Security Management System User Guide

Oracle FLEXCUBE Universal Banking

Release 14.0.0.0.0

Part No. E88855-01

December 2017

ORACLE

Security Management System User Guide
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
https://www.oracle.com/industries/financial-services/index.html

Copyright © 2007, 2017, 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 anyoperating 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 useand 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.

Contents

1. Preface 1-1
1.1 Introduction 1-1
1.2 Audience 1-1
1.3 Documentation Accessibility 1-1
1.4 Organization 1-1
1.5 Abbreviations 1-2
1.6 Glossary of Icons 1-2
1.7 Related Documents 1-2
2. Security Management 2-1
2.1 Introduction 2-1
2.2 User Limit Maintenance 2-1
2.2.1 Invoking User Limit Maintenance Screen 2-1
2.2.2 Limits Button 2-2
2.2.3 Tills Button 2-3
2.2.4 Group Code Restriction 2-4
2.2.5 General Ledgers Button 2-4
2.3 Role Branch Limits Maintenance 2-5
2.3.1 Invoking Role Branch Limits Maintenance Screen 2-6
2.4 Limits Role Maintenance 2-6
2.4.1 Invoking Limits Role Maintenance 2-6
2.5 Alerts for Users 2-8
2.5.1 Defining Alerts for Users 2-8
2.6 Multi-Factor Authentication 2-9
2.6.1 Logging into Oracle FLEXCUBE by Multi-Factor Authentication 2-9
2.6.2 Maintaining Multi-Factor Authentication Limits 2-10
2.6.3 Viewing Multi-Factor Authentication - Limit Maintenance Summary 2-12
3. Associated Functions 3-1
3.1 Current Users 3-1
3.1.1 View Current Users 3-1
3.2 Error Messages 3-2
3.2.1 Maintaining Error Messages 3-2
3.3 Branch Status 3-3
3.3.1 Viewing Branch Status 3-3
4. Reports 4-1
4.1 Security Management System Violations Log Report 4-1
4.1.1 Generating Security Management System Violations Log Report 4-1
4.1.2 Contents of the Security Management System Violations Log Report 4-2
4.2 User Profile Report 4-3
4.2.1 Generating User Profile Report 4-3
4.2.2 Contents of the User Profile Report 4-4
4.3 Changes Report 4-4
4.3.1 Generating Change Report 4-5
4.3.2 Contents of the Changes Report 4-5
4.4 Inactive Users Aging Analysis Report 4-6

4.4.1 Generating Inactive Users Aging Analysis Report 4-6
4.4.2 Contents of the Inactive Users Aging Analysis Report 4-6
4.5 SMS User Inactive Log Report 4-6
4.5.1 Generating SMS User Inactive Log Report 4-6
4.5.2 Contents of the Inactive Users Log Report 4-7
4.6 Online Performance Statistics Report 4-7
4.6.1 Generating Online Performance Statistics Report 4-7
4.6.2 Contents of the Online Performance Statistics Report 4-8
4.7 Role Profile Created Report 4-9
4.7.1 Generating Role Profile Created Report 4-9
4.7.2 Contents of the Report 4-10
4.8 User Profile Report 4-10
4.8.1 Generating User Profile Report 4-11
4.8.2 Contents of the Report 4-11
4.9 User Entitlement Report 4-13
4.9.1 Generating User Entitlement Report 4-13
4.9.2 Contents of the Report 4-14
5. Function ID Glossary 5-1

1. Preface

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.

This user manual is a supplement to the Core SMS user manual and contains only specific functionalities and information related to Oracle FCUBS Core SMS. Hence, this document should be read in conjunction with the Core SMS user manual from the perspective of completeness in flow and understanding.

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. To set up security management parameters for the Bank.
SMS Administrator for the Bank	To set the SMS bank parameters. To identify the Branch level SMS Administrators.
SMS Administrator for the Branch	To create User and Rsddole profiles for the branches of your bank. 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 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

1.4 Organization

This manual is organized into the following chapters:

Chapter	Description
Chapter 1	*About this Manual* gives information on the intended audience. It also lists the various chapters covered in this User Manual.

Chapter 2	*Security Management* explains how to define and maintain the security of the banking system in terms of users access and roles.
Chapter 3	*Associated Functions* discusses on the details pertaining to defining and maintaining additional security options such as clearing user profile, changing system time level, maintaining SSO parameters, error Messages, and viewing user activity, branch status, and so on.
Chapter 5	*Reports* provides a list of reports that can be generated in this module.
Chapter 6	*Function ID Glossary* has alphabetical listing of Function/Screen IDs used in the module with page references for quick navigation.

1.5 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
The System	This term is always used to refer to Oracle FLEXCUBE
SI	Standing Instructions
MM	Money Market
RM	Relationship Manager

1.6 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

1.7 Related Documents

- The Procedures User Manual

- Common Core - Security Management System User Guide

2. Security Management

2.1 Introduction

This chapter contains the following sections:

- Section 2.2, "User Limit Maintenance"
- Section 2.3, "Role Branch Limits Maintenance"
- Section 2.4, "Limits Role Maintenance"
- Section 2.5, "Alerts for Users"
- Section 2.6, "Multi-Factor Authentication"

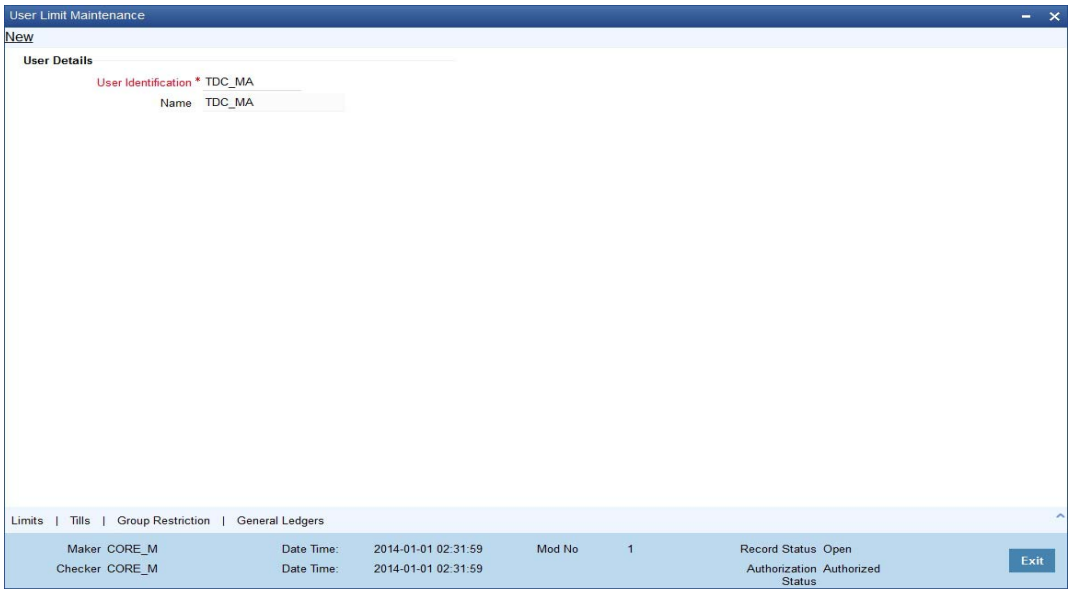
2.2 User Limit Maintenance

This section contains the following topics:

- Section 2.2.1, "Invoking User Limit Maintenance Screen"
- Section 2.2.2, "Limits Button"
- Section 2.2.3, "Tills Button"
- Section 2.2.4, "Group Code Restriction"
- Section 2.2.5, "General Ledgers Button"

2.2.1 Invoking User Limit Maintenance Screen

You can maintain the user limit and till details in the 'User Limit Maintenance' screen. You can invoke this screen by typing 'SMDLMTIL' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



User Identification

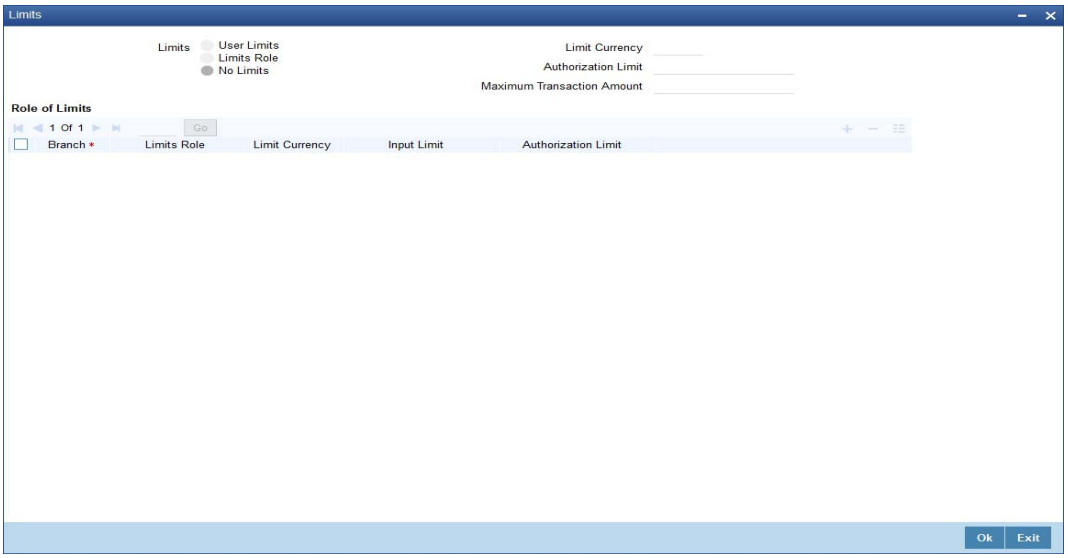
Specify the user identification code. Alternatively, you can select the user identification code from the option list. The list displays all valid values.

Name

The system displays the name of the user.

2.2.2 Limits Button

Click ‘Limits’ button to invoke the Limits screen.



Limits

Select the limits from the following options:

- User Limits - Select this option to maintain user limits.
- Limits Role - Select this option to maintain the limits role.
- No Limits - Select this option to place no restrictions on the user.

Limit Currency

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.

Authorization Limit

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

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.

Maximum Transaction Amount

Specify the maximum amount that the user can enter in a single transaction.

Role of Limits

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.

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:

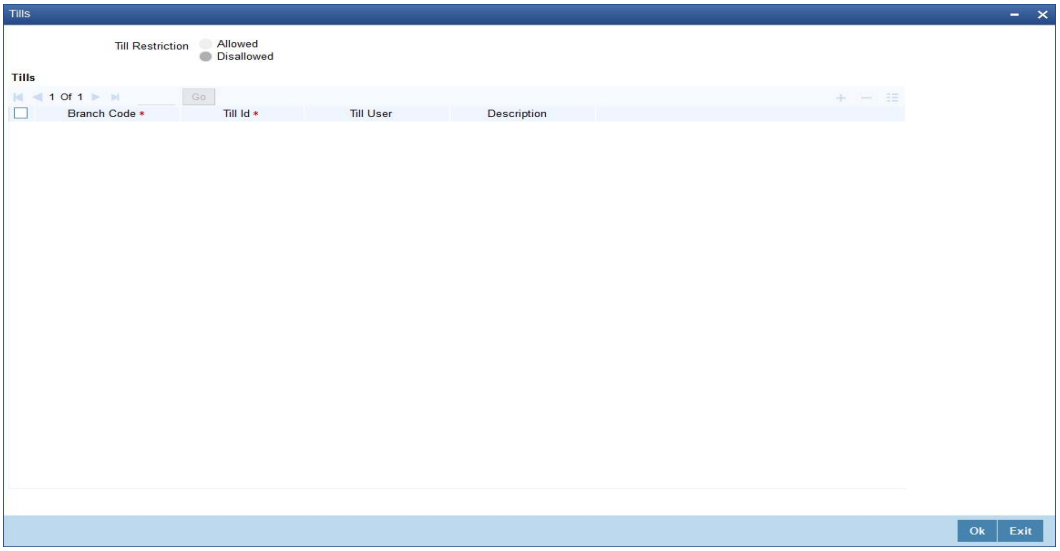
- Limits Currency
- Input Limit
- Authorization Limit

Note

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).

2.2.3 Tills Button

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.



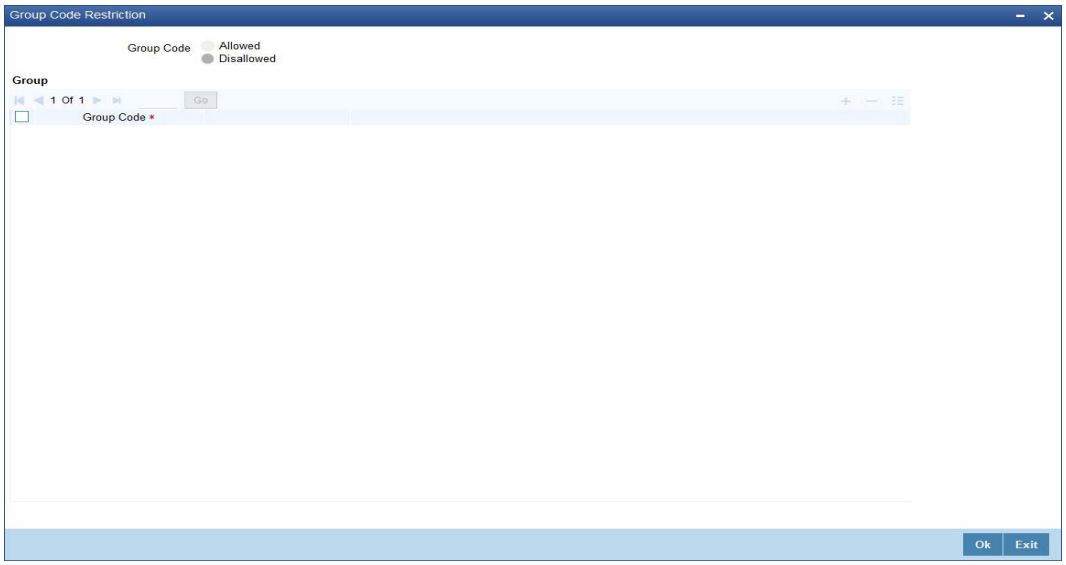
You can either allow or disallow the user from using certain tills.

- 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.

2.2.4 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

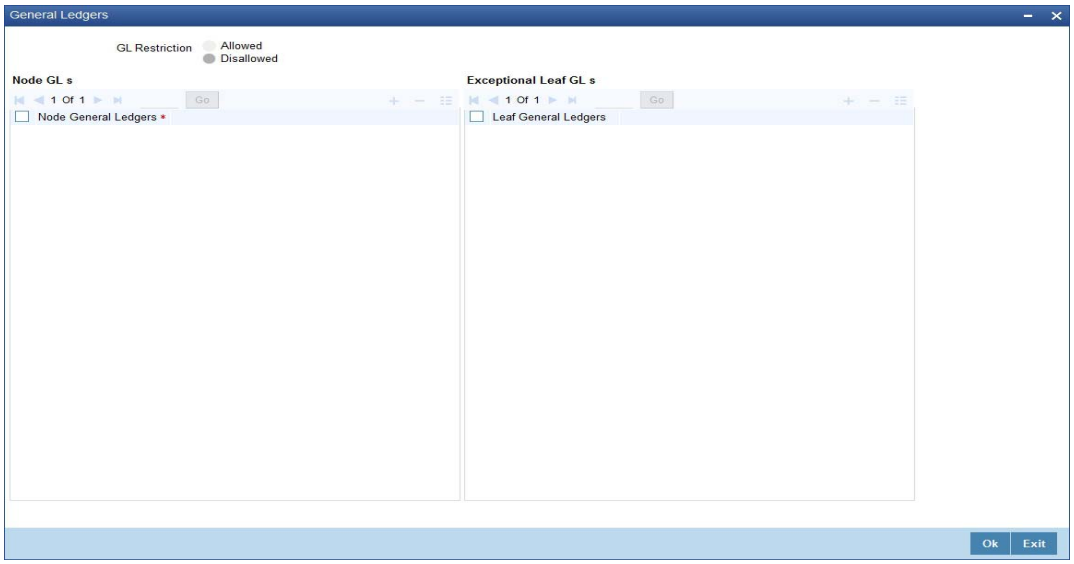
System describes the group code selected by the user.

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 error message “User is restricted to query or modify the account”.

2.2.5 General Ledgers Button

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

GLs and Leaf GLs. Leaf GLs maintained in the section ‘Exception Leaf GLs’ will be excluded from this restriction. 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 that you want to restrict. If you want to allow/disallow posting to some leaf GLs from the selected node GL, specify them in the Exception Leaf GLs list.

For instance, if we have a node GL 100000000 and it has four leaf GLs 100000087, 100000088, 100000089 and 100000090 and the posting is allowed only to one of the leaf GL 100000089, then you have to select GL restriction as Disallowed and give the node GL under Node GLs and the leaf node GL 100000089 under Exceptional Leaf GLs.

Similarly, if you want to allow posting to all leaf GLs under a node GL and disallow posting to some leaf GLs, then select GL Restriction as Allowed and specify the node GL under section node GLs and the leaf GLs to be disallowed under the section Exception Leaf GLs.

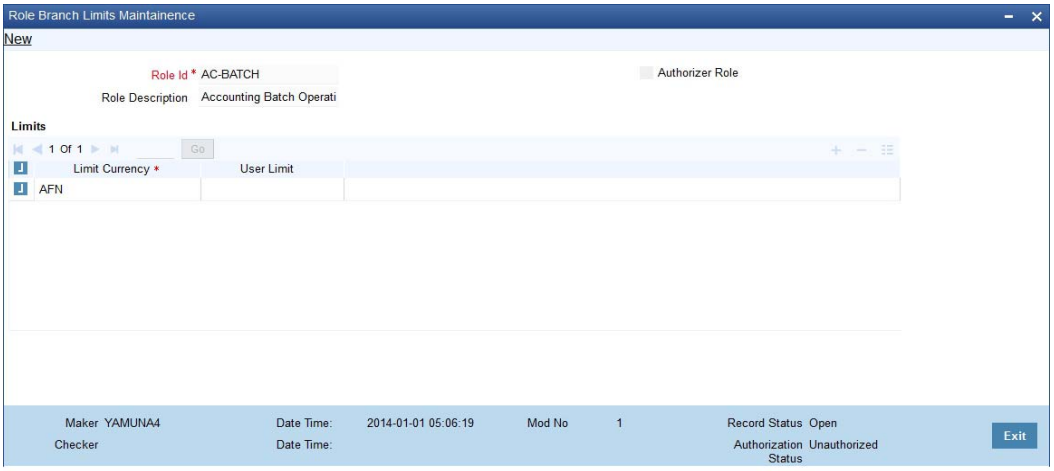
2.3 Role Branch Limits Maintenance

This section contains the following topics:

- Section 2.3.1, "Invoking Role Branch Limits Maintenance Screen"

2.3.1 Invoking Role Branch Limits Maintenance Screen

You can maintain role branch limits in the Role Branch Limits Maintenance screen. To invoke this screen type 'SMDRBLMT' in the field at the top right corner of the Application toolbar and click the adjoining arrow button.



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.

Role ID

Specify the role identification number. Alternatively you can select the role ID from the option list. The list displays all valid values.

Role Description

The system displays the role description.

Authorizer Role

Check this box to enable authorizer role.

Limit Currency

Specify the limit currency. Alternatively, you can select the currency from the option list. The limit displays all valid values.

User Limit

Specify the user specific limit.

2.4 Limits Role Maintenance

This section contains the following topics:

- Section 2.4.1, "Invoking Limits Role Maintenance"

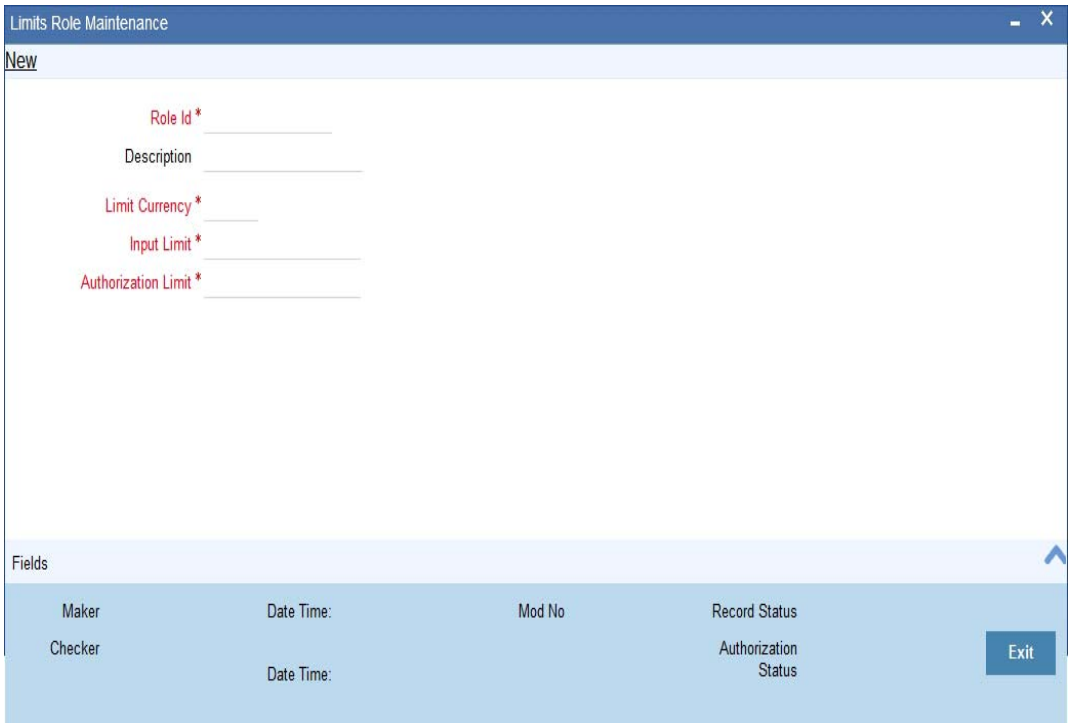
2.4.1 Invoking Limits Role Maintenance

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



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.

Note

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.

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

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

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.

Note

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).

The role limits maintained in the screen ‘SMDRLMNT’ are not applicable for web branch.

2.5 Alerts for Users

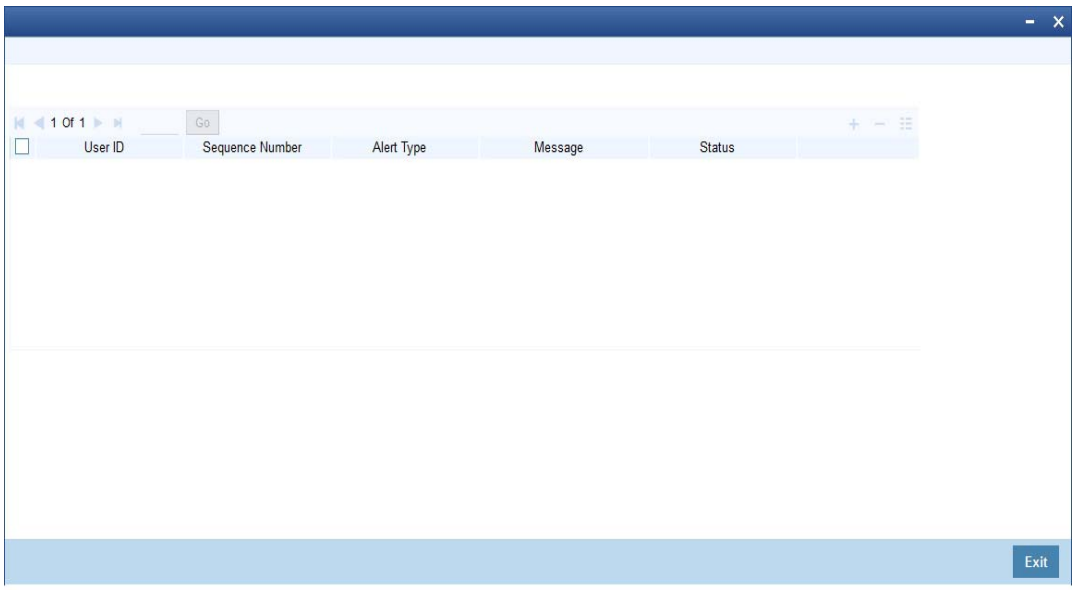
This section contains the following topics:

- Section 2.5.1, "Defining Alerts for Users"

2.5.1 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.

2.6 Multi-Factor Authentication

This section contains the following topic:

- Section 2.6.1, "Logging into Oracle FLEXCUBE by Multi-Factor Authentication"
- Section 2.6.2, "Maintaining Multi-Factor Authentication Limits"
- Section 2.6.3, "Viewing Multi-Factor Authentication - Limit Maintenance Summary"

2.6.1 Logging into Oracle FLEXCUBE by Multi-Factor Authentication

Multi-Factor Authentication (MFA) is an authentication mode, which provides further level of authentication apart from the regular user ID and password authentication.

After successful login validation to FLEXCUBE, the system validates whether the user is enabled for MFA as maintained at the ‘User Maintenance’ (SMDUSRDF) screen. If you are MFA enabled, you are eligible for transactions greater than MFA limit and the system displays the MFA login screen and defaults the user ID.

You can specify the following details:

Multi-Factor Id

The system displays the Multi-Factor authentication ID linked to the user ID.

Multi-Factor PIN

Specify the Multi-Factor PIN for MFA.

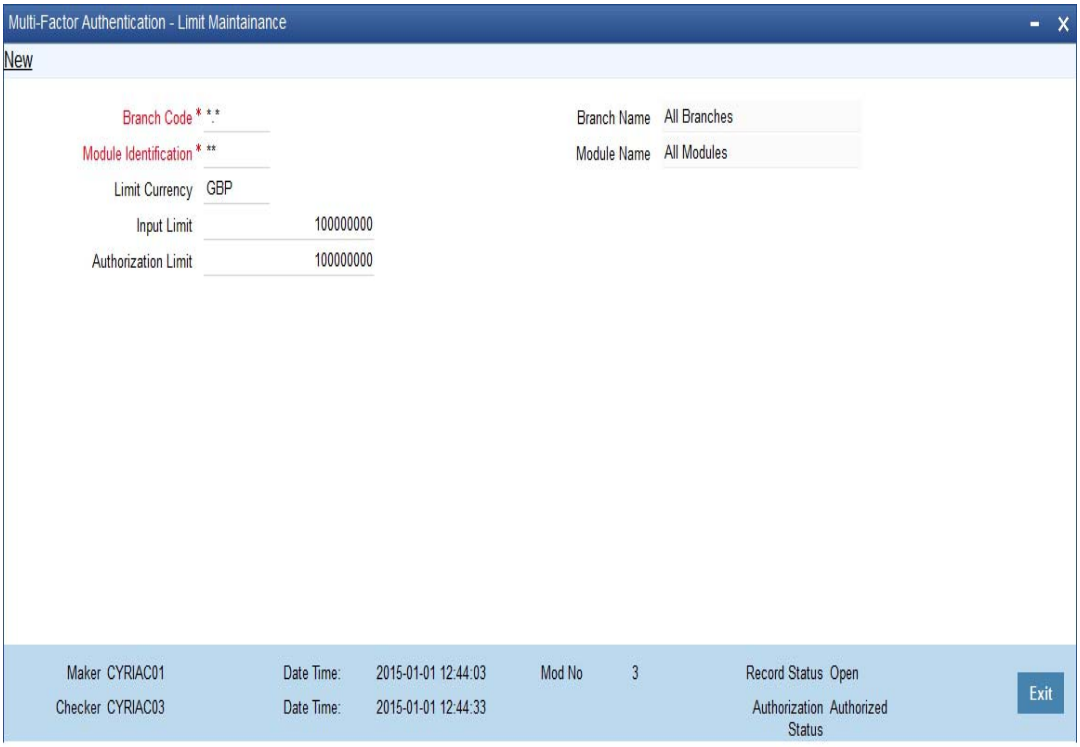
The system generates the MFA PIN just before the authentication, which expires in a short time. The generated MFA PIN is communicated to the user in multiple ways, such as text messages sent to the user's mobile phone or electronic devices.

The system prompts the user to input the MFA token as a second password and validates the user's authenticity. This process reduces the risk posed by using only user ID or password mechanism. If the MFA pin is validated successfully, the user's session is marked as 'Multi-Factor Authenticated'. Else, it is marked as 'Multi-Factor Not Authenticated'.

2.6.2 Maintaining Multi-Factor Authentication Limits

You can capture Multi-Factor Authentication (MFA) limits branch-wise and module-wise in the 'Multi-Factor Authentication - Limit Maintenance' screen. MFA limit indicates the limit above which MFA is required. The process of MFA can be determined by the parameters set at the individual user level. MFA limits can be used to authorize transactions above certain limit.

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



You can specify the following details here:

Branch Code

Specify the branch code for MFA limit. Alternatively, you can select the branch code from the option list. The list displays all the branches in the country maintained in the system and a value **, which indicates all branches.

Branch Name

The system displays the name of the branch code.

Module Identification

Specify the module code for MFA limit. Alternatively, you can select the module code from the option list. The list displays all the modules maintained in the system and a value **, which indicates all modules.

Module Name

The system displays name of the module for the selected module code.

Limit Currency

Specify the currency code in which the limit amount can be specified. Alternatively, you can select the currency code from the option list. The list displays all the currencies maintained in the system.

Input Limit

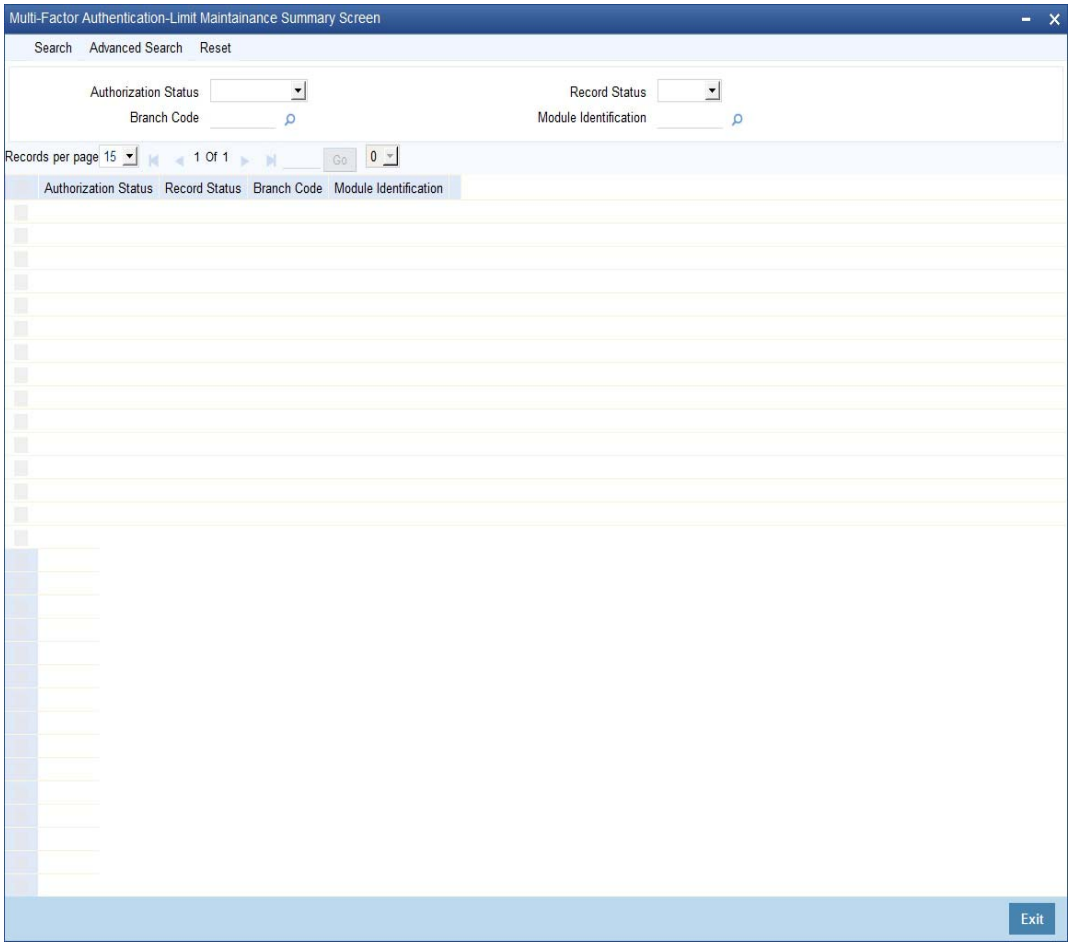
Specify the limit amount for input.

Authorization Limit

Specify the authorization limit amount for authorizer.

2.6.3 Viewing Multi-Factor Authentication - Limit Maintenance Summary

You can view multi-factor authentication limit maintenance in the 'Multi-Factor Authentication - Limit Maintenance Summary' screen. You can invoke this screen by typing 'SMSMFALM' in the field at the top right corner of the Application toolbar and clicking on the adjoining arrow button.



In the above screen, you can base your queries on any or all of the following parameters and fetch records:

- Authorization Status
- Branch Code
- Record Status
- Module Identification

Click 'Search' button. The system identifies all records satisfying the specified criteria and displays the following details for each one of them:

- Authorization Status
- Branch Code
- Record Status
- Module Identification

3. Associated Functions

This chapter contains the following sections:

- Section 3.1, "Current Users"
- Section 3.2, "Error Messages"
- Section 3.3, "Branch Status"

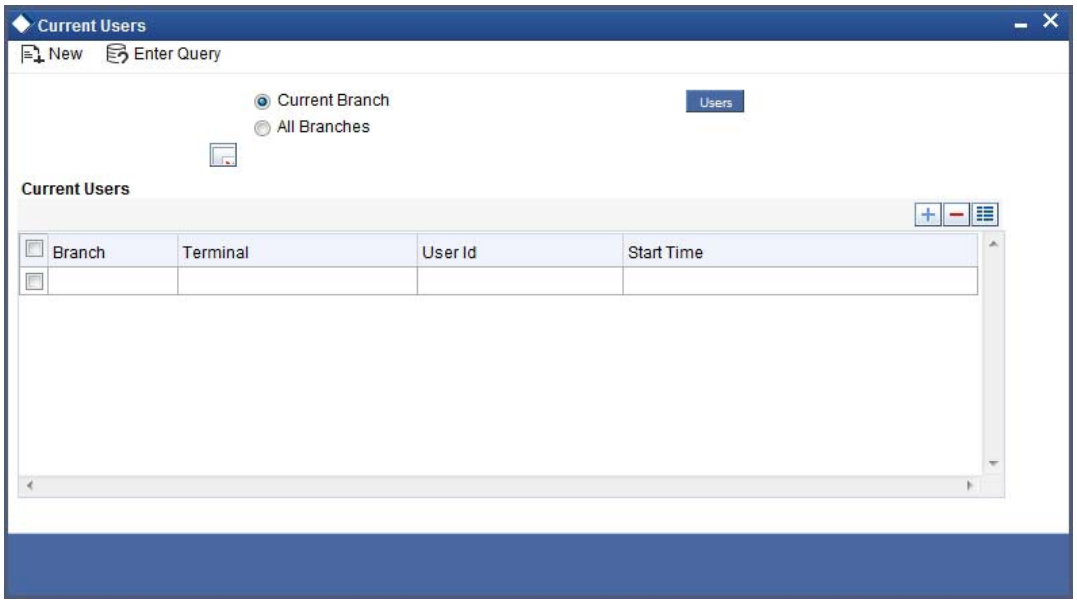
3.1 Current Users

This section contains the following topics:

- Section 3.1.1, "View Current Users"

3.1.1 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

3.2 Error Messages

This section contains the following topics:

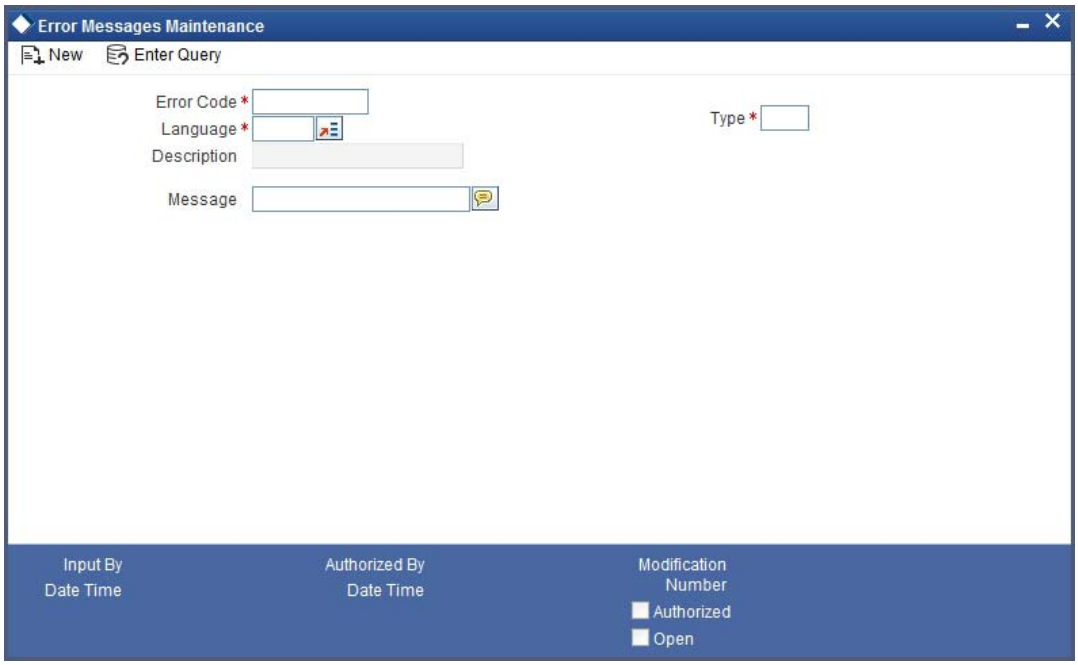
- Section 3.2.1, "Maintaining Error Messages"

3.2.1 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 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.

3.3 Branch Status

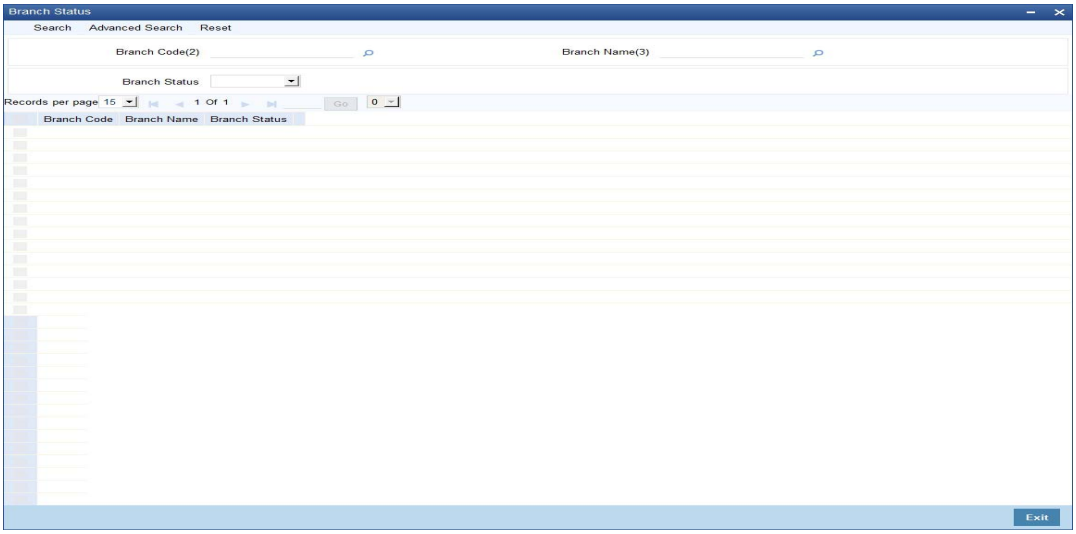
This section contains the following topics:

- Section 3.3.1, "Viewing Branch Status"

3.3.1 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. Reports

The chapter contains the following sections:

- Section 4.1, "Security Management System Violations Log Report"
- Section 4.2, "User Profile Report"
- Section 4.3, "Changes Report"
- Section 4.4, "Inactive Users Aging Analysis Report"
- Section 4.5, "SMS User Inactive Log Report"
- Section 4.6, "Online Performance Statistics Report"
- Section 4.7, "Role Profile Created Report"
- Section 4.8, "User Profile Report"
- Section 4.9, "User Entitlement Report"

4.1 Security Management System Violations Log Report

This section contains the following topics:

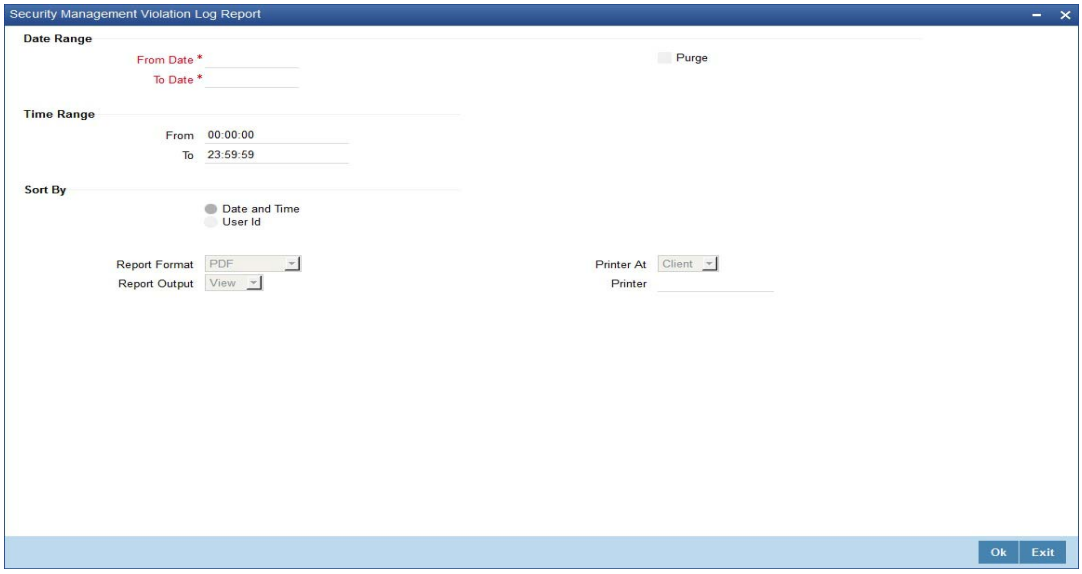
- Section 4.1.1, "Generating Security Management System Violations Log Report"
- Section 4.1.2, "Contents of the Security Management System Violations Log Report"

4.1.1 Generating 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:



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.

4.1.2 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

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

4.2 User Profile Report

This section contains the following topics:

- Section 4.2.1, "Generating User Profile Report"
- Section 4.2.2, "Contents of the User Profile Report"

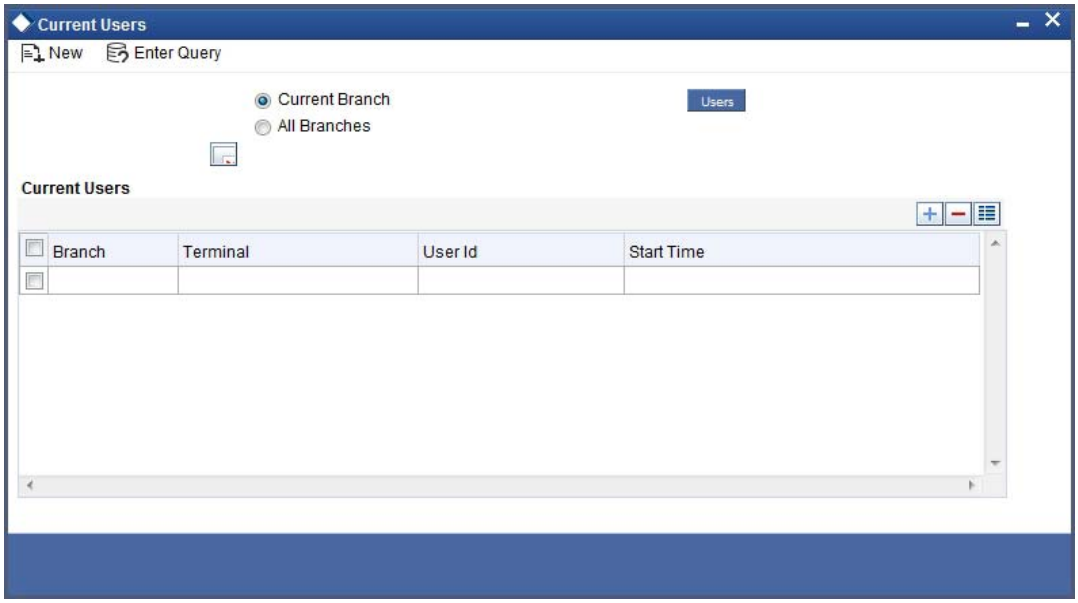
4.2.1 Generating User Profile Report

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:



4.2.2 Contents of the User Profile Report

Field Name	Field Description
Branch Code and Name	The code allotted to the branch and the full name of the branch.
Date and Time	At which the report was generated.
Printed by	The user who has generated the report.
Spool File	If the report has been printed onto a spool file, the name of the spool file is given here.
Sort on	The criteria on which the details have been sorted.
Date Range	The period for which the report is generated.
User-ID	The ID of the user whose details are being reported.
Name	The name of the user whose details are being reported.
Time Level	The time level of the user.
Language Code	The language assigned to the user.
Profile Expires On	The date on which the user profile is due to expire.
Status	The status of the user - enabled, on hold or disabled.
Function-ID	The function allowed for the user.
Function Description	The description of the function.
Link with Role Definition	If the user has been linked to a role, the role-ID is given here.
Maximum Transaction Amount	The maximum amount that the user can enter in a single transaction.
Maximum Authorization Amount	The maximum amount that a transaction can have if it has to be authorized by this user.
Branch Code	The branch in which the user profile is defined.
Branch Name	The name of the branch in which the user has signed on.
Currency Code	The S.W.I.F.T code of the currency in which the user can operate.
Currency Name	The name of the currency in which the user can operate.
Customer Code	The customer whose accounts can be handled by the user.
Customer Name	The name of the customer whose accounts can be handled by this user.
Restrictive Passwords - User	The passwords defined as restrictive passwords for the user.

4.3 Changes Report

This section contains the following reports:

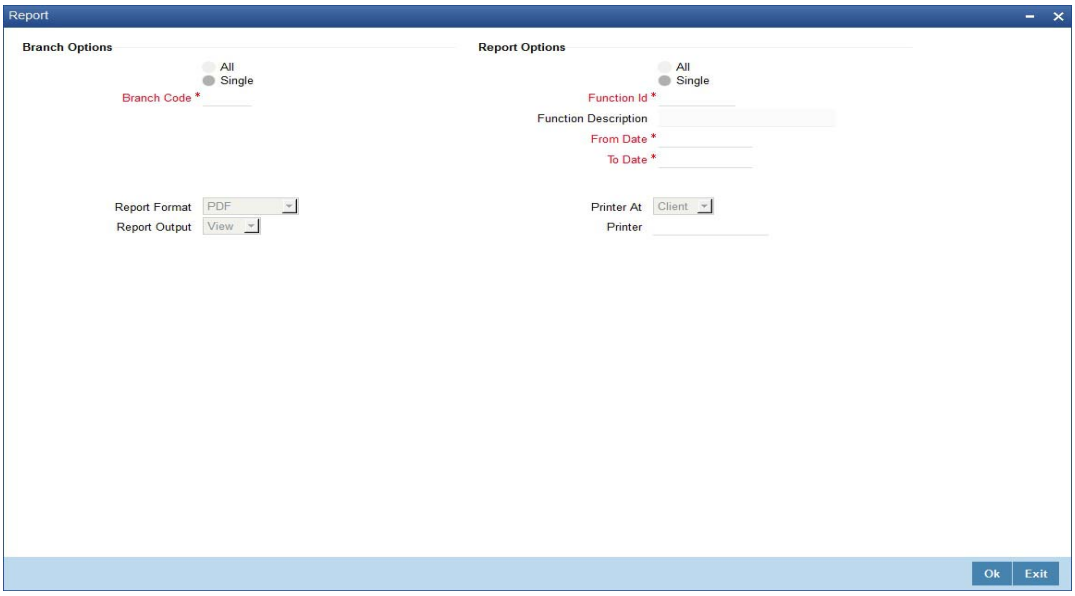
- Section 4.3.1, "Generating Change Report"
- Section 4.3.2, "Contents of the Changes Report"

4.3.1 Generating Change 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.



4.3.2 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

Field Name	The field that has been maintained
Input by	The Id of the person who input the details of the transaction
Old Value	The value in the field before it was modified
New Value	The value in the field after it was modified

Date & Time	The date and time of the transaction
Authorizer ID	The Id of the person who authorized the transaction
Date & Time	The date and time when the transaction was authorized
Record Stat	The status of the record
Auth Stat	The authorization status
Function ID	The function ID
Mod Number	The module number
Table Name	The table name

4.4 Inactive Users Aging Analysis Report

This sections contains the following topics:

- Section 4.4.1, "Generating Inactive Users Aging Analysis Report"
- Section 4.4.2, "Contents of the Inactive Users Aging Analysis Report"

4.4.1 Generating 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.

4.4.2 Contents of the Inactive Users Aging Analysis Report

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

4.5 SMS User Inactive Log Report

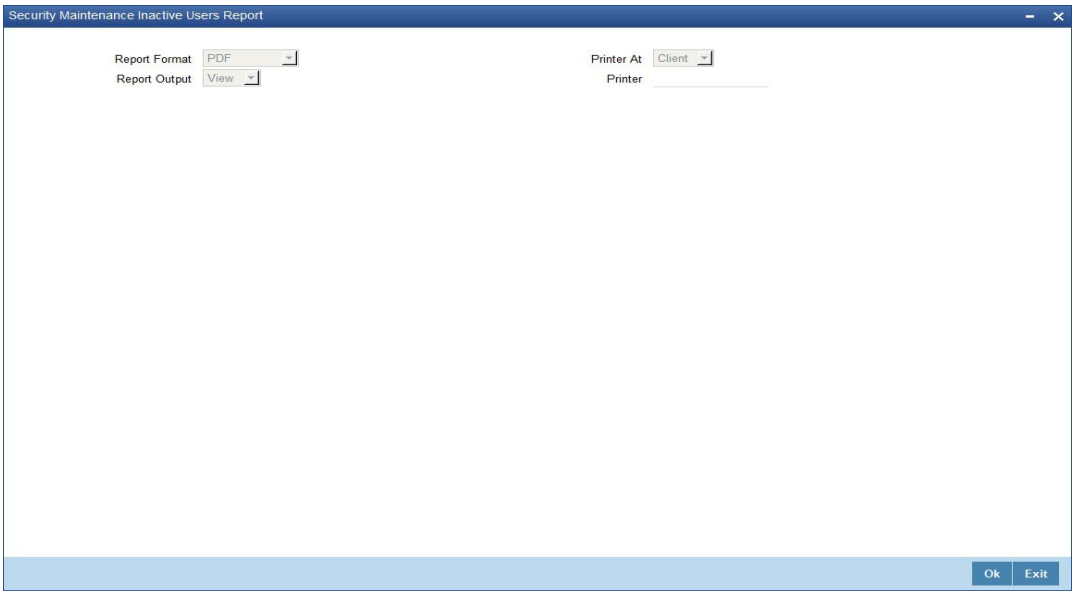
This section contains the following topics:

- Section 4.5.1, "Generating SMS User Inactive Log Report"
- Section 4.5.2, "Contents of the Inactive Users Log Report"

4.5.1 Generating 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.



4.5.2 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.

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

4.6 Online Performance Statistics Report

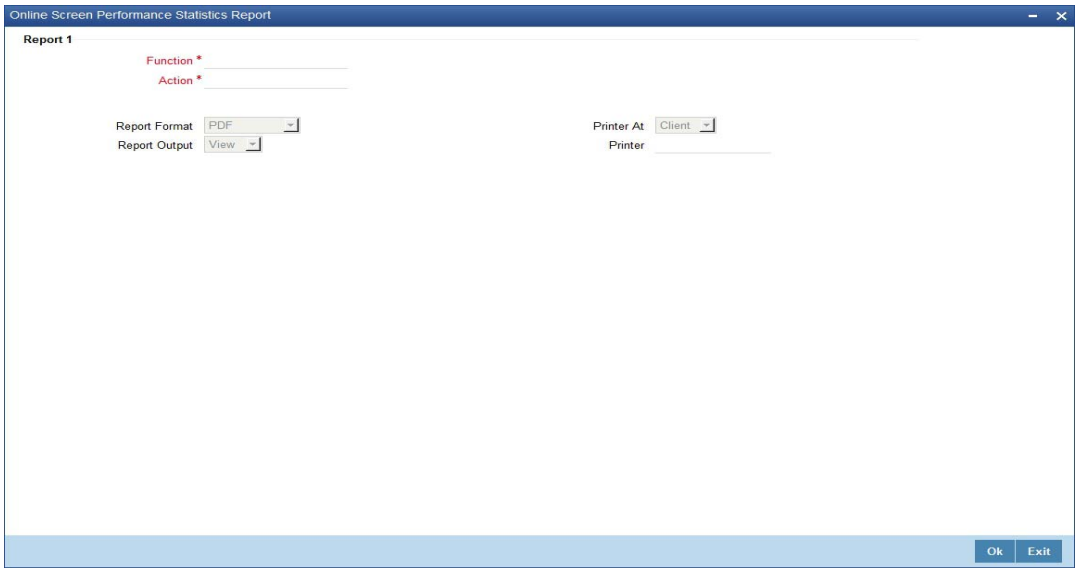
The section contains the following topics:

- Section 4.6.1, "Generating Online Performance Statistics Report"
- Section 4.6.2, "Contents of the Online Performance Statistics Report"

4.6.1 Generating 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.



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.

Note

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

4.6.2 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.

Term	Description
Function Id	This indicates function action of the screen.

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

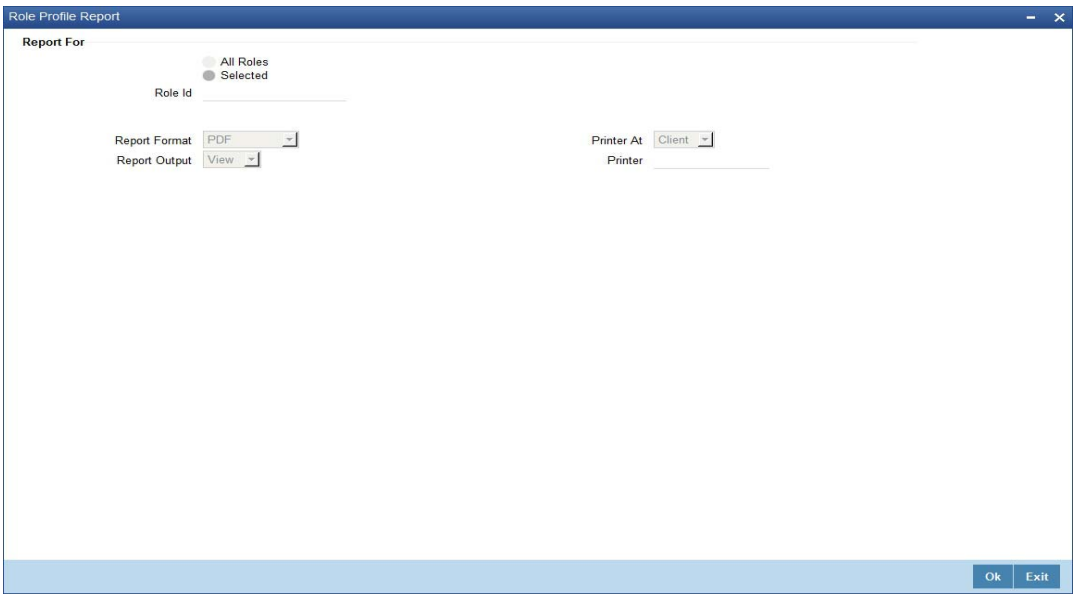
4.7 Role Profile Created Report

This section contains the following topics:

- Section 4.7.1, "Generating Role Profile Created Report"
- Section 4.7.2, "Contents of the Report"

4.7.1 Generating 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 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'.

4.7.2 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
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

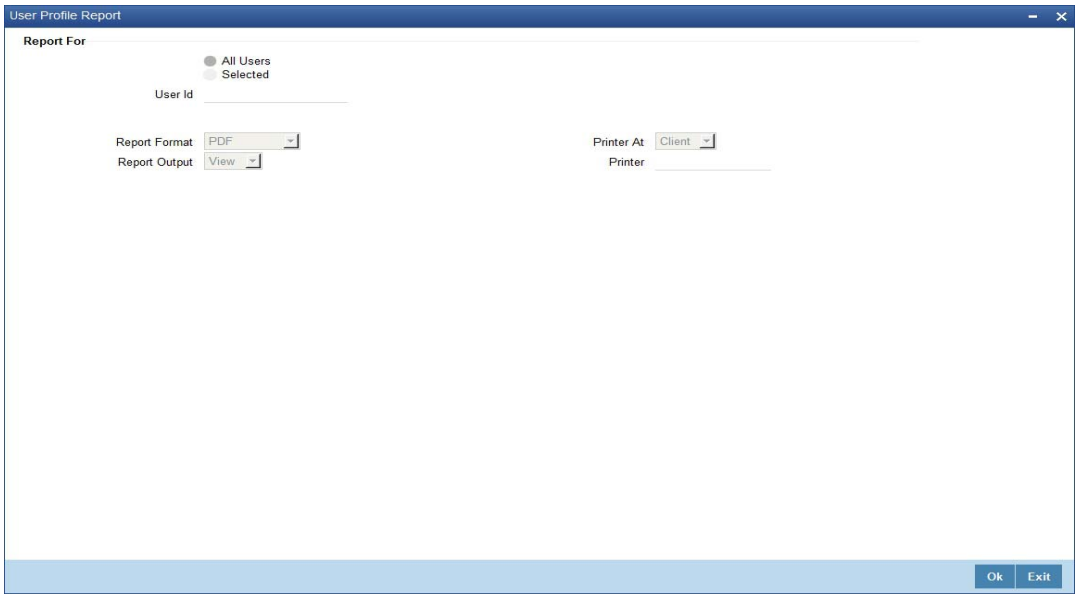
4.8 User Profile Report

This section contains the following topics:

- Section 4.8.1, "Generating User Profile Report"
- Section 4.8.2, "Contents of the Report"

4.8.1 Generating 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.



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'.

4.8.2 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
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
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 Authoriza-tion 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

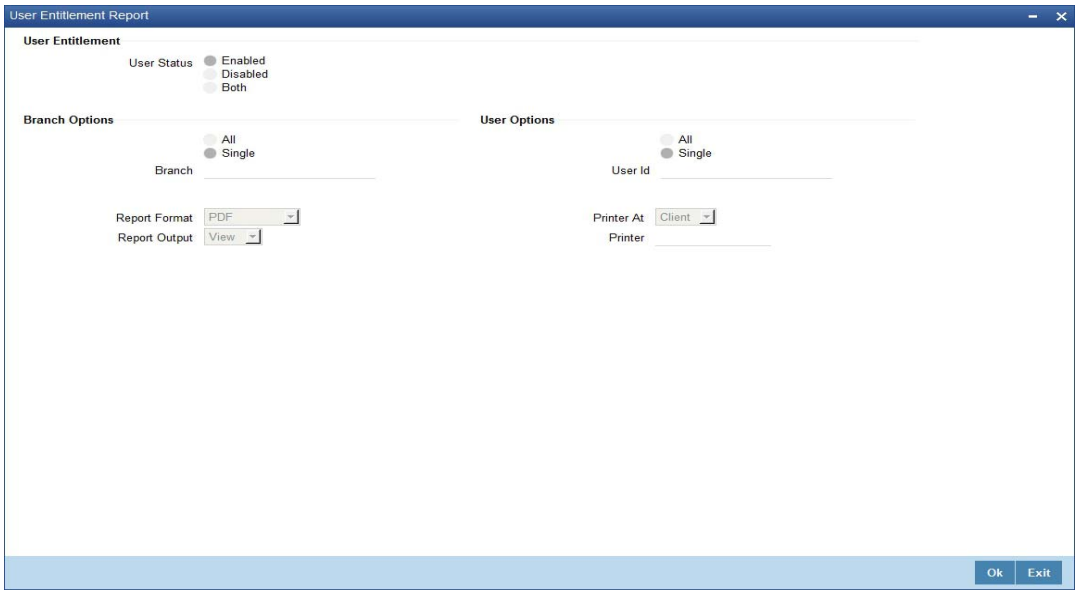
4.9 User Entitlement Report

This section contains the following topics:

- Section 4.9.1, "Generating User Entitlement Report"
- Section 4.9.2, "Contents of the Report"

4.9.1 Generating 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'.

4.9.2 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

5. Function ID Glossary

C

CSDERMSG 3-2

S

SMDLMTIL 2-1
SMDMFALM 2-10
SMDRBLMT 2-6
SMDRLMNE 2-7
SMDUSALR 2-8
SMRONSTA 4-8
SMRPINST 4-7
SMRPUSPR 4-11
SMRPVLLG 4-1
SMRUSREN 4-13
SMSBRNST 3-3
SMSMFALM 2-12