

Security Management System User Guide
Oracle FLEXCUBE Universal Banking

Release 12.87.06.0.0

Part No. F22925-01

May 2020

Security Management System User Guide
May 2020
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/

Copyright © 2007, 2020, 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.

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	1-3
2. Security Management	2-1
2.1 Introduction	2-1
2.2 Setting up Parameters at the Bank Level	2-1
2.2.1 <i>Invalid Logins</i>	2-2
2.2.2 <i>Specifying Parameter</i>	2-3
2.3 Defining a Limits Role	2-4
2.3.1 <i>Working of the Limits</i>	2-5
2.3.2 <i>Differentiating Normal and MF Users</i>	2-6
2.3.3 <i>Tills</i>	2-8
2.3.4 <i>General Ledgers</i>	2-9
2.3.5 <i>Limits</i>	2-9
2.3.6 <i>Group Code Restriction</i>	2-11
2.4 Defining Alerts for Users	2-12
2.5 Single Sign On (SSO) Enabled Environment	2-13
3. Associated Functions	3-1
3.1 CView Current Users	3-1
3.2 Maintaining Error Messages	3-1
3.3 Viewing Branch Status	3-2
4. Error Codes and Messages	4-1
5. Reports	5-1
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	5-2
5.2.1 <i>Contents of the Security Management System Violations Log Report</i>	5-3
5.3 User Profile Report	5-3
5.3.1 <i>Contents of the User Profile Report</i>	5-5
5.4 Changes Report	5-5
5.4.1 <i>Contents of the Changes Report</i>	5-6
5.5 SMS User Inactive Log Report	5-7
5.5.1 <i>Contents of the Inactive Users Log Report</i>	5-7
5.6 Online Performance Statistics Report	5-8
5.6.1 <i>Contents of the Online Performance Statistics Report</i>	5-8
5.7 Changes Log Report	5-9
5.7.1 <i>Contents of the Report</i>	5-10
5.8 User Profile Report	5-11
5.8.1 <i>Contents of the Report</i>	5-11

5.9	Role Profile Report	5-13
5.9.1	<i>Contents of the Report</i>	5-13
5.10	User Entitlement Report	5-14
5.10.1	<i>Contents of the Report</i>	5-15
6.	Function ID Glossary	6-1

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.

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 1	<i>About this Manual</i> gives information on the intended audience. It also lists the various chapters covered in this User Manual.
Chapter 2	<i>Security Management</i> explains how to define and maintain the security of the banking system in terms of users access and roles.





Chapter 3	<i>Associated Functions</i> 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 4	<i>Error Codes and Messages</i> lists all the error codes with the associated messages that you can encounter while working with this module.
Chapter 5	<i>Reports</i> provides a list of reports that can be generated in this module.
Chapter 6	<i>Function ID Glossary</i> has alphabetical listing of Function/Screen ID's 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

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 is divided into several sections for configuring system parameters. The 'Bank Level Parameters' section includes fields for 'Head Office', 'Site Code' (with a red asterisk indicating it is required), and 'Activation Key'. The 'Password Length (Characters)' section has input fields for 'Maximum' (set to 15) and 'Minimum' (set to 8). The 'Invalid Logins' section contains checkboxes for 'Cumulative' and 'Successive'. The 'Parameters' section 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', along with checkboxes for 'Display Legal Notice' and 'Password External'. The 'Warning Screen Text' section has a text input field. The 'Screen Saver Details' section has a checkbox for 'Screensaver Required'. At the bottom, there are tabs for 'Branch Restrictions', 'Password Restrictions', and 'Fields', and a table with columns for 'Maker', 'Checker', 'Mod No', 'Date Time', 'Record Status', and 'Authorization Status'. An 'Exit' button is located in the bottom right corner.

Note

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.

Password External

The password external is enabled if the PASSWORD_EXTERNAL is maintained as 'Y' in the property file. However, you cannot edit this check box.

If 'Password External' is enabled then you cannot modify the user and the password.

SMinimum 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

Note

You can specify any number between 1 and 11 in each of these fields. The minimum length of special characters should not be less than or equal to zero. 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

-
- ☐ Security Management
 - ☐ Maintenance
 - ➔ Branch Restrictions
 - ➔ Department Maintenance
 - ➔ Error Messages
 - ➔ Function Description
 - ➔ Landing Page
 - ➔ Language Codes
 - ➔ MBean
 - ➔ Queues
 - ➔ Registry Details - Sys Admin

2.3 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 'SMDRLMNE' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot shows the 'Role Limits Maintenance' application window. The window title is 'Role Limits Maintenance'. The toolbar contains 'New' and 'Enter Query' buttons. The main area contains five input fields: 'Role Id *', 'Description', 'Limit Currency *', 'Input Limit *', and 'Authorization Limit *'. Below the main area is a 'Fields' section with labels for 'Maker', 'Checker', 'Mod No', 'Date Time:', 'Date Time:', 'Record Status', and 'Authorization Status'. An 'Exit' button is located in the bottom right corner.

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.

Authorization Limit

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

2.3.1 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.

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.

2.3.2 Differentiating Normal and MF Users

Check the 'MFi User' box to indicate that the user is a Microfinance (Account Officer) user. By default, the system leaves this box unchecked to indicate that all users would be normal users.

Note

An account officer can book loan accounts for customers who are linked to him/her.

For more details, refer to 'Linking Customers to Account Officers' in the Microfinance User Manual.

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.

Note

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.

Note

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.

Note

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

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.

Note

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.

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.

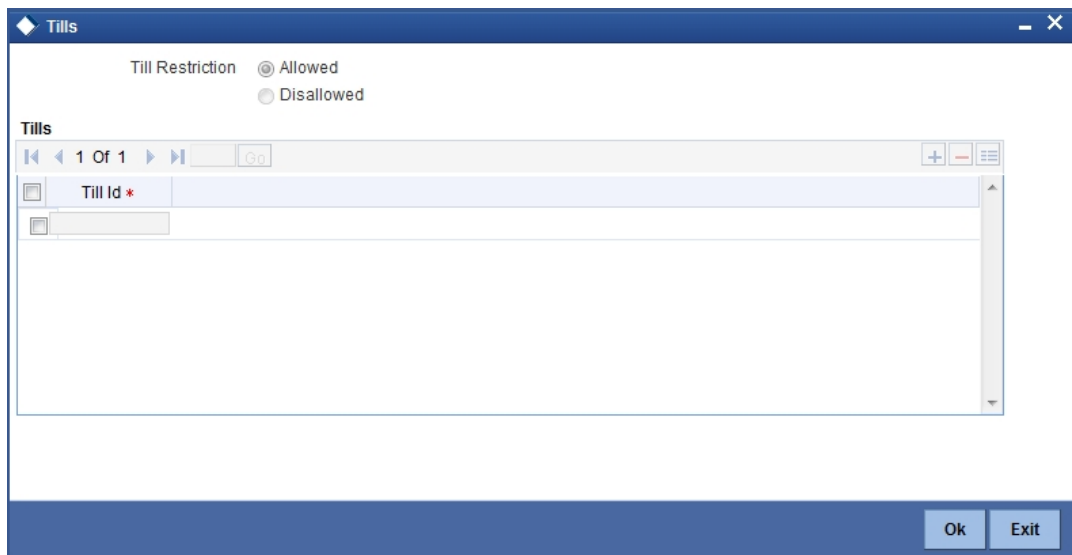
Screen Saver Details

Screensaver Interval (in seconds)

The system defaults the screen saver interval based on the screen saver details maintained in the bank parameters screen.

2.3.3 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.

2.3.4 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.

General Ledgers

GL Restriction Allowed
 Disallowed

Node GL s

Node General Ledgers *
<input type="text"/>

Leaf GL s

Leaf General Ledgers
<input type="text"/>

Ok Exit

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

2.3.5 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.

Limits

Limits User Limits
 Limits Role
 No Limits

Limit Currency
Maximum Transaction Amount
Authorization Limit

Role of Limits

Branch *	Limits Role	Limit Currency	Input Limit	Authorization Limit
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Ok Exit

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:

2.3.5.1 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

Note

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

2.3.5.2 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.

Note

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

Note

For Journal (Single and Multi-Offset), the check will be performed on each individual transaction i.e. each debit and credit entry. Role-wise limit setup is not applicable to retail teller transactions. Only User Limits is supported for retail teller transactions.

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.

2.3.6 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.

The screenshot shows a software window titled "Group Code Restriction". At the top, there are two radio buttons: "Allowed" (unselected) and "Disallowed" (selected). Below this is a table with the following structure:

Group Code *	Group Description

At the bottom right of the window, there are two buttons: "Ok" and "Exit".

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.

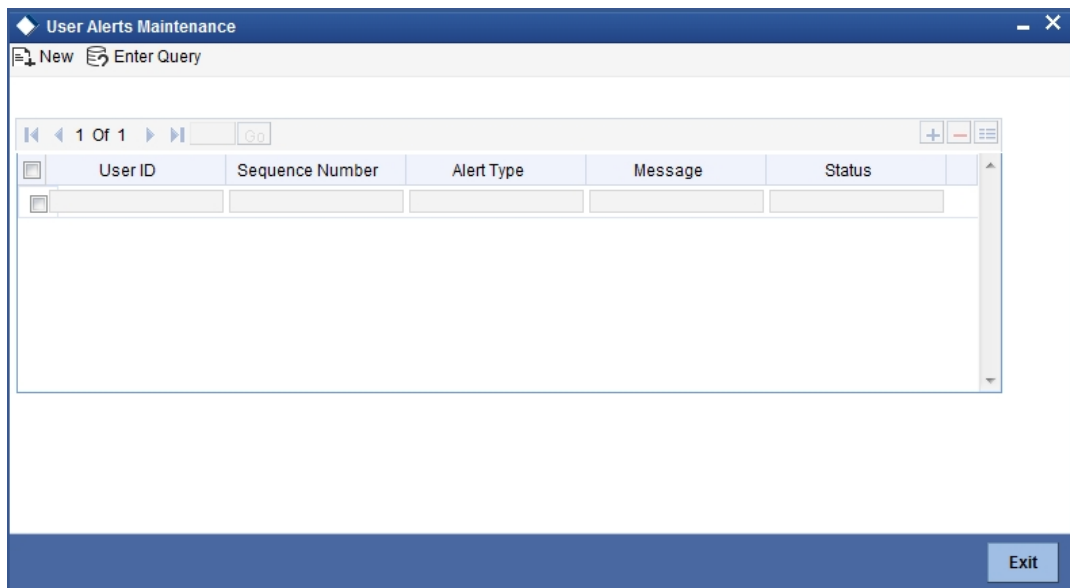
Note

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”.

2.4 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:

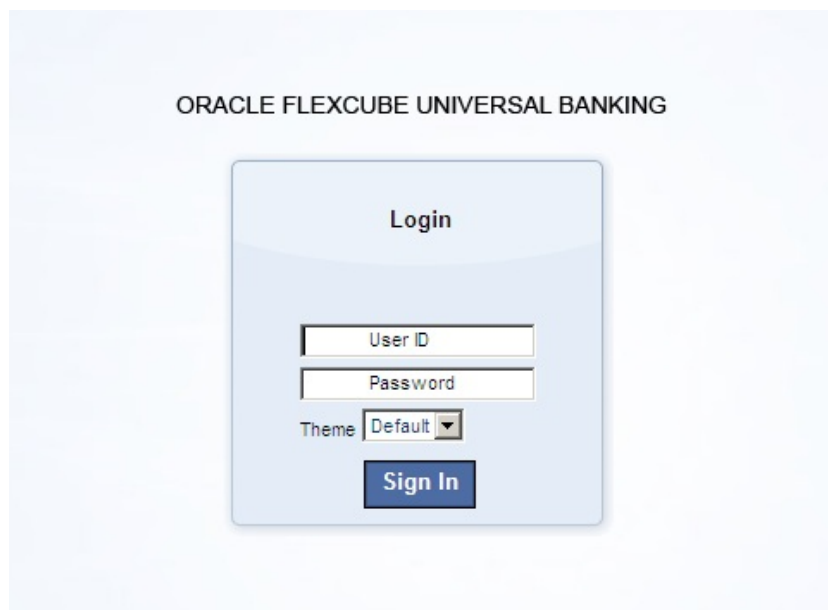
- P -Processed
- U -Unprocessed

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.

2.5 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.

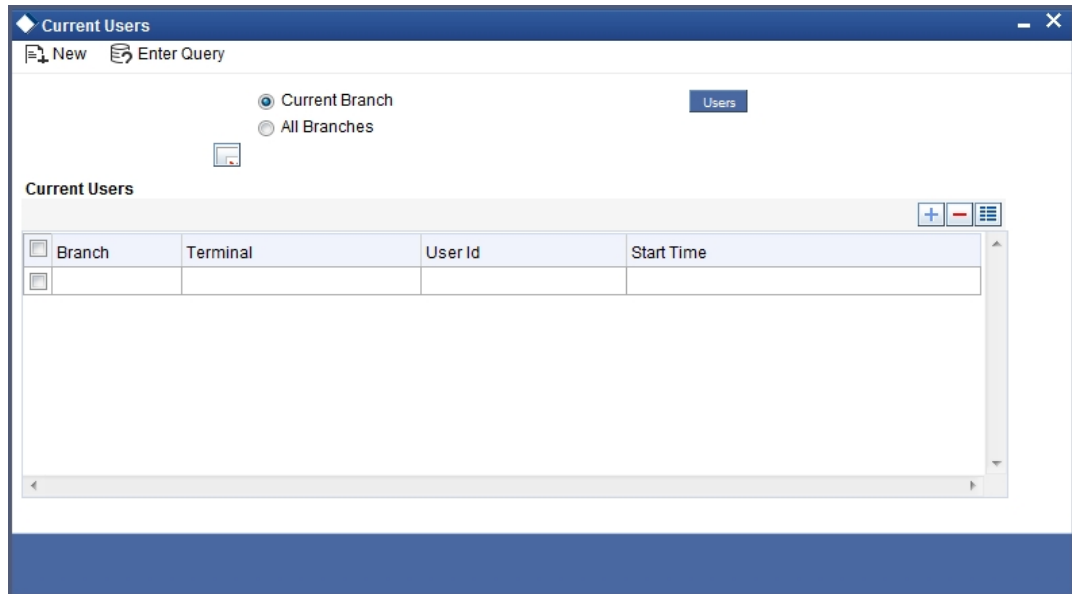


After successful authentication and authorization of the user is carried out by the LDAP (Oracle Internet Directory), a request is forwarded to gain access into Oracle FLEXCUBE. On clicking the 'Submit' button you can directly get into Oracle FLEXCUBE without specifying Oracle FLEXCUBE user id and password.

3. Associated Functions

3.1 CView 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 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 'CSDERRMS' 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 title bar reads 'Error Messages Maintenance'. Below the title bar is a toolbar with 'New' and 'Enter Query' buttons. The main workspace contains several input fields: 'Error Code *', 'Language *', and 'Type *' (with a dropdown menu showing 'Ignore'). To the right, there are fields for 'Message', 'Language Description', and 'Record Status'. At the bottom, there is a status bar with fields for 'Maker', 'Checker', 'Date Time', 'Mod No', 'Authorization Status', and an 'Exit' button.

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.

Language Description

Specify the description for the language code.

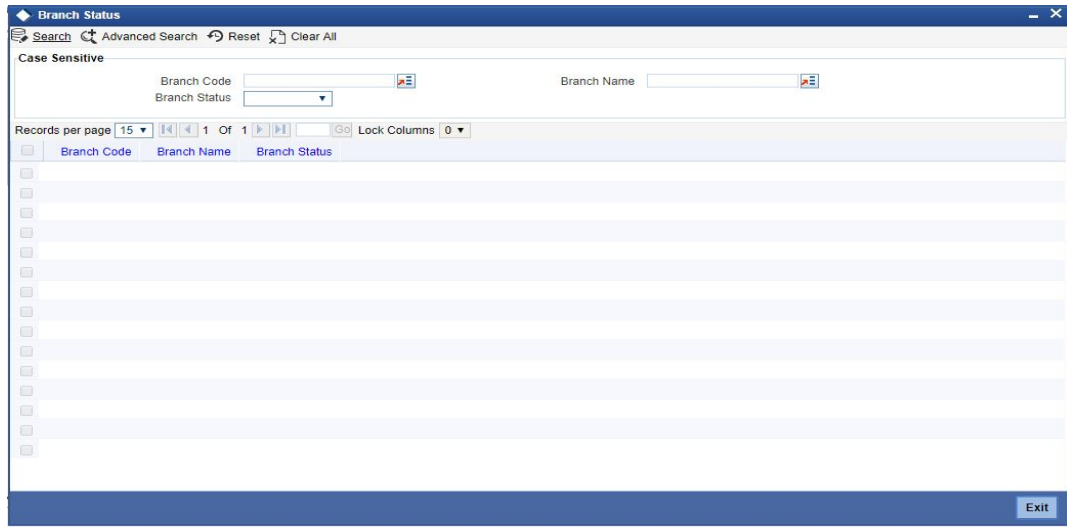
Message

Specify the error message that has to be displayed.

3.3 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

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 window titled "Events Log" with a "Report For" section. It includes radio buttons for "All Users" (selected) and "Selected Users", a "User Id" text box, "From Date" and "To Date" date pickers, a "Purge" checkbox, "Report Format" (PDF) and "Report Output" (Print) dropdowns, and "Printer At" (Client) and "Printer" text boxes. "Ok" and "Exit" buttons are at the bottom right.

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.

User ID	The user who initiated the event.
Function Description	The name of the function that activated the event.
Start Time	The time at which the event was initiated.
End Time	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.
Branch Code	The code allotted to the branch .
Terminal ID	The system ID where the application is launched
System Start Time	The time when the user starts the application
System End Time	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, and a "Purge" checkbox.
- Time Range:** Includes "From" and "To" time pickers, with "00:00:00" and "23:59:59" displayed.
- Sort By:** Includes radio buttons for "Date ant 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:** An empty text box.

At the bottom right, there are "Ok" and "Exit" 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

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.

5.3 User Profile Report

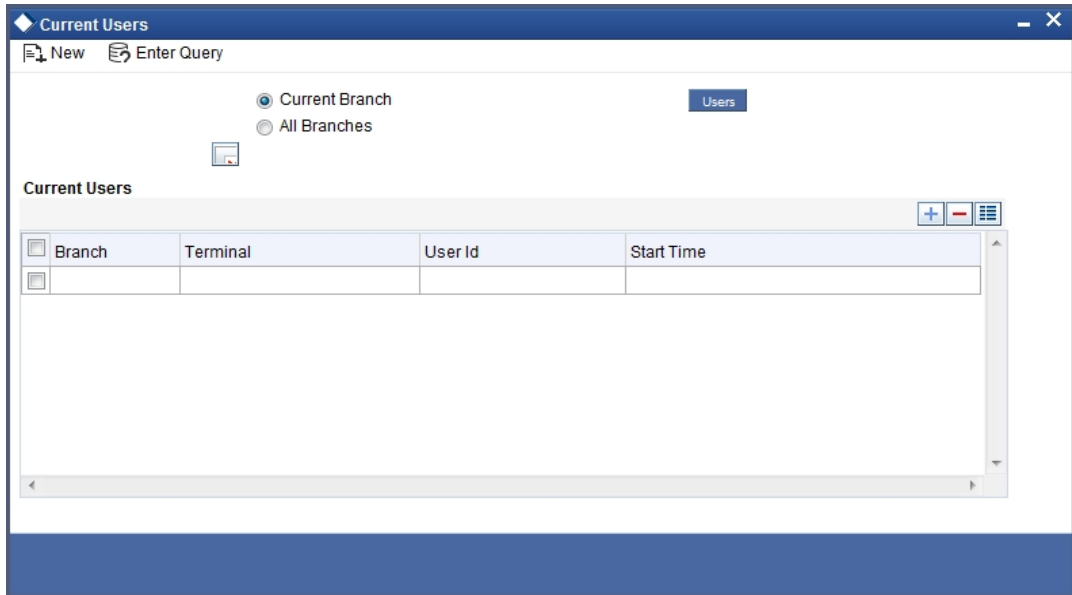
The details of all the user profiles that have been defined are available in the form of a report. The User Profile Report gives details of user profiles maintained for all or specific users. It includes:

- 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

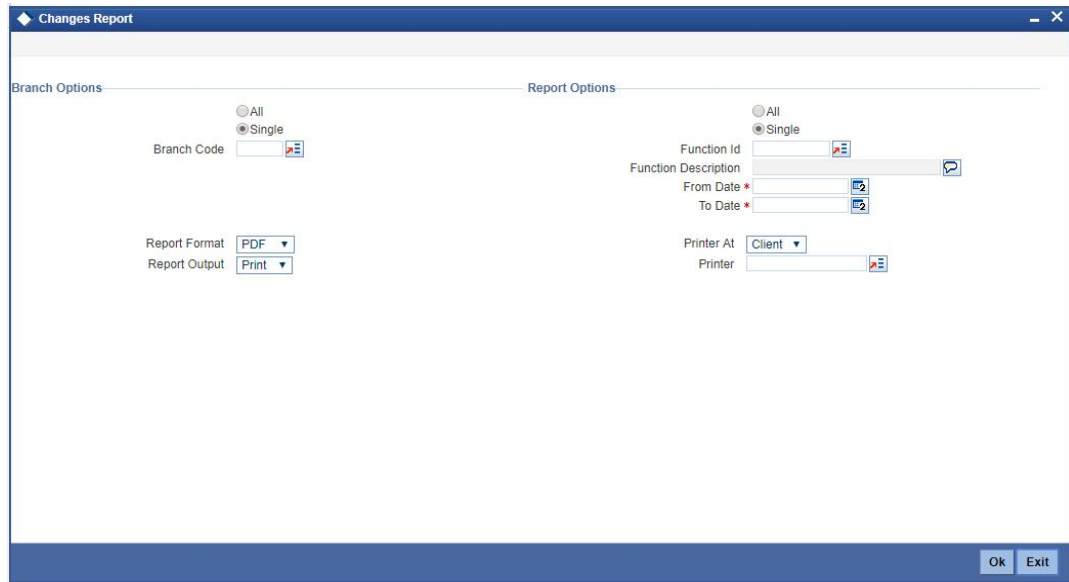
Branch Code and Name	The code allotted to the branch and the full name of the branch.
Date and Time	At which the report was generated.
Printed by	The user who has generated the report.
Spool File	If the report has been printed onto a spool file, the name of the spool file is given here.
Sort on	The criteria 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.

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

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

5.5 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.

5.5.1 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.

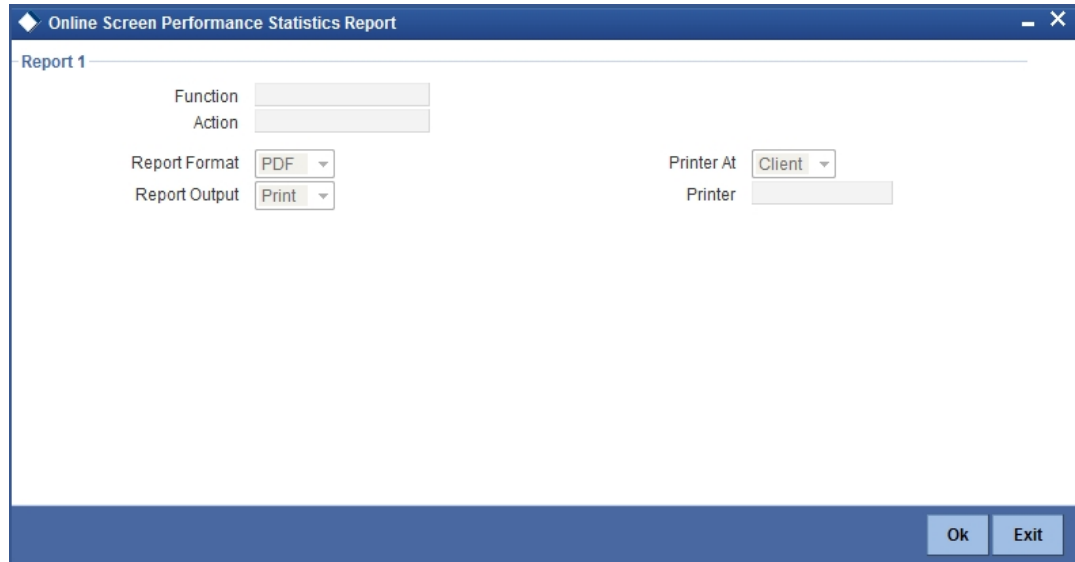
Body of the report

The following details are displayed in the report.

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

5.6 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.

5.6.1 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.

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.

5.7 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.

◆ Changes Log Report

Report Options

Function Id *

Unauthorized

All Changes

Print Copies

Report Format PDF

Report Output Print

Printer At Client

Printer

Ok Exit

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.

5.7.1 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

5.8 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.

The screenshot shows a dialog box titled "User Profile Report". It has a "Report For" section with two radio buttons: "All Users" (selected) and "Selected". Below this is a "User Id" text input field. There are two rows of dropdown menus: "Report Format" set to "PDF" and "Report Output" set to "Print". On the right side, there are "Printer At" and "Printer" dropdown menus, with "Printer At" set to "Client". At the bottom right, there are "Ok" and "Exit" buttons.

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'.

5.8.1 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
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 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
------------------	-----------------------------------------------------------

5.9 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'.

5.9.1 **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:

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	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

5.10 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'.

5.10.1 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:

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. Function ID Glossary

S

SMDBKPRM 2-2
SMDCUUSR 5-4
SMDRLMNE 2-5
SMDUSALR 2-12
SMRMCLOG 5-9
SMRONSTA 5-8
SMRPCHLG 5-6

SMRPEVLG 5-1
SMRPINST 5-7
SMRPUSPR 5-11
SMRPVLLG 5-2
SMRROLPR 5-13
SMRUSREN 5-14
SMSBRNST 3-2