

Security Management System  
Oracle FLEXCUBE Universal Banking  
Release 12.0.1.13.10  
[July] [2013]  
Oracle Part Number E51465-01



# Table of Contents

|           |                                                             |            |
|-----------|-------------------------------------------------------------|------------|
| <b>1.</b> | <b>ABOUT THIS MANUAL.....</b>                               | <b>1-1</b> |
| 1.1       | INTRODUCTION.....                                           | 1-1        |
| 1.2       | AUDIENCE.....                                               | 1-1        |
| 1.3       | ABBREVIATIONS.....                                          | 1-1        |
| 1.4       | GLOSSARY OF ICONS.....                                      | 1-2        |
| 1.5       | RELATED DOCUMENTS.....                                      | 1-2        |
| <b>2.</b> | <b>SECURITY MANAGEMENT.....</b>                             | <b>2-1</b> |
| 2.1       | INTRODUCTION.....                                           | 2-1        |
| 2.2       | SETTING UP PARAMETERS AT THE BANK LEVEL.....                | 2-2        |
| 2.2.1     | <i>Invalid Logins.....</i>                                  | 2-2        |
| 2.2.2     | <i>Specifying Parameter.....</i>                            | 2-3        |
| 2.2.3     | <i>Specifying Warning Screen Text.....</i>                  | 2-3        |
| 2.2.4     | <i>Specifying Parameters for User Passwords.....</i>        | 2-3        |
| 2.2.5     | <i>Placing Restrictions on User Passwords.....</i>          | 2-5        |
| 2.2.6     | <i>Branch Restrictions for Specific Applications.....</i>   | 2-6        |
| 2.2.7     | <i>Password Restrictions.....</i>                           | 2-7        |
| 2.3       | USER DETAILS MODIFICATION IN BULK.....                      | 2-8        |
| 2.4       | CREATING COMMON BRANCH RESTRICTIONS.....                    | 2-10       |
| 2.5       | DEFINING FUNCTIONS.....                                     | 2-12       |
| 2.6       | DEFINING A USER ROLE.....                                   | 2-15       |
| 2.6.1     | <i>The Procedure for Defining Role Profiles.....</i>        | 2-16       |
| 2.6.2     | <i>Defining Functions for a Role Profile.....</i>           | 2-16       |
| 2.6.3     | <i>Branch Restriction.....</i>                              | 2-17       |
| 2.6.4     | <i>Account Class Restriction.....</i>                       | 2-18       |
| 2.6.5     | <i>Rights.....</i>                                          | 2-18       |
| 2.6.6     | <i>Password Restriction.....</i>                            | 2-20       |
| 2.6.7     | <i>Copying the Role Profile of an Existing Role.....</i>    | 2-21       |
| 2.6.8     | <i>Closing a Role Profile.....</i>                          | 2-21       |
| 2.6.9     | <i>Defining Roles for Oracle FLEXCUBE Branch Users.....</i> | 2-21       |
| 2.7       | DEFINING A LIMITS ROLE.....                                 | 2-22       |
| 2.8       | DEFINING USER HOLIDAYS.....                                 | 2-24       |
| 2.9       | VIEWING HOLIDAY SUMMARY DETAILS.....                        | 2-25       |
| 2.10      | DEFINING A USER PROFILE.....                                | 2-27       |
| 2.10.2    | <i>Restricted Passwords.....</i>                            | 2-35       |
| 2.10.3    | <i>Roles.....</i>                                           | 2-36       |
| 2.10.4    | <i>Rights.....</i>                                          | 2-37       |
| 2.10.5    | <i>Functions.....</i>                                       | 2-39       |
| 2.10.6    | <i>Tills.....</i>                                           | 2-41       |
| 2.10.7    | <i>Account Classes.....</i>                                 | 2-41       |
| 2.10.8    | <i>General Ledgers.....</i>                                 | 2-42       |
| 2.10.9    | <i>Limits.....</i>                                          | 2-43       |
| 2.10.10   | <i>Branches.....</i>                                        | 2-45       |
| 2.10.11   | <i>Products.....</i>                                        | 2-46       |
| 2.10.12   | <i>Group Code Restriction.....</i>                          | 2-47       |
| 2.10.13   | <i>Disallowed Functions.....</i>                            | 2-48       |
| 2.10.14   | <i>Users Holiday.....</i>                                   | 2-49       |
| 2.10.15   | <i>Centralized Role.....</i>                                | 2-50       |
| 2.10.16   | <i>Dashboard Mapping.....</i>                               | 2-51       |
| 2.10.17   | <i>Copying the User Profile of an Existing User.....</i>    | 2-53       |
| 2.10.18   | <i>Deleting a User Profile.....</i>                         | 2-53       |

|           |                                                                               |            |
|-----------|-------------------------------------------------------------------------------|------------|
| 2.10.19   | <i>Closing a User Profile</i> .....                                           | 2-53       |
| 2.11      | SPECIFYING DEPARTMENT DETAILS .....                                           | 2-53       |
| 2.12      | DEFINING ALERTS FOR USERS .....                                               | 2-54       |
| 2.13      | SINGLE SIGN ON (SSO) ENABLED ENVIRONMENT .....                                | 2-56       |
| <b>3.</b> | <b>ASSOCIATED FUNCTIONS</b> .....                                             | <b>3-1</b> |
| 3.1       | CLEARING A USER ID .....                                                      | 3-1        |
| 3.2       | CHANGING THE SYSTEM TIME LEVEL.....                                           | 3-2        |
| 3.3       | VIEW CURRENT USERS .....                                                      | 3-3        |
| 3.4       | DEFINING LANGUAGE CODES .....                                                 | 3-4        |
| 3.5       | CHANGING THE BRANCH OF OPERATION .....                                        | 3-5        |
| 3.6       | CHANGING THE USER PASSWORD.....                                               | 3-5        |
| 3.7       | MAINTAINING SSO PARAMETERS .....                                              | 3-6        |
| 3.8       | MAINTAINING TRANSACTION STATUS CONTROL .....                                  | 3-7        |
| 3.9       | MAINTAINING ERROR MESSAGES.....                                               | 3-8        |
| 3.9.1     | <i>Configuring Customized Hot Keys for Launching Screens</i> .....            | 3-9        |
| 3.10      | VIEWING USER ACTIVITIES .....                                                 | 3-10       |
| 3.11      | VIEWING BRANCH STATUS.....                                                    | 3-10       |
| <b>4.</b> | <b>ERROR CODES AND MESSAGES</b> .....                                         | <b>4-1</b> |
| 4.1       | ERROR CODES .....                                                             | 4-1        |
| <b>5.</b> | <b>REPORTS</b> .....                                                          | <b>5-1</b> |
| 5.1       | EVENTS LOG REPORT .....                                                       | 5-1        |
| 5.1.1     | <i>Contents of the Events Log</i> .....                                       | 5-1        |
| 5.2       | SECURITY MANAGEMENT SYSTEM VIOLATIONS LOG REPORT .....                        | 5-3        |
| 5.2.1     | <i>Contents of the Security Management System Violations Log Report</i> ..... | 5-4        |
| 5.3       | USER PROFILE REPORT.....                                                      | 5-4        |
| 5.3.1     | <i>Contents of the User Profile Report</i> .....                              | 5-5        |
| 5.4       | CHANGES REPORT .....                                                          | 5-6        |
| 5.4.1     | <i>Contents of the Changes Report</i> .....                                   | 5-7        |
| 5.5       | INACTIVE USERS AGING ANALYSIS REPORT .....                                    | 5-8        |
| 5.5.1     | <i>Contents of the Inactive Users Aging Analysis Report</i> .....             | 5-8        |
| 5.6       | SMS USER INACTIVE LOG REPORT .....                                            | 5-8        |
| 5.6.1     | <i>Contents of the Inactive Users Log Report</i> .....                        | 5-9        |
| 5.7       | ONLINE PERFORMANCE STATISTICS REPORT.....                                     | 5-10       |
| 5.7.1     | <i>Contents of the Online Performance Statistics Report</i> .....             | 5-10       |
| 5.8       | BATCH PERFORMANCE STATISTICS REPORT.....                                      | 5-11       |
| 5.8.1     | <i>Contents of the Performance Statistics report</i> .....                    | 5-12       |
| 5.9       | CHANGE CONTROL LOG REPORT.....                                                | 5-13       |
| 5.9.1     | <i>Contents of the Report</i> .....                                           | 5-14       |
| 5.10      | EVENT LOG REPORT.....                                                         | 5-15       |
| 5.10.1    | <i>Contents of the Report</i> .....                                           | 5-16       |
| 5.11      | CHANGES LOG REPORT .....                                                      | 5-17       |
| 5.11.1    | <i>Contents of the Report</i> .....                                           | 5-17       |
| 5.12      | NEW USER CREATED REPORT .....                                                 | 5-18       |
| 5.12.1    | <i>Contents of the Report</i> .....                                           | 5-19       |
| 5.13      | ROLE PROFILE CREATED REPORT.....                                              | 5-20       |
| 5.13.1    | <i>Contents of the Report</i> .....                                           | 5-21       |
| 5.14      | USER PROFILE REPORT.....                                                      | 5-22       |
| 5.14.1    | <i>Contents of the Report</i> .....                                           | 5-23       |
| 5.15      | ROLE PROFILE REPORT.....                                                      | 5-24       |
| 5.15.1    | <i>Contents of the Report</i> .....                                           | 5-25       |
| 5.16      | USER ROLE SUMMARY REPORT.....                                                 | 5-26       |
| 5.16.1    | <i>Contents of the Report</i> .....                                           | 5-27       |
| 5.17      | USER ENTITLEMENT REPORT.....                                                  | 5-28       |

|           |                                     |            |
|-----------|-------------------------------------|------------|
| 5.17.1    | <i>Contents of the Report</i> ..... | 5-29       |
| <b>6.</b> | <b>SCREEN GLOSSARY</b> .....        | <b>6-1</b> |
| 6.1       | FUNCTION ID LIST.....               | 6-1        |

---

# 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 startup parameters in the individual client workstations.<br>To set up security management parameters for the Bank. |
| SMS Administrator for the Bank   | To set the SMS bank parameters.<br>To identify the Branch level SMS Administrators.                                                       |
| SMS Administrator for the Branch | To create User and Rsddole profiles for the branches of your bank.<br>Will also grant access to the various functions to the Users.       |
| A Oracle FLEXCUBE user           | Any user of Oracle FLEXCUBE whose activities are traced by the SMS module.                                                                |

## 1.3 Abbreviations

| Abbreviation | Description              |
|--------------|--------------------------|
| FC           | Oracle FLEXCUBE          |
| AEOD         | Auto End of Day          |
| BOD          | Beginning of Day         |
| EOD          | End of Day               |
| EOTI         | End of Transaction Input |
| EOFI         | End of Financial Input   |

| Abbreviation | Description                                          |
|--------------|------------------------------------------------------|
| The System   | This term is always used to refer to Oracle FLEXCUBE |
| SI           | Standing Instructions                                |
| MM           | Money Market                                         |
| RM           | Relationship Manager                                 |

## 1.4 Glossary of Icons

This User Manual may refer to all or some of the following icons.

| Icons                                                                              | Function    |
|------------------------------------------------------------------------------------|-------------|
|   | Exit        |
|   | Add row     |
|   | Delete row  |
|  | Option List |

## 1.5 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.

#### **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.

#### **User Profiles**

The user profile of a user contains the User ID, the password and the functions to which the user has access.

#### **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 Administrator 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.

#### **Restricted Access to Branches**

You can indicate the branches from where a user can operate in the Restricted Access screen.

#### **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 invalid password attempt, the last login time of a user etc.

#### **Audit Trail**

Whenever a record is saved in the module, the ID of the user who saved the record is displayed in the 'Input By' field at the bottom of the screen. The date and time at which the record is saved is displayed in the Date/Time field.

A record that you have entered should be authorized by a user, bearing a different login ID, before the EOD is run. Once the record is authorized, the ID of the user who authorized the record will be displayed in the 'Authorized By' field. The date and time at which the record was authorized is displayed in the 'Date/Time' field positioned next to the 'Authorized By' field.

The number of modifications that have happened to the record is stored in the field 'Modification Number'. The Status of the record whether it is Open or Closed is also recorded in the 'Open' checkbox.

## 2.2 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.

You can invoke the 'SMS Bank Parameters Maintenance' screen by typing 'SMDBANKP' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot shows the 'SMS Bank Parameters Maintenance' application window. It contains several sections for configuring security parameters:

- Bank Level Parameters:** Includes input fields for 'Head Office', 'Site Code \*', and 'Activation Key'. It also has 'Password Length (Characters)' with 'Maximum' set to 15 and 'Minimum' set to 8. Under 'Invalid Logins', there are checkboxes for 'Cumulative' and 'Successive'.
- Parameters:** Includes fields for 'Password Repetitions', 'Force Password Change After', 'Intimate User (Before Password Expiry)', 'Archival Period (in days)', 'Minimum Days Between Password Changes', and 'Dormancy Days'. There is a checkbox for 'Display Legal Notice'. On the right side, there are fields for 'Maximum Consecutive Repetitive Characters', 'Minimum Number Of Numeric Characters In Password', 'Minimum Number Of Special Characters In Password', 'Minimum Number of LowerCase Characters in Password', and 'Minimum Number of UpperCase Characters in Password'.
- Warning Screen Text:** A section for entering warning messages, currently empty.
- Bottom Section:** Contains tabs for 'Branch Restrictions', 'Password Restrictions', and 'Fields'. Below the tabs are fields for 'Maker', 'Checker', 'Mod No', 'Date Time:', 'Record Status', and 'Authorization Status'. An 'Exit' button is located in the bottom right corner.

 You can modify the Bank Parameters only when the Head Office branch is in the transaction input stage.

### 2.2.1 Invalid Logins

You can specify the allowable number of times an invalid login attempt is made by a user. Each user accesses the system through a unique User ID and password. While logging on to the system, if either the User Id or the Password is wrong, it amounts to an invalid login attempt.

You can stipulate the allowable number of cumulative invalid attempts made during the course of a day, as well as the allowable number of consecutive or successive invalid attempts made at a time. In either case, if the number of invalid attempts exceeds the stipulated number, the user ID is disabled.

By default, the allowable number of cumulative invalid attempts is six, and the allowable number of consecutive invalid attempts is three. You can change the default and specify the allowable number of attempts in each case. You can specify an allowable number for cumulative attempts between 6 and 99, and for consecutive (successive) attempts, between 3 and 5.

Once specified, you can change the allowable number of cumulative or consecutive login attempts, provided you do so only at a time when no users are logged in to the system.

When authentication of credentials is unsuccessful due to an incorrect user ID, then the user id will not be logged in the audit logs. In case the user id is correct and the password is wrong, the attempt is logged in the audit log and the successive and cumulative failure count is incremented. When the user id and password are correct, this is logged into the audit logs.

## **2.2.2 Specifying Parameter**

### **Archival Period in Days**

You can specify the period (in calendar days) for which the audit trail details of system security related activities (such as usage of the system by a user, activities by the system administrator, etc.) should be maintained. The system defaults to a value of 30, which you can change.

You can specify an archival period that is greater than or equal to 7 calendar days.

### **Dormancy Days**

Oracle FLEXCUBE allows you to automatically disable the profile of all the users who have not logged into the system for a pre-defined period of time. A user ID is considered dormant if the difference between the last login date and the current date is equal to or greater than the number of 'Dormancy Days' that you specify in this screen. This is reckoned in calendar days i.e. inclusive of holidays.

All dormant users (whose home branch is same as the current branch) are disabled during the end of day run at the current branch.

## **2.2.3 Specifying Warning Screen Text**

### **Warning Screen Text**

At your bank, you may require a warning message containing legal requirements and security policy to be displayed to all users before allowing them to login to Oracle FLEXCUBE.

You can specify the text (content) of such a message, in the Warning Screen Text field. This message will be displayed soon after a user launches the Oracle FLEXCUBE login screen. 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.

## **2.2.4 Specifying Parameters for User Passwords**

You can specify the following parameters that would govern user passwords:

## **Password Length (characters)**

You can indicate the range of length (in terms of number of characters) of a user password. The number of characters in a user password is not allowed to exceed the maximum length, or fall below the minimum length that you specify here.

The minimum length defaults to 8, and the maximum length to 15. You can change the defaults and specify the required range. If you do so, you can specify a minimum length between 6 and 15 characters, and a maximum length between 10 and 15 characters. The minimum length that you specify must not exceed the maximum length that you have specified.

## **Force Password Change after**

The password of a user can be made valid for a fixed period after which a password change should be forced. In the 'Force Password Change after' field, you can specify the number of calendar days for which the password should be valid. After the specified number of days has elapsed for the user's password, it is no longer valid and a password change is forced.

The number of calendar days defined here will be applicable for a password change of any nature - either through the 'Change Password' function initiated by the user or a forced change initiated by the system.

The system defaults to a value of 30, which can be changed. If you change it, the number of days you specify here should be between 15 and 180 days, inclusive.

## **Password Repetitions**

You can stipulate the number of previous passwords that cannot be set as the new current password, when a password change occurs.

The system defaults to a value of three (i.e., when a user changes the user password, the user's previous three passwords cannot be set as the new password). You can change the default, and if you do, you can specify a number between one and five, inclusive.

The following example illustrates how this works.

### **Example**

While setting up the Bank Level Parameters, you have given a value of '2' in the Password Repetitions field. Mr. Smith is a user of the system with the following details:

USER ID SMITH

Password STEELE

If Mr. Smith wants to change his password, he should invoke the Change Password screen. He cannot choose his old password (STEELE) again. He now enters his new password as SMITHS.

Smith wants to change his password for the second time. As the last two passwords cannot be used (Password Repetitions = 2 in the Bank Level Parameters table), he cannot enter either STEELE or SMITHS as his new password. He should enter a different password.

The number you specify here should be greater than or equal to 1 and less than or equal to 5.

## **Minimum Days between Password Changes**

You can specify the minimum number of calendar days that must elapse between two password changes. After a user has changed the user password, it cannot be changed again until the minimum number of days you specify here have elapsed.

## **Intimate Users (before password expiry)**

The number of days for which a password is to be valid is defined in the 'Force Password Change' after field. You can also indicate the number of working days before password expiry that a warning is to be issued to the user. When the user logs into the system (the stipulated number of days before the expiry date of the password), a warning message will continue to be displayed till the password expires or till the user changes it.

By default, the value for this parameter is two (i.e., two days before password expiry). You can change the default if required. If you do, you can specify a number greater than zero and less than or equal to five.

### **Example**

The value specified in the Intimate User (Before Password Expiry) field is 2 and a user's password is due to expire on 31/01/09. The warning message is displayed on 29/01/09 and 30/01/09 whenever the user logs in.

## **2.2.5 Placing Restrictions on User Passwords**

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

### **Maximum Consecutive Repetitive Characters**

You can define the maximum number of allowable repetitive characters occurring consecutively, in a user password. This specification is validated whenever a user changes the user password, and is applicable for a password change of any nature - either through the 'Change Password' function initiated by the user or a forced change initiated by the system.

### **Example**

The value specified in the Maximum Consecutive Repetitive Characters field is 3 and a user decides to change his password to STUDDDD123. The System will not allow this password change as the Maximum Repetitive Characters value has exceeded in the recurrence of 'D' in the password.

### **Minimum Number of Special Characters in Password**

You can define minimum number of special characters allowed in a user 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 Special Characters = 1

### **Minimum Number of Numeric Characters in Password**

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

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

- Minimum No of Numeric Characters = 1



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 special characters and the minimum number of numeric characters is less than or equal to the 'Maximum Password Length'.

### **Minimum Number of Lower Case Characters in Password**

You can define the minimum number of lowercase characters allowed in a user password. The allowed lower case characters are from the US-ASCII character set only. 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 Lower Case Characters = 1
- Maximum No of Numeric Characters = Maximum Password Length

### **Minimum Number of Upper Case Characters in Password**

You can define the minimum number of upper case characters allowed in a user password. The allowed upper case characters are from the US-ASCII character set only. 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 Upper Case Characters = 1
- Maximum No of Numeric Characters = Maximum Password Length

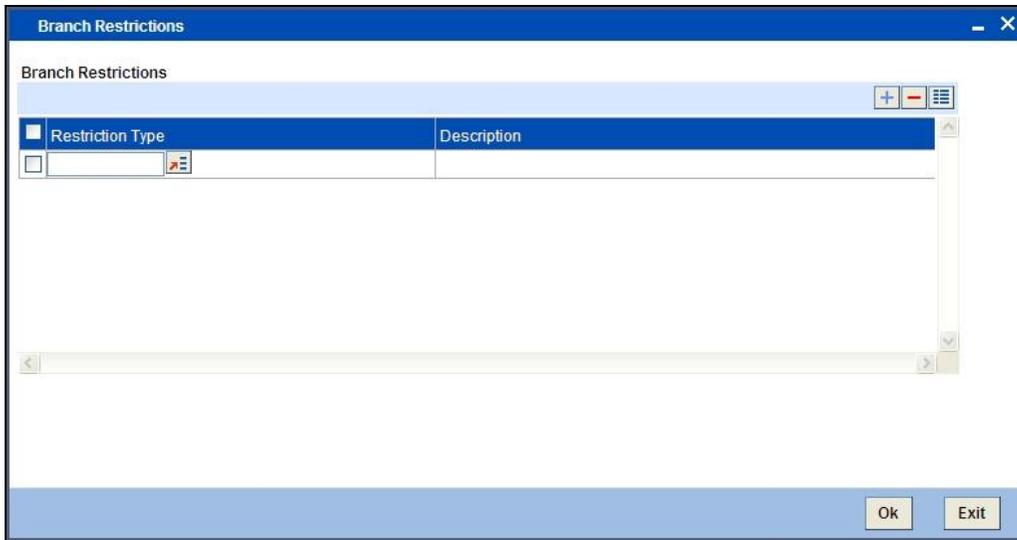
## **2.2.6 Branch Restrictions for Specific Applications**

You can restrict administrators of branches from performing operations related to specific functions in branches other than their home branch. These are referred to as 'Branch Restrictions for Specific Applications'. You can also maintain a list of branches in which the administrator of a certain branch is allowed / restricted to perform specific operations. These other restrictions are referred to as 'Common Branch Restrictions'.

According to the restrictions you maintain, the administrator of a specific branch is allowed to perform specific operations in the administrator's home branch, as well as any branch found in the list of allowed branches.

According to your requirements, the implementers at your installation configure a list of the specific functions or applications for which you might wish to maintain such branch restrictions. You can maintain branch restrictions for each of these applications, as required.

In the 'Branch Restrictions' screen, you can specify the applications for which you intend to maintain branch restrictions. To invoke the 'Branch Restrictions' screen, click 'Branch Restrictions' button in the 'SMS Bank Parameters Maintenance' screen.



For maintaining the Branch Restrictions for an application, click add icon to add a record to the list. Then click on each field's option list to select the application for which you intend to maintain branch restrictions.



You cannot create common branch restrictions for an application that you have not specified in this screen.

### **Example**

You wish to restrict branch administrators from performing operations in the following applications, in branches other than their home branch:

- User administration (creation, modification and viewing of user profiles)
- End of Day (EOD) operations
- Maintaining rules for ICCF components
- Maintaining branch restrictions for IC rates

In the Restriction Type field in the SMS Branch Restriction Type screen, select USRADMIN (to maintain branch restrictions for User Administration), EODOPERATN (to maintain branch restrictions for EOD operations); ICCFRULE (to maintain branch restrictions for maintaining ICCF rules) and ICRATES (to maintain branch restrictions for IC rates).

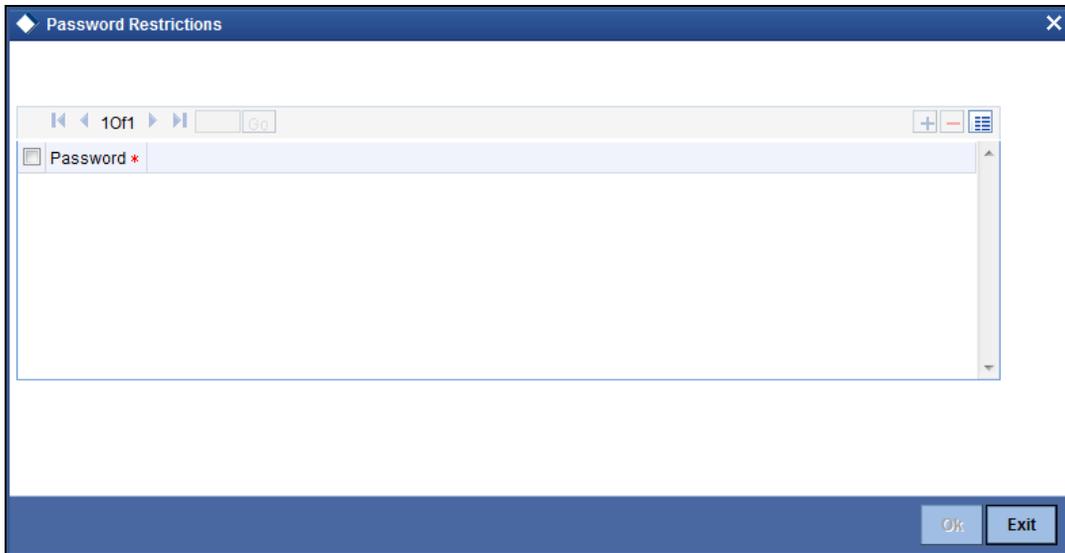
## **2.2.7 Password Restrictions**

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 assigned the same 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 'Password Restrictions' button to define restricted passwords at the bank level that should not be used by any user of the bank.



To add a password to the 'Password' list, click add icon. To select a record in the list use the check box beside it.

After you listed the restrictive passwords in the 'Password' list, click 'Ok' button to save the password restrictions.

## **2.3 User Details Modification in Bulk**

You can change or reset user passwords in bulk if you have the system admin rights. After modification of the user list, click 'Save', The modified user list will be stored in a temporary table. The lists of users which are modified and mapped with a unique sequence number will not be available until the particular sequence number is authorized. When the particular sequence number is authorized those user details will be changed and updated.

You can invoke this screen by typing 'SMDCHPWD' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot shows a software interface titled "User Credentials Change". At the top left, there is a "New" icon. Below it are three input fields: "Sequence Number \*", "Process Date", and "Description". Below these fields is a table with the following columns: "User Identification \*", "Name", "Password", and "Reset Password". The table contains one row with empty fields. At the bottom of the window, there are labels for "Maker", "Checker", "Mod No", "Date Time:", "Record Status", and "Authorization Status". An "Exit" button is located in the bottom right corner.

In this screen, the following information is to be provided.

### **Sequence Number**

Click on 'New' icon to generate a new 'Sequence Number'.

### **Process Date**

Select a date by clicking on the calendar icon beside the field. This field is generally useful for querying purpose.

### **Description**

Provide a description of what modification is being done on selected user ids.

### **User Id**

Select the User Id to be changed from the option list provided.

### **Name**

Name of the user specific to the selected user id will be displayed in this field.

### **Password**

Password of the selected user id will be displayed here. This field will be editable only if the 'Auto Generation Required' option is not selected at the application level. If the 'Auto Generation Required' option is checked, the password will be auto generated by the application.

## Reset Password

Select this checkbox to reset the password in case of user ids where password needs to be auto generated.

## 2.4 Creating Common Branch Restrictions

To recall, in the Branch Restrictions maintenance, you have identified those applications and operations, for which you intend to maintain branch restrictions. Having done this, you must proceed to create the appropriate common branch restrictions for each branch administrator. You can maintain these restrictions in the common 'Branch Restrictions' screen.

You can invoke this screen by typing 'SMDBRRES' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



This can be done only at the head office branch.

| Branch Code * | Description |
|---------------|-------------|
|               |             |

In this screen, you create common branch restrictions by specifying the information described below.

### User Branch

You must first select the home branch of the administrator for which you are maintaining common branch restrictions, in the User Branch field.

## Restriction Type

You must also indicate the specific application for which you wish to maintain common branch restrictions, for the administrator of the selected branch. You can only specify a restriction type that has been maintained in the SMS Branch Restriction Type maintenance.

## Branch Restriction

You maintain common branch restrictions by creating a list of branches for each administrator, in which the administrator will either be allowed / disallowed access to perform operations related to the selected application (Restriction Type). You can maintain either an 'allowed' or a 'disallowed' restriction list.

The common branch restrictions you maintain are applicable for operations in the selected application (Restriction Type) in the home branch (User Branch) of the administrator and the list of allowed / disallowed branches.

### Example

You have created the following common branch restrictions:

| Home Branch | Restriction Type | Allowed Branches   |
|-------------|------------------|--------------------|
| 000         | USRADMIN         | 000, 001, 002, 005 |
| 001         | USRADMIN         | 001, 006           |
| 002         | ICCFRULE         | 002, 005, 006      |
| 005         | EODOPERATN       | 002, 005, 006      |
| 006         | ICRATES          | 004, 005, 006      |

The administrator of branch 000 can perform user administration for the branches 000, 001, 002 and 005, but not for 006. Similarly, the administrator of branch 002 can create ICCF rules in branches 002, 005 and 006, but not in branches 000 and 001.

When the administrator of branch 000 attempts to create a new user in the User Profile screen, the branches available in the Home Branch field in the screen will be 000, 001, 002 and 005.



Note the following:

- The administrator of the head office branch is allowed to perform all operations in any of the other branches
- When a new branch is created, it must be manually added to the allowed / disallowed list, as required
- For those applications (Restriction Types) that you have specified in the SMS Branch Restriction Types maintenance, you must create the appropriate common branch restrictions in the Common Branch Restrictions screen. If no restrictions have been created in the Common Branch Restrictions screen for a specific branch for an application chosen in the SMS Branch Restriction Types maintenance, operations pertaining to the application will not be allowed from that branch.
- To allow the administrator of a certain branch to perform operations pertaining to a specific application for all branches, you can either maintain an allowed list with all branches selected or maintain a disallowed list with none of the branches selected.

## 2.5 Defining Functions

Any function that is a part of the system should be defined through the 'Function Description Maintenance' screen before it is available for execution. Mostly, our professionals carry out this activity. You can modify the description of the function that appears in the Application Browser through this screen. You can invoke this screen by typing 'SMDFNDSC' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot shows the 'Function Description' application window. The window title is 'Function Description' and it contains a 'New' form. The form has several input fields: 'Function Id \*', 'Module List \*', 'User Function Id', 'Name', 'Type' (dropdown), and 'Menu Head' (dropdown). There are two columns of checkboxes: the left column includes 'Tanking Required', 'Dual Authorization', 'Remarks Required', 'Excel Export Required', 'Multi Branch Access', and 'Field Log Required'; the right column includes 'Available', 'Automatic End of Day aware', 'Log Event', 'Customer Access', 'Auto Authorization', 'Head Office Function', and 'Duplicate task check'. Below the form is a 'Function Description' table with columns for 'Language Code \*', 'Main Menu', 'Sub Menu 1', 'Sub Menu 2', 'Balloon Help', and 'Description'. At the bottom, there is a 'Field Properties' section with fields for 'Maker', 'Date Time', 'Mod No', 'Record Status', and 'Authorization Status', along with an 'Exit' button.

The following details are captured here:

### Function Identification

Select the Function id for which you want to give access rights, from the option list.

### Module

Select the module to which the Function id has to be mapped. All Functions are mapped to specific modules.

### Name

Specify the executable to open the Function Id.

### Type

Select the type of Function Id here from the drop-down list. The options available are:

- Form
- Report
- Stored Procedure

## Menu Head

Select the menu head from the drop-down list. The options available are:

- Module
- Report

You can then specify the rights to the different actions for the functions by checking against the action. These actions can be:

- Static Maintenance Functions
  - 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)
- 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)
  - View (to see the details of the contract)
- 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 delete icon.

## Custom Function ID

Specify a custom function id which can be used as an alias for the function id selected.

If you input this value in the field at the top right corner of the Application tool bar and click on the adjoining arrow button, system will check for the mapped function id and will launch that function id screen.

## Tanking Required

Check this box to indicate that the maintenance records that are created or modified in the system, for the function Id specified here, need to be tanked till they get authorized.

The new or the modified records are written to the static tables only after authorization.

*For more details on tanking of maintenance records refer the Core Services user manual.*

### **Dual Authorization**

Check this box to enable dual authorization for records that are created or modified in the system, for the specified function id. If dual authorization is enabled then after creation or modification of a maintenance record, an intermediate verifier (First Authorizer) has to verify the record before the record can actually be authorized.



You cannot enable both 'Dual Authorization' and 'Auto Authorization' for a function id at the same time, as they are mutually exclusive.

### **Remarks Required**

Check this box to enable capturing of maker remarks on the actions like save, close and reopen of records belonging to the selected function id.

If this box is checked then system pops up a 'Maker Remarks' window and forces the maker to save remarks while saving, closing or reopening a record, The checker/authorizer can view the maker remarks entered and also enter remarks for each modification while authorizing the record.

### **Excel Export Required**

Check this box to enable data export for the selected function id.

If this box is checked, system allows you to export data from records belonging to the selected function id into an excel file.

### **Multi Branch Access Required**

Check this box to configure dual access framework for the function ID.



Note the following:

- If the function level check box is unchecked, the transactions will be posted in the current branch.
- Dual access functionality is enabled only when the 'Multi Branch Access' check box is checked at 'User ID' and 'Function ID' levels.

### **Available**

Check this box to make the Function accessible in the Oracle FLEXCUBE menu. The definition of the menu would be as specified in the Column at the bottom of the 'Function Description Maintenance' screen. If this box is unchecked, then this screen will not be accessible from the menu even if it is selected for the Role that is assigned to the user.

### **Automatic End Of Day aware**

Check this box to consider the Function for an AEOD run.

### **Log Event**

Check this box to enable the event log for a particular Function ID, Oracle FLEXCUBE maintains an extensive log of the activities of every user. This can later be used for reporting on the user activities.

## Cust Access

Check this box to make the Function available to Users who are classified as Customers.

## Auto authorization

As configured for your installation according to your requirement, automatic authorization is applicable for a pre-shipped list of functions. For those functions, you can revoke the applicability of automatic authorization, if required.

It is not possible to indicate the applicability of automatic authorization for any other functions than those pre-shipped functions configured for your installation.

## Head Office Function

Check this box to enable the Function to be handled only by the users of the Head Office. Users of the other branches would be only allowed to view the Function.

### 2.5.1.1 Defining the Menu

The Oracle FLEXCUBE menu can be defined in the Function Description section.

You can define menu appearance for a given Language. The Menu can only be drilled down up to two sub menu levels.

#### Example

For Language Code 'ENG' if the Main menu value is given as Security Management', Sub Menu1 as 'Maintenance' and Sub Menu2 as 'Function Description' for Function id SMDFNDSC then on the Oracle FLEXCUBE menu it would appear as follows:



## 2.6 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 that 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.

The roles defined will be effective only after dual authorization.

## 2.6.1 The Procedure for Defining Role Profiles

Role profiles are defined in the 'Role Maintenance' screen. You can invoke this screen by typing 'SMDROLDF' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screen is as shown below:

The screenshot shows a software window titled "Role Profile Definition". At the top left is a "New" button. Below it are two text input fields: "Role Id \*" and "Role Description". Under "Role Description" is a checkbox labeled "Centralisation Role". A horizontal menu bar contains buttons for "Maintenance", "Reports", "Batch", "Online", "Process Stage Rights", "Acc Class Restriction", "Branch Restriction", "Rights", "Password Restriction", "Web Branch", "Branch Limit", and "Fields". The bottom section of the window has labels for "Maker", "Checker", "Mod No", "Date Time:", "Record Status", and "Authorization Status". An "Exit" button is located in the bottom right corner.

## 2.6.2 Defining Functions for a Role Profile

After you have defined the basic attributes of a role profile (the Role Identification, Description) you should define the functions to which the role profile has access. Check centralization role to specify that the role is applicable for centralized users. The role is automatically associated with all branches accessible to you, if the multi branch operational parameter is enabled. The various functions in the system fall under different categories.

To assign a function to a role in the 'Role Maintenance' screen, you must click the function category button to which the function belongs. The function category buttons in the 'Role Maintenance' screen are as follows:

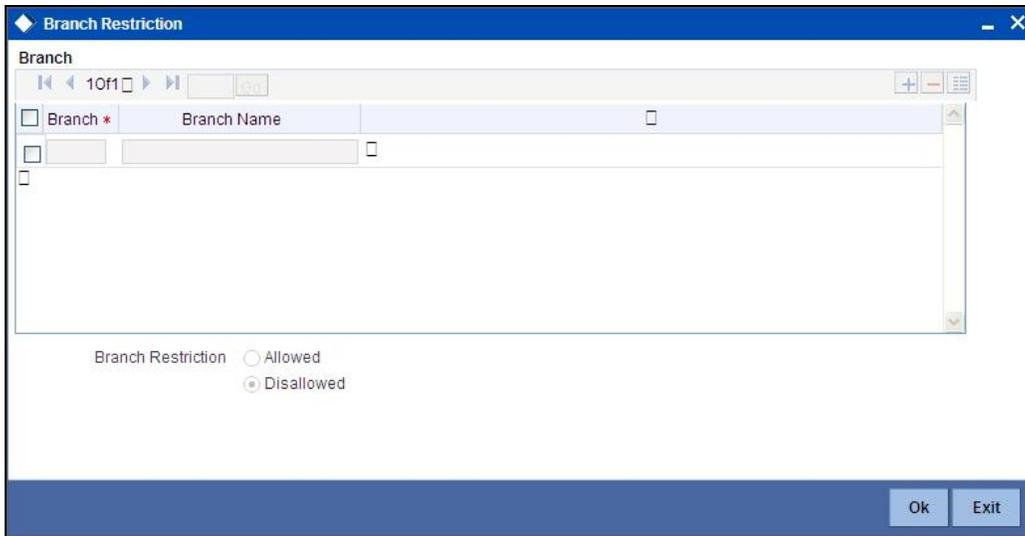
- **Maintenance** - Functions related to the maintenance of static tables
- **Reports** - Functions related to the generation of reports in the various modules
- **Batch** - Functions related to the automated operations (like automatic liquidation of contract, interest, etc.)
- **On Line** - Functions related to contract processing
- **Process** - Functions related to workflow
- **Acc Class Restriction** –Functions related to restricting the role from using certain account classes

- **Branch Restriction** – Functions related to restricting the association of roles to certain branches.
- **Rights** – Functions related to giving necessary rights for perform various operations in respect of incoming and outgoing messages
- **Password Restriction** – Functions related to creating a list of words that the users, having a certain Role are likely to use as Passwords and on which restrictions can be placed.
- **Web Branch** – Functions related to the Teller Module for the role of branch users.
- **Branch Limit** – Function related to setting up Branch limits.
- **Fields** – Functions related to User Defined Fields.

The lower portion of the Role Description screen has buttons corresponding to each of the above function categories. Click on a button to view the corresponding screen.

### 2.6.3 Branch Restriction

You can specify the branches to which the role profile is associated, and for which it is available. Click 'Branch Restriction' button in the 'Role Maintenance' screen. The 'Branch Restriction' screen is opened.



You can maintain a list of branches for which the role is either:

- Allowed
- Disallowed

Choose the 'Allowed' option to maintain an allowed list, and the 'Branch Restrictions' list will show the list of allowed branches. Choose the 'Disallowed' option, to maintain a disallowed list of branches.

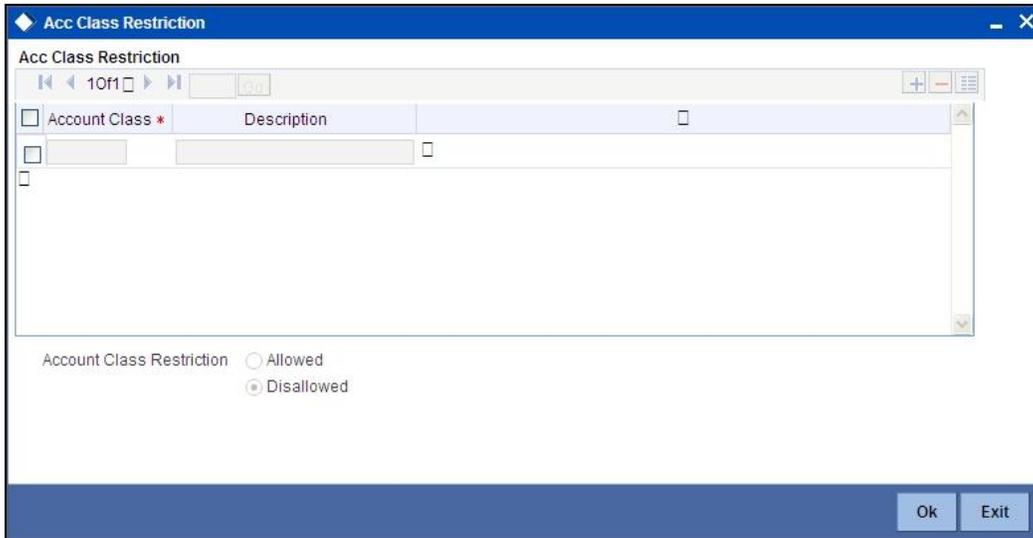
If you maintain an 'Allowed' list, then the role profile will be available only for those branches that you specify in the Branch Restrictions list. Similarly, if you maintain a 'Disallowed' list, then the role profile will not be available only for those branches that you specify in the Branch Restrictions list.

After choosing either the 'Allowed' or 'Disallowed' option, click add icon to add a record under the 'Branch Restrictions' list. Into each added record field, select the required branch from the adjoining option list.

## 2.6.4 Account Class Restriction

You can restrict the role from using certain account classes that are maintained in Oracle FLEXCUBE. Click 'Acc Class Restriction' to specify the account class restrictions. The 'Account Class Restriction' screen is displayed.

The screen is as shown below:



You can either allow or disallow association of the role with certain account classes. Subsequently, specify the account classes, which have to be restricted for the role.

After choosing the 'Allowed' or 'Disallowed' option, click add icon to add a record under the 'Account Class Restrictions' list. Into each added record's field, select the required account class from the adjoining option list.

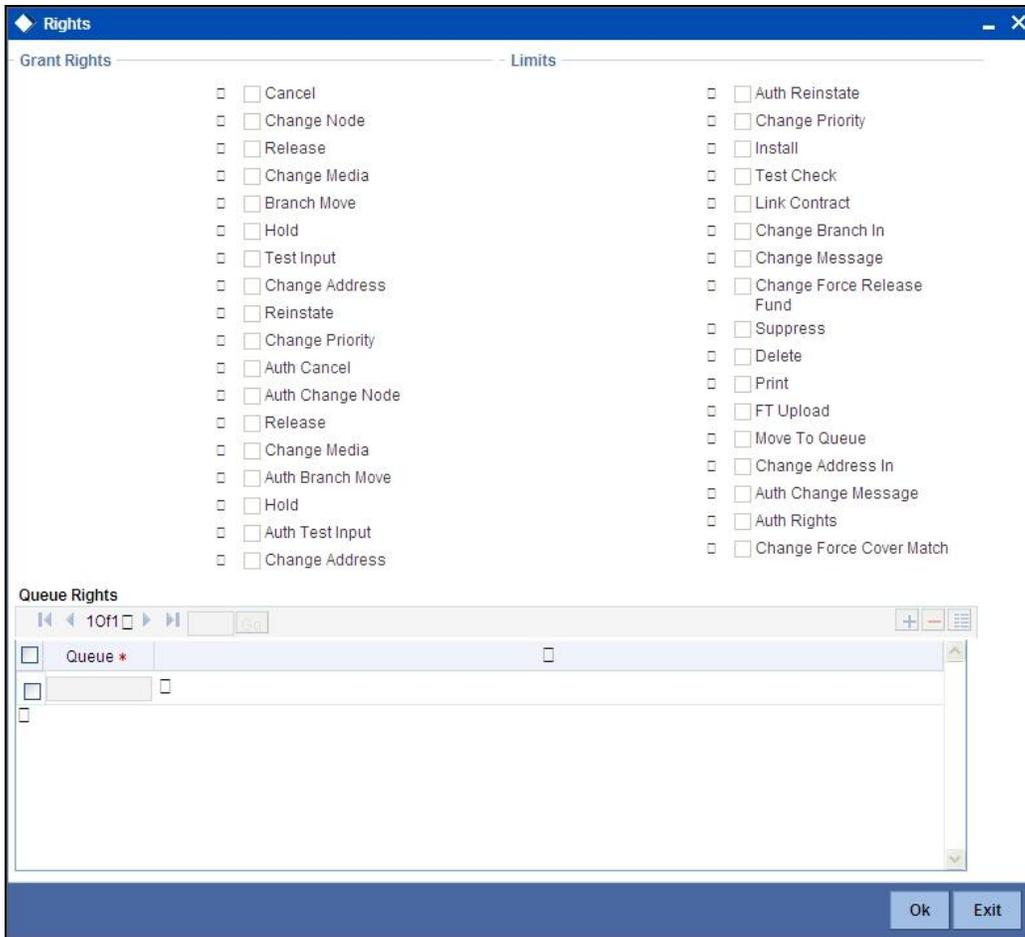
*For more details about account class restriction, refer Account Class Restriction at User Role maintenance and User Profile maintenance levels of this user manual.*

## 2.6.5 Rights

For a role profile, you can specify the necessary rights to perform various operations in respect of incoming and outgoing messages, in the Messaging module of Oracle FLEXCUBE. You can grant specific permissions for operations on messages, as well as allot the messaging queues to which the role has access.

In the 'Role Maintenance' screen, click 'Rights' button to open the 'Rights' screen. Here you can grant the rights pertaining to the Messaging module, to the role.

The screen is as shown below:



Check against the messaging operations for which you want to grant the permission.

### **Granting rights pertaining to operations on messages**

You can grant permissions for the following operations on outgoing messages:

- Generating a message
- Printing a message
- Placing a message on hold
- Releasing a message on hold
- Canceling a message
- Inserting a testword
- Reinstating a message
- Changing the priority of a message
- Request information relating to Status of a message
- Request cancellation of a message
- Changing the media through which a message is transmitted
- Changing the address to which a message is to be sent
- Moving a message to another branch
- Changing the node from which a message should be generated

- Authorization of any of the operations listed above, in respect of outgoing messages

You can grant permissions for the following operations on incoming messages:

- Printing a message
- Authorizing a testword
- Routing a message to a queue
- Associating a message with a contract
- Uploading incoming messages
- Making changes (edit) incoming messages. You can also grant permissions for changing the branch and the address in incoming messages
- Authorizing changes made to incoming messages
- 'Force Release' payment message transactions with 'Funding Exception' status and insufficient funds
- Suppressing a message
- Deleting a message

Granting each of these permissions in the Rights screen enables the user having this role to perform the corresponding functions in the Incoming and Outgoing Message Browsers. The appropriate button in the Browser, in each case, is enabled for the users associated with the role.

*For details regarding each of these operations in respect of both incoming and outgoing messages, consult the **Messaging System** user manual*

Apart from these functions, you can also grant permission for the cover matching function for incoming payment message transactions.

*For details regarding uploading incoming payment transaction messages and cover matching for incoming payment transactions, refer the 'Straight Through Processing' chapter in the Funds Transfer user manual.*

### **Grant Queues**

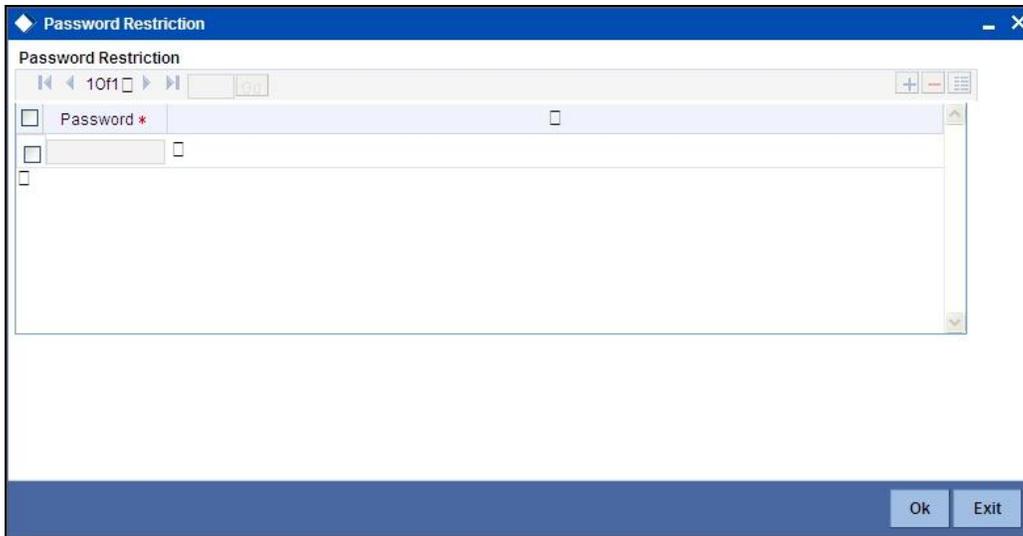
You can grant the message queues to which the role has access, and in which users associated with the role can perform messaging operations according to the messaging rights you have assigned. The required queues can be selected and listed in the 'Queues' list under the 'Grant Queues' section.

## **2.6.6 Password Restriction**

System allows you to create a list of words that the users, having a certain Role are likely to use as Passwords and on which restrictions can be placed. 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 'Password Restriction' button 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.

The screen is as shown below:



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.

### **2.6.7 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.

Select 'Copy' from the Actions menu in the Application toolbar or click copy icon. 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.

### **2.6.8 Closing a Role Profile**

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

Select 'Close' from the Actions menu in the Application toolbar 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 closed.

You will be prompted to confirm the closure. The Role Profile will be closed only if you confirm the Closure.

### **2.6.9 Defining Roles for Oracle FLEXCUBE Branch Users**

You can define a role with functions typically performed by you from Oracle FLEXCUBE Branch system. You can maintain the role 'Teller' and select the branch function from the 'Web branch' button.



In case you wish to give access of the host functions to the 'Teller', you can attach role like 'ALLROLES' or other role with host functions in addition to the 'Teller' role. You can do this at the User Profile level for the branch you are allowed.

## 2.7 Defining a Limits Role

Oracle FLEXCUBE allows you to place restrictions on the amount specified by a user when processing a transaction. You can also restrict users with authorization rights from authorizing transactions with amounts beyond a specific limit.

To achieve this, you can define Input Limits and Transaction Authorization Limits for a user at the time of maintaining a User Profile in Oracle FLEXCUBE. The input limits and authorization limits will be made applicable to the following types of transactions:

- Payment transactions (FTs)
- Single Entry Journal transactions
- Multi Offset transactions
- Teller transactions

Oracle FLEXCUBE allows you to maintain different Role Limits, which can then be linked to a user profile. The limits defined for the attached role will be applicable to the user profile to which it is linked. The Role Limits are maintained in the 'Role Limits Maintenance' screen. You can invoke this screen by typing 'SMDRLMNT' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot displays the 'Role Limits Maintenance' application window. The title bar includes a 'New' button and window control icons. The main area contains a form with the following fields: 'Role Id \*', 'Description', 'Limits Currency \*', 'Input Limit \*', and 'Authorization Limit \*'. The 'Description' field has a help icon. Below the form is a 'Fields' section with a blue header. It contains 'Input By' and 'Authorized By' (both with 'Date Time' sub-labels), 'Modification Number', and two checkboxes labeled 'Authorized' and 'Open'. An 'Exit' button is located in the bottom right corner of the form area.

### Role Identification

The Id that you specify here will uniquely identify the Role Limit throughout the system. A Role Limit is distinct from the User Role, in that the Role Limit is designated for the specific purpose of enabling you to set transaction amount processing limits that you wish to impose on a user.

### Description

You can specify a brief description for the Role Limit being defined.

## Limits Currency

Here you will indicate the currency in which the limits (transactions amounts) will be expressed. If a user captures a transaction in a different currency, Oracle FLEXCUBE will convert the transaction amount to the Limits Currency and then perform the validations.



For currency conversions, the system will use the mid-rate of the STANDARD exchange rate type maintained in your system.

## Input Limit

Specify the maximum amount that a user (to which the limits role is associated) is allowed to process while entering a transaction.

## Authorization Limit

Specify the maximum amount that a user (to which the limits role is associated) is allowed to process while authorizing a transaction.

### 2.7.1.1 Working of the Limits

#### Input Limit

If the transaction amount exceeds the input limit maintained for the Role, the system displays an override message. Selection of the 'OK' button in the message window will allow the user to continue despite exceeding the limits. If the user selects the 'Cancel' button, he will not be able to continue with transaction processing.

#### Authorization Limit

If the transaction amount that the user is attempting to authorize exceeds the authorization limit maintained for the Role, the system displays an override message. Selection of the 'OK' button in the message window will allow the user to continue with the authorization despite exceeding the limits. If the user selects the 'Cancel' button, he will not be able to continue with authorizing the transaction.

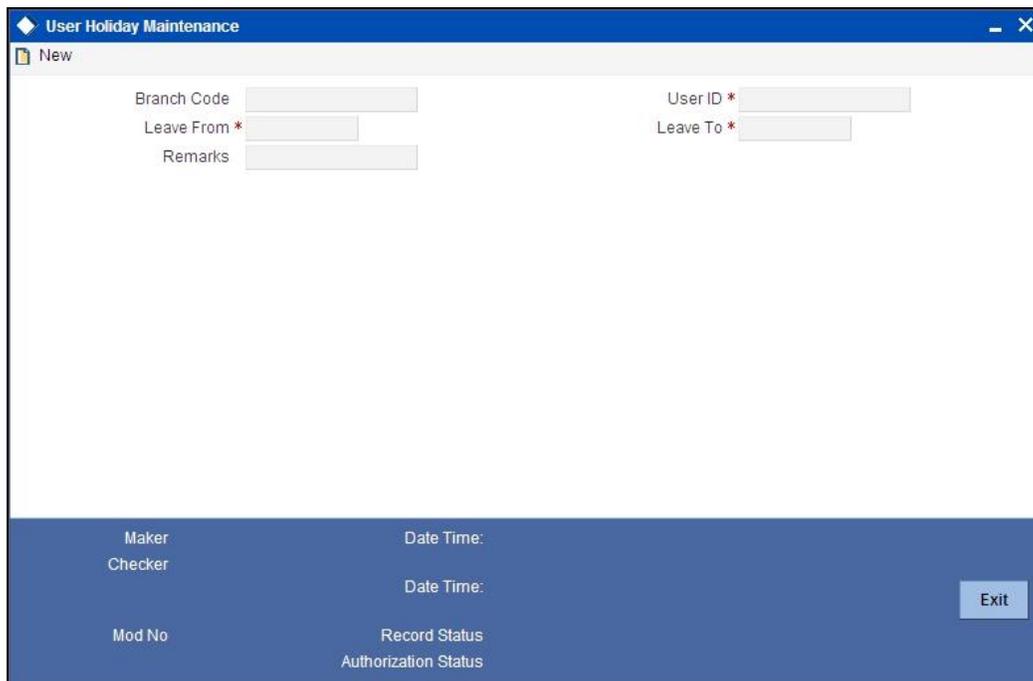


The role limits (input and authorization) would apply to a user with which the limits role has been associated, for operations in any of the modules listed above (that is, payment transactions, single entry journal transactions, multi-offset transactions).

## 2.8 Defining User Holidays

You can block a specific user login for a certain time frame by defining holiday slots for that user profile. You can define holiday slots through the 'User Holiday Maintenance' screen. You can invoke this screen by typing 'SMDUSHOL' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The 'User Holiday Maintenance' screen is shown below.



The screenshot shows a software window titled "User Holiday Maintenance". Inside the window, there is a "New" button at the top left. Below it, there are five input fields arranged in two columns. The left column contains "Branch Code", "Leave From \*", and "Remarks". The right column contains "User ID \*" and "Leave To \*". At the bottom of the window, there are several labels: "Maker", "Checker", "Mod No", "Date Time:", "Record Status", and "Authorization Status". An "Exit" button is located in the bottom right corner.

Specify the following details:

### **Branch Code**

The branch code of the user selected in the 'User ID' field is displayed here.

### **User ID**

Specify the user ID of the user for whom you want to define the holiday period. The adjoining option list displays all the valid user profiles maintained in the system. You can select the appropriate one.

### **Leave From**

Select the start date for the holiday period from the adjoining calendar.

### **Leave To**

Select the end date for the holiday period from the adjoining calendar.

The user will not be allowed to log in within the specified holiday range.

### **Remarks**

Specify a brief description for the holiday.

You can maintain multiple holiday slots for a user but the system will not allow including a specific day in more than one slot.

## 2.9 Viewing Holiday Summary Details

You can view holiday periods maintained for any user profile in the 'Users Holiday' screen. You can also invoke this screen by typing 'SMSUSHOL' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screen is as shown below:

The screenshot displays the 'User Holiday Summary' application window. At the top, there are search filters for 'Authorization Status', 'Record Status', 'Branch Code', 'User ID', 'Leave From', and 'Leave To'. Below these are 'Search' and 'Advanced Search' buttons, along with 'Refresh' and 'Reset' buttons. A pagination bar indicates 'Records per page 15' and '1 Of 1'. The main area is a table with columns: 'Authorization Status', 'Record Status', 'Branch Code', 'User ID', 'Leave From', 'Leave To', 'Maker ID', and 'Maker Date Star'. The table is currently empty. An 'Exit' button is located at the bottom right of the window.

You can query for records based on the following criteria:

- Authorization Status
- Record Status
- Branch Code
- User ID
- Leave From
- Leave To

Click 'Search' button. Based on your preferences, the system identifies all records satisfying the criteria and displays the following details for every record:

- Authorization Status
- Record Status

- Branch Code
- User ID
- Leave From
- Leave To
- Maker ID
- Maker Date Stamp
- Checker ID
- Checker Date Stamp

## 2.10 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. The user profiles will be effective only after dual authorization.

You can create User Profiles through the 'User Maintenance' screen. You can invoke this screen by typing 'SMDUSRDF' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button. The 'User Maintenance' screen is shown below.

Specify the following details:

### User Identification

Specify the user identification. This ID identifies the user whose profile you are defining. In a user ID, you can use alphabets in upper or lower case, numbers 0 to 9 and \_ (underscore).

The number of characters in a User ID should be greater than or equal to six and less than 12.

## Name

Specify the name of the user.

## Classification

- **Staff** - All internal users of the bank can be classified as Staff. You can include any of the functions available in the system in the user profile.
- **Branch** - This indicates a branch user. This is used to identify a branch user and branch specific user maintenance for Branch user.

### 2.10.1.1 Restrictions on User Profile Administration

A branch administrator can create, modify or delete user profiles only in the Head Office, Home branch of the administrator or in those branches that are allowed for the restriction type USRADMIN, in the Common Branch Restrictions.

When the administrator of a branch attempts to create a new user in the User Profile screen, the branches available in the Home Branch field in the screen are only those allowed branches maintained in the Common Branch Restrictions for restriction type 'USERADMIN'.

*For details about the Common Branch Restrictions, refer the section 'Creating Common Branch Restrictions' in this user manual.*

#### Example

You have created the following branch restrictions:

| Home Branch | Restriction Type | Allowed Branches   |
|-------------|------------------|--------------------|
| 000         | USRADMIN         | 000, 001, 002, 005 |
| 001         | USRADMIN         | 001, 006           |

The administrator of branch 000 can perform user administration for the branches 000, 001, 002 and 005, but not for 006.

When the administrator of branch 000 attempts to create a new user in the User Profile screen, the branches available in the Home Branch field in the screen will be 000, 001, 002 and 005.

## Language

Select the Language in which the Users screen have to be defined, from the option list. The Language Codes maintained through the 'Language codes' screen will be available for selection.

## Home Branch

By default the Current Branch is displayed here. All users have to be attached to a branch.

## User Status

Select the status of the user from the options available. The options available are:

- Enabled
- Hold
- Disabled

For a user to be able to login to Oracle FLEXCUBE, his status should be set as '**Enabled**'. The field '**Status Changed on**' displays the date and time when the Status of the User was last changed.

## Customer Number

For User Profiles of your choice, Oracle FLEXCUBE allows you to restrict the viewing and printing of Balances (in case of accounts) and financial details of contracts involving customers who also happen to be employees of your bank. In order to enable this option, while creating the User Profile of the employee you can link the customer number (CIF ID) of the employee with the User ID.

## Supervisor Identification

Specify the ID of the supervisor of the user. The option list displays all valid supervisor identifications maintained in the system. Choose the appropriate one.

In case of relationship managers, you can also use this field to define the RM hierarchy. For defining RM hierarchy in this method, you need to select the RM user who is one level up in the hierarchical order as the supervisor.

If the user is the superior in the RM hierarchical order, you can specify his/her own user ID as supervisor ID. The supervisor ID option list also shows the user ID of the user being maintained. This means, you can define an RM user as his/her own supervisor.



The RM hierarchy defined in this method is enabled only if the checkbox 'RM Hierarchy Setup Required' is not checked in 'Bank Parameters Maintenance' screen.

## Supervisor Name

Based on the supervisor ID selected, the system displays the name of the supervisor.

## Department Code

Specify the department code. The adjoining option list displays a list of all the valid department codes maintain in the system. You can choose the appropriate one.

## Department Description

The system displays the Department description.

## Tax Identifier

Specify the tax identifier code of the customer to monitor Anti Money Laundering activities.

A user with restricted access will not be able to view/print details of contracts involving the product in all Contract Functions and Contract Summary screens for the following modules:

- Teller
- Retail Teller
- Clearing
- Utility Payments
- Funds Transfer
- Payment and Collections
- The Contract Online and Cycle Due screen of SI
- Foreign Exchange (online and payment)
- The Contract Online, Value Dated Amendments and Payments Input screens of MM

- The Contract Online put, Value Dated Amendments, Payments Input and Loans Assignment screens of LD

The other functions to which the user will have restrictive rights is as follows:

- Ad-hoc loan statement generation
- Queries – Accounting Entries
- Customer Based Information Retrieval
- Limits Overrides showing account balances
- Message Browser
- Payments and Collections Message browser



In the Payments and Collection module the restriction is applicable to product categories and *not* products.

If a balance exception has occurred, the balances are not displayed for the restricted user but will be replaced by \*\*.



The restricted users will be able to:

- View/print financial information pertaining to contracts *they have* initiated or view/print balances pertaining to *their own* accounts
- Post transactions to the staff accounts or create contracts for staff members, even if the user is restricted to view/print balances / contract information pertaining to other colleagues.
- In case of balance exception during transaction posting, the balance will not be displayed. The Exception Message will only state that the account will be ‘overdrawn’ on account of the transaction.
- Post transactions and view transaction information until the contract is authorized. After authorization, such users cannot access the contract

*The only exception is that when the user has captured a contract, the user will be allowed to view the details till the contract gets authorized.*

## LDAP DN

The LDAP Details that have been maintained in the SSO screen have to be input here. Clicking on the ‘Validate’ button validates the LDAP details entered in the **Single Sign On**. The application will verify if only one user ID in FLEXCUBE UBS is mapped to the subject (DN) while authentication via SSO.

## Time Level

Time level is defaulted to nine here. You can specify the time level you need to maintain at the User level, if needed. You can specify values between zero and nine.

Time level can be specified at two levels - at the Branch level and at the User level.

If you need to login, then the time level maintained at your User Profile should be greater than or equal to that maintained at the Branch level.

Time levels are maintained to prevent you from logging into the application when the system is processing EOC batch. Before EOC Operations, the time level of the system is increased, so that it is higher than that maintained at the User level. However, if you are not logged out when the Time level is raised to the one higher than yours, then you can continue to use the application.

You can modify time level at user profile level when branch is at Transaction Input stage.

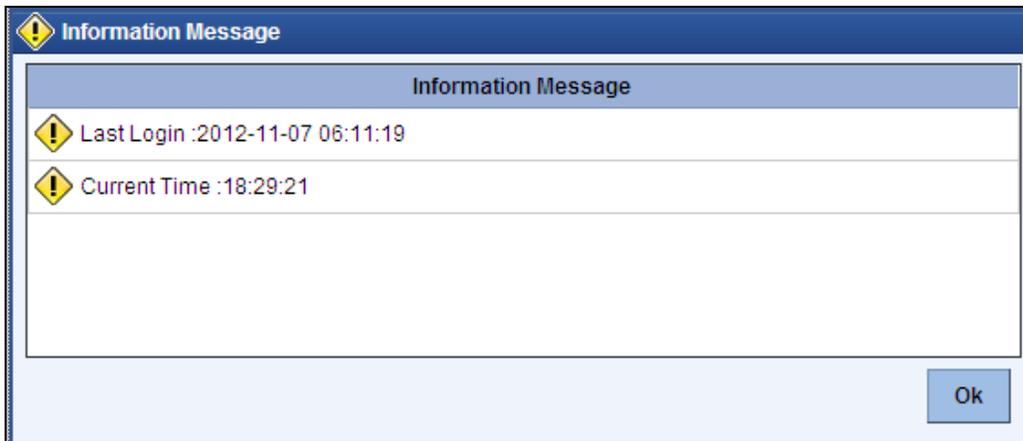
 After modifying the time level value to the value you need to maintain, move the cursor to any other field and then click the save icon.

*For more details, refer the Security Management System User Manual.*

### **Last Signed On**

This is a display field which shows the Date and Time of the Users last Login.

On each Sign on into the System, this field gets displayed as a Message to the User.



### **Staff Customer Rectification Required**

Check this box to restrict a staff user from viewing, modifying or authorizing other staff customer account details. If this box is unchecked then the staff user can view the CIF/account details of other staff customers in the CIF/Account Maintenance or any query screens.

The staff user can view his/her own account details but won't be able to input or authorize a transaction irrespective of the selection of this box. In this screen, the Customer id of the staff is linked with the user id created for the staff.

 All amend or authorize operations will fail with invalid account / CIF message if you try to amend or authorize own or other staff CIF / account details. The view restriction will not apply to the transaction or contract screens in which the other staff accounts are involved. The view restriction will not apply to the Oracle FLEXCUBE reports.

### **ELCM User ID**

Specify the ELCM user ID which will be used by ELCM system to perform the ELCM maintenance.

 ELCM User ID would be unique across all the instances of FCUBS and it should be controlled operationally.

## ELCM User ID

Specify the ELCM user ID which will be used by ELCM system to perform the ELCM maintenance.



ELCM User ID would be unique across all the instances of FCUBS and it should be controlled operationally.

### Multi Branch Access Required

Check this box if you need to configure dual access framework for the specified User ID.

### Other RM Customer Access Restricted

You can restrict the users' access to the transactions of the customers who are assigned to a different relationship manager. Check this box to restrict the user from viewing, creating, authorizing or amending the transactions of the customers who are not assigned to him/her. The customers not assigned to the RM include the customers assigned to other relationship managers as well as those who are not assigned to any relationship manager.

If you do not check this box, the user can view, create, authorize and amend the transactions of the customers assigned to other relationship managers.

This is applicable to the users created with their role as 'Relationship Manager'.

### Show Dashboards

Check this box if you want the system to display all the Dashboards assigned to your 'User Role, on the landing page.

### Alerts on Home

Check this box if you want the system to display the Alerts, relevant to you, on the landing page.

### Auto Authorize

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

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.

#### Example

You have enabled automatic authorization for the following branches in the Branch Parameters:

| Branch | Automatic Authorization Enabled |
|--------|---------------------------------|
| 000    | Yes                             |
| 001    | No                              |
| 002    | Yes                             |

In the Function Description maintenance, automatic authorization has been enabled for the following functions:

| <b>Function</b>                  | <b>Automatic Authorization Enabled</b> |
|----------------------------------|----------------------------------------|
| Customer Information Maintenance | Yes                                    |
| LD Contract Online               | Yes                                    |
| Customer Account Maintenance     | Yes                                    |
| FT Contract Online               | No                                     |

You have maintained automatic authorization rights for specific users in the User Profile maintenance as shown below:

| <b>User</b> | <b>Automatic Authorization Enabled</b> |
|-------------|----------------------------------------|
| Ronald      | Yes                                    |
| George      | Yes                                    |
| Smith       | No                                     |

You have also maintained transaction access rights for the users as shown below:

| <b>User</b> | <b>Branch</b> | <b>Function</b>                  | <b>Input access</b> | <b>Authorize Access</b> |
|-------------|---------------|----------------------------------|---------------------|-------------------------|
| Ronald      | 000           | Customer Information Maintenance | Yes                 | Yes                     |
| Ronald      | 001           | Customer Information Maintenance | Yes                 | Yes                     |
| Ronald      | 000           | FT Contract Online               | Yes                 | Yes                     |
| Ronald      | 000           | Customer Account Maintenance     | Yes                 | No                      |
| George      | 001           | LD Contract Online               | Yes                 | Yes                     |
| George      | 000           | Customer Account Maintenance     | Yes                 | Yes                     |
| Smith       | 000           | LD Contract Online               | Yes                 | Yes                     |
| Smith       | 000           | Customer Account Maintenance     | Yes                 | Yes                     |

According to your maintenance, automatic authorization would be performed as shown below:

| User   | Branch | Function                         | Automatic Authorization on Save? | Reason                                                                                                                                                                                                                       |
|--------|--------|----------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ronald | 000    | Customer Information Maintenance | Yes                              | Input and Authorize rights enabled for the user, as well as automatic authorization rights enabled for the user, branch and function.                                                                                        |
| Ronald | 001    | Customer Information Maintenance | No                               | Automatic authorization not enabled for branch 001                                                                                                                                                                           |
| Ronald | 000    | FT Contract Online               | No                               | Automatic authorization not enabled for the FT Contract Online function                                                                                                                                                      |
| Ronald | 000    | Customer Account Maintenance     | No                               | Authorization access not enabled for the user                                                                                                                                                                                |
| George | 001    | LD Contract Online               | No                               | Automatic authorization not enabled for branch 001                                                                                                                                                                           |
| George | 000    | Customer Account Maintenance     | Yes                              | Input and Authorize rights enabled for the user, as well as automatic authorization rights enabled for the user, branch and function. The user can also authorize any maintenance done by the user Ronald in this function.. |
| Smith  | 000    | LD Contract Online               | No                               | Authorization access not enabled for the user                                                                                                                                                                                |

*For more details about automatic authorization, consult the Common Procedures user manual.*

### **User Identification**

Specify the User Id with which a User logs into Oracle FLEXCUBE. This User Id is unique across all branches. The minimum length of Userid must be six and the maximum number can be 12 characters.

### **User Reference**

Specify an external reference number for the User Id.

### **User Password**

#### **Password**

Specify the Users Password here. This is a Hidden Field. The Password set must not be a restricted word. It should also be governed by the parameters set in the SMS Bank Parameters table, like Maximum and Minimum length, Number of Alphabetic and Numeric characters etc.



If the application level parameter which indicates the auto generation of the password is required or not is set to Y (Yes), then this field will be disabled and the system will create a random password in accordance with the parameters maintained at the level of the bank. The new password will be send to the respective user via mail.

### **Password Changed On**

The date when the password was last changed gets displayed here.

### **Email**

Specify a valid Email id at the time of user creation. All system generated passwords shall be communicated to the user via this mail id.

### **Start Date**

Specify the date from which the User is valid. The Branch date gets defaulted if no other value is specified.

### **End Date**

Specify the End Date upto which the User is valid. By default the user does not have an End Date associated, unless otherwise specified.

## **Invalid Logins**

### **Cumulative**

The number of Cumulative Invalid Login attempts allowed for a User before the User status gets Disabled is specified in the 'SMS Bank Parameters' screen. The actual attempts that a user makes when he logs into Oracle FLEXCUBE get displayed here.

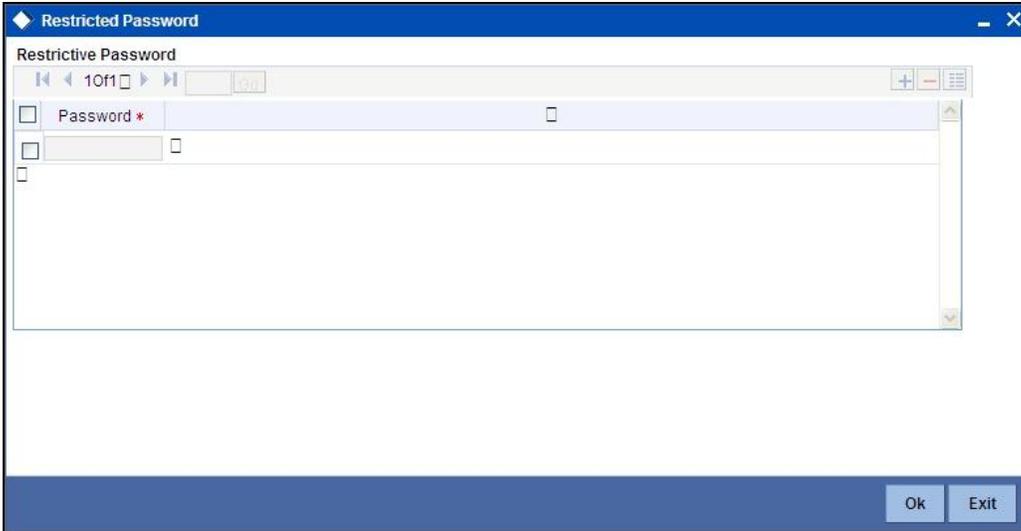
### **Successive**

The number of Successive Invalid Login attempts allowed for a User before the User status gets Disabled is specified in the 'SMS Bank Parameters' screen. The actual attempts that a user makes while he logs into Oracle FLEXCUBE get displayed here.

## **2.10.2 Restricted Passwords**

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 persons, bank, department, etc. as a password, as these 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.

To specify a list of passwords that the user is not allowed to use, click 'Restricted Passwords' button in the User Profile definition screen,

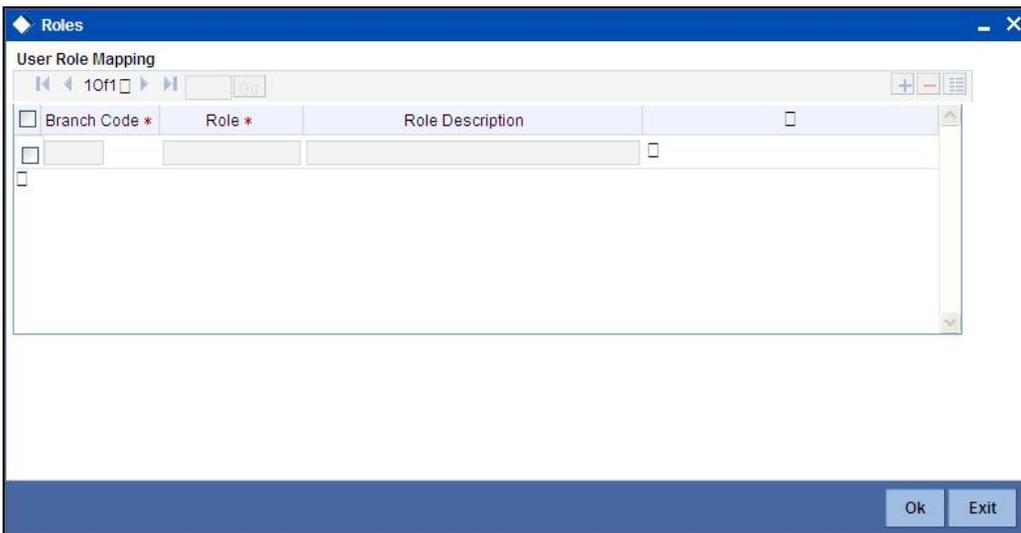


The user for whom you are defining the restrictive passwords cannot use restrictive passwords defined in the Bank Level Parameters screen and the Role Profile screen.

### 2.10.3 Roles

A Role is always associated to a User for a specific Branch. The values set at the Role level are directly inherited by the User for that branch, like Functions Ids, Account Class and Branch Restrictions, Input and Authorization Limits etc.

To attach the user profile you are defining to a role, you must use the 'Roles' screen. Click 'Roles' button and the 'Roles' screen will be displayed. The roles to be attached to the user profile can be listed under 'Roles' list.



Specify the following details:

#### **Branch Code**

Specify the branch code assigned to the user role. The option list displays all the valid branch codes maintained in the system. You can choose the appropriate one.

## Role

Specify the role assigned to the user for the selected branch. The option list displays all valid roles maintained in the system. Choose the appropriate one.



You can assign the role of Relationship Manager to a user by selecting 'RM-ROLE'.

## Role Description

Based on the role selected, the system displays the role description.

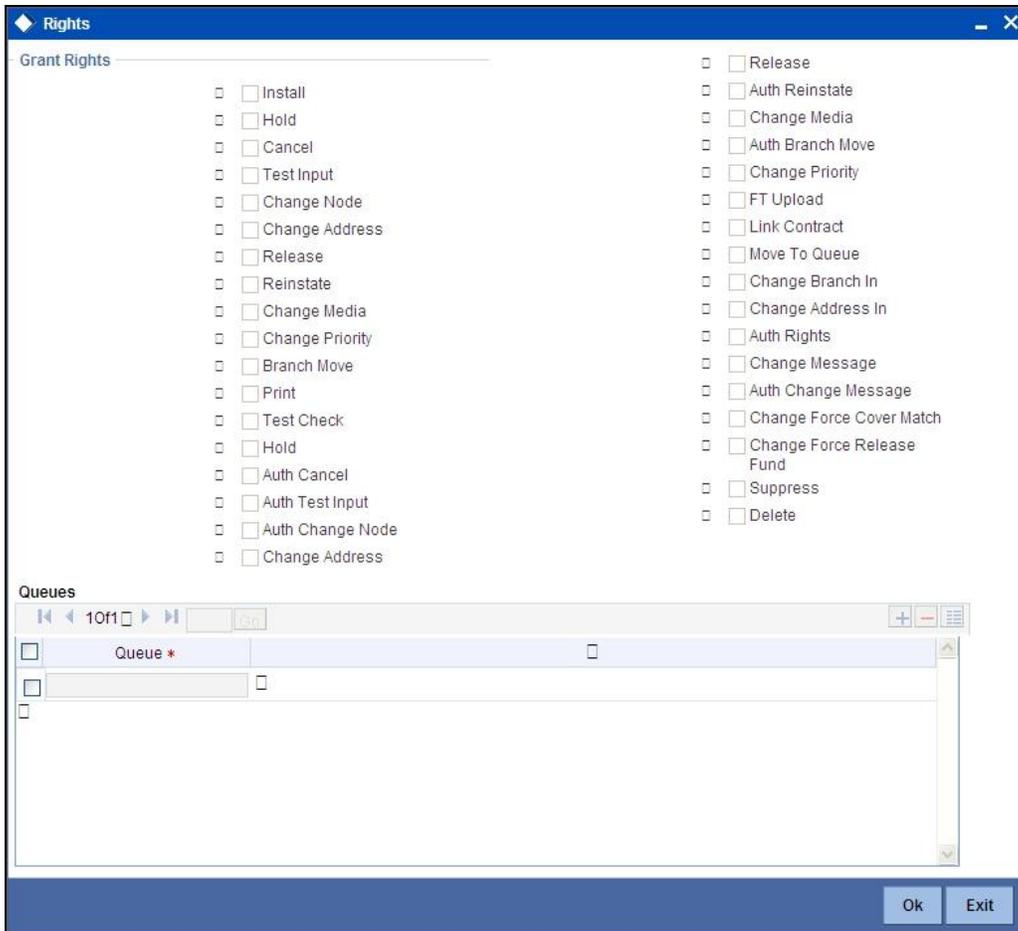
Click add icon to add a record under the 'Roles' list. Specify the above details to attach more roles to the user.

To delete a role(s) that has been attached to a user profile, check the box beside it and click delete icon.

### 2.10.4 Rights

A user should have the necessary rights to perform various operations in respect of incoming and outgoing messages, in the Messaging module of Oracle FLEXCUBE. You can grant specific permissions for operations on messages, as well as allot the messaging queues to which the user has access. In the User Maintenance screen, click 'Rights' button to grant these rights pertaining to the Messaging module, to the user.

The screen is as shown below:



Check against the messaging operations for which you want to grant the permission.

### Granting rights pertaining to operations on messages

You can grant permissions for the following operations on outgoing messages:

- Generating a message
- Printing a message
- Placing a message on hold
- Releasing a message on hold
- Canceling a message
- Inserting a test word
- Reinstating a message
- Changing the priority of a message
- Requesting status of a message
- Requesting cancellation of a message
- Changing the media through which a message is transmitted
- Changing the address to which a message is to be sent
- Moving a message to another branch
- Changing the node from which a message should be generated

- Authorization of any of the operations listed above, in respect of outgoing messages

You can grant permissions for the following operations on incoming messages:

- Printing a message
- Authorizing a test word
- Routing a message to a queue
- Associating a message with a contract
- Uploading incoming messages
- Making changes (edit) incoming messages. You can also grant permissions for changing the branch and the address in incoming messages
- Authorizing changes made to incoming
- 'Force Release' payment message transactions with 'Funding Exception' status and insufficient funds
- Suppressing a message
- Deleting a message

Granting each of these permissions in the Rights screen enables the user to perform the corresponding functions in the Incoming and Outgoing Message Browsers. The appropriate button in the Browser, in each case, is enabled for the user.

*For details regarding each of these operations in respect of both incoming and outgoing messages, consult the Messaging System user manual*

Apart from these functions, you can also grant permission for the cover matching function for incoming payment message transactions.

*For details regarding uploading incoming payment transaction messages and cover matching for incoming payment transactions, refer the Straight Through Processing chapter in the Funds Transfer user manual.*

## **Queues**

You can allot the message queues to which the user has access, and in which the user can perform messaging operations according to the messaging rights you have assigned. The required queues can be selected and listed in the 'Queues' list under the 'Grant Queues' section.

### **2.10.5 Functions**

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
- You have given access to individual functions to a profile to which roles are attached

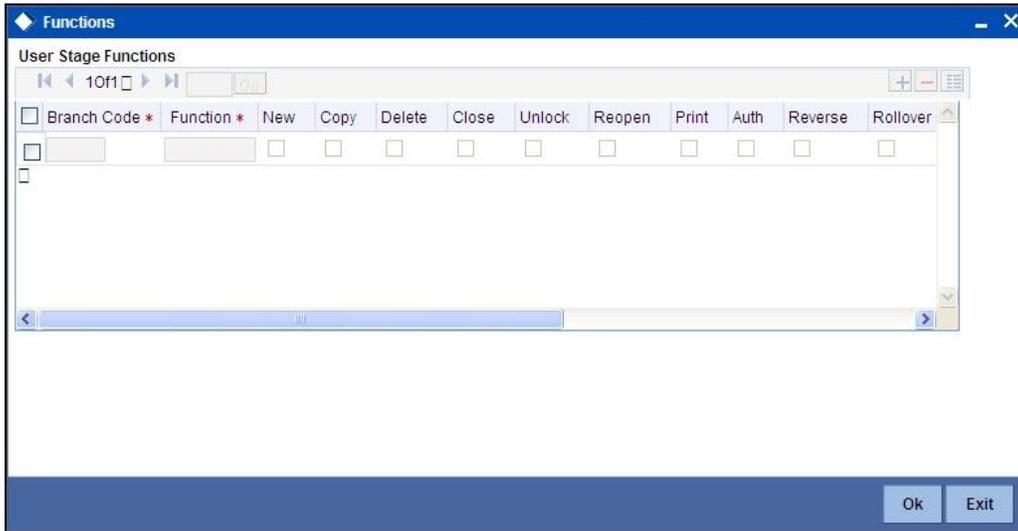
The rights for Function IDs that figure in both the role and user specific functions will be applied as explained in the following example.

#### **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.

To give access to functions for the user profile you are defining, click 'Functions' button in the 'User Profile Definition' screen. The 'Functions' screen will be displayed as shown below:



The various functions in the system fall under different categories.

To assign a function to a user profile in the User Functions screen, you must select the tab of the function category to which the function belongs. The function categories and their respective tab in the User Functions screen are as follows:

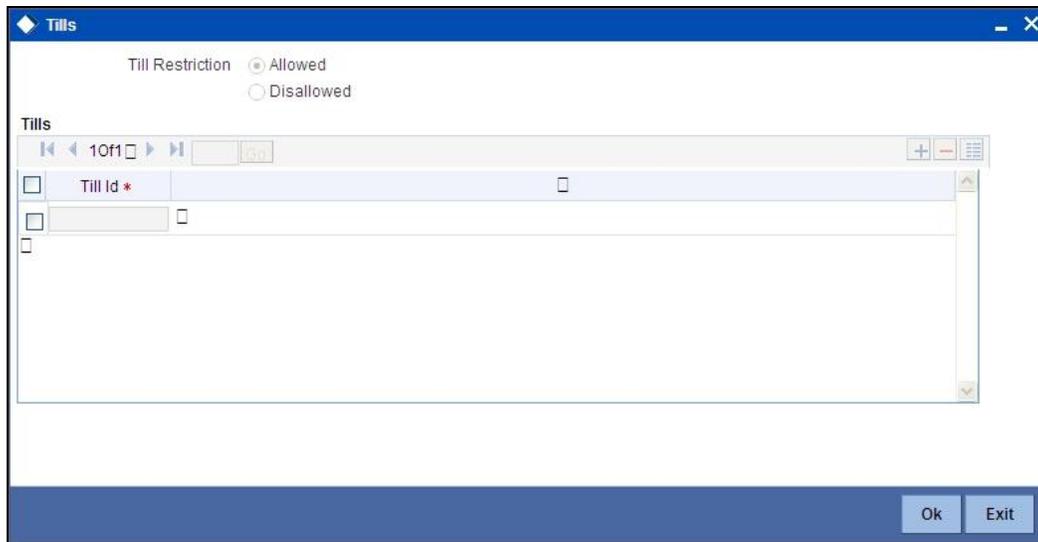
| Category (Tab) | Description                                                                                             |
|----------------|---------------------------------------------------------------------------------------------------------|
| Maintenance    | Functions relating to the maintenance of static tables.                                                 |
| On-line        | Functions relating to contract processing.                                                              |
| 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.                                 |
| Process        | Functions relating to access rights for the tasks under a process                                       |

Click on the corresponding category tab to associate the required functions as described below:

To add a function, click add icon. At Function Identification, you should select the function for which you want to give rights. The adjoining option list displays 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.

## 2.10.6 Tills

You can restrict the user from using certain tills maintained at your bank. Such restrictions can be specified in the 'Tills' screen. Click 'Tills' button to invoke the 'Tills' 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

After choosing either the 'Allowed' or 'Disallowed' option, click add icon to add a record under the 'Tills' list. Into each added field select the required Till Id by clicking the adjoining option list.

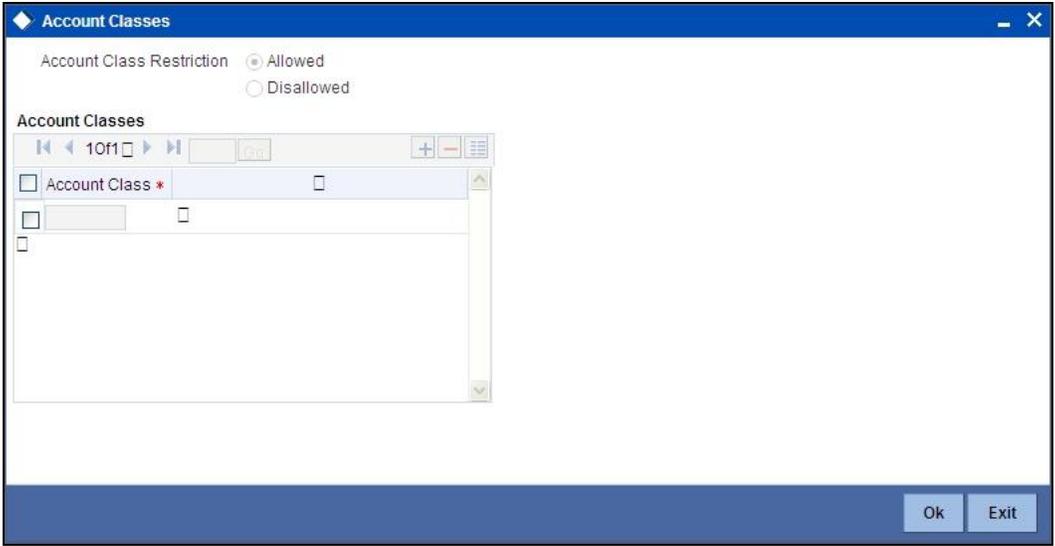
## 2.10.7 Account Classes

You can restrict the user from using certain account classes that are maintained in Oracle FLEXCUBE in two ways.

- You can map an user role which has an account class restriction at User Role level, for an allowed branch in the Roles button at User Profile level.  
Restricted account classes can be viewed in 'Account Class' option list at User Role level and not at User Profile level.
- Select account classes from the 'Account Class' option list and then select an option from the following at User Profile level:
  - Allowed–Select to allow selected account classes and disallow unselected account classes.
  - Disallow–Select to disallow selected account classes and allow unselected account classes.

In both the cases, user can query customer accounts belonging to restricted account class. However, the system will not allow creation and modification of an account under restricted account class.

Click 'Account Classes' button to specify such account class restrictions.

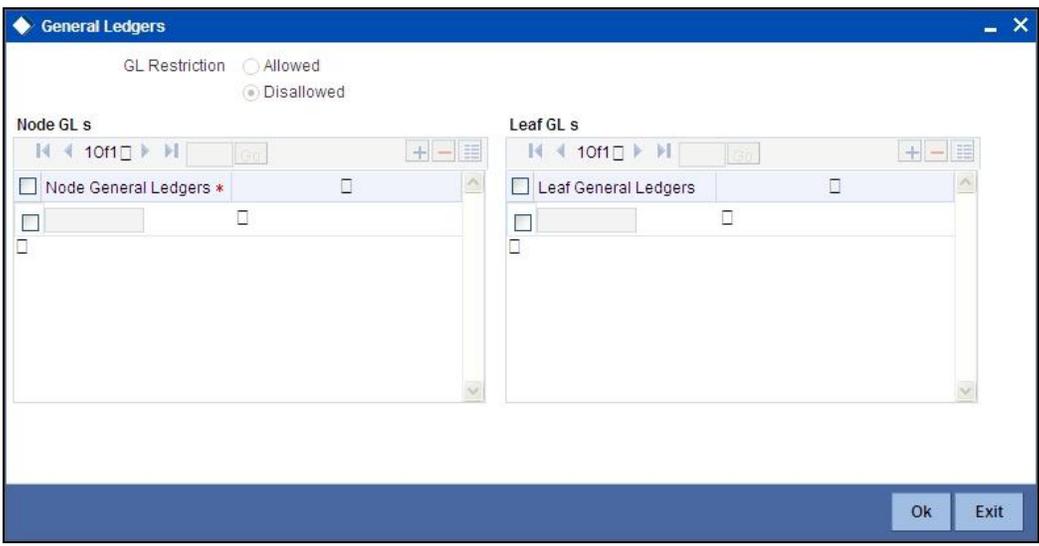


You can either allow or disallow the user from using certain account classes. Subsequently, specify the account classes, which have to be allowed or restricted for the user depending on the option selected. The following options are provided:

- Allowed–Select to allow user to use specified account classes.
- Disallowed–Select to disallow user to use specified account classes.

**2.10.8 General Ledgers**

You can restrict the user from posting entries to certain General Ledgers (GLs) maintained in Oracle FLEXCUBE. Further, you can restrict the user from posting entries to specific node and leaf GLs. Click 'General Ledgers' button 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.

## 2.10.9 Limits

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. You can also associate a user limits or limits at the role level with a user profile. Click 'Limits' button to indicate the limits.

| Branch * | Limits Role | Limit Currency | Input Limit | Authorization Limit |
|----------|-------------|----------------|-------------|---------------------|
|          |             |                |             |                     |

In this screen, you can choose to:

- Define user specific limits
- Link a Limits Role to the User Profile
- Maintain No Limits

The manner in which FLEXCUBE handles each of the above options is explained below:

### 2.10.9.1 Specifying User Specific

If you choose to maintain User Limits, you will need to specify the following details:

- Limit Currency
- Maximum Transaction Amount
- Authorization Limit

When a user processes a transaction, the system will convert the transaction amount (if the transaction is in a different currency) to the currency in which the limit amount is expressed based on the Standard Mid Rate. During authorization or approval of a transaction, if the amount exceeds the limits maintained for the specific user, the system will display an override message.

When such an override is sought, the user will be allowed to continue processing depending upon the sensitivity assigned to the override. The implementers at your installation configure this sensitivity, depending upon your requirements. If it has been configured as 'ignore' or 'warning', the user can continue processing (despite exceeding the input limit) by selecting 'OK' in the override message window, or select 'Cancel' to terminate the processing. If configured to be an 'error', the user cannot proceed with the transaction without authorization.

The system will validate the user authorization limit at the following stages of a transaction:

- Local authorization

- When the transaction is assigned to user manually
- On locking the assigned record
- On authorizing the records



The User Limits maintained for a User Profile are common and applicable across all the branches of your bank.

### **2.10.9.2 Specifying Role of Limits**

You can link a Limits Role to the User Profile. The Limits maintained for the role will be applicable to the user profile to which it is linked.

If you select the Limits Role option, you will be required to specify the following details:

#### **Branch**

For a user, you can assign Limit Roles specific to each branch of your bank. Depending on the branch in which the user operates, the relevant Limits Role will be made applicable. You can select the branch from the option-list available.



You can attach only one Limits Role to a branch. Further, if you choose not to attach a Limits Role to a particular branch, the system will not validate the limits in that branch.

#### **Limits Role**

All the Limits Roles maintained at your bank will be displayed in the option-list. You can select the Roles you wish to link to the user profile. On selection of the Role, the following details get defaulted:

- Limits Currency
- Input Limit
- Authorization Limit



For Journal (Single and Multi-Offset) and Teller transactions, the check will be performed on each individual transaction i.e. each debit and credit entry.

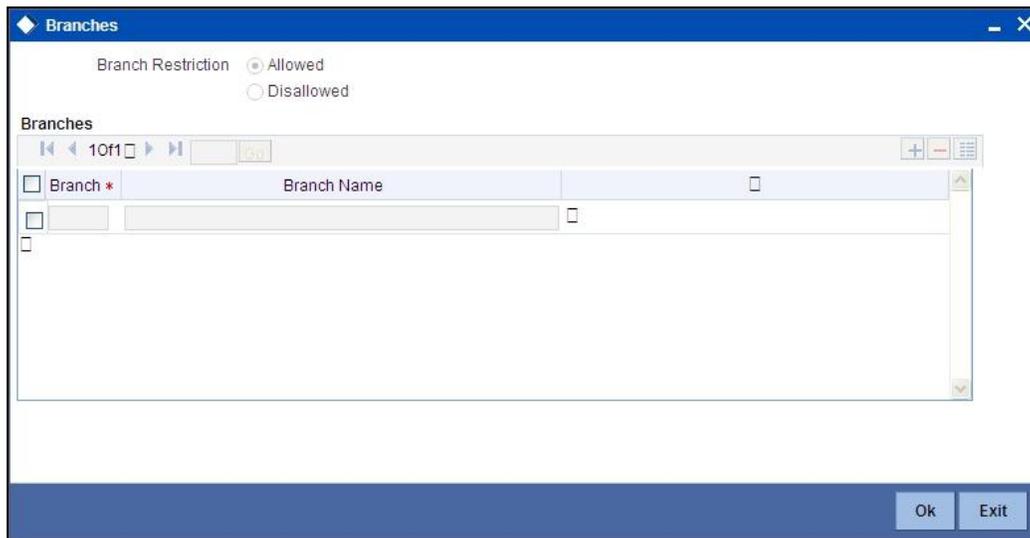
#### **No Limits**

Select the No Limits option, to place no restrictions on the user. The user will be allowed to specify any amount during transaction processing. Likewise, users with authorization rights will be allowed to authorize transactions without any restrictions on the amount involved in the transaction.

## 2.10.10 Branches

To specify the branches from which the Staff and Branch users of the bank can operate, you must use the 'Branches' screen.

Click 'Branches' button in the User Maintenance screen and 'Branches' screen will be displayed as shown below.



You can maintain a list of branches to which the user is either:

- Allowed
- Disallowed

To maintain an allowed list of branches choose the Allowed option. Then the 'Branch Restrictions' list will show the list of allowed branches. To maintain a disallowed list of branches, choose the Disallowed option.

If you maintain an 'allowed' list, then the user profile will be available only for those branches that you specify in the Branch Restrictions list. Similarly, if you maintain a 'disallowed' list, then the user profile will not be available only for those branches that you specify in the Branch Restrictions list. Any branch that is 'Disallowed' will not appear to that user in his 'Change Branch' list.

After choosing either the 'Allowed' or 'Disallowed' option, click add icon to add a record under the 'Branch Restrictions' list. Into each added record's field, select the required branch by clicking the adjoining option list.



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
- 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.

## 2.10.11 Products

You can restrict the user from using certain products maintained in FLEXCUBE. Such product restrictions for the user can be specified in the 'Products' screen. Click 'Products' button and the 'Products' screen will be displayed.

The screenshot shows a software window titled "Products". It contains two identical sections. Each section features a table with the following columns: "Product Code \*", "Product Description", and a small square icon. Below the table, there are two radio button options: "Posting Restriction" with "Allowed" selected, and "Access Restriction" with "Allowed" selected. At the bottom right of the window, there are "Ok" and "Exit" buttons.

In this screen you can place the following restrictions on the User Profile:

- Posting Restriction
- Access Restriction

Users who have posting restrictions will not be able to process transactions involving restricted products. Users with access restrictions will not be allowed to view or print financial details of contracts involving restricted products.

To allow or disallow the user from posting into/accessing certain products by

- Select the option 'Allowed' if you want to allow the user to post entries into/access certain products
- Select the option 'Disallowed' to disallow the user from posting/accessing certain products

After choosing the 'Allowed' or 'Disallowed' option, click add icon to add a record under the 'Products' list. Into each added record's field select the required Product Code by clicking the adjoining option list.



Note the following:

- If for a product the Access restriction has not been maintained but Posting is allowed the restricted user can post transactions for that product and can view the contract information until such time that the contract gets authorized.
- For the PC module, you can apply restrictions on product categories.

### 2.10.12 Group Code Restriction

You can restrict the group code for the selected Oracle FLEXCUBE user id using 'Group Code Restriction' screen. To invoke this screen, click 'Group Code Restriction' button in 'User Maintenance' screen.

#### **Group Code**

Specify whether the group code is allowed or disallowed for the Oracle FLEXCUBE user ID. You can select one of the following:

- Allowed
- Disallowed

#### **Group Code**

Specify group code which is allowed or disallowed for the Oracle FLEXCUBE user. You can select any or all of the following:

- Retail
- Corporate

#### **Group Description**

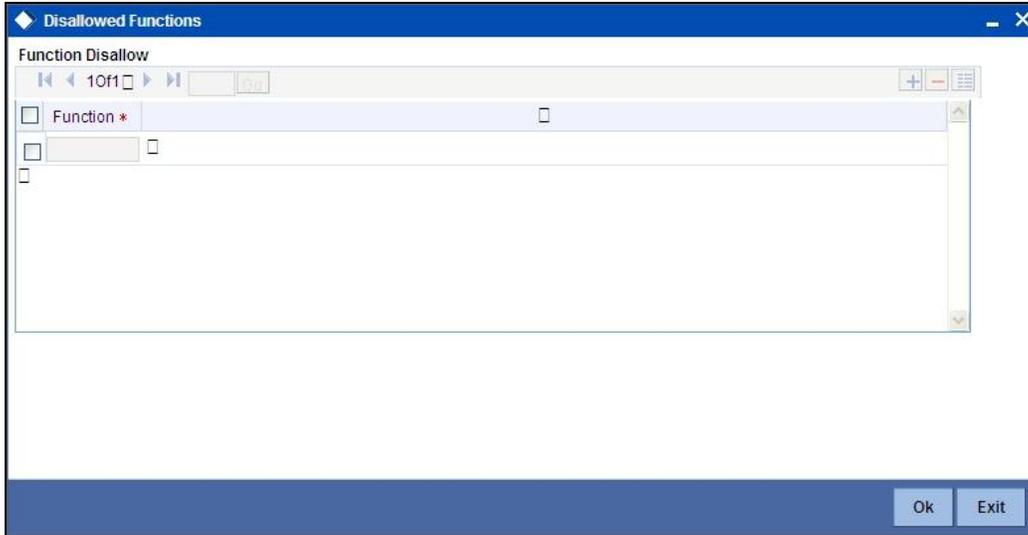
System describes the group code selected by the user.

 User will be able to query or modify the account details only for those customers whose group code is allowed to him. If a user tries to query or modify the account of the customer whose group code is restricted for him, system will display the following error message:

User is restricted to query or modify the account.

### 2.10.13 Disallowed Functions

You can restrict certain functions from being performed by a user. You can specify such restrictions in the 'Disallowed Functions' screen. Click 'Disallowed Functions' button to invoke this screen.



Click add icon to add a record under the 'Function' list. Into each added field, select the required function by clicking the adjoining option list.

## 2.10.14 Users Holiday

You can view holiday periods maintained for the user profile in the 'Users Holiday' screen. Click 'Users Holiday' button to invoke this screen.

The screen is as shown below:

The screenshot displays the 'User Holiday Summary' window. At the top, there are search filters for Authorization Status, Record Status, Branch Code, User ID, Leave From, and Leave To. Below these are buttons for Export, Search, Advanced Search, Refresh, and Reset. A pagination bar shows 'Records per page 15' and '1 Of 1'. The main area contains a table with the following data:

| <input type="checkbox"/> | Authorization Status | Record Status | Branch Code | User ID  | Leave From | Leave To   | Maker ID | Maker Date St |
|--------------------------|----------------------|---------------|-------------|----------|------------|------------|----------|---------------|
| <input type="checkbox"/> | Authorized           | Closed        | 000         | 30300M03 | 2011-09-05 | 2011-09-30 | 30300A03 | 2011-09-02    |
| <input type="checkbox"/> | Authorized           | Open          | 001         | 31581A01 | 2012-03-14 | 2012-03-15 | 31581A02 | 2011-09-02    |
| <input type="checkbox"/> | Authorized           | Open          | 001         | 31581A05 | 2012-03-21 | 2012-03-22 | 31581A02 | 2011-09-02    |
| <input type="checkbox"/> | Authorized           | Open          | 000         | 30300A05 | 2011-10-01 | 2011-10-01 | 30300A03 | 2011-09-30    |
| <input type="checkbox"/> | Authorized           | Open          | 001         | 31581A01 | 2013-03-02 | 2013-03-30 | 31581A02 | 2011-09-05    |
| <input type="checkbox"/> | Authorized           | Open          | 001         | 31581A01 | 2014-03-02 | 2014-03-31 | 31581A02 | 2011-09-05    |
| <input type="checkbox"/> | Authorized           | Open          | 000         | 30300A05 | 2013-06-30 | 2013-06-30 | 30300A12 | 2013-06-30    |

An 'Exit' button is located at the bottom right of the window.

The following details are displayed:

- Authorization Status
- Record Status
- Branch Code
- User ID
- Leave From
- Leave To
- Maker ID
- Maker Date Stamp
- Checker ID
- Checker Date Stamp

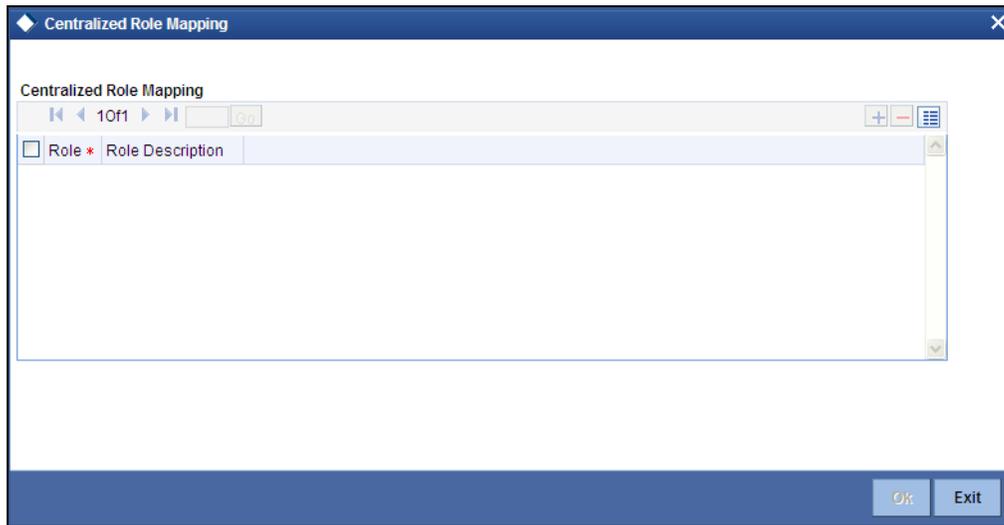


The above screen can be used only for viewing the holiday summary of the user specified in the 'User Holiday Maintenance' screen. Hence all the query fields such as Authorization Status, Branch Code, User ID etc will be disabled.

For more information about viewing holiday details for any user profile, refer the section 'Viewing Holiday Summary Details' in this document.

### 2.10.15 Centralized Role

The centralization role can be linked to a user here. You can view centralized role maintained for the user profile in the 'Centralized Role' screen. Click 'Centralized Role' button to invoke this screen.



If the multi branch operational parameter is enabled and the centralization roles are defined, then the roles are automatically assigned to the branches based on the branch restricted details specified in the user maintenance screen. You can also include additional list of normal roles from the Roles sub screen.



You cannot assign a centralized role to a subset of allowed branches of a user. You have to manually assign the normal role to each applicable branch.

## 2.10.16 Dashboard Mapping

If you checked the 'Show Dashboards' check box in the main page of the 'User Maintenance' screen, then you can map the specified 'User' to one or more Dashboards in the 'Dashboard Maintenance' sub-screen. Click 'Dashboard Mapping' button to invoke this screen.



| Function Id | Description | Sequence Number | Clause Wizard | Where Clause | Show In Dash board |
|-------------|-------------|-----------------|---------------|--------------|--------------------|
|-------------|-------------|-----------------|---------------|--------------|--------------------|

The system defaults the following from the main screen:

- User Identification
- Name

Click 'Populate' button, the system displays DFIs mapped to the specified 'User Role'. The system defaults the following details:

- Function ID – Function ID of the Dashboard assigned to the 'User'.
- Description – Description of the Dashboard

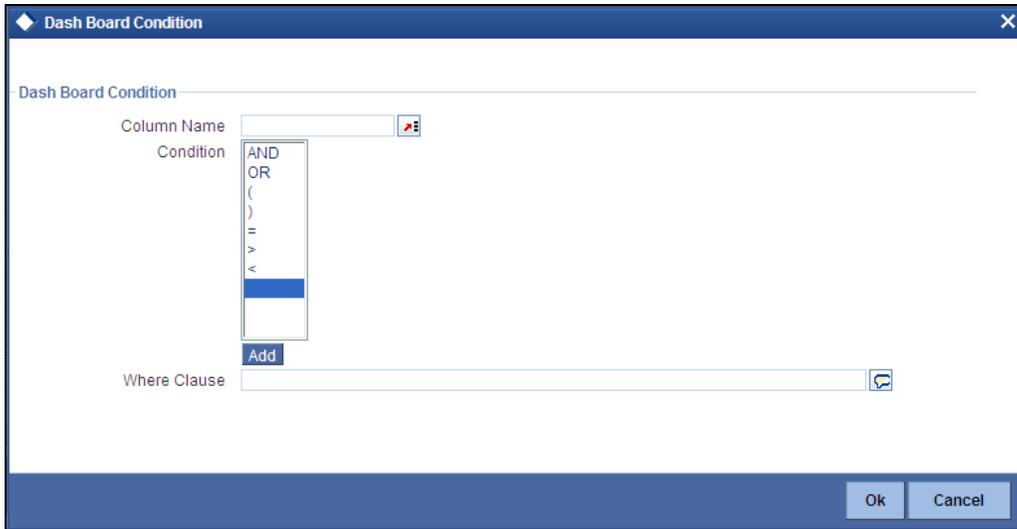
You can maintain the following details for the dash:

### Sequence Number

Specify the sequence number, based on the 'User' preference.

## Clause Wizard

Click to invoke 'Dashboard Condition' sub-screen. You can maintain filter conditions for each DFI the 'User' is mapped to.



You can maintain filter conditions for a specific Dashboard:

### Column Name

Specify the column name for which you want to maintain filter conditions. The adjoining option list displays all valid columns available in the Dashboard. Choose the appropriate one.

### Condition

Select the filter condition you want to maintain. The following conditions are available:

- AND
- OR
- (
- )
- =
- >
- <

Click 'Add' to add the selected conditions to 'Where Clause'.

### Where Clause

Here, the system defaults the values specified in 'Dashboard Condition' screen.

### Show in Dashboard

Check this box if you want to display a specific Dashboard assigned to the 'User'.

### **2.10.17 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.

Select 'Copy' from the Actions menu in the Application toolbar. 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.

### **2.10.18 Deleting a User Profile**

Enter the User ID. The details defined will be displayed. Select 'Delete' from the Actions menu in the Application toolbar to delete an existing user profile. Only users that have not been authorized can be deleted by the creator. You will be prompted to confirm the deletion. The user profile will be deleted only if you confirm the deletion.

### **2.10.19 Closing a User Profile**

Users Ids that are no longer usable can be closed. For Closing, Enter the User ID. The details defined will be displayed. Select 'Close' from the Actions menu in the Application toolbar to close an existing user profile. The profile can be closed only if the User is currently not logged on to the system.

You will be prompted to confirm the Closure. The user profile will be closure only if you confirm the Closure.

## **2.11 Specifying Department Details**

Oracle FLEXCUBE allows you to maintain department details in the system. However, only privileged administrative users can edit the department details. You can capture department details in the 'Department Maintenance' screen. You can invoke this screen by typing 'SMDDPTMT' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot shows a software window titled "Department Maintenance". At the top left, there is a "New" button. Below it, the section "Department Details" contains three text input fields, each with a red asterisk indicating a required field: "Department Code \*", "Department Short Name \*", and "Department Description \*". The bottom of the window features a dark blue footer area with several labels: "Maker", "Checker", "Mod No", "Date Time:", "Record Status", and "Authorization Status". An "Exit" button is located in the bottom right corner of this footer area.

### **Department Details**

Here you can specify the following:

#### **Department Code**

Specify the department code. You can enter a maximum of 3 alphanumeric characters.

#### **Department Short Name**

Specify the department short name. You can enter a maximum of 10 alphanumeric characters.

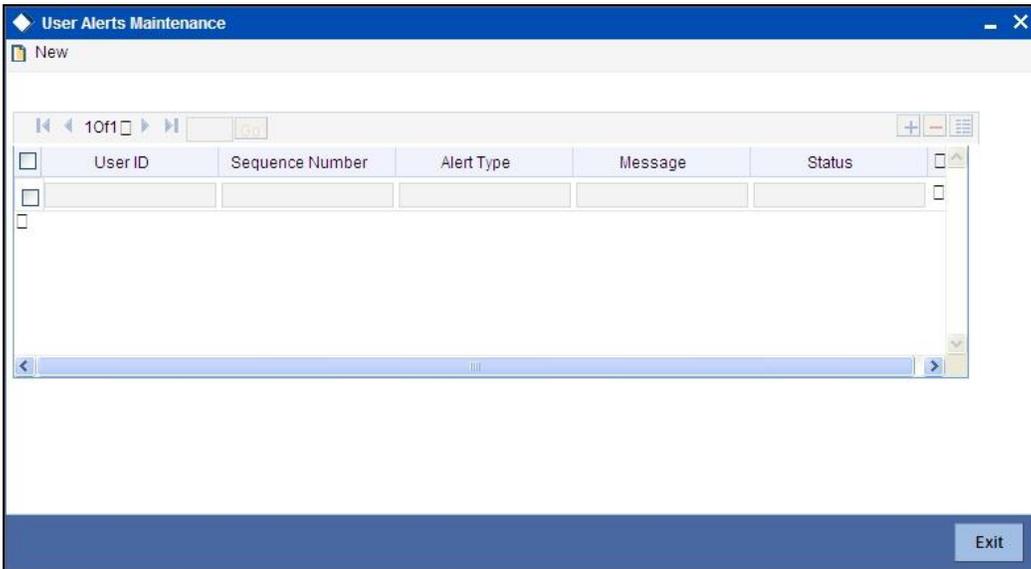
#### **Department Description**

Specify the department description. You can enter a maximum of 225 alphanumeric characters.

## **2.12 Defining Alerts for Users**

Oracle FLEXCUBE allows you to define and send text messages to a destination user. These text messages will be displayed as an alert on the dashboard when the destination user logs in to the application. The user can then pick up the unprocessed messages and process it.

You can define the message for a destination user in the 'User Alerts' screen. You can invoke this screen by typing 'SMDUSALR' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



The following details are captured here:

**User Id**

Specify the id of the destination user to whom the message has to be sent.

**Sequence No**

Specify the sequence number of the message that you are defining.

**Alert Type**

Specify the alert type as I (Information).

**Message**

Specify the message that has to be sent to the destination user.

**Status**

Specify the status of the message as any of the following:

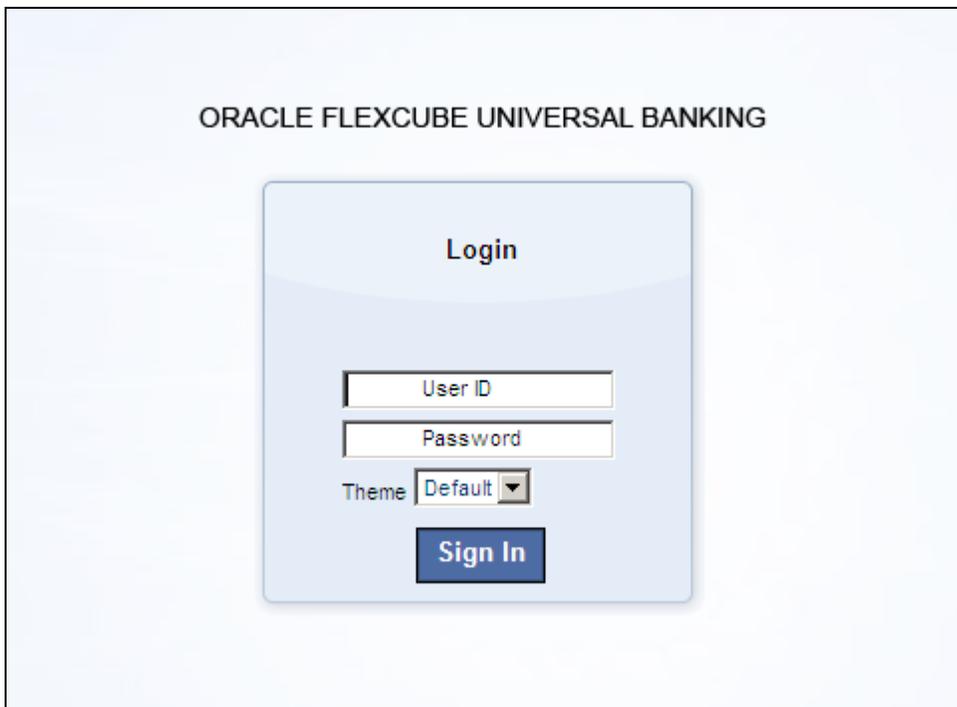
- P -Processed
- U -Unprocessed

After defining the message click 'Exit' button to exit from the screen.

For more details on how the destination user can view the alert messages refer section titled 'Unprocessed Alerts' in the chapter 'Getting Started with Oracle FLEXCUBE' in 'Procedures' User Manual.

## 2.13 Single Sign On (SSO) Enabled Environment

Provided you have opted for the SSO Enabled option at bank level, you can log in from an LDAP (Oracle Internet Directory) external system into Oracle FLEXCUBE through the screen shown below.



After successful authentication and authorization of the user is carried out by the LDAP (Oracle Internet Directory), a request is forwarded to gain access into Oracle FLEXCUBE. On clicking the 'Submit' button you can directly get into Oracle FLEXCUBE without specifying Oracle FLEXCUBE user id and password.

## 3. Associated Functions

### 3.1 Clearing a User ID

When a User logs into the system, the system maintains a record of the user with the date and time of login. On a successful, normal log out this record gets deleted.

Occasionally, you may come across a situation when a user who is logged into the system is forced out. However, the ID of the user 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' screen. You can invoke this screen by typing 'CLRU' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

| Branch Code | User Id  | User Name  |
|-------------|----------|------------|
| 004         | 36697T1  | PRAHLAD    |
| 004         | SIVAKAN  | SIVAKANNAN |
| 004         | SIVAAUTO | SIVAKANNAN |

You can search for the users based on the following parameters:

- User Id
- Branch Code

Once you have specified the parameters click 'Fetch' button. The system lists the following details of the users who have logged into the application:

- Branch Code
- User ID
- User Name

To force log out a user, check the box against the relevant user record and click 'Clear' button. The system will display a message to confirm the clear operation. To force log out all the users in a page, check the box against the header row, which will select all the users in the page. Further click the 'Clear' button. The selected users are logged off from the application.

### 3.2 Changing the System Time Level

The time level is allotted at two levels — at the system (branch) level and at 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. The time level can be between zero and nine.

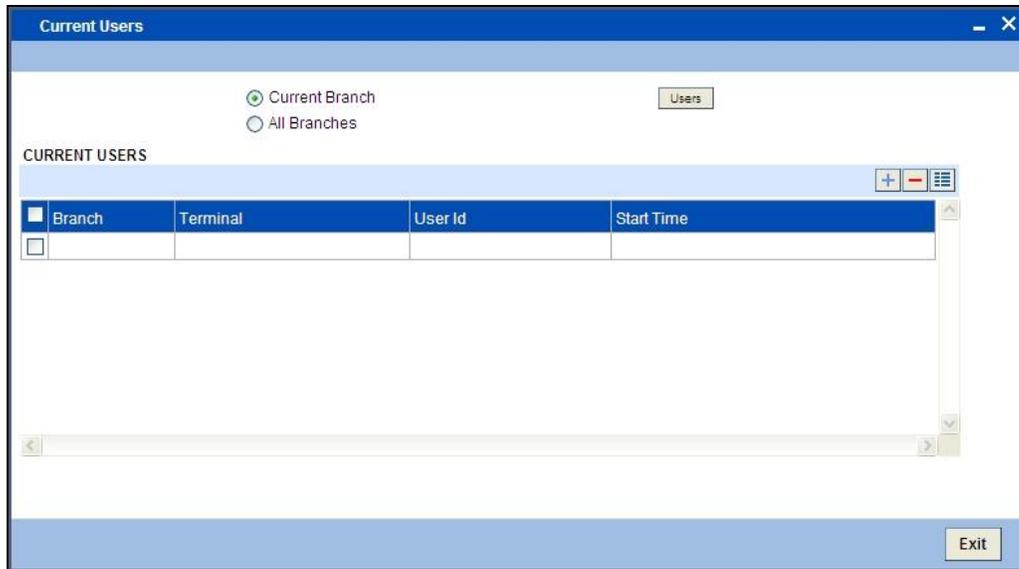
You can change time level of the branch by using the 'Change Time Level' screen. You can invoke this screen by typing 'SMDCHGTL' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button. Click 'Users' button for a display of the details of users who are currently logged in.

This screen shows a list of all users who are currently logged in and their respective Time Levels. When the Time Level of the branch is changed the system validates and displays a message if the Time Level of any of the Users is lesser than that of the newly changed value. These users can continue to log onto and work on the system till they log off. When they try to log in back the system validates and only allows such users access whose time levels are greater than that of the system

The screenshot shows the 'Change Time Level' application window. It features a blue title bar with the text 'Change Time Level' and standard window controls. The main area contains several input fields and a table. At the top, there are fields for 'Branch', 'New Time Level', and 'Current Time Level', along with a 'Users' button. Below this is a section titled 'User Time Level' containing a table with columns for 'User Id', 'Terminal', and 'Time Level'. The table has a header row and one data row. At the bottom of the window, there are fields for 'Input By', 'Authorized By', and 'Modification Number', along with checkboxes for 'Authorized' and 'Open', and an 'Exit' button.

### 3.3 View Current Users

The user of a branch can view a list of all the users logged in from the current branch or from any other the branches through the 'Current Users' screen.



The following details are captured here:

#### **Branch**

You are allowed to view users logged in from the current branch as well as any other branch. Select the any of the following options and click 'Users' button to view the current users of that branch:

- Current Branch
- All Branches

The following user details are displayed here:

- Branch – The branch from which the user has logged in
- Terminal – The terminal/system from which the user has logged in
- User Identification – The name of the user
- Start Time – The time when the user logged in

## 3.4 Defining Language Codes

Every language that is supported by the system is identified by a Language Code. In Oracle FLEXCUBE, this code is a three character alphanumeric code.

Invoke the 'Language Code Maintenance – Detailed' screen by typing 'SMDLNGCD' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot shows a web-based form titled "Language Code" with a "New" icon in the top left corner. The form contains the following fields:

- Language Code \* (text input)
- Language Name \* (text input)
- Display Direction (text input)
- Language ISO Code (text input)

At the bottom of the form, there are three columns of fields:

- Input By (text input)
- Authorized By (text input)
- Modification Number (text input)

Below these fields are two checkboxes: "Authorized" and "Open". An "Exit" button is located in the bottom right corner.

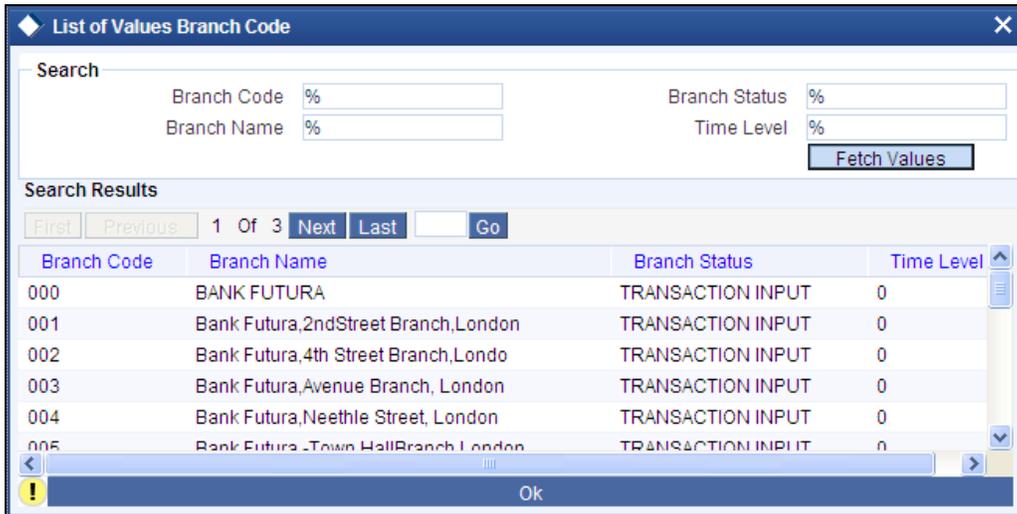
### Example

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

### 3.5 Changing the Branch of Operation

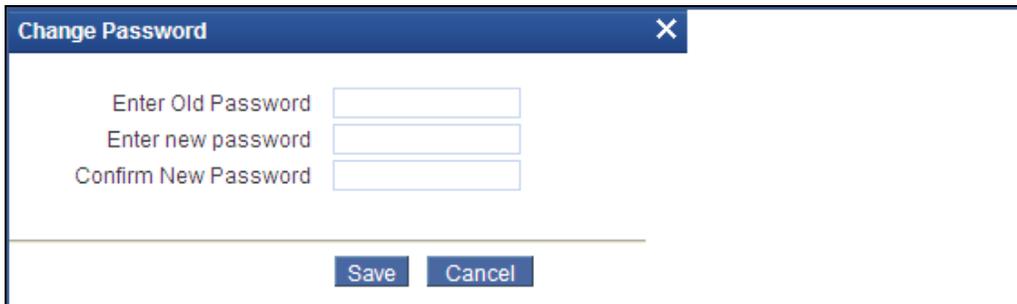
Through this function, you can change the branch of operation to a branch other than the one you are signed on to. The branches to which you can change into will be defined in your user profile. You can change your branch of operation only when a function that has been initiated by you in the current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

The screen is as shown below:



### 3.6 Changing the User Password

The Password of a User can be changed either when it expires or at the will of the user using the 'Change Password' screen.



The following details are captured here:

**Enter Old password**

Specify the old password which has to be changed.

**Enter new password**

Specify the new password.

**Confirm new password**

Specify the new password.

Click 'Save' to save the new password. Click 'Cancel' to exit the screen.

### 3.7 Maintaining SSO Parameters

LDAP is an external directory system which stores the details regarding user ids and password.

Once SSO has been enabled for your bank, the SSO parameters need to be maintained. This can be done using the 'Single Sign On Maintenance' screen. You can invoke this screen by typing 'SMDSOPRM' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot shows a window titled "LDAP Maintenance" with a "New" tab. The main area contains six input fields, each with a red asterisk and a help icon:

- LDAP Host \*
- LDAP Port \*
- LDAP Admin Id \*
- LDAP Password \*
- LDAP Base \*
- Time Out Duration(Seconds) \*

At the bottom, there is a "Fields" section with the following labels:

- Input By: Date Time
- Authorized By: Date Time
- Modification Number:  Authorized,  Open

An "Exit" button is located in the bottom right corner.

The following details can be maintained in this screen:

#### **LDAP Host**

Indicate the machine or server name where LDAP (Oracle Internet Directory) is installed.

#### **LDAP Port**

Specify the network Port number where the LDAP (Oracle Internet Directory) listen to the Server.

#### **LDAP Admin id**

Specify the admin user id of the LDAP (Oracle Internet Directory).

#### **LDAP Password**

Specify the Password for the LDAP Admin User which is provided during installation.

#### **LDAP Base**

Specify the directory information tree (DIT) structure under which the data is to be stored, which is provided during installation. This is used while validating the user present in the LDAP (Oracle Internet Directory).

### Time Out Duration (Sec)

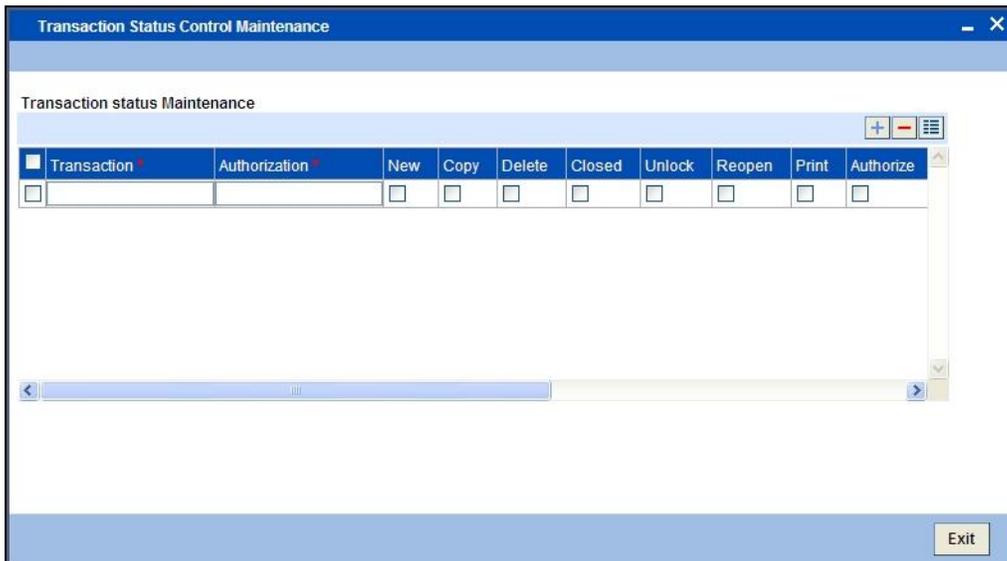
You can stipulate the allowable idle time (in seconds) that a user can spend without performing any activity, after logging in to the system.

## 3.8 Maintaining Transaction Status Control

The 'Transaction Status Control Maintenance' screen allows the user to define the various action buttons depending on the status of the contract. You can invoke this screen by typing 'SMDTXNST' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button. For each Transaction Status, the record status 'Authorized' or 'Unauthorized', could also affect the Action buttons.

Some of the statuses that a Contract could have are:

- Y-Irrevocable
- A-Authorized
- U-Unauthorized
- V-Reversed
- L-Liquidated
- S-Closed
- H-Hold
- K-Cancelled
- N-NON-CUMULATIVE
- T-TIME
- O-OUR



Check the box against a transaction record to select the actions allowed for that transaction. Following are the actions that are allowed on a record:

- New
- Copy
- Delete

- Close
- Unlock
- Reopen
- Print
- Auth
- Reverse

### 3.9 Maintaining Error Messages

Error codes provide step by step support for maintenances and contract Input for a User. The Error codes are uploaded into the system at Software installation. However the 'Description' and 'Type' of the error can be modified from the Oracle FLEXCUBE Menu. Each Error Code can be of the following types:

- Override(O)
- Ignore / Warning (I)
- Error(E)

You can maintain error messages using the 'Error Messages Maintenance' screen. You invoke this screen by typing 'CSDERMSG' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow.

The screenshot shows the 'Error Messages Maintenance' application window. The window has a blue title bar with the text 'Error Messages Maintenance' and standard window control buttons (minimize, maximize, close). Below the title bar is a toolbar with a 'New' icon and an 'Enter Query' button. The main area contains several input fields: 'Error Code \*', 'Language \*', 'Description', and 'Message'. There are also dropdown menus for 'Type \*' and 'Language \*'. At the bottom, there are fields for 'Input By', 'Authorized By', and 'Modification Number', along with checkboxes for 'Authorized' and 'Open', and 'Ok' and 'Exit' buttons.

The following details are captured here:

#### **Error Code**

Specify a code for the error message here.

#### **Language**

Specify the language code of the error message.

## Description

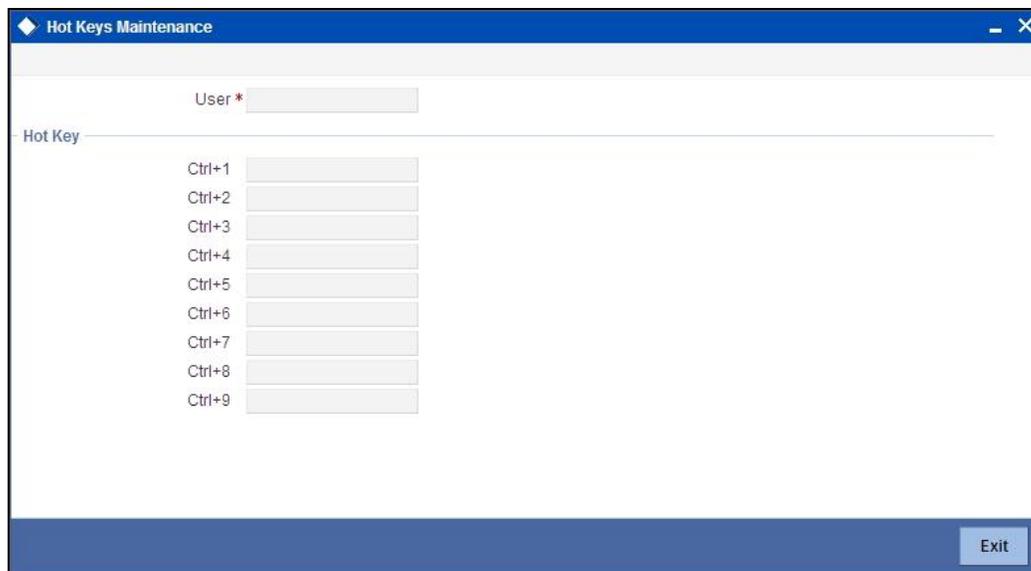
Specify the description for the language code.

## Message

Specify the error message that has to be displayed.

### 3.9.1 Configuring Customized Hot Keys for Launching Screens

Oracle FLEXCUBE allows you to configure Hot keys or Shortcut keys for function ids, using which you can launch the function id screens without typing the function ids. For this you need to map each function id to a hot key using the 'Hot Key Maintenance' screen. To invoke the 'Hot Keys Maintenance' screen click the option 'Hot Keys' under 'Options' menu. You invoke this screen by typing 'SMDHOTKY' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



The screenshot shows a window titled "Hot Keys Maintenance". At the top, there is a "User \*" field. Below it, a section labeled "Hot Key" is separated by a horizontal line. Under this section, there are nine rows, each with a label (Ctrl+1 through Ctrl+9) and an empty input field. At the bottom right of the window is an "Exit" button.

The following details are captured in this screen:

#### **User Id**

The id of the user who has logged in is displayed here.

#### **Hot Key Details**

Here, you can map a function id against each hot key. You can select the function id to be mapped against the hot key from the adjoining option list.

### 3.10 Viewing User Activities

You can view a log of activities of Oracle FLEXCUBE users through the 'User Activity' screen. Note that you can view user activities only through Oracle FLEXCUBE host system. This screen is not available for viewing in the branch installations. You can invoke this screen by typing 'SMSUSRAC' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screen is displayed as below:



You can query for records based on the following criteria:

- User ID
- Branch Code
- Function ID

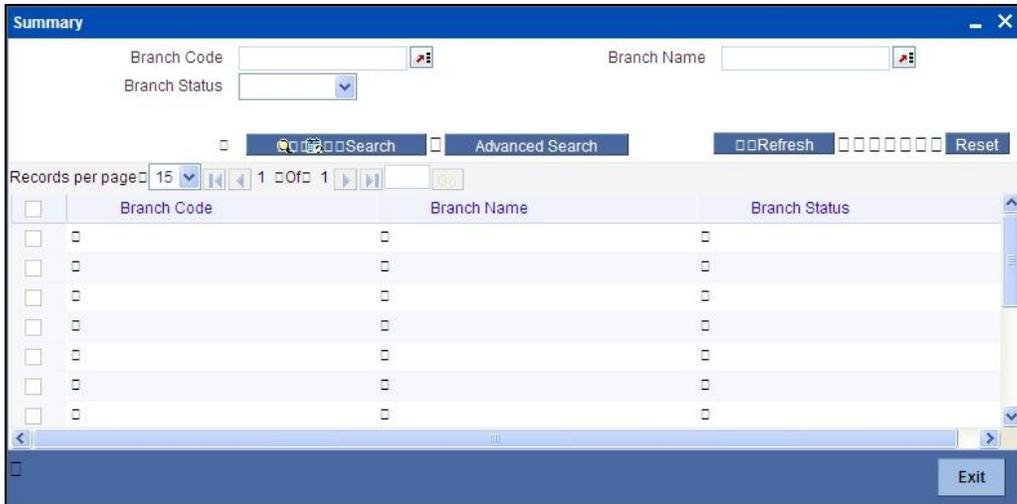
Click 'Search' button. Based on your preferences, the system identifies all records satisfying the criteria and displays the following details for every record:

- User ID
- IP Address
- Branch Code
- Function ID
- Sequence No
- System Start Time
- System End Time
- Exit Flag

### 3.11 Viewing Branch Status

You can view the host connectivity status of various branches through the 'Branch Status' screen. You can invoke this screen by typing 'SMSBRNST' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screen is displayed as below:



You can query for records based on the following criteria:

- Branch Code
- Branch Name
- Branch Status

Click 'Search' button. Based on your preferences, the system identifies all records satisfying the criteria and displays the following details for every record:

- Branch Code
- Branch Name
- Branch Status

---

## 4. Error Codes and Messages

### 4.1 Error Codes

| Error Code | Message                                                                                                |
|------------|--------------------------------------------------------------------------------------------------------|
| SM-00001   | Unauthorized installation. Contact Oracle Financial Services 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 log in. 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-00030   | This function is currently not available for execution                                                 |
| SM-00031   | This form \$1 is not available. Contact your branch system 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                                                        |

| <b>Error Code</b> | <b>Message</b>                                                                        |
|-------------------|---------------------------------------------------------------------------------------|
| 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-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-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                                             |

| <b>Error Code</b> | <b>Message</b>                                                                         |
|-------------------|----------------------------------------------------------------------------------------|
| 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-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?                                                        |
| 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                                 |

| <b>Error Code</b> | <b>Message</b>                                                                                          |
|-------------------|---------------------------------------------------------------------------------------------------------|
| 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-00140          | Guest ID not defined in branch \$1                                                                      |
| SM-00150          | Maximum value encountered                                                                               |
| 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-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 Oracle Financial Services 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-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 |

| <b>Error Code</b> | <b>Message</b>                                                                                          |
|-------------------|---------------------------------------------------------------------------------------------------------|
| 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-00185          | Password can not contain more than \$1 consecutive characters                                           |
| 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 lesser than Min password length                               |
| SM-00189          | Min password numeric length can not be Greater than Min password length                                 |
| SM-00200          | Maximum No of Consecutive Characters should be Greater than 0                                           |
| SM-00201          | The transaction amount exceeds the maximum input amount for the user                                    |
| SM-00202          | The User is Un-Authorized                                                                               |
| SM-00203          | The Last Login date was - \$1                                                                           |
| SM-00204          | Failed to validate transaction limits for the User                                                      |
| SM-00205          | Limits Id already exists                                                                                |
| SM-00206          | Dormancy Days Should be Greater than 0                                                                  |
| SM-00207          | Warning Screen Text can not be Null                                                                     |
| SM-00208          | Role Limits attached to the User are Unauthorized                                                       |
| SM-00209          | Restriction type cannot be null                                                                         |
| SM-00251          | Value for legal notice is needed.                                                                       |
| SM-00252          | Value for legal notice is not needed.                                                                   |

| <b>Error Code</b> | <b>Message</b>                                                             |
|-------------------|----------------------------------------------------------------------------|
| SM-00300          | Values for user limits are not applicable for the chosen transaction limit |
| SM-00301          | Values for role limits are not applicable for the chosen transaction limit |
| 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 i-flex 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-00610          | No functions defined for the user                                          |
| SM-00612          | You are not logged on                                                      |
| SM-00900          | Process completed                                                          |
| SM-00901          | Please select user ids to Enable                                           |
| SM-00998          | Password should be alphanumeric                                            |
| 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                                                             |

| <b>Error Code</b> | <b>Message</b>                                                                                        |
|-------------------|-------------------------------------------------------------------------------------------------------|
| 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-01019          | Function id is not available for current module                                                       |
| SM-01099          | Your Current amount decimal separator is not '\$1'. Please ask IT to change machine oracle settings.' |
| SM-01100          | Entries in SMS bank parameters missing                                                                |
| SM-01101          | Could not get today s date for the head office                                                        |
| SM-01102          | Bank code not maintained in branch table                                                              |
| SM-01103          | Local currency not maintained in bank table                                                           |
| 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-0200           | Cannot restrict current password                                                                      |
| SM-02000          | Internal error: exception raised in \$1                                                               |
| SM-02001          | Enter from date                                                                                       |

| <b>Error Code</b> | <b>Message</b>                                                              |
|-------------------|-----------------------------------------------------------------------------|
| 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-06500          | Document Long Description is Mandatory                                      |
| SM-0999           | You do not have access to this function                                     |
| 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                                          |
| SM-10003          | Branch is closed                                                            |
| SM-10004          | Number of invalid logins since last logout = \$1                            |
| SM-10005          | This Function has been linked to a role                                     |
| SM-3001           | User does not have rights                                                   |
| SM-3002           | Incorrect User ID or password                                               |
| SM-555555         | Sign off allowed only from home branch                                      |
| SM-555556         | Logout allowed only from home branch                                        |
| SM-555557         | Triggers in the database are disabled. Please contact System Administrator. |
| SM-666666         | Amount exceeds users authorization limit                                    |

| <b>Error Code</b> | <b>Message</b>                                                                        |
|-------------------|---------------------------------------------------------------------------------------|
| SM-66666          | Amount exceeds users authorization limit                                              |
| SM-700007         | Terminal ID should be Four Characters in Length                                       |
| SM-7001           | Invalid User Id or Password                                                           |
| SM-7002           | User does not have rights                                                             |
| SM-7003           | Invalid Login                                                                         |
| SM-7004           | User already logged in                                                                |
| SM-7005           | User Status is Disabled                                                               |
| SM-7006           | User Status on Hold                                                                   |
| SM-7007           | Your Time level does not permit you to Login                                          |
| SM-7008           | Please change Password now!                                                           |
| SM-7010           | Password file missing or corrupt                                                      |
| SM-7011           | Oracle built in problem                                                               |
| SM-7012           | Password due to expire on \$1                                                         |
| SM-7013           | User Profile expired                                                                  |
| SM-7014           | Wrong Password                                                                        |
| SM-7015           | Enter Password again                                                                  |
| SM-7016           | The New and Confirmed Passwords do not match                                          |
| SM-7017           | Enter Passwords again                                                                 |
| SM-7018           | The Password entered is Restricted. Try another Password                              |
| SM-7019           | The Password entered has already been used. Try another Password                      |
| SM-7020           | Length of Password is less than \$1 characters                                        |
| SM-7021           | Length of Password is more than \$1 characters                                        |
| SM-7022           | The Password string contains special characters that are not allowed. Retype Password |

| <b>Error Code</b> | <b>Message</b>                                                                         |
|-------------------|----------------------------------------------------------------------------------------|
| SM-7023           | Password cannot contain more than \$1 consecutive identical characters                 |
| SM-7024           | You cannot change Password today                                                       |
| SM-7025           | The password should be mix of alphabetic and numeric characters                        |
| SM-7026           | Control Clerks Passwords do not match. Retype Passwords again                          |
| SM-7027           | There are Users currently logged in with a lesser time level. Do you want to change?   |
| SM-7028           | User Id already exists.                                                                |
| SM-7029           | Cumulative Invalid Logins - Number should be greater than 5 and less than 100          |
| SM-7031           | Password prevent reuse value should be between 1 and 5 Minimum                         |
| SM-7032           | Password length should be between 6 and 10                                             |
| SM-7033           | Maximum Password Length should be between 9 and 12                                     |
| SM-7034           | Password expiry message - between 0 and 5                                              |
| SM-7035           | Password change after message - no of days should be greater than 15 and less than 180 |
| SM-7036           | User Access to \$1 \$2 denied                                                          |
| SM-7037           | Consecutive Password Characters should be greater than 1                               |
| SM-7038           | The User is un-authorized                                                              |
| SM-7039           | The Last Login date was - \$1                                                          |
| SM-7040           | Password Changed Successfully                                                          |
| SM-7041           | Invalid Password. Bad Sign On                                                          |
| SM-7042           | Invalid Name. Bad Sign On                                                              |
| SM-7043           | Successive Invalid Logins                                                              |
| SM-7044           | Forced Disable Cumulative Invalid Logins                                               |
| SM-7045           | Forced Disable Password expired.                                                       |
| SM-7046           | Password changed                                                                       |

| <b>Error Code</b> | <b>Message</b>                                                               |
|-------------------|------------------------------------------------------------------------------|
| SM-7047           | User initiated Password change                                               |
| SM-7048           | Forced password change                                                       |
| SM-7049           | Status Enabled                                                               |
| SM-7050           | Status put on                                                                |
| SM-7051           | Hold User already Signed on                                                  |
| SM-7052           | Do you want to reset Cumulative Invalid Logins to 0 ?                        |
| SM-7053           | Number of Invalid Logins Since Last Logout = \$1                             |
| SM-7054           | User Password Changed Successfully                                           |
| SM-7055           | Change password now !!                                                       |
| SM-7056           | Terminal Id not set                                                          |
| SM-7057           | Message Digest not matched                                                   |
| SM-7058           | User Not Logged In. Please login again                                       |
| SM-7059           | Fast Path Cannot Contain Special Characters                                  |
| SM-7060           | Currency sold and Currency bought can not be same.                           |
| SM-7070           | Branch date is ahead of host date, cannot proceed                            |
| SM-77777          | User does not have rights to authorize the override                          |
| SM-AUTH01         | The transaction amount exceeds the maximum authorization amount for the User |
| SM-BRN01          | Not a Valid user for Branch                                                  |
| SM-BRN02          | Password for Branch User cannot be null                                      |
| SM-BVALUE1        | \$1 Back value days cannot be null                                           |
| SM-C0050          | Invalid Branch Code                                                          |
| SM-C0051          | Function ID Already attached                                                 |
| SM-C0052          | Branch or Function id should not be null                                     |

| <b>Error Code</b> | <b>Message</b>                                                  |
|-------------------|-----------------------------------------------------------------|
| SM-CHBRLO         | Change Branch to Home Branch In-Order to Logoff.                |
| SM-CHBRSO         | Change Branch to Home Branch In-Order to Signoff.               |
| SM-CLBRN01        | Branch User Profile Updated at Host                             |
| SM-CLS001         | Users attached to Role. Close?                                  |
| SM-CV001          | Sequence no cannot be null                                      |
| SM-CV002          | Sequence no is a numeric field                                  |
| SM-CV003          | Group ID cannot be null                                         |
| SM-CV004          | Module code cannot be null                                      |
| SM-CV005          | Source code cannot be null                                      |
| SM-CV006          | Template ID cannot be null                                      |
| SM-CV007          | Duplicate broker ID                                             |
| SM-CV008          | Liquidation code cannot be null                                 |
| SM-CV009          | Duplicate details in record not allowed                         |
| SM-CV010          | Basis amount to cannot be null                                  |
| SM-CV011          | Floor basis amount has to be less than basis amount to          |
| SM-CV012          | Rate cannot be null for percentage type                         |
| SM-CV013          | Min amount cannot be more than floor charge for percentage type |
| SM-CV014          | Max amount cannot be less than floor charge for percentage type |
| SM-CV015          | Flat amount cannot be null for flat amount type                 |
| SM-CV016          | Invalid rate, rate is too high                                  |
| SM-CV017          | Floor basis amount cannot be null                               |
| SM-CV018          | Floor charge cannot be null                                     |
| SM-CV019          | Basis amount to cannot be less than basis amount from           |

| <b>Error Code</b> | <b>Message</b>                                                                 |
|-------------------|--------------------------------------------------------------------------------|
| SM-CV020          | Duplicate rule code                                                            |
| SM-CV021          | Minimum amount must be less than maximum amount                                |
| SM-CV022          | Maximum amount must be more than minimum amount                                |
| SM-CV023          | Rule cannot be null                                                            |
| SM-CV024          | Group already exists                                                           |
| SM-CV025          | The record is already closed                                                   |
| SM-CV026          | Intermediate table has to be entered                                           |
| SM-CV027          | Upload table has to be entered                                                 |
| SM-CV028          | Cube table has to be entered                                                   |
| SM-CV029          | Source field cannot be null                                                    |
| SM-CV030          | Destination field cannot be null                                               |
| SM-CV031          | Destination field already maintained                                           |
| SM-CV032          | Group ID already maintained                                                    |
| SM-CV033          | Template ID already maintained for this group                                  |
| SM-CV034          | Sequence no already maintained for this group                                  |
| SM-CV035          | Invalid column name                                                            |
| 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                      |

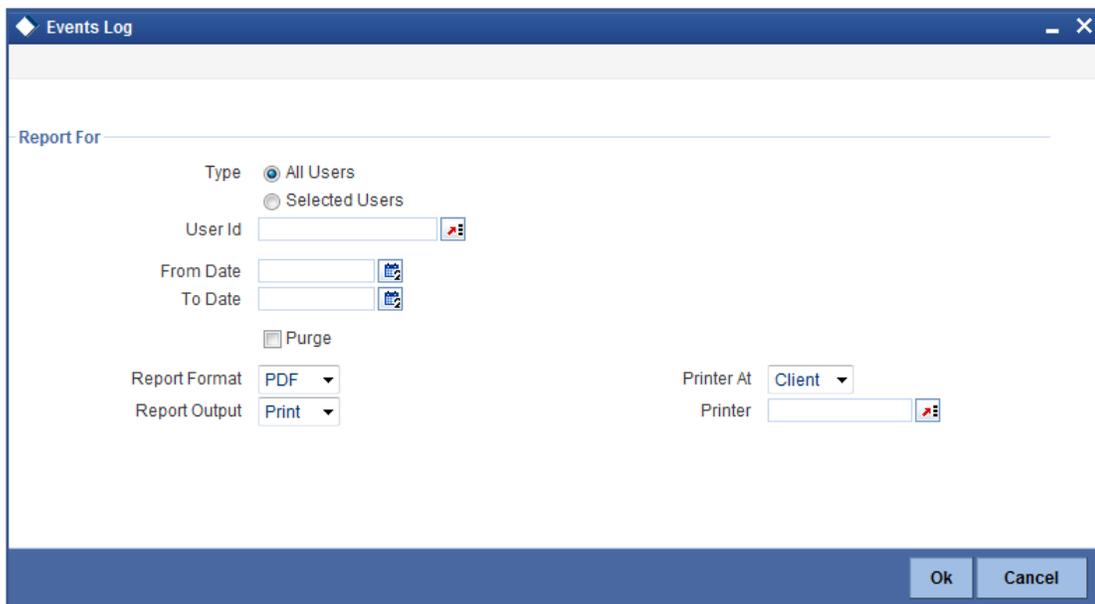
| <b>Error Code</b> | <b>Message</b>                                                                                                            |
|-------------------|---------------------------------------------------------------------------------------------------------------------------|
| SM-DEMO07         | Demo version expired, please contact i-flex!!!                                                                            |
| SM-DEMO08         | Demo version allows only \$1 contracts.                                                                                   |
| SM-DEMO09         | Demo version expires today                                                                                                |
| SM-DTCH01         | Users are running functions.                                                                                              |
| SM-DTCH02         | AEOD dates not maintained                                                                                                 |
| SM-DTCH03         | Wrong branch status to run this form                                                                                      |
| SM-EFIN01         | Users in transactions input                                                                                               |
| SM-EXTUS          | Oracle FLEXCUBE has been launched from another application. Sign off disallowed. Please exit                              |
| SM-FND01          | Menu items not populated                                                                                                  |
| 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-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. |

## 5. Reports

### 5.1 Events Log Report

The Events Log report gives details of all events that occurred over a period in time. You can specify the period for which you require the report when you invoke the report function.

To invoke the screen to generate this report, type 'SMRPEVLG' in the field at top right corner of the Application tool bar and click the adjoining arrow button.



The screenshot shows a dialog box titled "Events Log" with a blue header and a white body. The dialog is titled "Report For" and contains the following controls:

- Type:** Two radio buttons: "All Users" (selected) and "Selected Users".
- User Id:** A text input field with a small icon to its right.
- From Date:** A date input field with a calendar icon to its right.
- To Date:** A date input field with a calendar icon to its right.
- Purge:** A checkbox.
- Report Format:** A dropdown menu currently set to "PDF".
- Report Output:** A dropdown menu currently set to "Print".
- Printer At:** A dropdown menu currently set to "Client".
- Printer:** A text input field with a small icon to its right.

At the bottom right of the dialog are two buttons: "Ok" and "Cancel".

#### Report For

Indicate the user of the report by choosing one of the options.

- All Users
- Selected Users

#### **From Date**

Indicate the start date by using the adjoining calendar.

#### **To Date**

Indicate the end date by using the adjoining calendar.

#### **Purge**

Check this box to purge the document.

Click 'OK' to generate the report.

#### 5.1.1 Contents of the Events Log

The contents of this report are discussed under the following heads:

### *Header*

The Header carries the title of the report, information on the branch code, the ID of the user who generated the report, the date and time at which it was generated, the branch date, the modules covered in the report.

### *Body of the report*

The following details are displayed in the report.

|                             |                                                                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User ID</b>              | The user who initiated the event.                                                                                                           |
| <b>Function Description</b> | The name of the function that activated the event.                                                                                          |
| <b>Start Time</b>           | The time at which the event was initiated.                                                                                                  |
| <b>End Time</b>             | The time at which the event was successfully completed or was aborted. If the event has not been completed, or 'Not Yet' is displayed here. |
| <b>Branch Code</b>          | The code allotted to the branch .                                                                                                           |
| <b>Terminal ID</b>          | The system ID where the application is launched                                                                                             |
| <b>System Start Time</b>    | The time when the user starts the application                                                                                               |
| <b>System End Time</b>      | The time when the user signs out of the application                                                                                         |

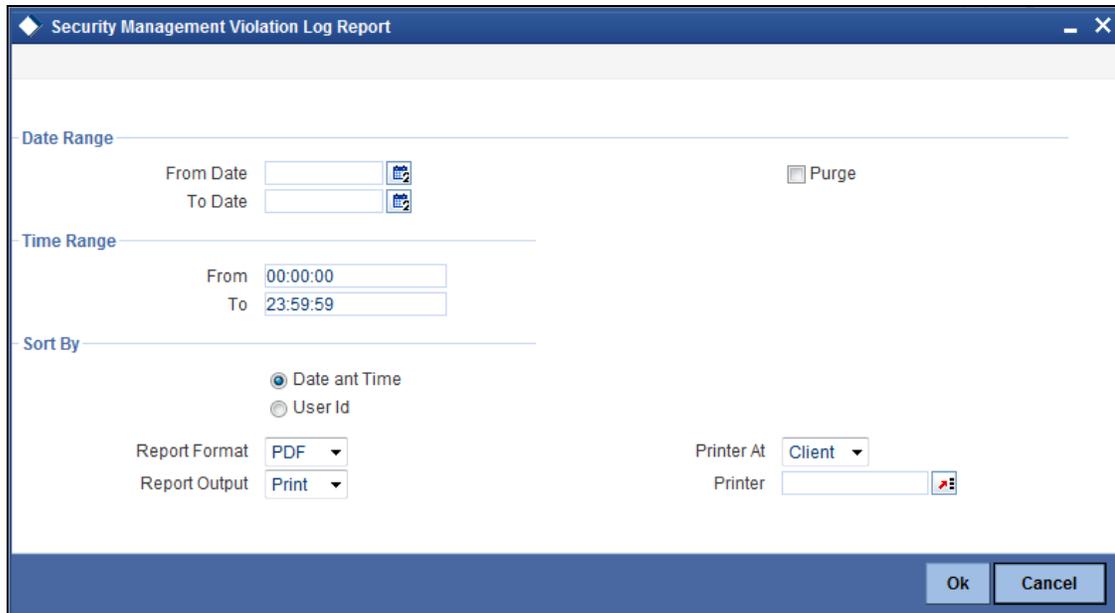
Total time spent on individual functions by individual users is also provided.

## 5.2 Security Management System Violations Log Report

Any attempt at violating the security of the system will be reported in the Security Violations report. You can generate this report for a particular period.

To invoke the screen to generate this report, type 'SMRPVLLG' in the field at top right corner of the Application tool bar and click the adjoining arrow button.

The screen is as shown below:



The screenshot shows a dialog box titled "Security Management Violation Log Report". It contains several sections for configuring the report:

- Date Range:** Includes "From Date" and "To Date" text boxes with calendar icons, and a "Purge" checkbox.
- Time Range:** Includes "From" and "To" text boxes with time values "00:00:00" and "23:59:59".
- Sort By:** Includes radio buttons for "Date and Time" (selected) and "User Id".
- Report Format:** A dropdown menu set to "PDF".
- Report Output:** A dropdown menu set to "Print".
- Printer At:** A dropdown menu set to "Client".
- Printer:** A text box with a printer icon.

At the bottom right, there are "Ok" and "Cancel" buttons.

Indicate the following details:

### **Date Range**

Indicate the date range.

#### **From Date**

Indicate the date from which you want to generate the violations report, using the adjoining calendar.

#### **To Date**

Indicate the date until which you want to generate the violations report, using the adjoining calendar.

### **Time Range**

Specify the time range that should be considered for the violations report.

### **Sort By**

Indicate the mode of sorting data in the report by choosing one of the following options:

- Date and Time

- User Identification

### **Purge**

Check this box to indicate that the report can be purged.

Click 'OK' button to generate the report.

## **5.2.1 Contents of the Security Management System Violations Log Report**

The contents of this report are discussed under the following heads:

### *Header*

The Header carries the title of the report, information on the branch code, the ID of the user who generated the report, the date and time at which it was generated, the branch date, the modules covered in the report.

### *Body of the report*

The following details are displayed in the report

|                             |                                                                                                 |
|-----------------------------|-------------------------------------------------------------------------------------------------|
| <b>User-ID</b>              | The user who was involved in the security management system violation.                          |
| <b>Start Time</b>           | The time at which the security management system was violated.                                  |
| <b>Message</b>              | The error message if any displayed by the system during validation                              |
| <b>Function Description</b> | The description of the function that was executed by the user, which resulted in the violation. |
| <b>Terminal ID</b>          | The terminal-ID of the terminal onto which the user was logged.                                 |

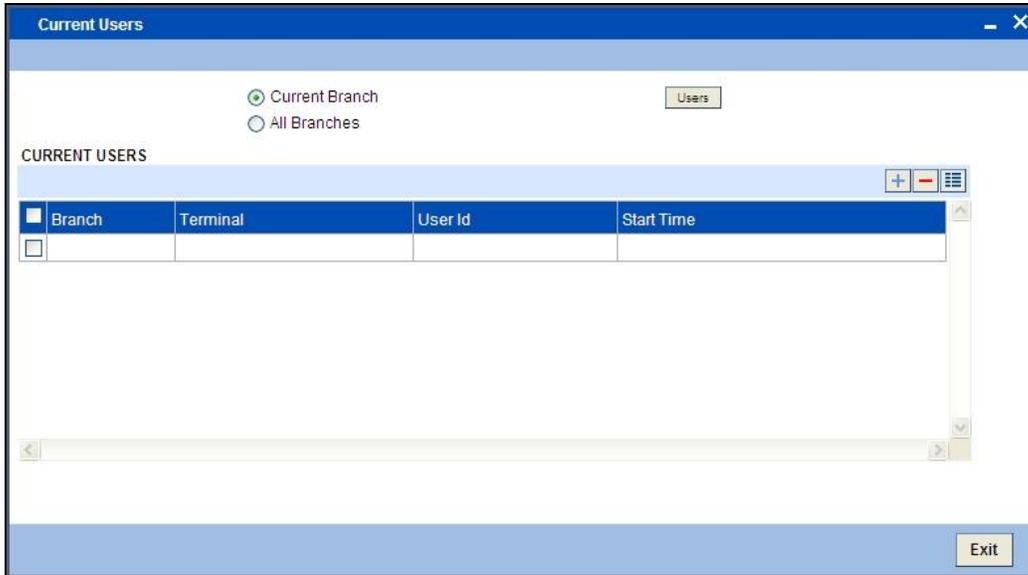
## **5.3 User Profile Report**

The details of all the user profiles that have been defined are available in the form of a report. The User Profile Report gives details of user profiles maintained for all or specific users. It includes:

- The functions attached to the role.
- The roles to which the user is attached.
- Amount limits for each user.
- Branches in which the user can operate.
- Currencies the user can use.
- Customers the user can deal with.
- Restrictive passwords defined for the user.

To invoke the screen to generate this report, type 'SMDCUUSR' in the field at the top right corner of the Application tool bar and click the adjoining arrow button.

The screen is as shown below:



### 5.3.1 Contents of the User Profile Report

|                             |                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------|
| <b>Branch Code and Name</b> | The code allotted to the branch and the full name of the branch.                            |
| <b>Date and Time</b>        | At which the report was generated.                                                          |
| <b>Printed by</b>           | The user who has generated the report.                                                      |
| <b>Spool File</b>           | If the report has been printed onto a spool file, the name of the spool file is given here. |
| <b>Sort on</b>              | The criteria on which the details have been sorted.                                         |
| <b>Date Range</b>           | The period for which the report is generated.                                               |
| <b>User-ID</b>              | The ID of the user whose details are being reported.                                        |
| <b>Name</b>                 | The name of the user whose details are being reported.                                      |
| <b>Time Level</b>           | The time level of the user.                                                                 |
| <b>Language Code</b>        | The language assigned to the user.                                                          |
| <b>Profile Expires On</b>   | The date on which the user profile is due to expire.                                        |
| <b>Status</b>               | The status of the user - enabled, on hold or disabled.                                      |
| <b>Function-ID</b>          | The function allowed for the user.                                                          |
| <b>Function Description</b> | The description of the function.                                                            |

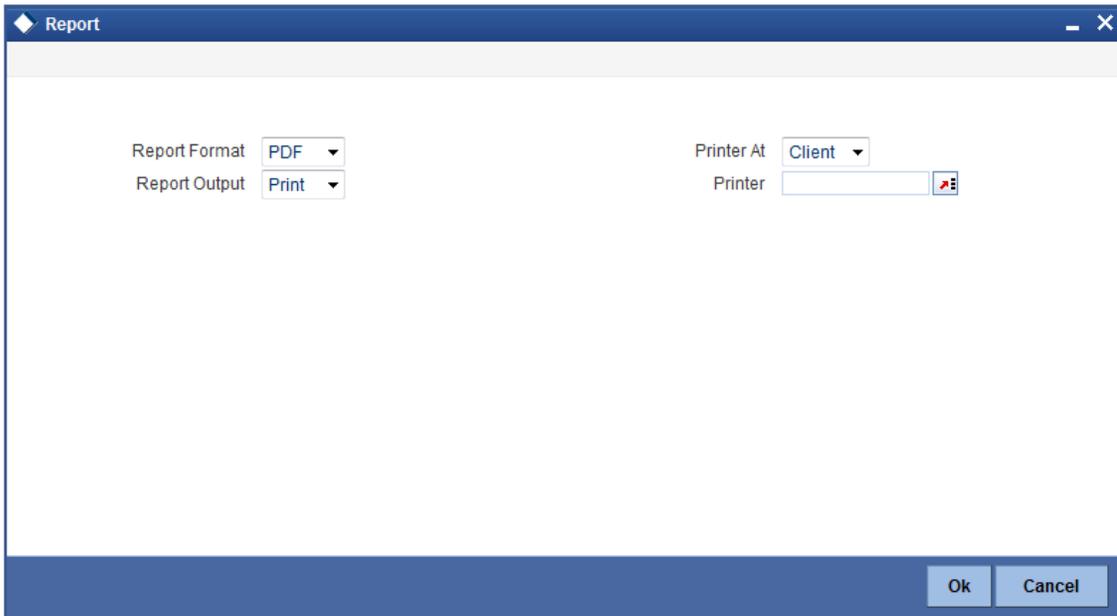
|                                     |                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Link with Role Definition</b>    | If the user has been linked to a role, the role-ID is given here.                       |
| <b>Maximum Transaction Amount</b>   | The maximum amount that the user can enter in a single transaction.                     |
| <b>Maximum Authorization Amount</b> | The maximum amount that a transaction can have if it has to be authorized by this user. |
| <b>Branch Code</b>                  | The branch in which the user profile is defined.                                        |
| <b>Branch Name</b>                  | The name of the branch in which the user has signed on.                                 |
| <b>Currency Code</b>                | The S.W.I.F.T code of the currency in which the user can operate.                       |
| <b>Currency Name</b>                | The name of the currency in which the user can operate.                                 |
| <b>Customer Code</b>                | The customer whose accounts can be handled by the user.                                 |
| <b>Customer Name</b>                | The name of the customer whose accounts can be handled by this user.                    |
| <b>Restrictive Passwords - User</b> | The passwords defined as restrictive passwords for the user.                            |

## 5.4 Changes Report

This report gives details of maintenance done on the following screen:

- Static Parameters screen
- Static User Profile Details screen
- Dynamic User Profile Details screen
- Static Role Profile Details
- Static User Profile Details

You can generate this report for a particular period using the 'Report' screen To invoke this screen type 'SMRPCHLG' in the field at top right corner of the Application tool bar and click the adjoining arrow button



#### 5.4.1 Contents of the Changes Report

The contents of this report are discussed under the following heads:

##### *Header*

The Header carries the title of the report, information on the branch code, the ID of the user who generated the report, the date and time at which it was generated, the branch date, the modules covered in the report.

##### *Body of the report*

The following details are displayed in the report

|                        |                                                               |
|------------------------|---------------------------------------------------------------|
| <b>Field Name</b>      | The field that has been maintained                            |
| <b>Input by</b>        | The Id of the person who input the details of the transaction |
| <b>Old Value</b>       | The value in the field before it was modified                 |
| <b>New Value</b>       | The value in the field after it was modified                  |
| <b>Date &amp; Time</b> | The date and time of the transaction                          |
| <b>Authorizer ID</b>   | The Id of the person who authorized the transaction           |
| <b>Date &amp; Time</b> | The date and time when the transaction was authorized         |
| <b>Record Stat</b>     | The status of the record                                      |

|                    |                          |
|--------------------|--------------------------|
| <b>Auth Stat</b>   | The authorization status |
| <b>Function ID</b> | The function ID          |
| <b>Mod Number</b>  | The module number        |
| <b>Table Name</b>  | The table name           |

## 5.5 Inactive Users Aging Analysis Report

This report gives details of users who have not used the system over a certain period. You should enter the period when you invoke the report. The details are sorted in ascending order of the date from which the user has not used the system.

Click 'OK' button if you want to generate this report. To come out of this screen without generating the report click 'Exit' button.

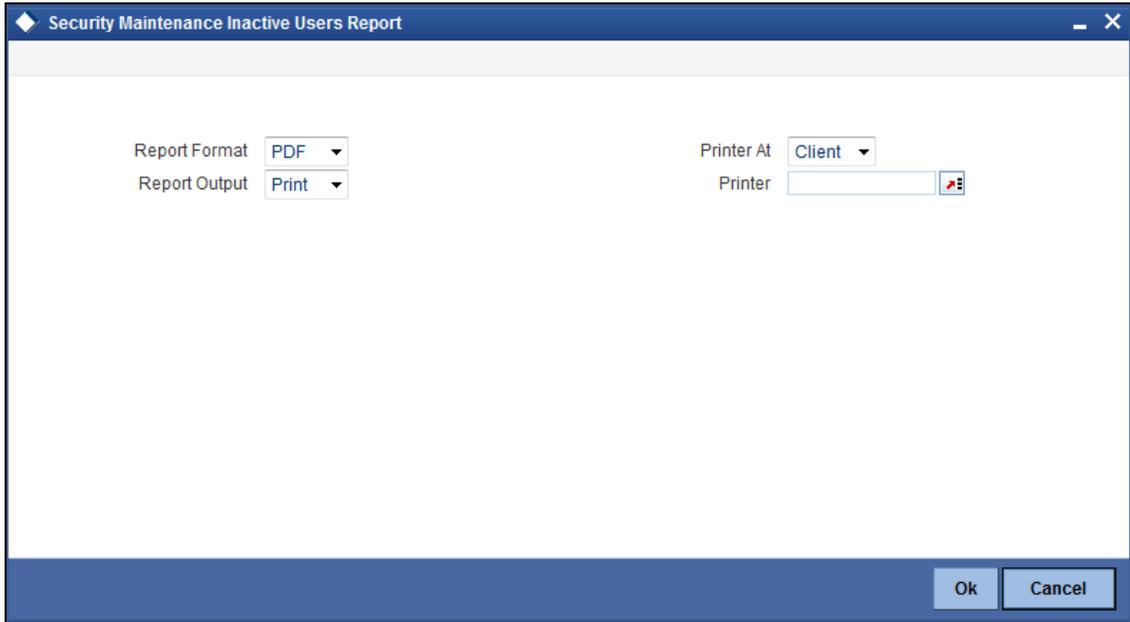
### 5.5.1 Contents of the Inactive Users Aging Analysis Report

|                          |                                                               |
|--------------------------|---------------------------------------------------------------|
| <b>User-ID</b>           | The ID of the user who has not been using the system          |
| <b>Inactive Since</b>    | The date from which the user has not accessed the system      |
| <b>Status</b>            | The status of the user - enabled, disabled, hold, inactive    |
| <b>Inactivity Period</b> | The number of days for which the user has not used the system |

## 5.6 SMS User Inactive Log Report

This report gives details of users who have not used the system over a certain period. You should enter the period when you invoke the report. The details are sorted in ascending order of the date from which the user has not used the system. In the Application Browser, this report is available under the SM module.

To invoke the screen 'Security Maintenance Inactive Users Report' type 'SMRPINST' in the field at top right corner of the Application tool bar and click the adjoining arrow button.



### 5.6.1 Contents of the Inactive Users Log Report

The contents of this report are discussed under the following heads:

#### *Header*

The Header carries the title of the report, information on the branch code, the ID of the user who generated the report, the date and time at which it was generated, the branch date, the modules covered in the report.

#### *Body of the report*

The following details are displayed in the report

|                               |                                                               |
|-------------------------------|---------------------------------------------------------------|
| <b>User-ID</b>                | The ID of the user who has not been using the system          |
| <b>Home Branch</b>            | The home branch of the bank.                                  |
| <b>Last Signed On</b>         | The date from which the user has not accessed the system      |
| <b>Inactive For (In days)</b> | The number of days for which the user has not used the system |

## 5.7 Online Performance Statistics Report

This report lists the maximum, minimum and average execution time for different actions across transactions in Oracle FLEXCUBE. You can generate this report using the 'Online Screen Performance Statistics Report' screen. To invoke this screen, type 'SMRONSTA' in the field at top right corner of the Application tool bar and click the adjoining arrow button.

Report 1

Function

Action

Report Format PDF

Report Output Print

Printer At Client

Printer

Ok Cancel

Specify the following details:

### **Function**

Specify the function ID for which performance statistics need to be collected. The adjoining option list displays all transaction related function IDs available in the system. You can select the appropriate one. You can also leave this field blank if you have mentioned the action. This will imply that the report needs to be generated for the given action across all function IDs.

### **Action**

Specify the action that needs to be performed on the function ID. The adjoining option list displays all operations for the functions IDs available in the system. You can select the appropriate one. You can also leave this field blank if you have mentioned the action. This will imply that the report needs to be generated for the given function ID across all actions.



Both the function and the action cannot be null at a time.

### 5.7.1 Contents of the Online Performance Statistics Report

The parameters specified while generating the report are printed at the beginning of the report. The contents of this report are discussed under the following heads:

#### *Header*

The Header carries the title of the report, information on the branch code, the ID of the user who generated the report, the date and time at which it was generated, the branch date, the modules covered in the report.

### Body of the report

The following details are displayed in the report.

|                     |                                                                              |
|---------------------|------------------------------------------------------------------------------|
| <b>Function Id</b>  | This indicates function action of the screen.                                |
| <b>Function Id</b>  | This indicates function ID of the screen.                                    |
| <b>Action</b>       | This indicates the action performed on the Function ID.                      |
| <b>Source</b>       | This indicates the source of the report.                                     |
| <b>Max Response</b> | This indicates the maximum execution time for the action on the Function ID. |
| <b>Min Response</b> | This indicates the minimum execution time for the action on the Function ID. |
| <b>Average</b>      | This indicates the average execution time of the report to be generated.     |
| <b>Count</b>        | This indicates the execution count for the report to be generated.           |
| <b>Log Time</b>     | Time of execution.                                                           |

## 5.8 Batch Performance Statistics Report

This report provides the maximum, minimum and average performance record of each batch operation across all the branches in Oracle FLEXCUBE. It also has the option of generating report within a given date and time range. You can generate this report using the 'Batch Performance Statistics Report' screen. To invoke this screen, type 'SMRBASTA' in the field at top right corner of the Application tool bar and click the adjoining arrow button.

The screenshot shows a dialog box titled "Batch Performance Statistics Report". It contains several input fields and dropdown menus for configuring the report. The "Report" section includes "Batch" and "Branch" text boxes. The "Period" section includes "Start Date" and "End Date" text boxes with calendar icons. The "Report Format" is set to "PDF" and "Report Output" is set to "Print". The "Printer At" is set to "Client" and there is a "Printer" text box. The dialog has "Ok" and "Cancel" buttons at the bottom right.

Specify the following details:

## **Report**

You can indicate the following details for report generation:

### **Batch**

Specify the batch for which the report has to be generated. The adjoining option list displays the list of all batches available in the system. You can select the appropriate one. However, you can leave this field blank if you have mentioned the branch. This will imply that the report needs to be generated for the given branch across all batches.

### **Branch**

Specify the branch for which the report has to be generated. The adjoining option list displays the list of all branches available in the system. You can select the appropriate one. However, you can also leave this field blank if you have mentioned the batch. This will imply that the report needs to be generated for the given batch across all branches.

### **Period**

Select the period within which the data for report generation should be fetched.

### **Start Date.**

Indicate the date from which records should be considered for report generation, using the adjoining calendar.

### **End Date**

Indicate the date until which records should be considered for report generation, using the adjoining calendar.

## **5.8.1 Contents of the Performance Statistics report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

### *Header*

The Header carries the title of the report, information on the branch code, the ID of the user who generated the report, the date and time at which it was generated, the branch date, the modules covered in the report.

### *Body of the report*

The following details are displayed in the report.

|                    |                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------|
| <b>EOC Stage</b>   | This indicates the End of Cycle stage.                                                           |
| <b>Branch Code</b> | This indicates the code of the branch.                                                           |
| <b>Start Time</b>  | This indicates the start time from which the records have been considered for report generation. |
| <b>End Time</b>    | This indicates the end time until which the records have been considered for report              |

|                     |                                                                |
|---------------------|----------------------------------------------------------------|
|                     | generation.                                                    |
| <b>Maximum Time</b> | This indicates the maximum time taken for the batch operation. |
| <b>Minimum Time</b> | This indicates the minimum time taken for batch operation.     |
| <b>Average Time</b> | This indicates the average time taken for batch operation.     |

## 5.9 Change Control Log Report

The Change Control Log report provides change control log details. You can invoke the screen by typing the code 'SMRCONTL' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.

You can specify the following parameters:

### **Branch Options**

You can generate the report based on the following branch criteria. The following options are available for section:

- All
- Single

### **Branch Code**

Specify a valid branch code for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

### **User Options**

You can generate the report based on the following User criteria. The following options are available for section:

- All
- Single

### **User**

Specify a valid User ID for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

### **Module Options**

You can generate the report based on the following Module criteria. The following options are available for section:

- All
- Single

### **Module Code**

Specify a valid module code for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

### **Main**

You can specify the following parameters:

#### **Date**

Specify a valid date for which you want to generate the report from the adjoining calendar.

## **5.9.1 Contents of the Report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

### **Header**

The following details are displayed in the header section:

| <b>Field Name</b> | <b>Field Description</b>                                  |
|-------------------|-----------------------------------------------------------|
| Branch            | Indicates Branch Code and Branch Name                     |
| Branch Date       | Indicates Current Date of the Branch                      |
| User ID           | Indicates User ID                                         |
| Date & Time       | Indicates the Date and Time when the report was generated |
| Module            | Indicates module for which report is generated.           |

### **Body of the Report**

The following details are displayed as body of the generated report:

| Field Name            | Field Description                   |
|-----------------------|-------------------------------------|
| Branch                | Indicates Branch Code               |
| User ID               | Indicates User ID                   |
| Module                | Indicates Module                    |
| Function Modified     | Indicates Function Modified         |
| Modification Number   | Indicates Modification Number       |
| Field Name            | Indicates Field Name                |
| Status                | Indicates Status                    |
| Old Value             | Indicates Amount                    |
| New Value             | Indicates Currency code             |
| Maker Date Checker ID | Indicates Maker Date and Checker ID |

## 5.10 Event Log Report

The Event Log report provides event log details. You can invoke the screen by typing the code 'SMREVNLO' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.

You can specify the following parameters:

### Input User

You can generate the report based on the following User criteria. The following options are available for section:

- All
- Single

### **User**

Specify a valid User ID for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

### **Start Date**

Specify start date of the event for which you want to generate the report from the adjoining calendar.

## **5.10.1 Contents of the Report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

### **Header**

The following details are displayed in the header section:

| <b>Field Name</b> | <b>Field Description</b>                                  |
|-------------------|-----------------------------------------------------------|
| Branch            | Indicates Branch Code and Branch Name                     |
| Branch Date       | Indicates Current Date of the Branch                      |
| User ID           | Indicates User ID                                         |
| Date & Time       | Indicates the Date and Time when the report was generated |
| Module            | Indicates module for which report is generated.           |

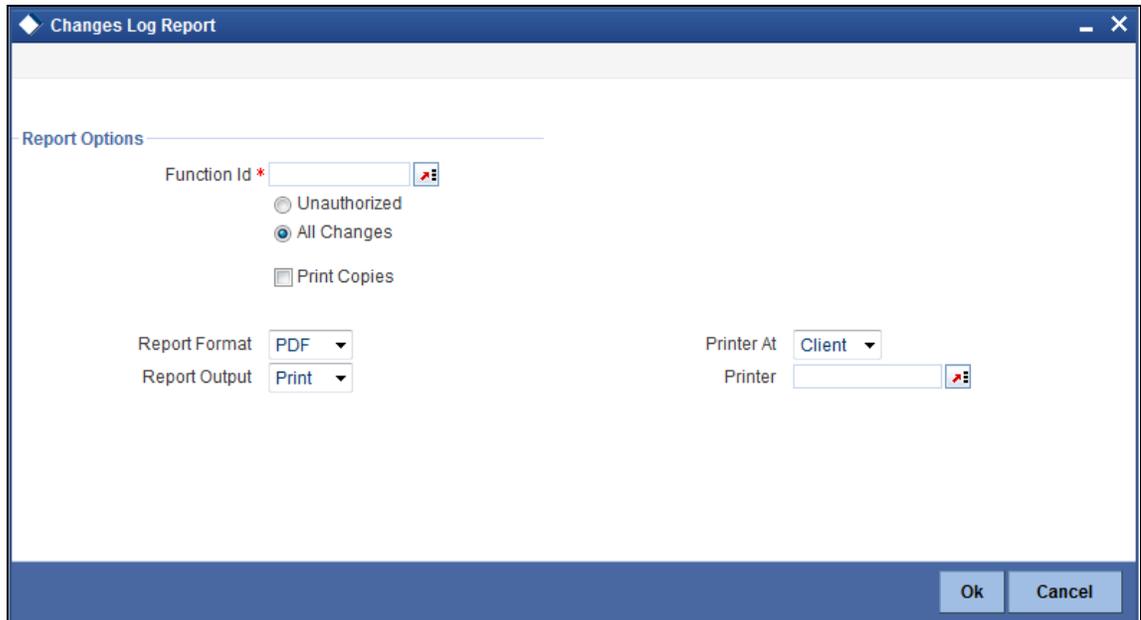
### **Body of the Report**

The following details are displayed as body of the generated report:

| <b>Field Name</b>  | <b>Field Description</b>              |
|--------------------|---------------------------------------|
| Start Date         | Indicates the start date of the event |
| End Date           | Indicates the end date of the event   |
| Application        | Indicates application details         |
| Current Branch     | Indicates current branch code         |
| Transaction Branch | Indicates transaction branch code     |
| User ID            | Indicates User ID                     |

## 5.11 Changes Log Report

The Changes Log report provides changes log details. You can invoke the screen by typing the code 'SMRMCLOG' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.



You can specify the following parameters:

### **Report Options**

You can specify the following parameters:

#### **Function ID**

Specify a valid Function ID for which you want to generate the report from the adjoining option list.

You can generate the report based on the following change criteria. The following options are available for section:

- Unauthorized
- All changes

#### **Print Copies**

Check this box if you wish to print copies of the report.

### 5.11.1 **Contents of the Report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

#### **Header**

The following details are displayed in the header section:

| Field Name  | Field Description                                         |
|-------------|-----------------------------------------------------------|
| Branch      | Indicates Branch Code and Branch Name                     |
| Branch Date | Indicates Current Date of the Branch                      |
| User ID     | Indicates User ID                                         |
| Date & Time | Indicates the Date and Time when the report was generated |
| Module      | Indicates module for which report is generated.           |

### Body of the Report

The following details are displayed as body of the generated report:

| Field Name          | Field Description             |
|---------------------|-------------------------------|
| Maintenance Program | Indicates Maintenance Program |
| Action              | Indicates Action              |
| Modification Number | Indicates Modification Number |
| Field Name          | Indicates Field Name          |
| New Value           | Indicates New Value           |
| Old Value           | Indicates Old Value           |
| Maker ID            | Indicates Maker ID            |
| Maker Date          | Indicates Maker Date          |
| Checker ID          | Indicates Checker ID          |
| Checker Date        | Indicates Checker Date        |

## 5.12 New User Created Report

The New User Created report provides details of the new users created. You can invoke the screen by typing the code 'SMRNEWUSR' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.

You can specify the following parameters:

### **Branch Options**

You can generate the report based on the following branch criteria. The following options are available for section:

- All
- Single

### **Branch Code**

Specify a valid branch code for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

### **User Creation**

You can specify the following parameter:

#### **From Date**

Specify date from when you want to generate the report from the adjoining calendar.

#### **To Date**

Specify date till when you want to generate the report from the adjoining calendar

## **5.12.1 Contents of the Report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

### **Header**

The following details are displayed in the header section:

| Field Name  | Field Description                                         |
|-------------|-----------------------------------------------------------|
| Branch      | Indicates Branch Code and Branch Name                     |
| Branch Date | Indicates Current Date of the Branch                      |
| User ID     | Indicates User ID                                         |
| Date & Time | Indicates the Date and Time when the report was generated |
| Module      | Indicates module for which report is generated.           |

### Body of the Report

The following details are displayed as body of the generated report:

| Field Name  | Field Description                                |
|-------------|--------------------------------------------------|
| Start Date  | Indicates the start date of the event            |
| User ID     | Indicates user ID                                |
| Creator     | Indicates creator's ID                           |
| Authorizer  | Indicates authorizer's ID code                   |
| Home Branch | Indicates home branch code                       |
| Role ID     | Indicates role ID to which the user ID is mapped |

## **5.13 Role Profile Created Report**

The Role Profile Created report provides details of the role profile created. You can invoke the screen by typing the code 'SMRPLPR' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.

You can specify the following parameters:

### **Report For**

You can generate the report based on the following role criteria. The following options are available for section:

- All Roles
- Selected

### **Role ID**

Specify a valid Role ID for which you want to generate the report from the adjoining option list, if you have selected 'Selected'.

## **5.13.1 Contents of the Report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

### **Header**

The following details are displayed in the header section:

| <b>Field Name</b> | <b>Field Description</b>                                  |
|-------------------|-----------------------------------------------------------|
| Branch            | Indicates Branch Code and Branch Name                     |
| Branch Date       | Indicates Current Date of the Branch                      |
| User ID           | Indicates User ID                                         |
| Date & Time       | Indicates the Date and Time when the report was generated |
| Module            | Indicates module for which report is generated.           |

## Body of the Report

The following details are displayed as body of the generated report:

| Field Name            | Field Description                                                          |
|-----------------------|----------------------------------------------------------------------------|
| Role ID               | Indicates role ID                                                          |
| Role Description      | Indicates role description                                                 |
| Functions Allowed     | Indicates function allowed for the role                                    |
| Branches Allowed      | Indicates branch code and name of the branches allowed                     |
| Account Class Allowed | Indicates the account class and description of the account classes allowed |
| Users Attached        | Indicates the User ID, Name and the branch of the Users attached           |

## 5.14 User Profile Report

The User Profile report provides details of the user profile. You can invoke the screen by typing the code 'SMRPUSPR' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.

◆ User Profile Report

Report For

All Users  
 Selected

User Id

Report Format **PDF** ▾  
Report Output **Print** ▾

Printer At **Client** ▾  
Printer

Ok Cancel

You can specify the following parameters:

### Report For

You can generate the report based on the following user criteria. The following options are available for section:

- All Users
- Selected

#### **User ID**

Specify a valid User ID for which you want to generate the report from the adjoining option list, if you have selected 'Selected'.

### **5.14.1 Contents of the Report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

#### **Header**

The following details are displayed in the header section:

| <b>Field Name</b> | <b>Field Description</b>                                  |
|-------------------|-----------------------------------------------------------|
| Branch            | Indicates Branch Code and Branch Name                     |
| Branch Date       | Indicates Current Date of the Branch                      |
| User ID           | Indicates User ID                                         |
| Date & Time       | Indicates the Date and Time when the report was generated |
| Module            | Indicates module for which report is generated.           |

#### **Body of the Report**

The following details are displayed as body of the generated report:

| <b>Field Name</b> | <b>Field Description</b>    |
|-------------------|-----------------------------|
| Branch            | Indicates branch code       |
| User ID           | Indicates User ID           |
| User name         | Indicates User name         |
| Category          | Indicates Category          |
| Language          | Indicates Language          |
| Time Level        | Indicates Time Level        |
| Status            | Indicates Status            |
| Status Changed On | Indicates Status Changed On |
| Last Signed On    | Indicates Last Signed On    |

| <b>Field Name</b>              | <b>Field Description</b>                                                   |
|--------------------------------|----------------------------------------------------------------------------|
| Password Changed               | Indicates Password Changed                                                 |
| Cumulative Invalid Logins      | Indicates Cumulative Invalid Logins                                        |
| Start Date                     | Indicates Start Date                                                       |
| End Date                       | Indicates End Date                                                         |
| Successive Invalid Logins      | Indicates Successive Invalid Login                                         |
| Max Input Limit                | Indicates Maximum Input Limit                                              |
| Max Authorization Limit        | Indicates Maximum Authorization Limit                                      |
| Max Online Authorization Limit | Indicates Maximum Online Authorization Limit                               |
| Roles Attached                 | Indicates ID and description of the roles attached for the User            |
| Functions Allowed              | Indicates ID and description of the functions allowed for the User         |
| Functions Disallowed           | Indicates ID and description of the functions disallowed for the User      |
| Branches Allowed               | Indicates branch code and name of the branches allowed                     |
| Account Class Allowed          | Indicates the account class and description of the account classes allowed |
| Branches Allowed               | Indicates ID and Name of the tills allowed                                 |
| Tills Allowed                  | Indicates the code and description of the tills allowed                    |
| Products Allowed               | Indicates the code and description of the product allowed                  |

## **5.15 Role Profile Report**

The Role Profile report provides details of the role profiles. You can invoke the screen by typing the code 'SMRROLPR' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.

You can specify the following parameters:

### **Role Profile**

You can generate the report based on the following role criteria. The following options are available for section:

- All
- Single

### **Role**

Specify a valid Role ID for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

## **5.15.1 Contents of the Report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

### **Header**

The following details are displayed in the header section:

| <b>Field Name</b> | <b>Field Description</b>                                  |
|-------------------|-----------------------------------------------------------|
| Branch            | Indicates Branch Code and Branch Name                     |
| Branch Date       | Indicates Current Date of the Branch                      |
| User ID           | Indicates User ID                                         |
| Date & Time       | Indicates the Date and Time when the report was generated |

| Field Name | Field Description                               |
|------------|-------------------------------------------------|
| Module     | Indicates module for which report is generated. |

### Body of the Report

The following details are displayed as body of the generated report:

| Field Name           | Field Description                              |
|----------------------|------------------------------------------------|
| Role                 | Indicates Role ID                              |
| Function             | Indicates Function name                        |
| Function Description | Indicates Function description                 |
| Branch Allowed       | Indicates branches allowed for the role        |
| Acc Class Allowed    | Indicates account classes allowed for the role |
| Limit Currency       | Indicates limit currency for the role          |
| Input Limit          | Indicates input limit for the role             |
| Authorizer Limit     | Indicates authorization limit for the role     |

## 5.16 User Role Summary Report

The User Role Summary report provides user role summary details. You can invoke the screen by typing the code 'SMRSUMRY' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.

You can specify the following parameters:

## **Status Report**

You can specify the following parameters

### **User Status**

You can generate the report based on the following user status criteria. The following options are available for section:

- Enabled
- Disabled

### **Role Options**

You can generate the report based on the following role criteria. The following options are available for section:

- All
- Single

### **Role Level**

Specify a valid role level for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

### **Branch Options**

You can generate the report based on the following branch criteria. The following options are available for section:

- All
- Single

### **Branch Code**

Specify a valid branch code for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

## **5.16.1 Contents of the Report**

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

### **Header**

The following details are displayed in the header section:

| <b>Field Name</b> | <b>Field Description</b>                                  |
|-------------------|-----------------------------------------------------------|
| Branch            | Indicates Branch Code and Branch Name                     |
| Branch Date       | Indicates Current Date of the Branch                      |
| User ID           | Indicates User ID                                         |
| Date & Time       | Indicates the Date and Time when the report was generated |

| Field Name | Field Description                               |
|------------|-------------------------------------------------|
| Module     | Indicates module for which report is generated. |

### Body of the Report

The following details are displayed as body of the generated report:

| Field Name  | Field Description                        |
|-------------|------------------------------------------|
| Branch      | Indicates Branch Code                    |
| Branch Name | Indicates Branch name                    |
| Role ID     | Indicates Role ID                        |
| User ID     | Indicates User ID                        |
| Status      | Indicates Status                         |
| No of Users | This indicates the total number of users |

## 5.17 User Entitlement Report

The User Entitlement report provides user entitlement details. You can invoke the screen by typing the code 'SMRUSREN' in the field at the top right corner of the Application tool bar and click on the adjoining arrow button.

You can specify the following parameters:

### User Entitlement

You can specify the following parameters

## User Status

You can generate the report based on the following user status criteria. The following options are available for section:

- Enabled
- Disabled

## Branch Options

You can generate the report based on the following branch criteria. The following options are available for section:

- All
- Single

## Branch Code

Specify a valid branch code for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

## User Options

You can generate the report based on the following user criteria. The following options are available for section:

- All
- Single

## User ID

Specify a valid user ID for which you want to generate the report from the adjoining option list, if you have selected 'Single'.

### 5.17.1 Contents of the Report

The parameters specified while generating the report are printed at the beginning of the report. Other content displayed in the report is as follows:

#### Header

The following details are displayed in the header section:

| Field Name  | Field Description                                         |
|-------------|-----------------------------------------------------------|
| Branch      | Indicates Branch Code and Branch Name                     |
| Branch Date | Indicates Current Date of the Branch                      |
| User ID     | Indicates User ID                                         |
| Date & Time | Indicates the Date and Time when the report was generated |
| Module      | Indicates module for which report is generated.           |

## Body of the Report

The following details are displayed as body of the generated report:

| Field Name               | Field Description                        |
|--------------------------|------------------------------------------|
| Home Branch              | Indicates Home Branch                    |
| Branch Name              | Indicates Branch Name                    |
| User ID                  | Indicates User ID                        |
| User Name                | Indicates User Name                      |
| User Category            | Indicates User Category                  |
| Created On               | Indicates Created On date                |
| Last Signed On           | Indicates Last Signed On date            |
| Password Changed On      | Indicates Password Changed On date       |
| Status                   | Indicates Status                         |
| Branch Allowed           | Indicates Branch Allowed for user        |
| Account Class Allowed    | Indicates Account Class Allowed for user |
| GL Allowed               | Indicates GL Allowed                     |
| Product Allowed          | Indicates Product Allowed for user       |
| Max Input Limit          | Indicates Max Input Limit                |
| Cumulative Invalid Login | Indicates Cumulative Invalid Login       |
| No of Successive Login   | Indicates No of Successive Login         |
| Max Authorization Limit  | Indicates Max Authorization Limit        |

---

## 6. Screen Glossary

### 6.1 Function ID List

The following table lists the function id and the function description of the screens covered as part of this User Manual.

| Function ID | Function Description                        |
|-------------|---------------------------------------------|
| CSDERMSG    | Error Messages Maintenance                  |
| SMDBANKP    | SMS Bank Parameters Maintenance             |
| SMDBRRES    | Branch Restrictions                         |
| SMDCHGTL    | Change Time Level                           |
| SMDCUUSR    | Current Users                               |
| SMDDPTMT    | Department Maintenance                      |
| SMDFNDS     | Function Description Maintenance            |
| SMDHOTKY    | Hot Keys Maintenance                        |
| SMDLNGCD    | Language Code Maintenance                   |
| SMDRLMNT    | Role Limits Maintenance                     |
| SMDROLD     | Role Maintenance                            |
| SMDSOPRM    | Single Sign On Maintenance                  |
| SMDTXNST    | Transaction Status Control Maintenance      |
| SMDUSALR    | User Alerts Maintenance                     |
| SMDUSHOL    | User Holiday Maintenance                    |
| SMDUSRDF    | User Maintenance                            |
| SMRBASTA    | Batch Performance Statistics Report         |
| SMRCONTL    | Change Control Log Report                   |
| SMREVNLO    | Event Log Report                            |
| SMRMCLOG    | Changes Log Report                          |
| SMRNWUSR    | New User Created Report                     |
| SMRONSTA    | Online Screen Performance Statistics Report |

| <b>Function ID</b> | <b>Function Description</b>                |
|--------------------|--------------------------------------------|
| SMRPCHLG           | Report                                     |
| SMRPEVLG           | Events Log                                 |
| SMRPINST           | Security Maintenance Inactive Users Report |
| SMRPRLPR           | Role Profile Created Report                |
| SMRPUSPR           | User Profile Report                        |
| SMRPVLLG           | Security Management Violation Log Report   |
| SMRROLPR           | Role Profile Report                        |
| SMRSUMRY           | Change Control Log Report                  |
| SMRUSREN           | User Entitlement Report                    |
| SMSBRNST           | Branch Status                              |
| SMSUSHOL           | User Holiday Summary                       |
| SMSUSRAC           | User Activity                              |



Security Management System  
[July] [2013]  
Version 12.0.1.13.10

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/](http://www.oracle.com/financialservices/)

Copyright © [2007], [2013], Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

**U.S. GOVERNMENT END USERS:** Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.