separate archival server. The archival database holds the archived contract information and can only be viewed – you cannot perform any other operation on it. To allow the user to view the archived information, you have to attach the relevant roles at the time of defining user profiles and roles. This is in addition to allowing the function id in the archival database.

The functions that have been defined for the role will be displayed, depending on the category to which the functions belong. For example, when you click on  , the access rights defined for the role regarding the static screens will be displayed. Similarly, for a display of the rights in any other category click on the respective tab. To delete a role that has been attached to a user profile, highlight it and click on  .

2.1.27 Functions for the User

In addition to attaching a user profile to a role, you can give rights to individual functions. For a user profile to which no role is attached, you can give access to specific functions.

If you have:

- Attached one or more roles to a user profile, or
- You have given access to individual functions to a profile to which roles are attached.

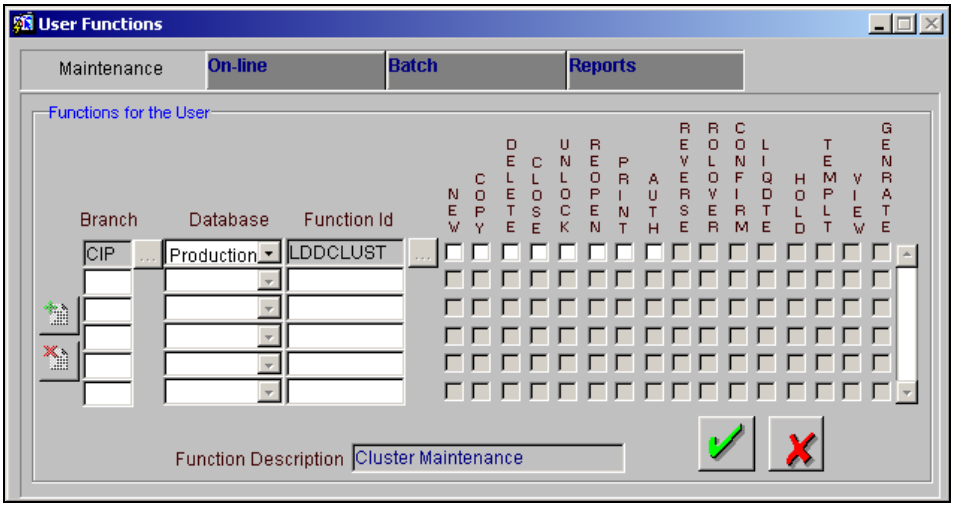
The rights for Function IDs that figure in both the role and user specific functions will be applied as explained in the following example.

Example

The role profile FXDP1 has access to New, Copy, Delete, Close, Reopen, Unlock and Print for the Forward Rates table.

You attach the user profile of Tanya to the role FXDP1. While allotting rights to individual functions for Tanya, you give rights to New, Copy, Delete and Close for the Forward Rates table. The role has access rights to Reopen, Unlock and Print in addition to these. In such a case, the user profile of Tanya will have rights to only the functions to which rights are given at the user profile level (that is, New, Copy, Delete and Close) even if the role FXDP1 has rights to other functions.

Click on  in the User Profile Definition screen to give access to functions for the user profile you are defining. The User Functions screen will be displayed.



The various functions in the system come under four categories. These categories and the tab in the User Functions screen that lets you define the rights for these categories are as follows:

Category	Description	Tab
Maintenance	Functions relating to the maintenance of static tables.	Maintenance
Reports	Functions relating to the generation of reports in the various modules.	Reports
Batch	Functions relating to the automated operations (like automatic liquidation of contract, interest, etc.)	Batch
On-line	Functions relating to contract processing.	On-line

To add a function, click on  . At Function ID, you should select the function for which you want to give rights. Click on  for a list of Function IDs belonging to the category along with their descriptions. From this list you can pick up the function for which you want to give access rights by double clicking on it when it is highlighted. You can then specify the rights to the different actions for the functions by checking the check box against the action. These actions can be:

2.1.27.1 Static Screens

- New (Define a new record).
- Copy (Copy details of an existing record).
- Delete (Delete an existing record).
- Close (Close an existing record).
- Unlock (to amend an existing record).
- Reopen (Reopen an existing record).
- Print (Print the details of selected records).
- Authorize (Authorize any maintenance activity on a record).

2.1.27.2 Contracts and On-Line Transaction Processing

- Reverse (reverse an authorized contract).
- Rollover (to manually roll over an existing contract into a new contract).
- Confirm (to indicate the counterparty or broker confirmation of a contract).
- Liquidate (to manually liquidate a contract).
- Hold (to put a contract on hold).
- Template (to save a contract as a template).
- View (to see the details of the contract).

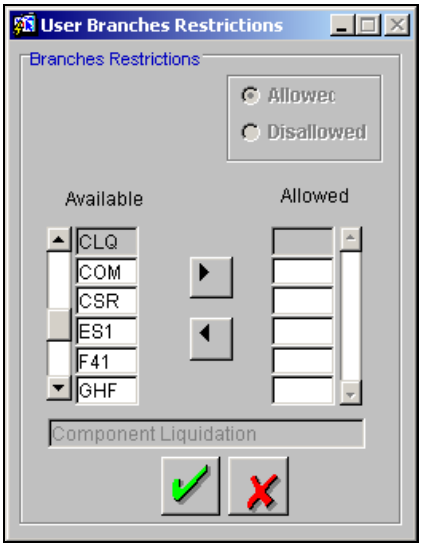
2.1.27.3 Reports

- Generate (to generate reports).
- View (view the reports).
- Print (print the reports).

To delete the access rights given for a function, select the Function ID and click on  .

2.1.28 Branches for the User

Through this screen, you can specify the branches from which the Staff and End of Day users of the bank can operate. Click on  in the User Definition screen to define the branches in which the user should be allowed to operate.



The User ID is displayed in the Branches for the User field. You can define the branches for this user.

To see the branches defined in the Branch Parameters screen, click on **Select**. A list of all the branch codes is displayed in a window. To allow the user access to a branch, highlight the branch code and click on  . The user can perform functions he has access to in the selected branch.

To disallow a user from accessing a branch, highlight the branch code and click on  . The user cannot access the selected branch. You can allow or disallow more than one branch to the user. To select all the branches displayed in the list, click on **Select All**.

The description of the branch as defined in the Branch screen is displayed here.

Note the following:

- The branch in which the user profile is defined is known as the Home Branch. The branches the user can access are known as the Host Branches.
- If the user belongs to the End-of-Day category, the user can perform functions he has access to in his Home Branch in the Host Branches also.
- You should create an ID called GUEST in each branch. When a user belonging to the Staff category changes the branch of operation, he can perform the functions defined for the GUEST ID in the Host Branch.

After specifying the branches, indicate whether the branches you have selected should be available for the user. If you select:

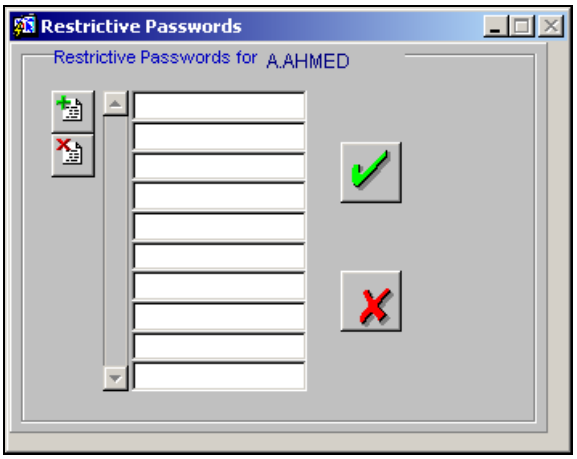
- Available (depending on the category, the user can access functions he has access to in all the selected branches).

- Not Available (the user cannot access functions in any of the selected branches).

2.1.29 Restrictive Passwords for the User

You can maintain a list of passwords that the user is most likely to use. For example, a user may tend to use the names of loved ones, the bank, department, etc. as a password as they are easy to remember. This might be a security risk as it will be easy for another person to guess a password. To prevent this, you can maintain a list of passwords that the user should not use. This list of restrictive passwords will be checked before a password is accepted when the user is changing passwords. If the password entered by the user exists in the list, it will not be accepted.

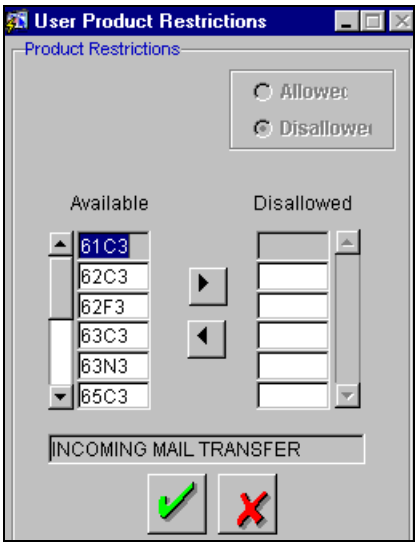
In the User Profile definition screen, click on  .



The user for whom you are defining the restrictive passwords cannot use restrictive passwords defined in the Bank Level Parameters screen and the Role Profile screen.

2.1.30 Restricting Products for the User

You can restrict the user from using certain products maintained in Oracle FLEXCUBE. Click on  to specify the product restrictions for the user. The ‘User Product Restrictions’ screen is displayed.



You can allow or disallow the user from using certain products.

- Select the option ‘Allowed’ if you want to allow the user to handle certain products.
- Select the option ‘Disallowed’ to disallow the user from using certain products.

The system displays LS, LD and SLT products maintained at your bank. Select the product and click on  . Based on your selection, the system will either allow/disallow the user from using the specified products.

Following screens display list of products based on the User Role product restriction:

- Borrower Facility Summary(LS)
- Borrower Tranche Summary(LS)
- Borrower Drawdown Summary(LS)
- Contract Dairy Events(LS)
- Fee Amendment(LS)
- Fee Liquidation(LS)
- Exchange rate fixing
- Interest rate fixing
- Draft Facilities(LS)
- Draft Tranches (LS)
- Draft Transfer(LS)
- Forward processing(LS)
- Manual Payment(LS)
- Margin Input(LS)
- Participant Transfer(LS)
- Split reprising(LS)
- Consolidate reprising(LS)
- Borrower Mnemonic(LS)
- Value dated amendment(LS)

- Contract Input(Loan & Commitment Operations)
- Contract Summary(Loan & Commitment Operations)
- Exchange rate amendment(Loan & Commitment Operations)
- Fee amendment(Loan & Commitment Operations)
- Fee Liquidation(Loan & Commitment Operations)
- Linkage Amendment(Loan & Commitment Operations)
- Loan manual rate revision(Loan & Commitment Operations)
- Manual Payment(Loan & Commitment Operations)
- Value dated amendment(Loan & Commitment Operations)
- LS/LD – Free format messages for Borrower / Participant/Summary
- Outgoing messages
- Draft trade
- Trade online
- Ticket Input

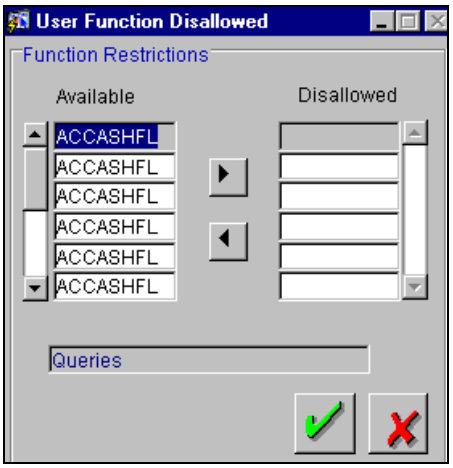
Note the following:

- You cannot perform any operation on a contract of product disallowed at 'User Roles' level, irrespective of it being allowed at 'Role Profile' level.
- At Draft Trade and Input levels, the system validates and displays CUSIP numbers with allowed Agency Tranche Product.
- If SLT product mapping exists for Origination Desk and SLT product is selected as 'Disallow' at 'User Roles' level, then the system displays the following error message:

Product Mapped for Internal Trade Booking

2.1.31 Disallowing Functions for the User

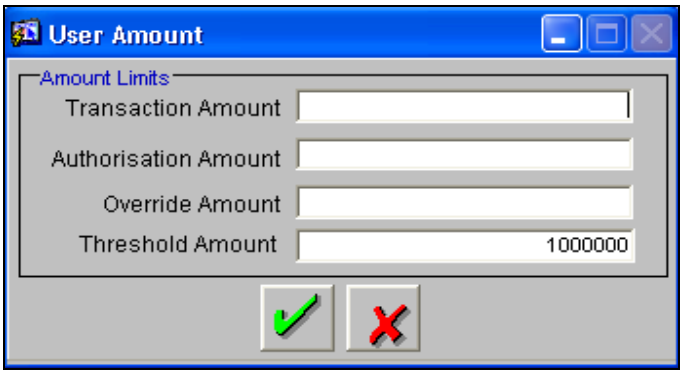
In Oracle FLEXCUBE, each screen is identified by a Function Id. You can restrict a user from accessing certain functions (screens). Click on to invoke the 'User Function Disallowed' screen.



The function Ids of all the screens is displayed. Select the Function Id and click on  to disallow the user from accessing the specified function.

2.1.32 Specifying Amount Limits for the User

You can place a limit on the transaction amount for a user. Consequently, the system will not allow the user to process transactions exceeding a specific limit. Click on  to indicate the limits.



In this screen, you can specify the following:

Amount Limit for Transactions

Express the amount in local currency. The user will not be allowed to process transactions exceeding the amount that you specify here.

Authorization Amount

Express the amount in local currency. Consequently, the user will not be allowed to authorize transaction amounts exceeding the authorization limit.

Override Amount

Express the amount in local currency. If the transaction amount exceeds the limit amount specified for the user, the system will display an override message. The user will be allowed to process further if the override limit is greater than the amount limit.

Threshold Amount

Specify the threshold amount in the local currency of user's home branch.

Example:

If the threshold amount specified for the user is 1MM, if the Commitment booking amount is 1.2MM then the commitment will not be authorized, the commitment will have to be authorized by other user.

Example

Case1: Let us assume the following:

- Transaction amount = USD 50,000
- Amount Limit = USD 40,000
- Override Limit = USD 50,000

Since the transaction amount is greater than the transaction amount limit, the system will display an override message. However, you can process further by ignoring the override as the override limit > amount limit.

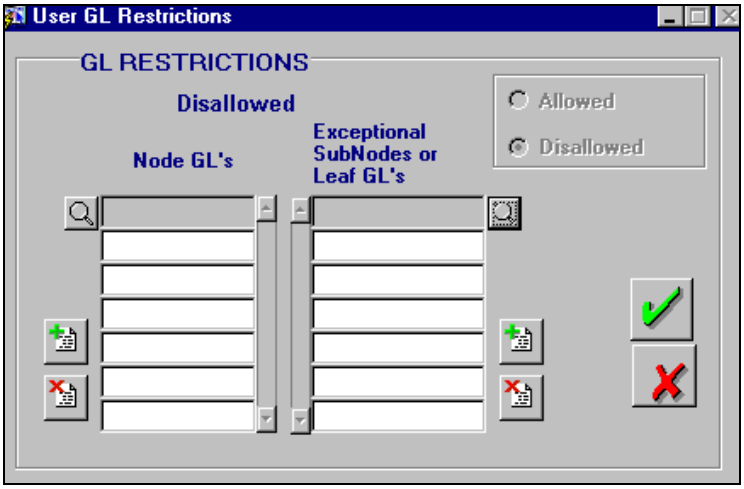
Case 2: For the same transaction amount and amount limit, if override limit= USD 40,000

Since the transaction amount is greater than the transaction amount limit, the system will display an override message. However, the system will not allow you to ignore the override as the override limit = amount limit.

2.1.33 Restricting GLs for the User

You can restrict the user from posting entries to certain GLs maintained in Oracle FLEXCUBE.

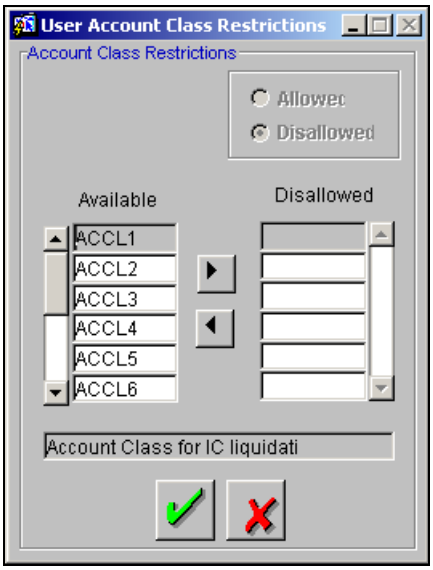
Further, you can restrict the user from posting entries to specific node and leaf GLs. Click on  to specify the GL restrictions.



You can either allow or disallow the user from using certain GLs. Select the node GLs and leaf GLs that you want to restrict.

2.1.34 Placing Account Class Restrictions

You can restrict the user from using certain account classes that are maintained in Oracle FLEXCUBE. Click on  to specify the account class restrictions.



You can either allow or disallow the user from using certain account classes. Subsequently, specify the account classes, which have to be restricted for the user.

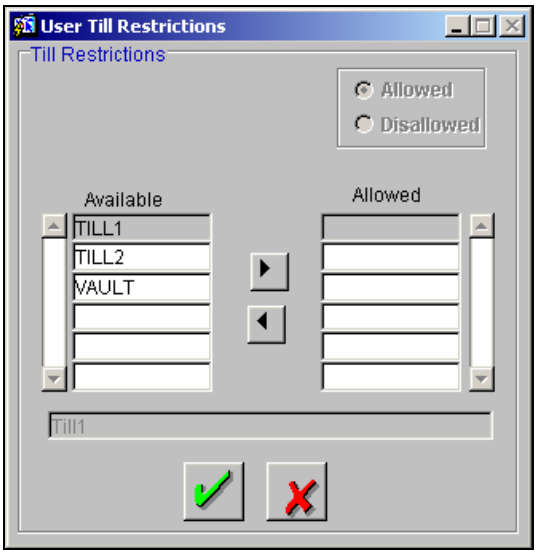
Additionally, if the account class is restricted, the user will not be able to view account balance of all the customer accounts belonging to the specified account class.

The following view screens will be disabled if the account class is disallowed for the user:

- Ad hoc Account statement generation during the day
- Accounting Entries details for Customer Account
- Customer Account Balances from Customer Information Retrieval
- Account Statements generated during EOD

2.1.35 Restricting Tills for the User

You can restrict the user from using certain tills maintained at your bank. Click on  to invoke the 'User Till Restrictions' screen.



You can either allow or disallow the user from using certain tills.

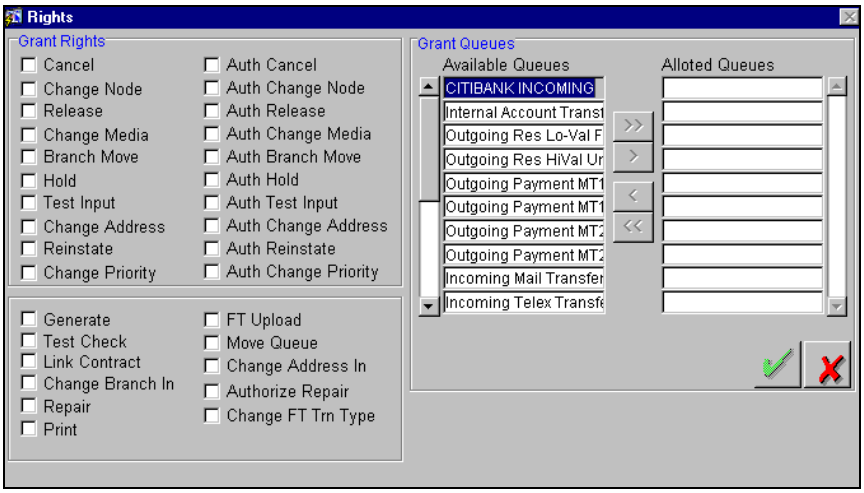
- Select the option 'Allowed' if you want to allow the user to manage certain tills.
- Select the option 'Disallowed' to disallow the user to manage certain tills.

The system will display the tills available at your bank. Select the till and click on  . Based on your selection, the system will either allow/disallow the user from using the specified tills.

2.1.36 Granting Rights for the User

A user should have the necessary rights to perform various operations in Oracle FLEXCUBE.

Click on  to grant the rights to the user.



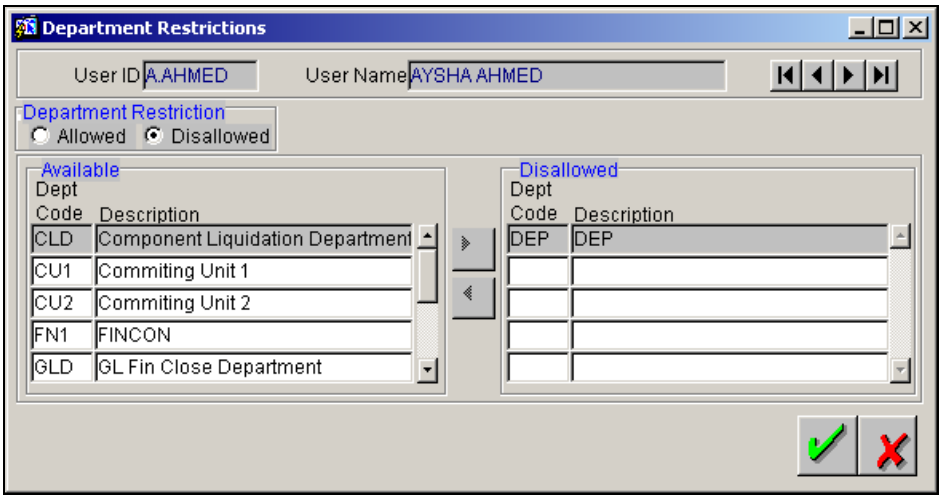
In this screen, you can grant rights for performing the various operations in Oracle FLEXCUBE. Check against the operations for which you want to grant the permission.

2.1.37 Defining Department Restrictions for the User

Every User Profile that you create will be attached to the branch where it is created. This means that the user can execute the functions defined for the profile from this branch.

As part of creating User Profiles you can define branch-wide department restrictions. Which means you can choose either to allow or restrict users of your bank from accessing specific departments within your branch. Consequently when users log into Oracle FLEXCUBE they will only be attached to those department to which they have been given access rights. Also the department and branch to which a user is attached to, will be displayed in the Title Bar of Oracle FLEXCUBE.

To invoke the Department Restrictions screen click on the icon in the User Profile Definition screen.



In this screen the User ID and the name assigned to the user whose profile you are creating will be displayed in the respective fields. You have to indicate other relevant details such as:

- Department Restriction
- Available/Disallowed

Specifying Department Restrictions

You have to indicate whether you are maintaining an allowed list of departments or a disallowed list. Under Department Restrictions, you can indicate this preference

Moving a Department to the Available /Allowed column

In the Department Restrictions screen, two columns are displayed:

- An Available list.
- An Allowed list.

The Allowed column that is displayed depends on the list that you have chosen to maintain. For example, if you have chosen to maintain an Allowed list of departments, the column will display the list of departments that you allow.

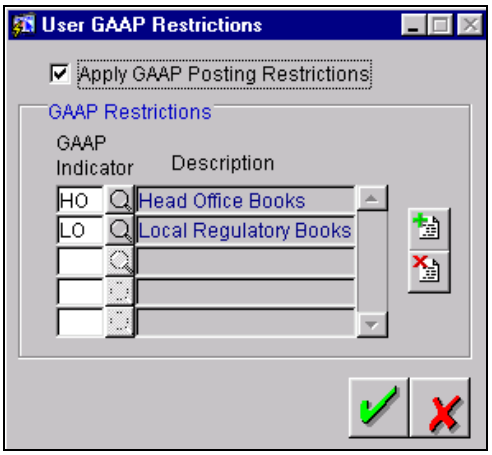
In the Available column, all the department codes maintained for your bank will be displayed. You can move a branch to the allowed column by using the keys provided for the same. Click to move an item from the available to the allowed list. Click to move an item back to the available column.

Subsequent to linking a user with a specific department(s) every transaction processed by the user will be tracked automatically by the department the user is attached to.

Similarly you will be allowed to generate a department-wise GL MIS report of the GL balances.

2.1.38 Placing GAAP Indicator Usage Restrictions on a User Profile

You can restrict the users of your bank from using specific GAAP indicators by placing usage restrictions on user profiles through the User GAAP Restrictions screen. Click on the button in the User Profile Definition screen the User GAAP Restrictions screen is displayed.



In this screen, you can indicate whether GAAP posting restrictions should be made applicable on a user profile by enabling the Apply GAAP Posting Restriction check box. If you enable the check box you must specify the GAAP indicators which should be restricted for the user profile.

The restrictions maintained for a user are enforced only while posting Journal and Multi-offset entries manually. During manual posting, for both journal and multi-offset entries, only the list of books common for a Branch, GL and User combination are made available for posting entries.

While uploading interfaces and contracts, the user level restrictions will not be enforced and the restrictions for a Branch, Account/ GL combination will be enforced. Also, User level restrictions are not made applicable for entries generating from products and entries that are posted to customer accounts.

2.1.39 Copying the User Profile of an Existing User

Often, you may have to create a user profile that closely resembles an existing one. In such a case, you can copy the existing profile on to the new one.

Choose Copy from the Action menu. A list of existing user profiles will be displayed. Click on the one you want to copy. All the details of the profile except the User ID and the password will be copied and displayed for the new user. Enter a unique User ID and give a password. You can change any of the details of the profile before saving it.

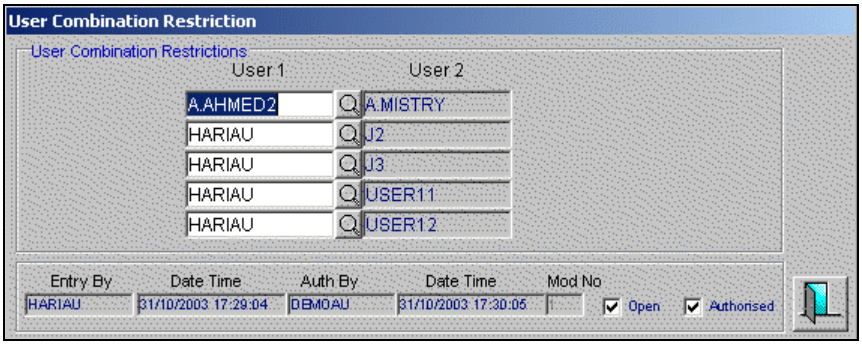
2.1.40 Deleting a User Profile

Select Delete from the Action menu to delete an existing user profile. Enter the User ID. The details defined will be displayed. The profile can be deleted only if the user is currently not logged on to the system. If the user has logged in, a message will be displayed and you cannot delete the profile. If the user is not logged in, you will be prompted to confirm the deletion. The user profile will be deleted only if you confirm the deletion.

2.2 Specifying User Combination Restriction

You can define a list of maker and checker combination that are disallowed through the User Combination Restriction screen.

Invoke the screen under User Administration in Security Maintenance from the Application Browser to define the list of user combination for the user profile you are defining. Any user with the specified user id will not be allowed to complete a transaction or any maintenance in the system.



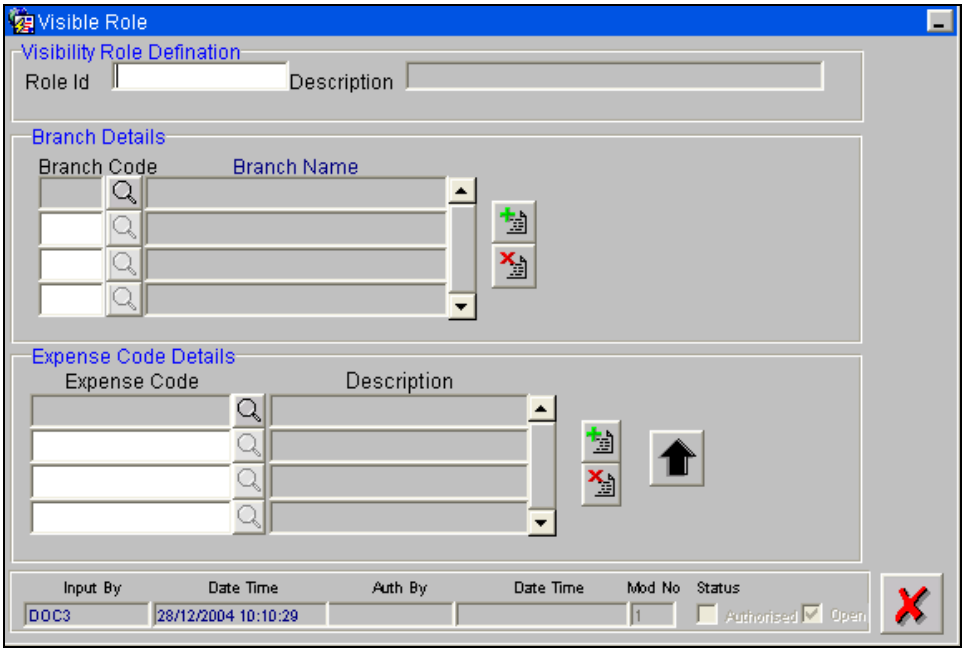
You can select the User1 and User2 to indicate the combination for which you want to maintain maker checker restriction. For example if User 1 is restricted with User 2, the system does not allow User 2 to authorize any record for which the maker id is User 1. Similarly, User 1 cannot authorize any records for maker id User 2.

STOP Also, User Combination restrictions are made applicable for entries generating from i-cube customer accounts.

2.3 Maintaining Visibility Roles

You can maintain Visibility Roles for the users and allow access to Customer and Contract information only to the users whose expense codes have privileges to the relevant information.

This visibility role maintenance you can do using, 'Visible Role' screen. To invoke this screen, choose **Security Maintenance** from the Application Browser. Thereafter, choose **SYS. Administrator** and **Visibility Role Maintenance** under it.



2.3.1.1 Visibility Role Definition

Role ID

Specify the identification of Visibility Role.

Description

Specify a short description of the Role Id.

2.3.1.2 Branch Details

Branch Code

Specify the branch code of the customer. You can filter data viewing for the user, based on the branch code you maintain here.

Branch Name

The description of the branch is displayed here.

2.3.1.3 Expense Code Details

Expense Code

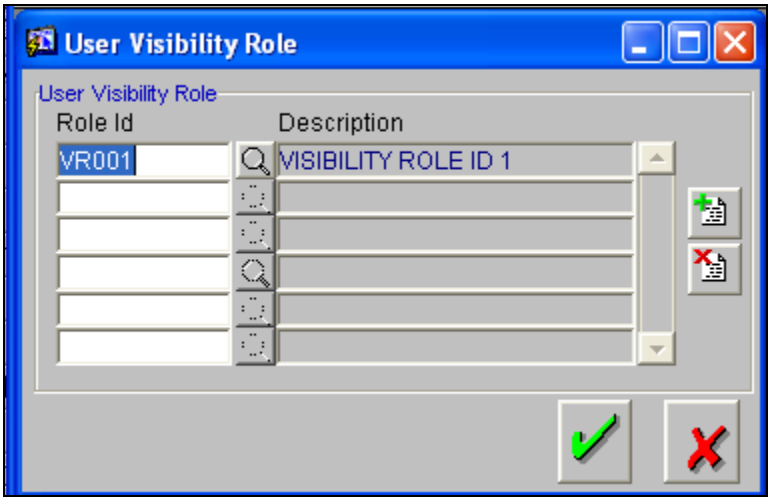
Specify the customer MIS for the Expense Code. You can filter data viewing for the user, based on the customer MIS you maintain here.

Description

The description of the Expense Code (Cust MIS) is displayed.

2.3.2 Mapping User Visibility Role to a User

Click VR in 'User Profile Definition' screen to invoke 'User Visibility Role' screen. Here, you can map Role Ids to a user for filtering data viewing.



Role ID

Specify the identification of the visibility role for the user. You can select this Role ID from the option list as well.

Description

The description of the corresponding Role Id is displayed in this field.

Note the following:

- The data filtering is applicable for the following screens in new/amendment and query modes
  - Loan/Commitment Contract Online Screen – Filtering in new mode is applicable in Counterparty Option List.
  - Borrower Subscreen Commitment Online Screen – Filtering in new/amendment mode is applicable for Borrower Option List.
  - Borrower Contact Screen
  - Borrower Address Screen
  - LD product maintenance
  - LD Reprice screen
  - LD Contract Summary screen

The data filtering is applicable for the following screens in the query mode based on the combination of expense code and user id

- Customer Maintenance Screen
- Customer Account Screen
- Loan Contract Online Screen
- Loan Contract Payment Screen
- Value Dated Amendment
- Customer Summary Screen
- Customer Account Summary Screen
- Borrower Contact Summary Screen
- Borrower Address Summary Screen
- Commitment/Loan Summary Screen
- Loan Quick Query Screen
- Commitment Quick Query Screen
- Loan Quick Reference Summary Screen
- Commitment Quick Reference Summary Screen

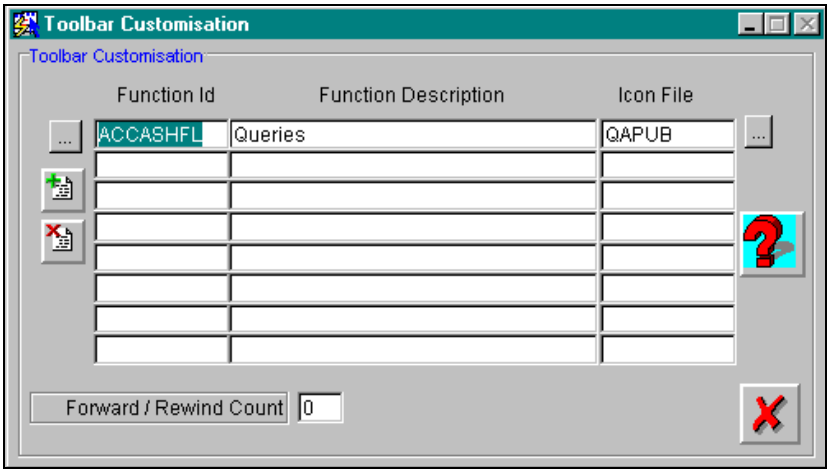
- New option is available in the following screens is applicable only after querying the given record
  - Value Dated Amendment
  - Loan Contract Payment Screen

3. Associated Functions

3.1 Customizing the Toolbar

The toolbar contains a set of icons where each icon is associated with an option in the main menu. Through this table, you can customize the toolbar by adding or deleting icons from it.

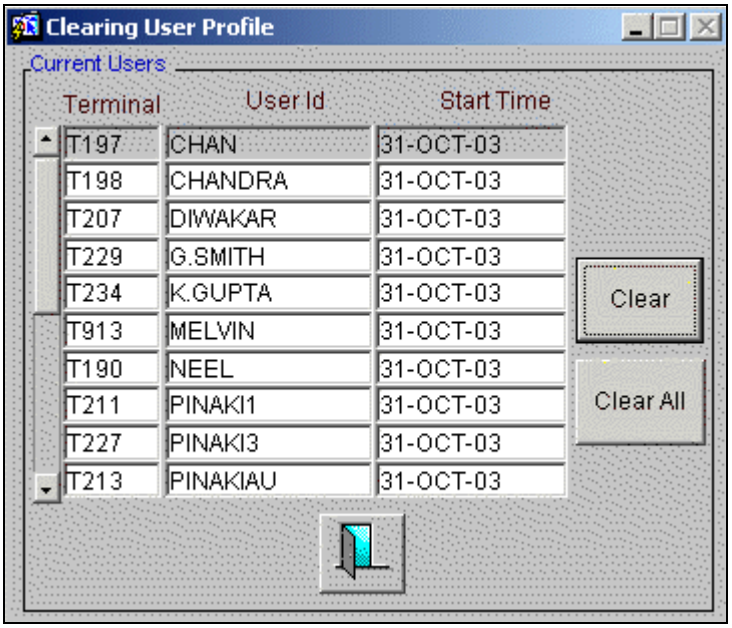
You can define the function for each icon. When you click on the icon, the file associated with it is activated and the corresponding function is performed. To invoke this screen, choose User Administration and Toolbar Definition under it.



3.1.1 Clearing a User ID

Occasionally, you may come across a situation when a user who is logged on was forced out of the system but the User ID still continues to have a status of Currently Logged In. In such a situation, the user will not be allowed to log in to the system again.

Such User IDs can be cleared through the Clear User Profile function. In the Application Browser, this function is available under the module Security Maintenance under Clear User. The user Id s of users currently logged into the system will be displayed.



Highlight the user Id you want to clear and click on 

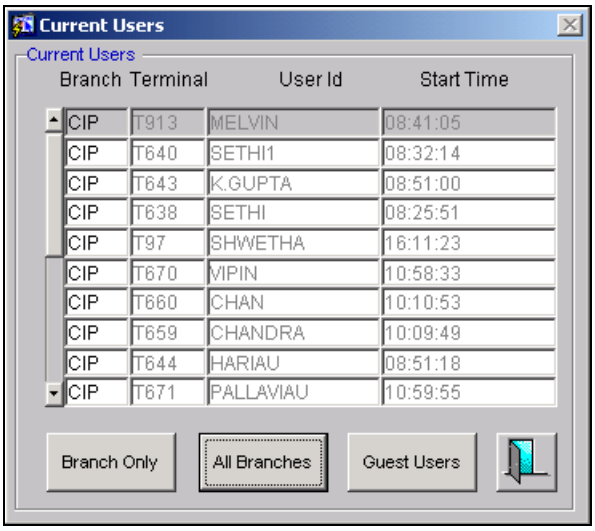
.

3.1.2 Current Users

In Oracle FLEXCUBE, it is possible for a user to view the other users who have logged on to the system.

To invoke the Current Users screen, click on the Security Maintenance module in the Application Browser, and select the Current Users option under this module. In this screen, you can view the other users who have logged into the system. This is applicable only for the following options:

- Branch Only
- All branches
- Guest users



3.1.3 Defining Function Description

This screen allows you to maintain a function description for various function ids of Oracle FLEXCUBE such as Forms, Reports and stored procedure. Each module and menu head has a function description.

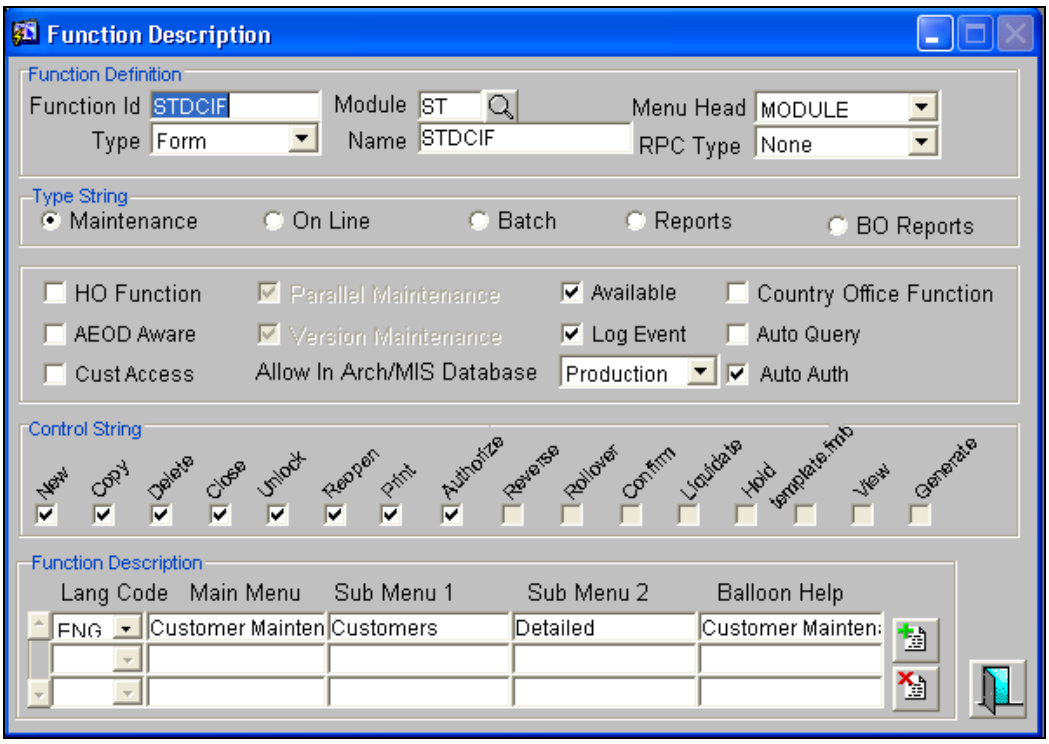
Based on the type of string - maintenance, online, batch, reports or BO reports, you can define the control strings and availability of the same in the Application Browser.

Auto Authorize

To indicate that a user is allowed to perform automatic authorization, you have to enable the 'Auto Authorize' option in the User Maintenance screen.

Note: For the maintenance to be authorized, the auto auth flag should be checked at both 'User Profile Definition' and 'Function Description' screens.

To access the Function Description screen, click on Security Maintenance in the Application Browser. Select the System administration option under it to open the screen.



The system allows the following events for Auto Authorization subject to the threshold limit.

3.1.3.1 Maintenance

Customer Level	Auto Auth/Manual
Borrower Setup	Auto Auth
Borrower Contacts Setup	Auto Auth
Borrower additional address setup	Auto Auth
Borrower Settlement Instructions setup	Manual

3.1.3.2 Commitment Contract Level

Commitment Level Events	Auto Auth/Manual
Commitment Booking/Setup	Conditional Auto Auth based on Threshold amount
Unused Commitment Fee payment	Auto Auth
Fee Rate change	Auto Auth

Commitment Level Events	Auto Auth/Manual
Fee amendment to change basis	Auto Auth
Commitment Increase/Decrease	Conditional Auto Auth based on Threshold amount
Commitment amendment	Auto Auth
Excess unused commitment Fee Refund	Manual
Payable/Receivable	Manual
all reversals like Loan Reversal, VAMI reversal, Fee Reversal	Manual
Value dated amendment to change commitment revolver/non-revolver flag change	Manual

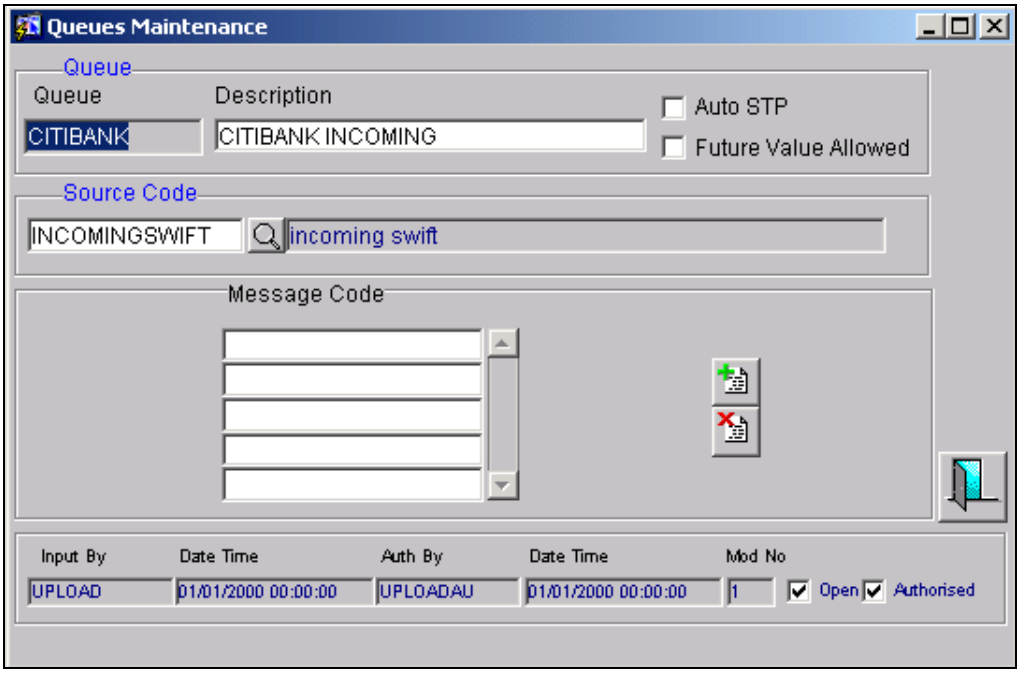
3.1.3.3 Loan Contract Level

Loan Level Events	Auto Auth/Manual
Loan Booking/Setup	Conditional Auto Auth based on Threshold amount
Loan Initiation	Conditional Auto Auth based on Threshold amount
Principal/Interest Payment; interest over payment; Interest waiver	Auto Auth
Loan Increase	Conditional Auto Auth based on Threshold amount
Interest Rate change , Basis Change	Auto Auth
LIBOR loan Manual rate Revision - Enhancement (new screen)	Auto Auth
Loan Renewal	Manual
Loan amendment	Auto Auth
Excess Interest Refund	Manual
Payable/Receivable	Manual
all reversals like Loan Reversal , Payment Reversal, VAMI reversal, Fee Reversal	Manual

3.1.4 Defining Messaging Queues

For uploading incoming messages from different sources, you can define different queues. Based on the setup, you can select other parameters such as Auto STP and Future value allowed.

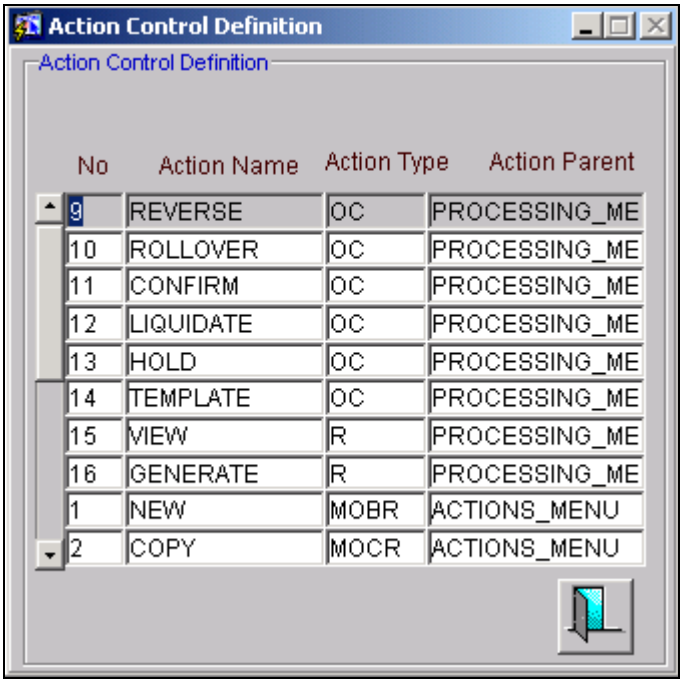
To invoke this screen, click on Security Maintenance in the Application Browser, and select the System administration option under this module.



3.1.5 Action Items Definitions

This screen displays the order in which the action menu and the processing menu are defined.

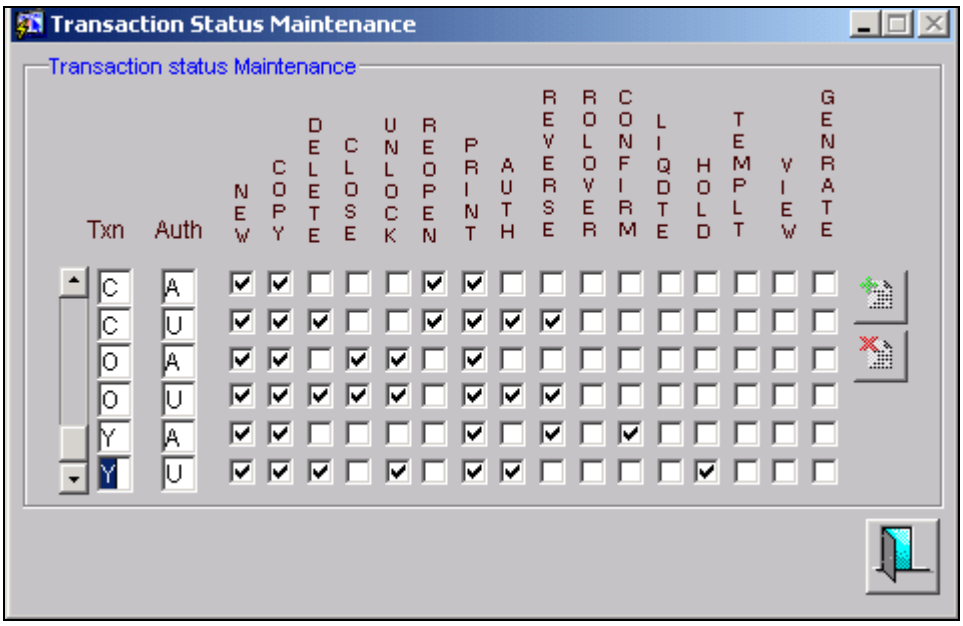
In the Application Browser select the Security Maintenance module and the System administration option under it to invoke the Action Control Definition screen.



3.1.6 Transaction Status

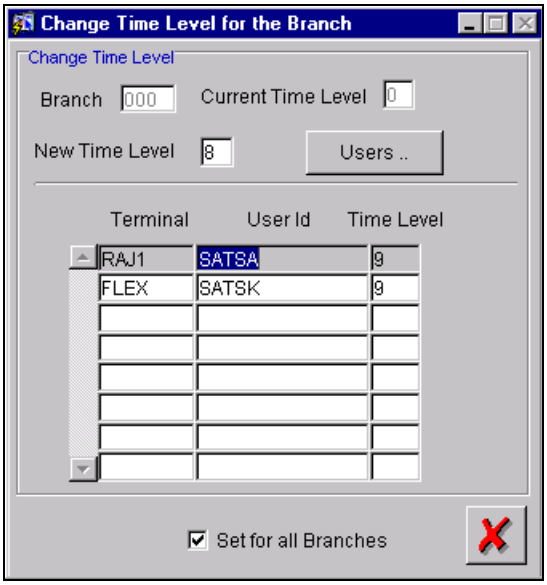
This screen displays the Transaction status control strings for different transaction and authorization statuses. For example, a record that is open and authorized cannot be deleted. Thus, the delete box is unchecked for this record.

To invoke the Transaction Status Maintenance screen, select the Security Maintenance module in the Application Browser and click on the System administration option under this module.



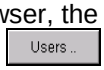
3.1.7 Changing the System Time Level

The time level is set at two levels: the system level and the user level. For a user to be able to login, the time level for the user profile should be greater than or equal to that of the system. You can set a time level that is between one and nine. To invoke this screen, choose System Administration and then Change Time Level.



You can set the time level, individually, for each branch, or opt to set a time level for all branches. Choose the 'Set for all Branches' option to enforce a specific time level on all branches of your bank.

Setting the time level is a convenient option during end-of-cycle operations. Just before beginning the End of Cycle operations (when it is necessary that no user is logged in) increase the time level of the system so that it is higher than that of any user. The users logged in will be able to complete the function they are currently running before they are logged out. You can then run the End of Cycle functions.

In the Application Browser, the Change Time Level function is available under Security Maintenance. Click on 

for a display of the details of users who are currently logged in.

3.1.8 Defining Language Codes

A Language Code identifies every language that is supported by the system. In Oracle FLEXCUBE, the language code is maintained as a three character alphanumeric code.

In the Application Browser, the Language Code Maintenance screen is available under the module Bank Parameters under Language Codes.

To add a Language Code, click on  . Enter the three digit alphabetical Language Code for Oracle FLEXCUBE.

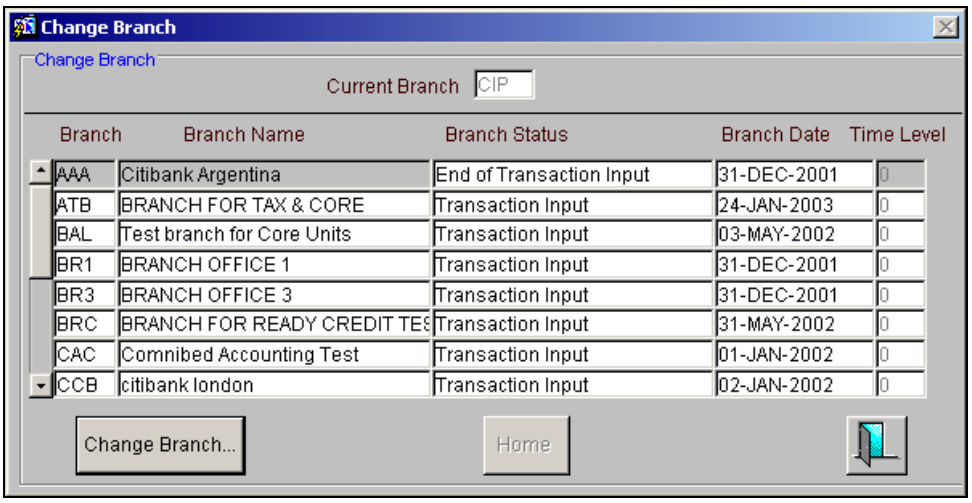
Example

For English, the code you could enter in Oracle FLEXCUBE could be ENG.

3.1.9 Changing the Branch of Operation

Through this function, you can change the branch of operation to a branch other than the one you are signed on to. The branches to which you can change into will be defined in your user profile. You can change your branch of operation only when a function that has been initiated by you in the current branch has been completed.

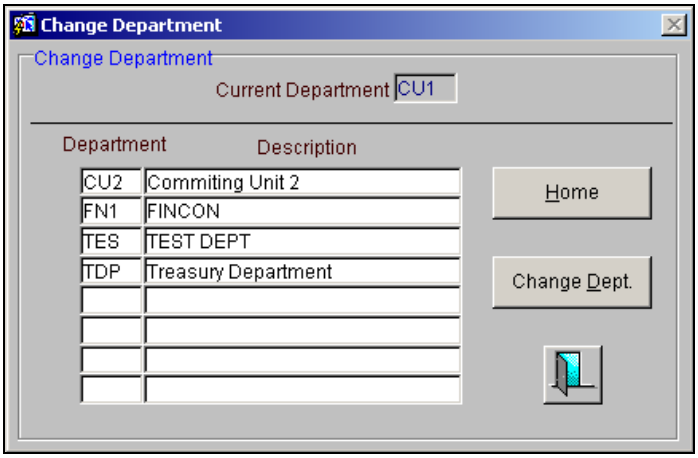
When you select the Change Branch option from the Menu under Options, the following details of the branches that have been defined are displayed:

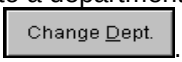


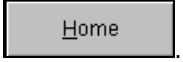
3.1.10 Changing the Department

The Change Department function allows you to change the department in which you are working to a department other than the one you are signed on to. The department to which you can change into will be defined in your user Profile.

When you select the option, the following details of the departments that have been defined are displayed:



You can move to a department other than the one in which you are working in by highlighting it and clicking on 

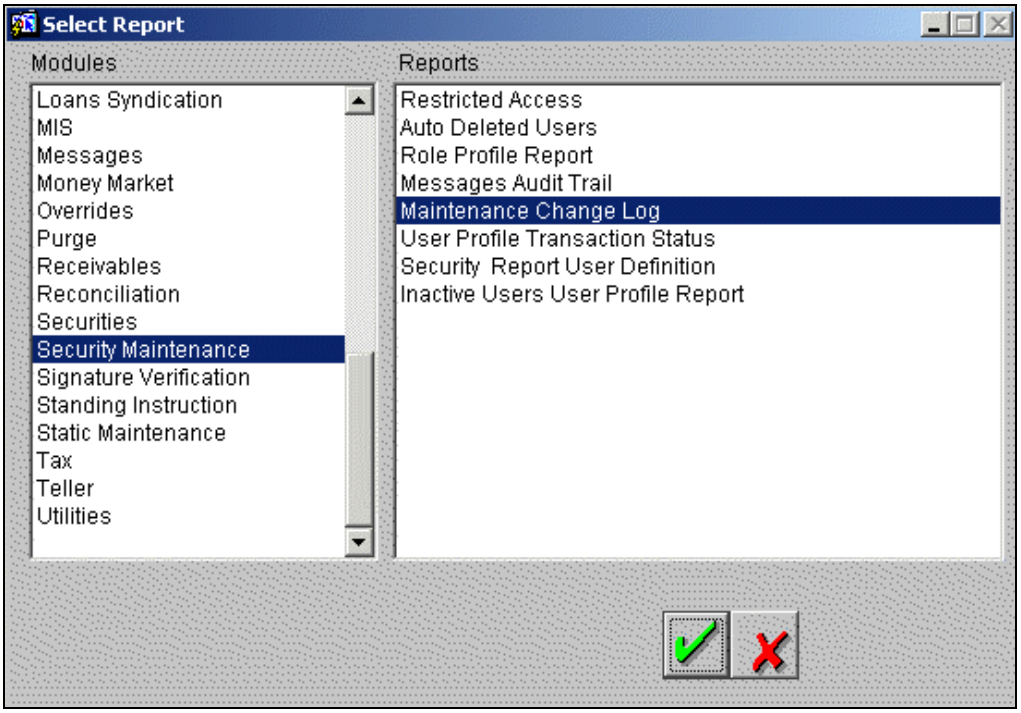
. Similarly if you want to move to the home department, click on 

.

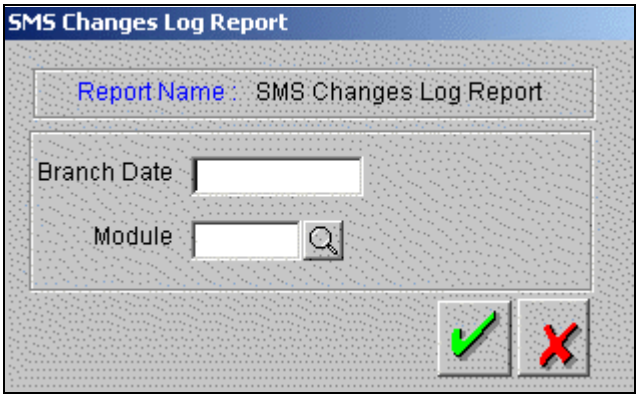
3.2 Maintaining a Log Report of SMS Changes

Whenever there is a change made to the user profile / role profile definitions in Oracle FLEXCUBE, you can track these changes through the SMS change log report screen. Here the system lists all the changes to security maintenance operations such as change to user profile / Role profile.

A report is generated that specifies the old values / new values for each role profile / user profile that has undergone change and also records the history details. To invoke this screen, from the Application Browser, choose Reports and then Generate.



Click on  to open the following screen.



You can select the report options from the option list.

Also an installation parameter will be available to set whether maintenance history is required or not. If maintenance history flag is set to “YES” then in the purge process the data that is deleted from record log and field log will be moved to a history table. History report can be taken from BO.

4. Error Codes and Messages

4.1 Error Codes and Messages for the Security Management System

ERR_CODE	Message
SM--00018	USER Record has been successfully CLOSED.
SM-00001	Unauthorised Installation . Contact Bank Representative
SM-00002	Licensed Number of Users exceeded. Try again after a while
SM-00003	GUEST Ids can sign on only via Change Branch function
SM-00004	Invalid Login
SM-00005	User already logged in
SM-00006	User Status is Disabled. Please contact your System Administrator
SM-00007	User Status on Hold. Contact your System Administrator
SM-00008	Your Time level does not permit you to Login . Contact your Branch System Administrator
SM-00009	Please change Password now!
SM-00010	Password file missing or corrupt
SM-00011	Contact your System Administrator. Oracle built in problem
SM-00012	SMTBS_PASSWORDS table missing or entries not found
SM-00014	Password due to expire on $1
SM-00015	User Profile expired. Contact Branch System Administrator
SM-00016	Your Time Level does not permit you to launch this function
SM-00018	Closure of user profile successful
SM-00019	USER Record has been successfully REOPENED.
SM-00020	Some of the Functions are NOT allowed in MIS Database
SM-00030	This Function is currently not available for execution
SM-00031	This Form $1 is not available. Contact your Branch System

ERR_CODE	Message
	Administrator
SM-00032	The Time Level in the Branch has changed. Your time level does not permit you to execute any Functions
SM-00033	The number of Users currently executing Functions in this Module has exceeded the License limit.
SM-00034	This Function is not available for Customer Access
SM-00035	This Function is not available for Staff Access
SM-00036	Function Id is not correct. Enter Function Id again
SM-00037	Main menu and Sub Menu Descriptions cannot be same
SM-00040	Wrong Password. Enter Password again
SM-00041	The New and Confirmed Passwords do not match. Enter Passwords again
SM-00042	The Password entered is Restricted. Try another Password
SM-00043	The Password entered has already been used. Try another Password
SM-00044	Length of Password is less than $1 characters
SM-00045	Length of Password is more than $1 characters
SM-00046	The Password string contains special characters that are not allowed. Retype Password
SM-00047	Password cannot contain more than $1 consecutive identical characters
SM-00048	You cannot change Password today.
SM-00049	The password should be mix of alphabetic and numeric characters.
SM-00050	Control Clerks Passwords do not match. Retype Passwords again
SM-00060	There are Users currently logged in with a lesser time level. Do you want to change?
SM-00070	You are currently executing some Functions. Exit from those Functions and try again
SM-00078	Product mapped for Internal trade booking
SM-00079	One or more SLT products are mapped for Internal trade booking

ERR_CODE	Message
SM-00080	User Id already exists.
SM-00081	Negative Amount not allowed
SM-00082	Start cannot be before today
SM-00083	End Date cannot be before Start Date
SM-00084	Start Date cannot be Null
SM-00085	User Profile saved
SM-00086	Could not save User Profile
SM-00087	User Profile deleted
SM-00088	Could not delete User Profile
SM-00089	Mandatory or not null fields are missing
SM-00090	Role Id already exists
SM-00091	Users attached to the Role.Cannot Delete
SM-00092	Role deleted
SM-00093	Invalid Role Id
SM-00094	Currency Code not defined
SM-00095	Branch Code not defined
SM-00096	Customer No not defined
SM-00097	Customer Category not defined
SM-00098	Role Profile Saved
SM-00099	This queue already exists
SM-00100	Cannot Delete the Role .There are Users attached to this Role.
SM-00101	Cannot Delete Function. There are Users attached to this Function.
SM-00102	Cannot Modify Function. There are Users attached to this Function.
SM-00103	Do You Want to Delete the User?
SM-00104	Do You Want to Delete the Role?

ERR_CODE	MESSAGE
SM-00105	Cannot delete role. Users attached to role.
SM-00110	Site Code -Length cannot be less than 4 characters
SM-00111	Cumulative Invalid Logins - Number should be greater than 5 and less than 100
SM-00112	Successive Invalid Logins - Number should be greater than 2 and less than 6
SM-00113	Password prevent reuse value should be between 1 and 5
SM-00114	Minimum Password length should be between 6 and 10
SM-00115	Maximum Password Length should be between 9 and 12
SM-00116	Graph Not Found. Contact your Branch Administrator
SM-00117	Password change after message - no of days should be greater than 15 and less than 180
SM-00118	Archival Period should be greater than 0
SM-00119	Enter the Role Description
SM-00120	Cannot Delete/Modify Role of other Branch
SM-00121	Idle time before Sign off should be between 30 and 600
SM-00122	Password expiry message - between 0 and 5
SM-00123	Enter a valid Module Id
SM-00125	Min password Length should be Less than Max Password length
SM-00126	Override Idle Time should be greater than 10
SM-00130	User Access to $1 $2 denied
SM-00131	Duplicate values encountered
SM-00132	Change Branch Allowed Only From Home Department
SM-00140	GUEST Id not defined in Branch $1
SM-00150	Maximum value encountered
SM-00151	User Status is Disabled. User will be logged off

ERR_CODE	MESSAGE
SM-00160	Users attached to the Language code. Cannot Delete
SM-00161	Language Code already exists. Try another one
SM-00170	Reserved word cannot be used
SM-00171	Max password Length can not be null
SM-00172	Min password Length can not be null
SM-00173	Min password alphabets length can not be greater than Max password alphabets length
SM-00174	Min password alphabets length can not be greater than Max password length
SM-00175	Min password alphabets length + Max password numeric length can not be greater than Max password Length
SM-00176	Min password alphabets length + Min password numeric length can not be greater than Min password Length
SM-00177	Min password numeric length can not be greater than Max password numeric length
SM-00178	Min password numeric length can not be greater than Max password length
SM-00179	Min password numeric length + Max password alphabets length can not be greater than Max password Length
SM-00180	Max password alphabets length can not be lesser than Min password alphabets length
SM-00181	Max password alphabets length can not be greater than Max password length
SM-00183	Max password numeric length can not be greater than Max password length
SM-00184	Max password numeric length can not be lesser than Min password numeric length
SM-00186	Password should contain atleast $1 Numeric characters
SM-00187	Password should contain atleast $1 Alphabetic characters
SM-00188	Min password alphabetic length can not be Greater than Min password length

ERR_CODE	MESSAGE
SM-00189	Min password numeric length can not be Greater than Min password length
SM-00191	Password should contain atmost $1 Numeric characters only
SM-00192	Password should contain atmost $1 Alphabetic characters only
SM-00200	Consecutive Password Characters should be greater than 1
SM-00201	Value should be 0 or greater
SM-00202	The User is un-authorized
SM-0020200	The Bank Parameters record is not authorized
SM-00203	The Last Login date was - $1
SM-00204	Notice before disable must be less than Disable after
SM-00205	Notice before delete must be less than Delete after
SM-00206	First Enter the value for Disable after
SM-00207	First Enter the value for Delete after
SM-00208	Gave problems in taking back up of user info
SM-00209	Disable after must be less than Delete after
SM-00500	Mandatory values missing or null
SM-00501	Activation Key contains irrelevant characters. Wrong Activation Key
SM-00502	Installation with this key already done. Cannot duplicate
SM-00503	Installation not done. Contact BSA or Bank representative
SM-00510	No Branches defined for User
SM-00520	Could not delete Function Role attached
SM-00530	Could not delete Function Users attached
SM-00540	Could not delete Function
SM-00550	Function successfully saved
SM-00560	Function not implemented
SM-00600	Category Normal allowed only for module SS

ERR_CODE	MESSAGE
SM-00610	No Functions Defined for the User
SM-00612	You are not logged on
SM-00997	Password Changed Successfully
SM-00999	First and last letter cannot be numeric
SM-01000	Invalid Password. Bad Sign On
SM-01001	Invalid Name. Bad Sign On
SM-01002	Successive Invalid Logins Forced Disable
SM-01003	Cumulative Invalid Logins Forced Disable
SM-01004	Password expired. Password changed
SM-01005	User initiated Password change.
SM-01006	Forced password change
SM-01007	Status Enabled
SM-01008	Status put on Hold
SM-01009	No of licensed Users for modules exceeded
SM-01010	No of licensed Users for Bank exceeded
SM-01011	Wrong Activation Key entered
SM-01012	Duplicate Terminal Id encountered.
SM-01013	SMS User profile Cleared
SM-01014	Restricted Access program invoked by Control Clerks
SM-01015	User Profile Definition Form invoked
SM-01016	Role Profile Definition Form invoked
SM-01017	SMS Bank Parameters Definition Form invoked
SM-01018	Wrong Control Clerk Password Entered
SM-01100	Entries in SMS Bank Parameters Missing
SM-01101	Could not get today's date for the head office

ERR_CODE	MESSAGE
SM-01102	Bank Code not maintained in Branch Table
SM-01103	Local Currency not maintained in Bank Table

ERR_CODE	MESSAGE
SM-01104	User already Signed on
SM-01105	User $1 in Branch $2 changed branch to Branch $3 as User $4
SM-01205	Both Passwords expired. Change Password Now
SM-01206	Password1 expired. Change Password Now
SM-01207	Password2 expired. Change Password Now
SM-02000	INTERNAL ERROR : Exception Raised in $1
SM-02001	Enter From Date
SM-02002	Enter To Date
SM-02003	From Date cannot be later than To Date
SM-02004	Enter From Time
SM-02005	Enter To Time
SM-02006	From Time cannot be later than To Time
SM-02007	Select all Users to use purge option
SM-02008	Role Id should be entered
SM-02009	User Id should be entered
SM-05000	Installation successful
SM-06001	User does not exist
SM-09999	INTERNAL ERROR : Unhandled Exception Raised
SM-10000	Do you want to reset Cumulative Invalid Logins to 0?
SM-10001	Head office Branch code is not valid
SM-10002	Language Code must be 3 characters

ERR_CODE	MESSAGE
SM-10003	Branch is Closed
SM-10004	Number of Invalid Logins Since Last Logout = $1
SM-20000	Could not get details for User Branch
SM-20001	You are Already Executing the Function
SM-20002	You have been Logged Out. Do You Want to Login Again ?
SM-20003	User Password Changed Successfully
SM-20004	Please Select a Branch
SM-3T-00001	You are already logged in. Do you want to clear the previous profile
SM-555555	Sign off allowed only from home branch
SM-555556	Logout allowed only from home branch
SM-66666	Amount Exceeds Users Authorization Limit
SM-77777	User Does not Have Rights to Authorize the Override
SM-C0050	Invalid branch code
SM-C0051	Duplicate record
SM-C0052	Null Function Id or Branch code - Delete record to proceed
SM-CHTML001	Enter a value between 0 and 9 for new-time-level
SM-DATE1	Failed to convert date format
SM-DEMO01	Oracle FLEXCUBE not properly installed, Exiting !
SM-DEMO02	Demo Version will Expire after $1 day(s)
SM-DEMO03	Welcome to Oracle FLEXCUBE
SM-DEMO04	Only one user is allowed to Login in Demo Version of Oracle FLEXCUBE, Exiting!
SM-DEMO05	Insufficient parameters to Launch Oracle FLEXCUBE, Exiting !
SM-DEMO06	Oracle FLEXCUBE Demo Version does not allow this function
SM-DEMO07	Demo Version Expired, Please Contact Bank !!!
SM-DEMO08	Demo Version Allows only $1 Contracts.

ERR_CODE	MESSAGE
SM-DEMO09	Demo Version Expires Today
SM-DTCH01	More than one user working
SM-DTCH02	AEOD Dates not maintained
SM-DTCH03	Wrong Branch status to run this form
SM-DTCH04	More than one function executing
SM-DTCH07	GLMISUPD/MIDATCOL still not completed. Wait till it finishes
SM-DTCHO1	User/s already logged in
SM-EFIN01	User(s) in Transactions Input
SM-EFIN02	Users are currently logged into the system. The branch status cannot be changed.
SM-EIMAN01	Branch Code is mandatory
SM-EIMAN02	Eoc Group is mandatory
SM-EIMAN03	Function Id is mandatory
SM-EIMAN04	Module Id is mandatory
SM-EIMAN05	Frequency is mandatory
SM-EIMAN06	Holiday Rule is mandatory
SM-EXTUS	Oracle FLEXCUBE has been launched from another application. Sign off disallowed. Please exit
SM-FND01	Menu Items Not Populated
SM-FND02	A function cannot be maintained only at country level
SM-IS001	Please select the AMC
SM-MISDB1	Direct Logon to MIS Database not allowed
SM-MISDB2	HOST maintenance is missing for home branch
SM-MISDB3	MIS and PRODUCTION is maintained as a single database
SM-NORIGHT	The user does not have rights for the function.
SM-NOTML	Please input the new time level.

ERR_CODE	MESSAGE
SM-OPS-001	Encountered unexpected error.
SM-OPS-002	Could not find the details of the branch
SM-OPS-003	Encountered unexpected error.
SM-OPS-004	Encountered unexpected error.
SM-OPS-006	Could not find the details of the branch or the date
SM-PRD02	Deletion NOT allowed as Periods beyond $1 exist for the Financial cycle
SM-PRD03	The Period End Date has to be the LAST Day of a Month
SM-PWC01	Password same as previously used password
SM-PWD01	Change password now !!
SM-QRY-01	The form is in the enter-query mode. Please click on the exit toolbar button or exit menu item to get to the normal mode.
SM-QRY01	The form is in the enter-query mode. Please click on the exit toolbar button or exit menu item to get to the normal mode.
SM-USR-001	Home branch should be in the list of allowed branches
SM-USR-002	Home branch should be in the list of allowed branches
SM-USR-003	Home department should be in the list of allowed departments
SM-USR-004	Home department should be in the list of allowed departments
SMS-0001	Same User of Key1 cannot Input Key2 Value. Try with another User ID
SMS-0002	About to Input Key1 value.
SMS-0003	About to Input Key2 value.
SMS-0004	Key1 Value Changed Successfully
SMS-0005	Key2 Value Changed Successfully
SMS-0006	Password Encryption Successful
SMS-0007	Key Value cannot be Empty
SMS-0008	Key should be 7 characters long
SMS-0009	Restricted / Invalid key

ERR_CODE	MESSAGE
SM_LOCKD	Contract Locked By Other User. Please try Again Later