

FLEXCUBE Enterprise Limits and Collateral Management
Oracle FLEXCUBE Universal Banking
Release 12.1.0.0.1
[May] [2018]



Table of Contents

1. ABOUT THIS MANUAL.....	1-3
1.1 INTRODUCTION	1-3
1.2 AUDIENCE	1-3
1.3 ORGANIZATION	1-3
1.4 ACRONYMS AND ABBREVIATIONS	1-3
1.5 GLOSSARY OF ICONS	1-3
1.6 RELATED DOCUMENTS	1-5
2. GETTING STARTED - GENERAL FEATURES AND PROCEDURES.....	2-1
2.1 INTRODUCTION	2-1
2.2 LOGGING IN.....	2-1
2.3 ORACLE FLEXCUBE ELCM SYSTEM MAIN SCREEN.....	2-3
2.4 APPLICATION BROWSER	2-3
2.4.1 Menu Browser.....	2-4
2.4.2 Workflow Browser	2-6
2.5 MENU BAR AND TOOLBAR FEATURES	2-8
2.5.1 Changing the Branch.....	2-9
2.5.2 Using Screen Code to Invoke Screens.....	2-10
2.6 DATA ENTRY AND MAINTENANCE	2-10
2.7 DATA ENTRY SCREEN FEATURES	2-11
2.7.1 Field Types.....	2-11
2.7.2 LOVs	2-12
2.7.3 Multi Record Blocks.....	2-12
2.7.4 Maker/Authorizer Details	2-13
2.8 SUMMARY SCREENS	2-14
2.9 AUTOMATIC AUTHORIZATION	2-15
2.10 USER DEFINED FIELDS (UDF)	2-15
2.10.1 Maintaining User Defined Fields	2-15
2.10.2 Mapping Function Field.....	2-20
2.10.3 Viewing the UDF Sub-Screens.....	2-21
2.11 REPORTS GENERATION	2-21
3. SECURITY MAINTENANCE	3-1
3.1 INTRODUCTION	3-1
3.2 MAINTAINING BANK PARAMETERS FOR A BRANCH.....	3-1
3.2.1 Specifying Branch Restrictions	3-6
3.3 CLEARING A USER ID	3-7
3.4 MAINTAINING FUNCTION DESCRIPTIONS.....	3-7
3.5 MAINTAINING CODES FOR SYSTEM LANGUAGES.....	3-9
3.6 MAINTAINING USER ROLE LIMITS	3-10
3.7 DEFINING A USER ROLES.....	3-11
3.8 MAINTAINING SINGLE SIGN ON DETAILS.....	3-14
3.9 DEFINING AND MAINTAINING SYSTEM USERS.....	3-15
3.9.1 Roles	3-18
3.9.2 Functions	3-18
3.9.3 Branches	3-19
3.9.4 Restricted Passwords.....	3-20
3.9.5 Disallowed Functions	3-21
3.10 ACCESS GROUP MAINTENANCE.....	3-21
3.10.1 Maintaining Access Group	3-21

3.11	PERSONALLY IDENTIFIABLE INFORMATION	3-22
3.12	MASKING.....	3-25
3.13	FORGETTING CUSTOMER PROCESS	3-25
3.14	FORGETTING USERS	3-26
3.15	LOG ACCESS.....	3-27
3.15.2	Back-end Logs	3-27
3.15.3	Audit Logs.....	3-28
3.15.4	Purging Logs	3-28
3.16	USER ADMINISTRATION - BRANCH RESTRICTIONS	3-28
3.17	MAINTAINING USER DATA RESTRICTION	3-29
3.17.1	Category Restrictions Tab	3-30
3.17.2	Liability Restrictions Tab.....	3-31
3.17.3	Source Restrictions Tab.....	3-31
3.17.4	Currency Restrictions Tab.....	3-32
3.18	VIEWING USER DATA RESTRICTION.....	3-33
4.	CORE MAINTENANCES	4-1
4.1	INTRODUCTION	4-1
4.2	MAINTAINING YOUR BANK PARAMETERS	4-1
4.3	MAINTAINING BRANCH PARAMETERS	4-3
4.4	MAINTAINING ELCM BRANCH PARAMETERS	4-6
4.5	MAINTAINING YOUR BRANCH HOLIDAYS	4-7
4.6	MAINTAINING COUNTRY CODES	4-8
4.7	MAINTAINING CUSTOMER INFORMATION DETAILS	4-9
4.7.1	Maintaining Customer Source Details.....	4-11
4.8	STATIC MAINTENANCES	4-12
4.9	STATIC TYPE MAINTENANCE.....	4-17
4.10	MAINTAINING THE SYSTEM DATE	4-17
5.	MAINTENANCE.....	5-1
5.1	INTRODUCTION	5-1
5.2	MAINTAINING PRODUCT DETAILS	5-1
5.3	DEFINING AND MAINTAINING CURRENCY DETAILS	5-2
5.3.1	Performing Currency Country Mapping.....	5-4
5.4	MAINTAINING CURRENCY PAIRS FOR FOREIGN EXCHANGE	5-4
5.5	SPECIFYING EXCHANGE RATES	5-6
5.6	VIEWING EXCHANGE RATES HISTORY	5-7
5.7	MAINTAINING CURRENCY RATE TYPES.....	5-7
6.	GATEWAY MAINTENANCE.....	6-1
6.1	INTRODUCTION TO ORACLE FLEXCUBE ELCM GATEWAY	6-1
6.2	DEFINING AN EXTERNAL SYSTEM	6-1
6.3	DEFINING ACCESS RIGHTS TO AN EXTERNAL SYSTEM	6-3
6.4	EXTERNAL COMMUNICATOR	6-4
6.5	INTERFACE DEFINITION	6-5
6.6	DEFINING THE NOTIFICATIONS ENROUTE	6-7
6.7	DEFINING NOTIFICATIONS INSTALLED MESSAGES	6-8
6.8	INCOMING MESSAGE BROWSER.....	6-9
6.9	OUTGOING MESSAGE BROWSER.....	6-10
6.10	INPUT FILE PROCESSING	6-12
6.11	OUTPUT FILE PROCESSING SCREEN.....	6-13
6.12	INPUT FILE PROCESS AND OUTPUT FILE PROCESS MONITOR.....	6-14
6.13	MAINTAINING UPLOAD SOURCES.....	6-15
7.	END OF DAY PROCESS	7-2
7.1	INTRODUCTION	7-2

7.2	SYSTEM DATE MAINTENANCE.....	7-2
7.3	MAINTAINING MANDATORY BATCH PROGRAMS.....	7-2
7.4	RUNNING THE END OF DAY BATCH PROCESS.....	7-3
7.5	VIEWING THE AEOD PROCESS DETAILS.....	7-5
7.6	EOD BATCH PROCESSING POST EOTI.....	7-5
7.6.1	Market Revaluation Batch (Screen Code: GEBMAREV).....	7-5
7.6.2	Currency Revaluation Batch (Screen Code: GEBCYREV).....	7-5
7.6.3	Utilization Batch (Screen Code: GEBUTILS).....	7-6
7.6.4	Facility Batch (Screen Code: GEBFACLT).....	7-6
7.6.5	Collateral Batch (Screen Code: GEBCOLAT).....	7-6
7.7	INTEGRATING ORACLE FLEXCUBE EOD PROCESS WITH ELCM.....	7-7
7.7.1	Commitment Batch (Screen Code: ELBCOMNT).....	7-7
7.7.2	Running EOD Process.....	7-7
8.	ANNEXURE 1- PERSONALLY IDENTIFIABLE INFORMATION.....	8-9
8.1	CREATING/QUERYING CUSTOMERS OF RESTRICTED ACCESSGROUP.....	8-9
8.2	MASKED/UNMASKED PII.....	8-9
9.	SCREEN GLOSSARY.....	9-1
9.1	FUNCTION ID LIST.....	9-1

1. About this Manual

1.1 Introduction

This manual is designed to help you to quickly get acquainted with the Oracle FLEXCUBE Enterprise Limits and Collateral Management (hereafter referred to as Oracle FLEXCUBE ELCM) system. It provides an overview and takes you through the various steps involved setting up and maintaining the Oracle FLEXCUBE ELCM system.

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
Back office data entry clerk	Input functions for funds
Back office managers/officers	Authorization functions
Product Managers	Product definition and authorization
End of day operators	Processing during end of day/ beginning of day

1.3 Organization

This manual is organized into the following chapters:

Chapter 1	About This Manual
Chapter 2	Getting Started – General Features and Procedures in Oracle FLEXCUBE ELCM
Chapter 3	Security Maintenance Services
Chapter 4	Core Maintenances
Chapter 5	Currency Maintenances
Chapter 6	Gateway Maintenances
Chapter 7	End Of Day Processes





1.4 **Acronyms and Abbreviations**




















You may find the following acronyms/abbreviations in this manual.

UI	User Interface
ELCM	Enterprise Limits and Collateral Management
FCUBS	Oracle FLEXCUBE Universal Banking Solution
GW	Gateway
HTTP	Hyper Text Transfer Protocol
XML	eXtensible Mark-up Language
XSD	XML Schema Definition
XSLT	eXtensible Stylesheet Language Transformations
BPEL	Business Process Execution Language
SMS	Security Services
ID	Identification Number
PK	Primary Key
RDBMS	Relational Data Base Management System
VD	Value Date
Mark EOTI	Mark End of Transaction Input
Mark TI	Mark Transaction Input
TD	Term Deposits
CIF	Customer Information File

1.5 **Glossary of Icons**

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

Icons	Function
	New
	Copy
	Save
	Delete

Icons	Function
	Unlock
	Print
	Close
	Re-open
	Reverse
	Template
	Roll-over
	Hold
	Authorize
	Liquidate
	Exit
	Sign-off
	Help
	Add row
	Delete row
	Option List
	Confirm
	Enter Query
	Execute Query

Refer the Procedures User Manual for further details about the icons.

1.6 **Related Documents**

- Oracle FLEXCUBE Enterprise Limits and Collateral Management User Guide

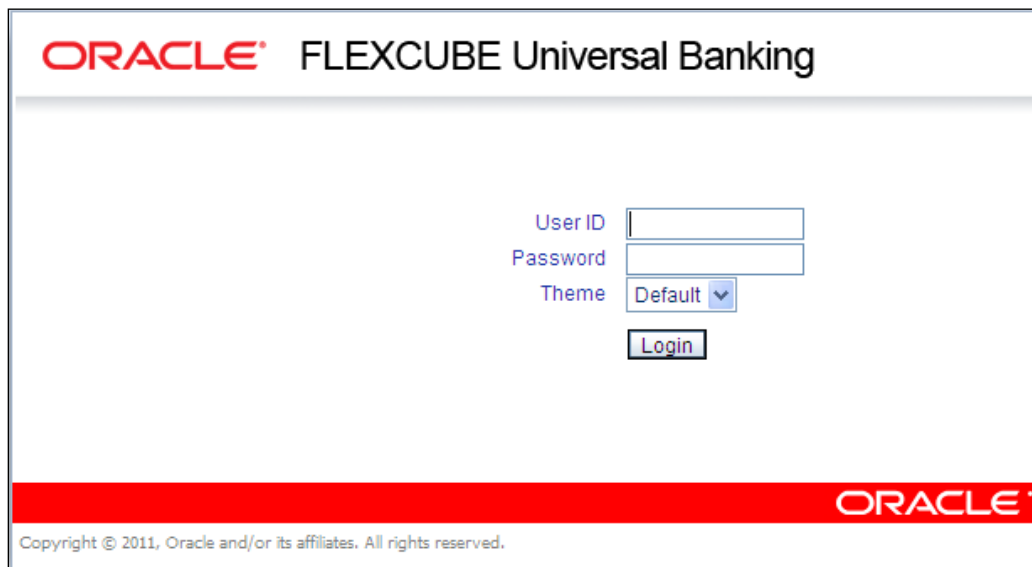
2. Getting Started - General Features and Procedures

2.1 Introduction

Oracle FLEXCUBE Enterprise Limits and Collateral Management is an enterprise application that enables banks to gain a holistic view of their exposure by centralizing limits definition process and collateral management. It is a real-time solution for exposure tracking, credit facility creation and renewal, collateral pooling and collateral valuation. It is capable of multi-currency, multi-entity and multi-instance operations.

2.2 Logging In

The Log In window to the Oracle FLEXCUBE Enterprise Limits and Collateral Management (Oracle FLEXCUBE ELCM) system is shown below.




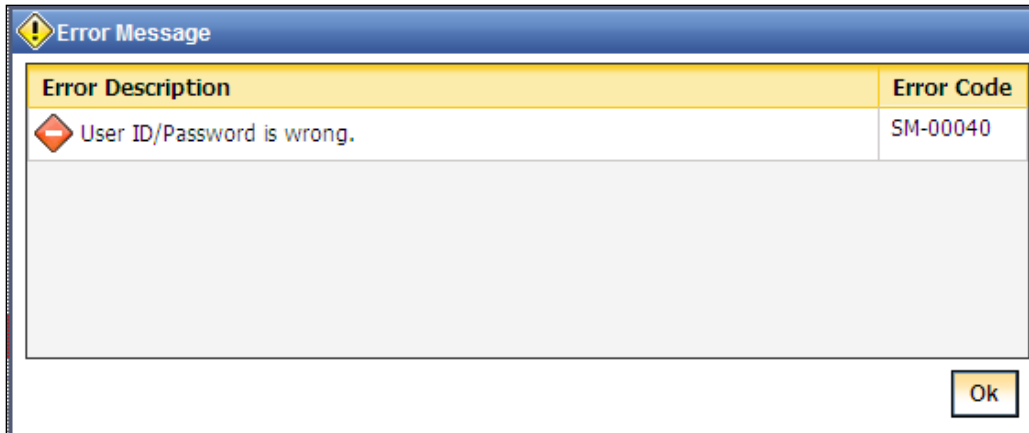
The screenshot shows the Oracle FLEXCUBE Universal Banking login interface. At the top, the Oracle logo is followed by the text 'FLEXCUBE Universal Banking'. Below this, there are three input fields: 'User ID', 'Password', and 'Theme'. The 'Theme' field is a dropdown menu currently set to 'Default'. Below these fields is a 'Login' button. At the bottom of the window, there is a red horizontal bar with the Oracle logo on the right and the copyright text 'Copyright © 2011, Oracle and/or its affiliates. All rights reserved.' on the left.

You can log into the system by entering your 'User ID' and 'Password'. Only users with valid access rights – a valid User ID and Password – can log into the system.

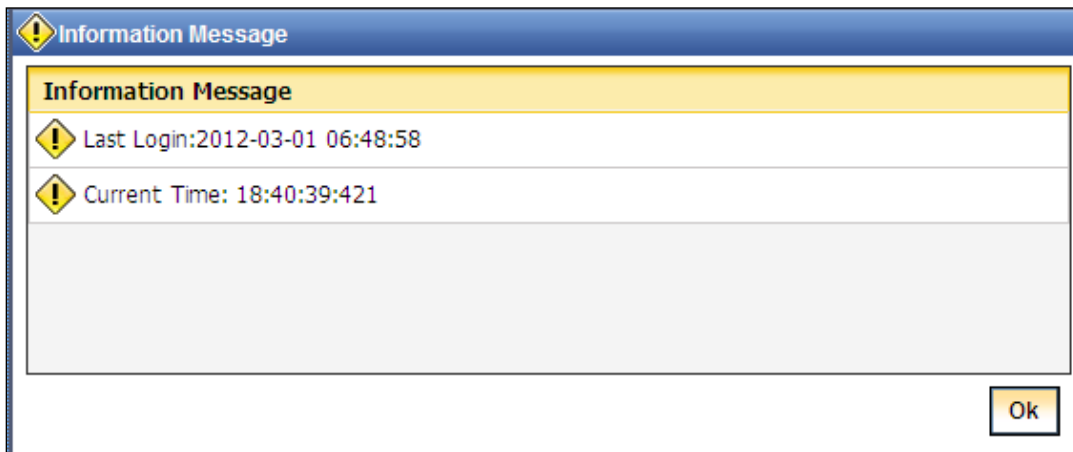
You may also select different background 'themes' for the user interface. The themes available are Default, Sandstone, and Classic.

Click 'Submit' button to login to the system.

 In case your User ID or Password (or both) is wrong, then the following screen is displayed. Click 'Ok' to try logging in again.



Upon successful login you are shown a message displaying the last login into the system.



Click 'Ok' to proceed.

When you log in for the first time you will be forced to change your password if the 'Force Password Change' option has been selected in User Profile Definition.



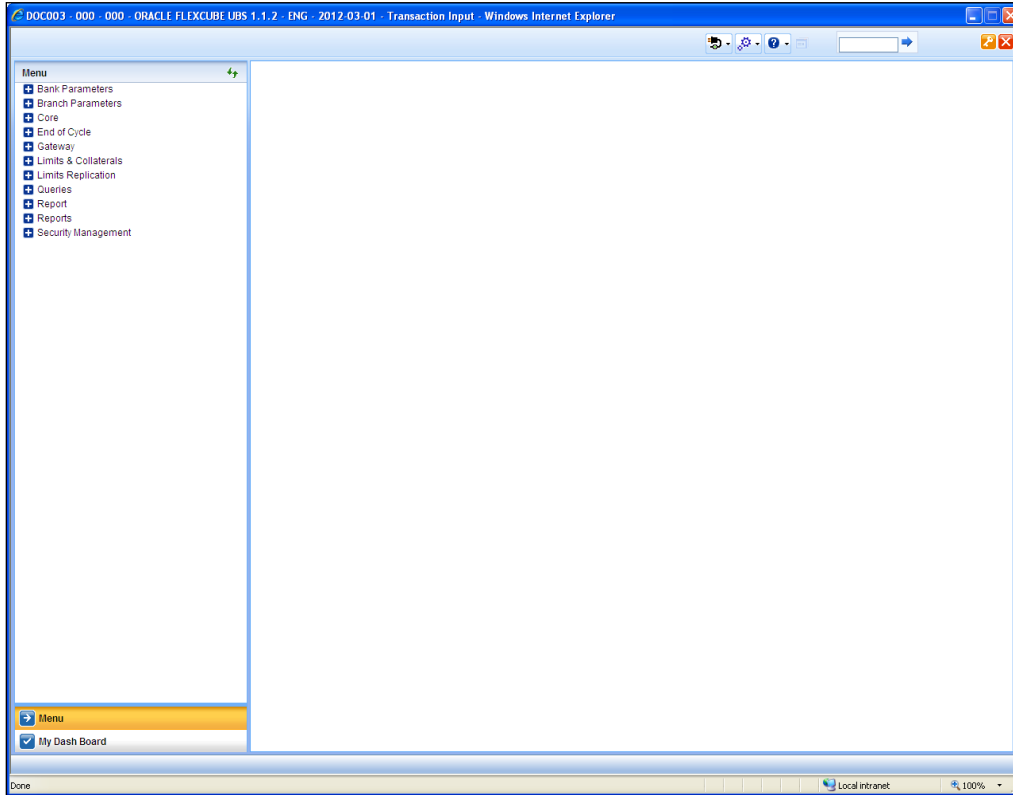
Your user profile will be disabled under any one the following circumstances:

- Number of successive invalid login attempts defined for your user ID has been reached
- Cumulative number of invalid login attempts defined for your user ID has been reached

In the above cases a message conveying that your user profile has been disabled will be displayed.

2.3 Oracle FLEXCUBE ELCM System Main Screen

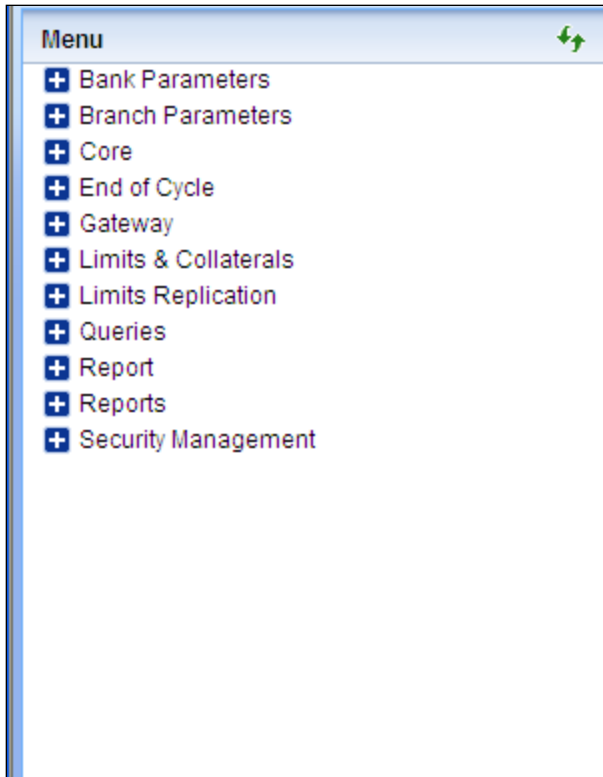
The Main screen of the Oracle FLEXCUBE ELCM system will be displayed on successful login as shown below.



The features of the main Oracle FLEXCUBE ELCM screen is are described in the sections below.

2.4 Application Browser

The Application Browser is the vertical bar found on the left side of the Main screen.



2.4.1 **Menu Browser**

The Menu Browser contains the operational modules to which you have access rights. For you, the Menu Browser may display some or all of the following modules depending on your access rights:

- Bank Parameters
- Branch Parameters
- Core
- End of Cycle
- Gateway
- Limits & Collaterals
- Limits Replication
- Queries
- Reports
- Security Management

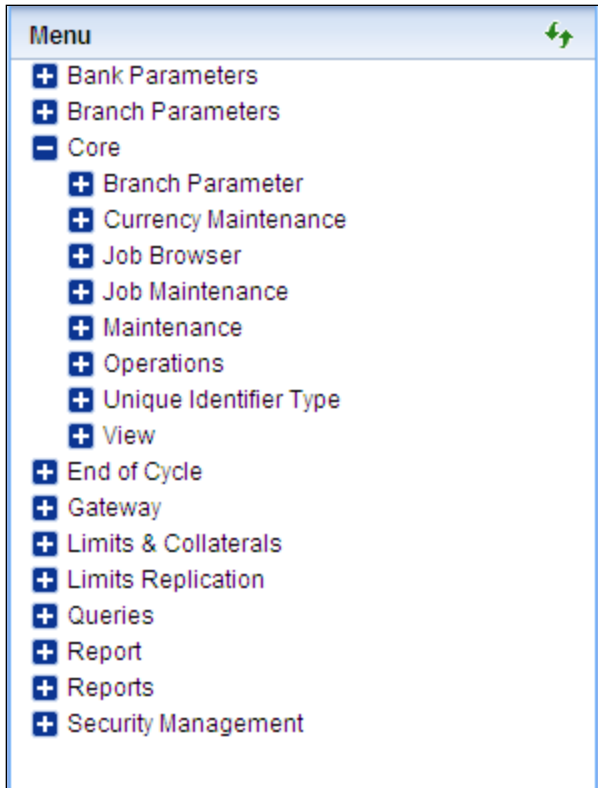
All your maintenances and operations are done via the screen available under the Menu Browser. The chapters in this user manual are also named according to the Menu Browser modules.

For more details on the Menu Browser modules, refer the relevant chapters.

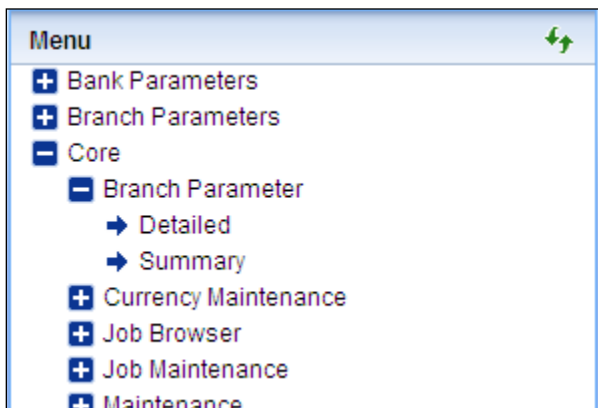
2.4.1.1 **Operating Menu Browser**

In the Menu Browser only the names of the operational modules are displayed.

To go to a particular screen under a module, click the module name. A collapsible list of functions available for that particular module will be displayed as shown below.



Click on a function to view its list of sub-functions.



Click on the item you need. The screen for the particular item will be displayed.

Example

If you click on Core, one of the functions you see displayed is Amount Text. If you click Amount Text the options available under it will be displayed:

- Detailed
- Summary

Click on any of the above to see the respective screen displayed.



Only those functions to which you have access rights in a module are displayed. If you do not have access rights to the module then the module is not displayed.

2.4.1.2 Operating the Screen Displayed

The screen displayed on clicking an item, from a Menu Browser function, is most often in view only mode. It can either be an existing record or a blank record. You can either create a new record or modify the existing record.

Creating a New Record

To create a new record, select 'New' from the Actions menu in the Application tool bar or click new icon.

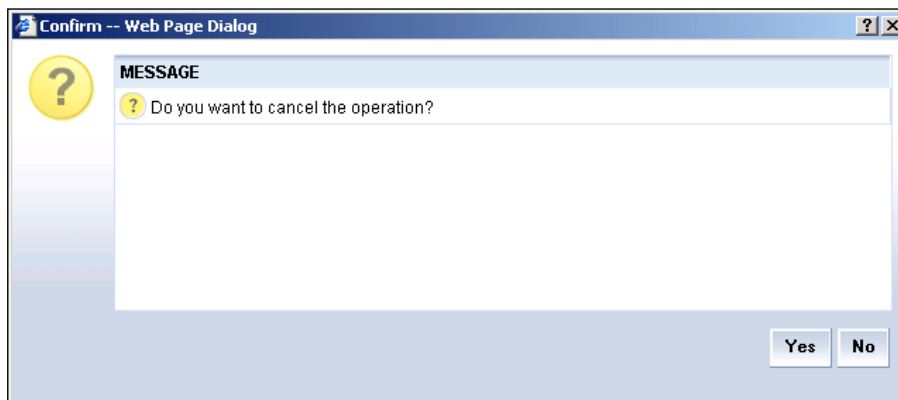
The fields in the screen will be enabled for entry. Upon finishing your entries, select 'Save' from the Actions menu in the Application tool bar or click save icon. Then click 'Exit' button to exit the screen.

Modifying an Existing Record

To modify an existing record, select 'Unlock' from the Actions menu in the Application tool bar or click unlock icon to unlock this record. This enables you to make the desired modifications in the screen.

On clicking 'Unlock' icon, 'Exit' button has changes to 'Cancel' button and 'Save' is enabled. Once your new entries are made, select 'Save' from the Actions menu in the Application tool bar or click save icon. Then click 'Exit' button to exit the screen.

If you do not want to save your changes, click 'Cancel'. A message gets displayed.



Click 'Yes' button to save your changes.

Click 'No' button to exit without saving the changes.

2.4.2 Workflow Browser

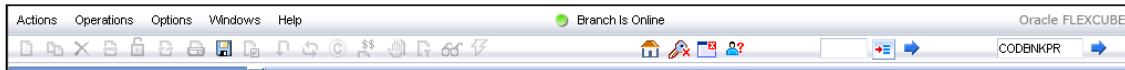
The Workflow Browser lists various task lists as given below:

- Pending
- Assigned
- Failed
- Un-assigned
- Asynchronous
- Completed








- Reversed
- Tanked
- Un-Tanked
- Search Tasks







2.5 Menu Bar and Toolbar Features

The Menu and Toolbar are found at the very top of the Main screen.



The Menu Bar and Toolbar operations are explained below.

Toolbar Icon	Menu Bar Path	Action
	Actions - New	New - Displays a record with no data so that you can enter data to create a new record
	Actions - Copy	Copy - Copies the details of the record on display on to a new record
	Actions - Delete	Delete - Deletes the details from the record on display
	Actions - Close	Close - Close a contract
	Actions - Reopen	Reopen - Reopen a closed contract
	Actions - Unlock	Unlock - Unlocks a record enabling you to make changes
	Actions - Print	Print - Prints details of the record on display
	Actions - Save	Save - Enables you to save the new record/changes you have made on the record on display
	Actions - Authorize	Authorize - Activates the authorization function. Authorization has to be done by a user other than the one who has created or modified a record. Authorization is normally done during End of Day processing.
	Operations - Reverse	Reverse
	Operations - Rollover	Rollover
	Operations - Confirm	Confirm
	Operations - Liquidate	Liquidate - Activates the liquidation function

Toolbar Icon	Menu Bar Path	Action
	Actions - Hold	Hold
		Template
		Generate
		Click to return to Home Branch operation
	Actions – Sign Off	Click to sign off from your login
	Actions - Exit	Click to Exit from and close the Oracle FLEXCUBE ELCM system

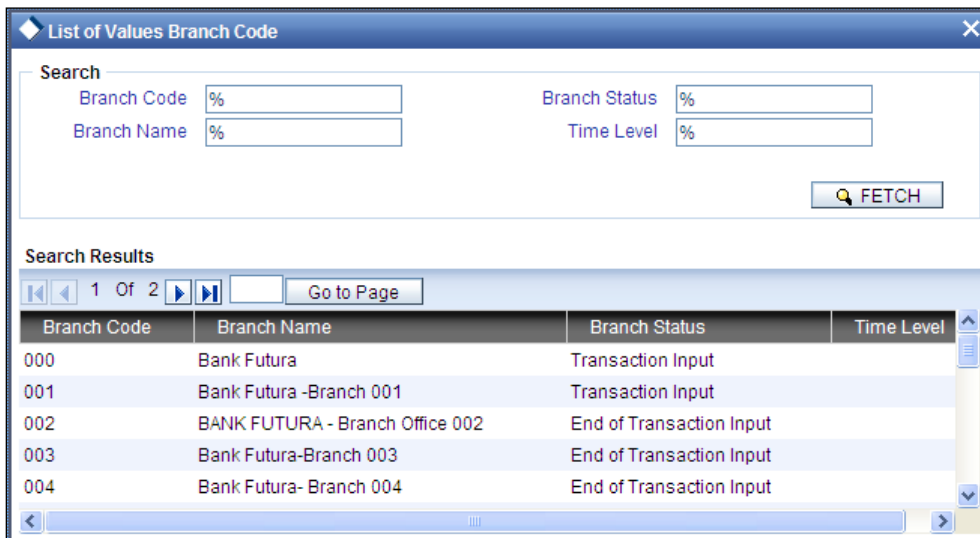
2.5.1 Changing the Branch

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

To change the branch you are operating from, use the feature shown below.



Click the adjoining option list to invoke the list of Branch Code as shown below.



List of Values Branch Code

Search

Branch Code

Branch Name


Branch Status

Time Level

Search Results

1 Of 2

Branch Code	Branch Name	Branch Status	Time Level
000	Bank Futura	Transaction Input	
001	Bank Futura -Branch 001	Transaction Input	
002	BANK FUTURA - Branch Office 002	End of Transaction Input	
003	Bank Futura-Branch 003	End of Transaction Input	
004	Bank Futura- Branch 004	End of Transaction Input	

From this list, click the Branch Code of the branch you wish to operate on. Next click  to change your operation to the selected branch.

2.5.2 Using Screen Code to Invoke Screens

To invoke a particular screen, you can use the Screen Code for the screen. Use the field at the top right corner of the Application Toolbar.



Enter the <Screen Code> of the screen you wish to invoke and then click the adjoining arrow button.



This facility is applicable only to Parent Screens and not to screens which are invoked from other screens.

2.6 Data Entry and Maintenance

Your inputs into the Oracle FLEXCUBE ELCM are of the following two types:

- Maintenances necessary for the system operation
- Recording customer transactions

For the above actions, the Oracle FLEXCUBE ELCM system has the following functionalities respectively:

- Functions that is necessary for the system's operation like Maintenance screens. These can be input via:
 - Direct Transaction Input
 - Workflow Transaction Input
- Functions that support customer transactions like Transaction entry screens.

Direct Transaction Input refers to cases when complete transaction details are available and are entered/ recorded in the system. After data entry, a user with proper Authorization Rights must authorize the transaction in the same day.

Direct transaction input involves two screens:

- Detailed screens – To enter or view all the data associated to the function/screen
- Summary screens – To set values for a predefined set of fields and then query for results based on it from the database.

Following actions are allowed for Direct Transaction Input:

Action	Select the action to
New	Create a new record
Modify	Modify an existing record
Close	Close a record. A closed record cannot be used for business transactions.
Reopen	Reopen a closed record
Delete	Delete a record from the database. A deleted record cannot be recovered.
Authorize	Authorize a record. Authorization of a record enables it for business transactions.
Query	Query a record from database. The query condition is based on the values provided for the primary fields. Use the Summary screen to query records for any other criterion. Query action gives only one record or no record as a result since it is based on just the primary field of the record.
Copy	Copy a record for re-using the entries in it for another record. You must query a record in order to copy. All the values except for primary fields are retained in Copy action.

2.7 Data Entry Screen Features

The following sections explain features commonly seen in most 'Detailed' screens and other screens which allow data entry.

2.7.1 Field Types

You will encounter three types of fields in most screens:

- Mandatory fields
- Optional fields
- Conditional fields

Mandatory Fields

Of the many fields in a screen, the inputs to some may be mandatory. This means that you cannot save your record without giving a valid input in such fields. Mandatory fields are denoted by an * in red.

A screenshot of a text input field. The label 'Bank Code' is in blue. To its right is a red asterisk, followed by the text 'CHO' in blue. The input field has a thin border and a small cursor at the end.

Optional Fields

The inputs to some of the fields in a screen may be optional. You may or may not give an input to such fields. Further, an optional field may have a default value; a value that the system puts in the field if you do not enter anything. Unless you change this default value, it will be taken as the input to the field. However, please note that all optional fields need not have default values. It is possible that some fields can be left blank.


Conditional Fields

There are some fields, which take input based on data in some other field(s). For example, in the Loans and deposits module, you have to specify the Cluster ID only if you are processing a deposit. It is not unusual that a conditional field also has a default.

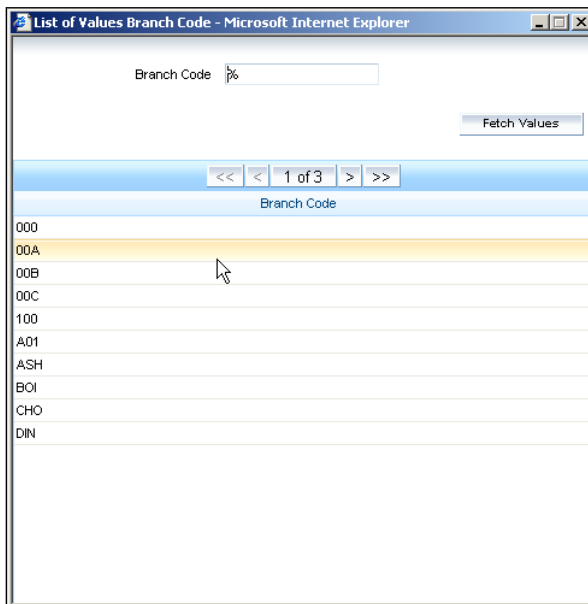
2.7.2 LOVs

Inputs to certain fields can be selected from the option list provided with the field. This option list will contain values that are valid inputs to the field. If a field has an option list, it will have an icon against it.

For example, consider the following field:



This field requires you to specify the branch code for an operation. If you click the option list, the system will display all valid inputs permitted to this field, as shown:



From this list, you can select an appropriate value. You will come across option lists whenever an entry into a field is based on prior records.

2.7.3 Multi Record Blocks

At times, you may need to maintain a number of records of the same nature, as part of a single transaction. Multi record blocks provides for such maintenances. Following is an example of a multi record block.

Currency Rates						
<input type="checkbox"/> Rate Type *	Mid Rate	Buy Spread	Sale Spread	Buy Rate	Sale Rate	
<input type="checkbox"/> CASH						
<input type="checkbox"/>						
<input type="checkbox"/>						

In the above instance, you can maintain a number of currency rates within the same screen. You may add more rows to the table using 'Plus' button. At any time during the entry, if you feel that a particular row is not required, you can check the box adjacent to the row and click 'Minus' to remove it. Additionally, you can view further details of a single record on the multi record block using 'Details' button.

2.7.4 Maker/Authorizer Details

Maker is a user who actually inputs details into the system. The system requires each such entry to be verified and authorized by a different user, called 'Authorizer'. Towards the bottom, on most screens, you will observe some details as shown:

Input By HANIT1	Date Time 9/19/2008 17:04:00	Modification Number 2	<input checked="" type="checkbox"/> Open	Exit
Authorized By HANIT	Date Time 9/19/2008 17:04:52		<input checked="" type="checkbox"/> Authorized	

This portion of the screen displays the following details:

- **Input By:** This is the name of the maker, who has actually input the details. The date and time of this entry is displayed adjacent to it.
- **Authorized By:** This is the name of the authorizer who verifies the details. The date and time of verification is displayed adjacent to it. The checkbox 'Authorized' will be clear for an entry which has not been authorized. In that case, you will not find any details of the authorizer.

2.8 Summary Screens

You can maintain a number of records in the system. A summary screen serves as a single window to access all records that bear the same characteristics. Summary screens display the details pertaining to each such record in a tabular format. You can browse such details and view the actual record on clicking a result record.

The screenshot displays the 'Facilities Summary -- Web Page Dialog' window. It features search filters at the top: Authorization Status (dropdown), Facility Code (text input), Line Currency (text input), Record Status (dropdown), Serial Number (text input), and Available Amount (text input). Below these are buttons for 'Search', 'Advanced Search', and 'Reset'. A table below shows a list of records with columns: Authorization Status, Record Status, Facility Code, Serial Number, Line Currency, Liability Id, Main Line, Available Amount, ID, and Line Start Date. The table contains 15 records. At the bottom, there are legends for Authorization Status (A - Authorized, U - Unauthorized) and Record Status (C - Closed, O - Open). An 'Exit' button is located at the bottom right.

Authorization Status	Record Status	Facility Code	Serial Number	Line Currency	Liability Id	Main Line	Available Amount	ID	Line Start Date
A	O	MLINECD01	8	USD	1001		685,000.00	1112	10/15/2008
A	O	SLINECD01	6	USD	1001	1112	485,000.00	1113	10/15/2008
A	O	MLINECD01	11	USD	1001		500,000.00	1201	10/15/2008
A	O	MLINE01	1	USD	1201		700,000.00	1202	10/18/2008
A	O	MLINE01	1	USD	1202		700,000.00	1203	10/18/2008
A	O	MLINE01	1	USD	2805		694,651.00	4801	10/20/2008
A	O	Z991	1	USD	1103		0.00	5002	10/15/2008
A	O	MLINE01	2	USD	2805		700,000.00	5103	10/15/2008
A	O	Z91	1	USD	1003		101,680.00	5301	10/15/2008
A	O	Z92	1	USD	1003		933.33	5302	10/15/2008
A	O	MLINE01	1	USD	3005		90,000.00	5401	10/15/2008
A	O	MLINE01	5	USD	1004		247,000.00	5402	10/29/2008
A	O	MLINE01	6	JPY	1005		12,098,140.00	5403	10/29/2008
A	O	MLINE01	1	USD	1002		100,000.00	5501	10/29/2008
A	O	MAINLINE01	1	USD	1007		100,000.00	5502	10/29/2008

On a summary screen, you can query the records based on various parameters. For instance, on the above screen, you can specify an Authorization Status in the given space and click 'Search' button to view all records that uses the same transaction code. Similarly, you can query the details based on different parameters, specific to each screen.

Advanced Search

The results displayed in usual summary view may amount to hundreds. To avoid wading through this mass of data, you can make a query to see only those records which are relevant to you at a particular time. The Advanced Search screen makes this possible. For this, click 'Advanced Search' button.

2.9 Automatic Authorization

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

When automatic authorization takes place,

- The authorization screen is not opened. Authorization is considered as full or complete authorization, which would mean that all unauthorized changes to the record would be authorized.
- The re-key fields configured for authorization in respect of the function are not required to be entered by the user.
- Messages in respect of overrides are not displayed, but are internally authorized. Similarly, overrides requiring confirmation are also automatically confirmed.
- Any applicable online message are generated and displayed. The user can respond based on the error type – For 'Ignore' error types, the system automatically generates the messages; for 'Override' error types, the user is prompted about whether message generation is required; for 'Error' error types, messages are not generated.
- The user's authorization limit is checked when automatic authorization takes place
- The maker/ checker validation is not performed when automatic authorization takes place

2.10 User Defined Fields (UDF)

You may wish to have your own additional fields in the Oracle FLEXCUBE ELCM system. These fields can be for your convenience or to suit the requirements of your bank. Limit Server facilitates this via the User Defined Fields (UDF) feature.

For you each UDF you can specify default values and validations for the field. Oracle FLEXCUBE ELCM system will validate all entries made using validations you define for a field.

2.10.1 Maintaining User Defined Fields

User Defined Fields can be defined using the 'User Defined Field Maintenance' screen. You can invoke the 'User Defined Field Maintenance' screen by typing 'UDDMNTFN' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Field Name and Description

To identify a field that you create name it with a unique identifier. Each field that you define in Oracle FLEXCUBE ELCM should be assigned a unique code. You can briefly describe the field in Description field. The description is for your information only. It will not be printed on any customer correspondence.

Field Type

The type of field that you can create in Oracle FLEXCUBE ELCM can be of the following formats:

- Number — Select this option to create a Numeric field
- Text — Select this option to create a Text field
- Date— Select this option to create a Date field
- Cube Entity —should you need to reuse any of the existing fields of Oracle FLEXCUBE ELCM, to enter additional details you can indicate the Field Type as Cube Entity. The Cube Entity can be any of the existing fields in Oracle FLEXCUBE ELCM like customer, currency, account, etc

Mandatory

You can make entry to a field mandatory. To do so select the 'Mandatory' check box. Leave it unselected to indicate that the field is not mandatory.

Usage Allowed

While defining a new User Defined Field, the scope or usage of the field that is being defined should be specified as 'Function' here.

Function

You can specify here the function Id of the screen in which the new field has to be used. Select the function ID from the list positioned next to this field. The function IDs of all the maintenance screens will be available here

For example, if you want to use the new field in the 'Collateral Types Maintenance - Detailed' screen, select the Function Id GEDCOLTY, thus allowing the usage of the field in the Collateral Types Maintenance screen only.

Amendable

You may choose to modify the value of a field after it is populated in the 'User Defined Field'/'Field Name to Value Definition' screen of Contract Input or Function Id screen. To allow amendments to the values after they are populated, select the 'Amendable' check box at the time of defining a new field.

2.10.1.1 Defining a Numeric Field

To define a numeric field, select 'Number' against 'Field Type'. You can set up validation rules for a numeric field using one of the following validation types:

- Range
- Length
- LOV
- None

Indicate your preferred validation type against the 'Validation Type' field. Select 'None' to indicate that no validation should be performed on entries made to this field.

Validation Type - Range

The Range validation type is applicable only to Numeric fields. In this validation you can specify the permissible range of values which can be entered in your field.

Specify your range using the 'Minimum Value' and 'Maximum Value' fields. Any valid entry to your field should be within the range specified.

Validation Type - Length

Select the validation type as 'Length' to indicate that the entry should be of a certain length. The length can either be fixed or can be within a maximum and minimum specified length.

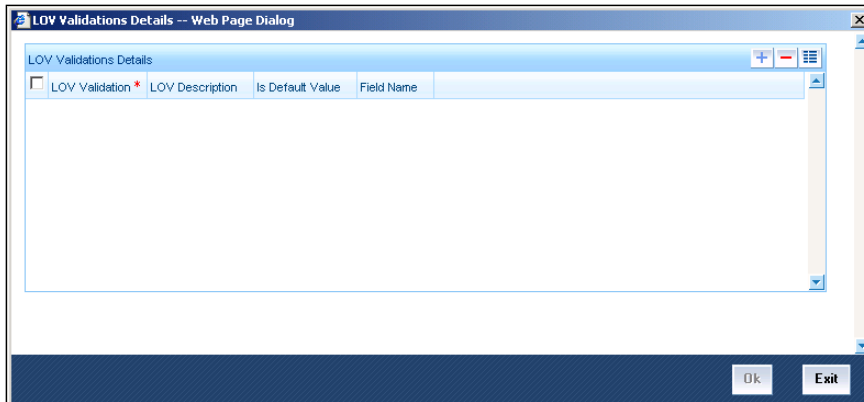
To specify a fixed length, select the 'Fixed Length' check box. Then specify the length against the 'Fixed Length' field.

Alternatively you may specify a length range using a maximum and minimum length. For this leave the Fixed Length check box un-selected. Then specify the length range using the 'Maximum Length' and 'Minimum Length' fields.

Validation Type - LOV (List of Values)

Select LOV to indicate that the entry to this field can be chosen from a predefined list.

To define the items that should be displayed on this list, click 'LOV' button. In the 'LOV Validation Details' screen you can define the list of values and their description. The items that you define for the list are displayed whenever the field is used.



2.10.1.2 Defining a Text Field

To define a text field, choose 'Text' against 'Field Type'.

A text field can contain alphabets of the English language or a combination of alphabets and numeric values.

You can specify validation rules using one of the following validation types applicable to a text field:

- Length
- Mask
- LOV
- None

You can indicate your preference at the Validation Type field of this screen. Choose 'None' to indicate that no validation should be performed on entries made to this field.

Validation Type - Length

Select the validation type as 'Length' to indicate that the entry should be of a certain length. The length can either be fixed or can be within a maximum and minimum specified length.

To specify a fixed length, select the 'Fixed Length' check box. Then specify the length against the 'Fixed Length' field.

Alternatively you may specify a length range using a maximum and minimum length. For this leave the Fixed Length check box un-selected. Then specify the length range using the 'Maximum Length' and 'Minimum Length' fields.

Validation Type - Mask

If you wish specify a data entry format in alphabets and numbers (i.e. a Mask) for a text field, then select the 'Mask' Validation Type.

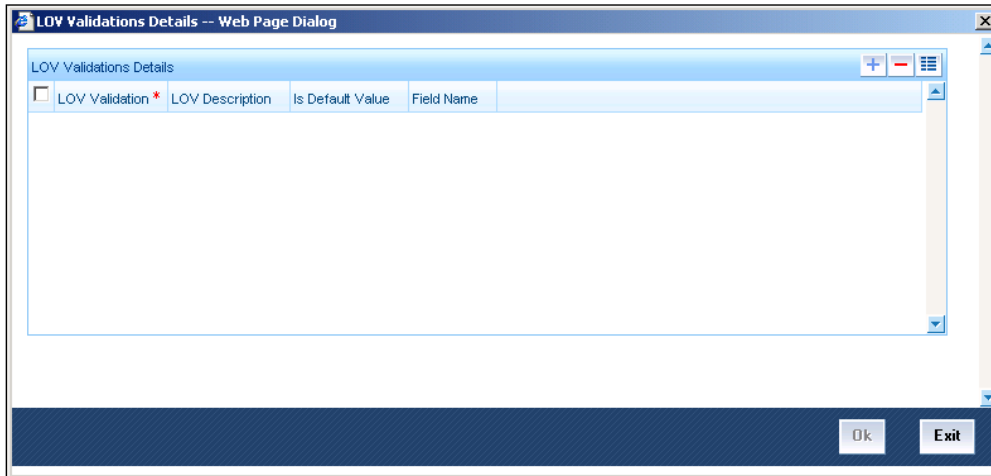
The Mask's format structure can consist solely of "a" or "n" or a combination of these. An "a" indicate an alphabet of the English language and "n" a numeric value. Specify your mask format against the 'Mask' field.

All entries made to the field will be validated against the format that you specify for the mask.

Validation Type - LOV (List of Values)

Select LOV to indicate that the entry to this field can be chosen from a predefined list.

To define the items that should be displayed on this list, click 'LOV' button. In the 'LOV Validation Details' screen you can define the list of values and their description. The items that you define for the list are displayed whenever the field is used.



2.10.1.3 Defining a Date Field

To define a Date field, select 'Date' as the Field Type. The validation types applicable to a date field are:

- LOV
- None

Select 'LOV' button so that an entry to the field can be made only from the predefined list that you maintain for the field. Select 'None' to indicate that no validation should be made for the field.

Back Dates and Future Dates

For a Date field, you can specify whether back and future dates can be entered. You can also specify how many days into the past or future the date entered can be.

To allow entry of past dates, select the 'Back Dates' check box. Then against 'Period Days', you must specify the number of days, into the past, up till when the Back Date entered can be.

To allow entry of future dates, select the 'Future Dates' check box. Then against 'Period Days', you must specify the number of days, into the future, till when the Future Date entered can be.

Example

If you indicate "3" as the back date period, the field will accept dates up to three days before the current system date as a valid entry.

2.10.1.4 Defining a Cube Entity

To reuse any of the existing fields of the Oracle FLEXCUBE ELCM application, specify the Field Type as 'Cube Entity'. Select the field type as 'Cube Entity'. Then click 'Cube Entity' to invoke the 'Cube Entity' screen.

A dynamic query can be written for the corresponding field. Through this query system will validate the entries made at the maintenance screen level for the new UDF defined.

If the field type is 'Cube Entity', the values of a field can be selected from Oracle FLEXCUBE ELCM tables. In the 'Cube Entity' screen, you need to specify the required Select Query which should select only one column.

Example:

You need to capture details of an additional branch for a maintenance/transaction. You can choose the Cube Entity field type and write a query for the defined field as

```
SELECT BRANCH_CODE FROM STTM_BRANCH WHERE BRANCH_LCY = 'USD'
```

The list of branches maintained according to the above query will be taken for validating with the input to the UDF field at the maintenance screen level

2.10.2 Mapping Function Field

To invoke the 'User Defined Fields Function Field Mapping' screen, first select 'User Defined Fields' from the Application Browser. Under it, click 'Field Mapping' and then click on the 'Detailed'. You can invoke the 'User Defined Fields Function Field Mapping' screen by typing 'UDDFNMT' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

In the above screen you can map the fields to be included in the specified Function ID/screen.

Function

You can specify here the function Id of the screen in which the new field has to be used. Select the function ID from the list positioned next to this field. The function IDs of all the maintenance screens will be available here.

Field Name

Specify the field name that should be mapped\used in the above function ID\maintenance screen.

2.10.3 Viewing the UDF Sub-Screens

You can view the User Defined Fields maintained for a particular screen/function in the UDF sub-screen of that screen.

To view the 'UDF' sub-screen, if any, for a screen, you need to click the 'Fields' button on that screen.

2.11 Reports Generation

Reports spooling will be a part of Oracle FLEXCUBE ELCM environment. The extracted reports can be handed off to a given External Report Analysis System. Oracle FLEXCUBE ELCM supports spooling of Reports for analysis.

The Oracle FLEXCUBE Enterprise Limits and Collateral Management system supports generation of the following reports as part of an external Oracle BIP Reports facility.

Report Id	Description
ELRPCOLT	Collaterals details
ELRPISUR	Issuer details

Report Id	Description
ELRPLIMT	Limit details
ELRPSECM	Securities
ELRPCLMT	Credit lines by maturity dates
ELRPOLNK	Pool Linkage report
ELRPCNEX	Country exposure report
ELRPCOUL	Collateral utilization of collateral party report
ELRPCOUT	Collateral utilization of credit lines
ELRPLIAB	Credit rating details
ELRPCRMO	Credit movements report
ELRPCUTI	Country utilization report
ELRPOLUT	Pool utilization report
ELRPISEX	Issuer exposure report by collateral type
ELRPLB	Liability summary report
ELRPLN	Line details report
ELRPML	Line summary report
ELRPNRLN	Movements to non-revolving lines
ELRPOVLN	Overdrawn lines
ELRPUTLD	Utilizations report -- date wise
ELRPUSEX	Issuer exposure report by security
ELRPUA	Utilizations report
ELRPPREX	Product Exposure Report
ELRPUT	Limits - Tenor wise Details Report
ELRPTN	Limits - Tenor wise Details Report
ELREXPSD	Exposure Details

3. Security Maintenance

3.1 Introduction

The SMS module of the Oracle FLEXCUBE Enterprise Limits and Collateral Management (hereafter referred to as Oracle FLEXCUBE ELCM) provides the following two functionalities:

- User Authentication
- User Authorization

The SMS module has maintenances which help to control user access to various other functionalities of the system.

SMS Module Features

- Only authorized users access the system – Logging into the system
- Creating User Roles and User Profiles
- Restricting the number of unsuccessful login attempts
- Restricting access to branches
- Tracking all the activities in the system – With respect to users?
- Providing Audit Trails

3.2 Maintaining Bank Parameters for a Branch

There are certain security parameters which are maintained specifically for each branch. These parameters apply to all users in the branch. The following are examples of such parameters:

- Parameters for password maintenance
- Parameters for Invalid login attempts

You can maintain bank level security parameters in the 'Bank Parameters Maintenance' screen. You can invoke the 'Fund Product Preferences Class Summary' screen by typing 'SMDBNKPR' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Enter the following details:

Site Code

Specify the site code of the bank branch site here.

Head Office

Specify the Head Office code of the branch's Head Office here

Invalid Logins – Cumulative and Successive

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 any of these are provided wrongly, it amounts to an invalid login attempt.

Against 'Cumulative' specify the maximum allowable number of cumulative invalid attempts made during the course of a day or made at a time. In either case, if the number of invalid attempts exceeds the specified number, the user ID will be disabled.

Against 'Successive' specify the maximum number of successive invalid login attempts. If the number of invalid attempts exceeds the specified number, the user ID will be disabled.

Once specified, you can change the allowable number of cumulative or successive 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.

Idle Time

Specify the allowable idle time (in seconds) that a user can spend without performing any activity, after logging in to the system. If no activity has been performed up to the end of stipulated idle time, the user is automatically signed off when the idle time has elapsed.

You can specify the idle time as any period between 30 and 600 seconds, inclusive.

Override Idle Time in Seconds

Specify the allowable time (in seconds) within which a response to an override must be entered. If no response is given up to the end of stipulated override idle time, the response to the override is deemed as 'Cancel', which means the override has been rejected.

Password Repetitions

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

Force Password Change after

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

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

Intimate Users (before password expiry)

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

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

Force Password change for a new user/Reset

You can indicate whether a new user should be forced to change the user password during the first login after the profile is created. If you indicate so, when a new user logs in for the first time after the profile has been created, a password change will be mandated by the system.

Minimum Days between Password Changes

You can specify the minimum number of calendar days that must elapse after a user changes the user password, after which the user can effect another password change. After a user has changed the user password, it cannot be changed again until the number of days you specify here has elapsed.

Dormancy Days

You can set the system to automatically disable the profile of all the users who have not logged in for a specified 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 here. This is 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.



You can modify the number of Dormancy Days only when your branch is in the transaction input stage.

Display Legal Notice

Select this check box to use the 'Warning Screen Text' option.

Warning Screen Text

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

You can specify the text (content) of such a message, in the Warning Screen Text field. This message will be displayed soon after a user initiates login. The user will be allowed to continue with the login process only after he clicks 'OK' button on the message window.

You can modify the contents of the message only during the transaction input stage. The changes will come into effect during the next login by a user.



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

Specifying Forget User Details

No of Days to Forget User

Enter the number of days, after which the system will forget user after they are not associated with the bank anymore. Once the user is forgotten you cannot view the details of the user.

Mask Character

Enter the character that you want to use to mask the user information, so that it is not visible to anyone.

Password Length (characters) – Maximum and Minimum

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

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

Maximum Consecutive Repetitive Characters

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

Minimum Number of Special Characters in Password

You can define minimum number of special characters allowed in a user password. The system validates these specifications only when a user chooses to change the password.

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

- Minimum No of Special Characters = 1

Minimum Number of Numeric Characters in Password

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

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

- Minimum No of Numeric Characters = 1



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

Minimum Number of Lower Case Characters in Password

You can define the minimum number of lowercase characters allowed in a user password. The allowed lower case characters are from the US-ASCII character set only. The system validates these specifications only when a user chooses to change the password

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

- Minimum No of Lower Case Characters = 1
- Maximum No of Numeric Characters = Maximum Password Length

Minimum Number of Upper Case Characters in Password

You can define the minimum number of upper case characters allowed in a user password. The allowed upper case characters are from the US-ASCII character set only. The system validates these specifications only when a user chooses to change the password

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

- Minimum No of Upper Case Characters = 1
- Maximum No of Numeric Characters = Maximum Password Length

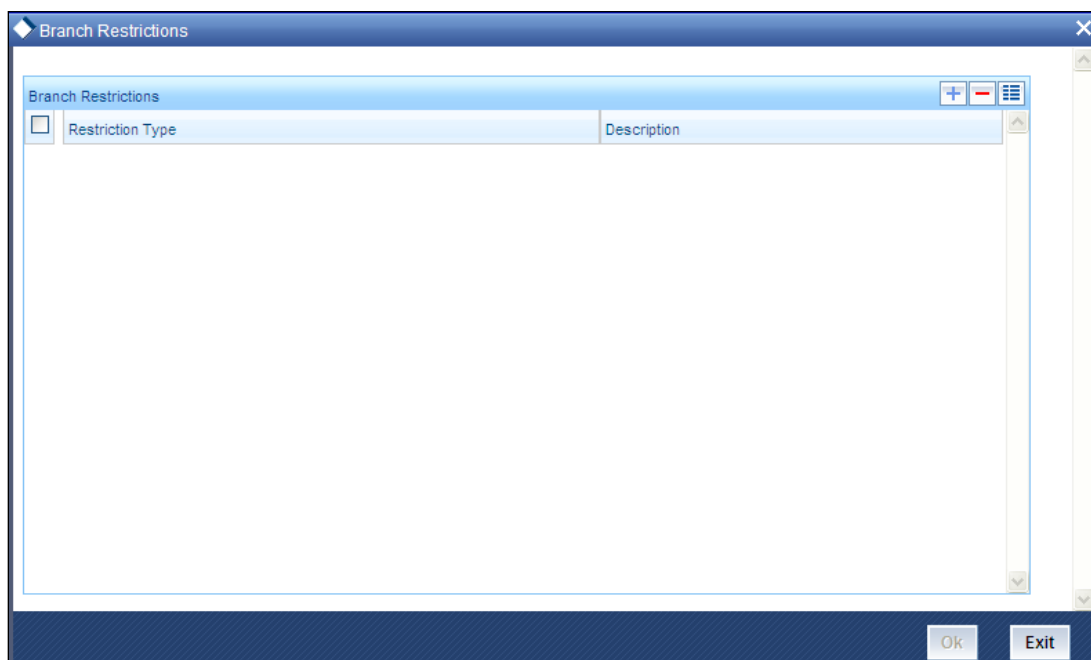
3.2.1 **Specifying Branch Restrictions**

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

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

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

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



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



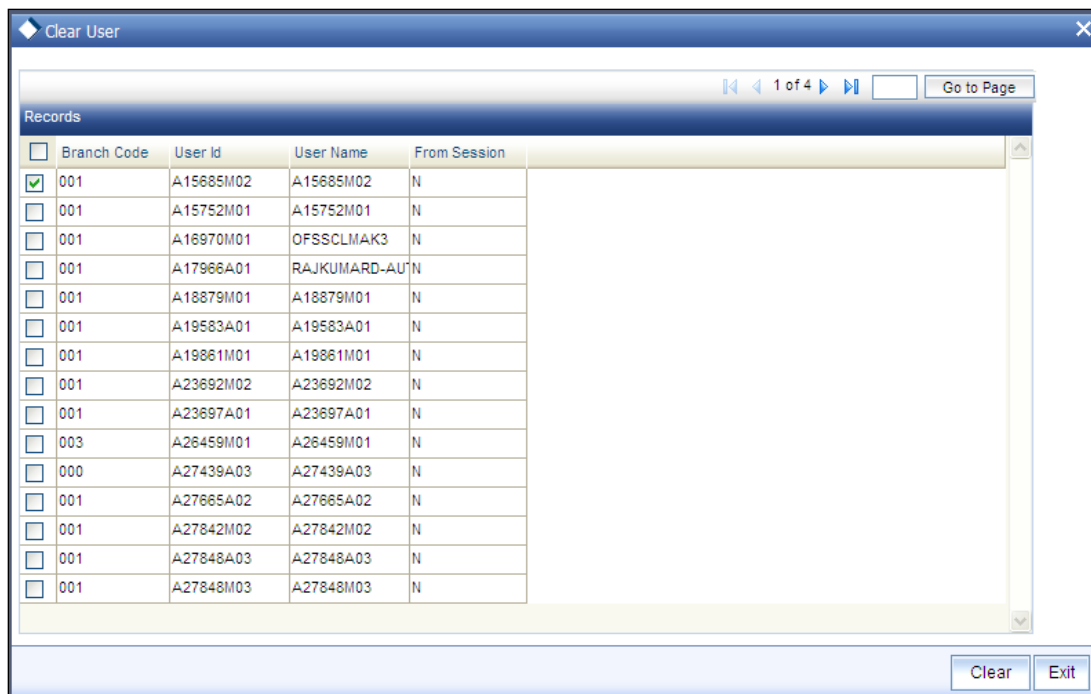
You cannot create common branch restrictions for an application that you have not specified in this screen.

3.3 Clearing a User ID

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

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

Such User IDs can be cleared through the 'Clear User Profile' screen. The IDs of the users currently logged into the system for that branch will be displayed. You can invoke this screen by typing 'CLRU' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



The screenshot shows a window titled 'Clear User' with a close button (X) in the top right corner. Below the title bar is a navigation bar with a 'Go to Page' field and a '1 of 4' indicator. The main area is a table with the following columns: Branch Code, User Id, User Name, and From Session. The table contains 15 rows of data. The first row is selected, indicated by a checkmark in the first column. At the bottom right of the window are 'Clear' and 'Exit' buttons.

	Branch Code	User Id	User Name	From Session
<input checked="" type="checkbox"/>	001	A15685M02	A15685M02	N
<input type="checkbox"/>	001	A15752M01	A15752M01	N
<input type="checkbox"/>	001	A16970M01	OFSSCLMAK3	N
<input type="checkbox"/>	001	A17966A01	RAJKUMARD-AU	N
<input type="checkbox"/>	001	A18879M01	A18879M01	N
<input type="checkbox"/>	001	A19583A01	A19583A01	N
<input type="checkbox"/>	001	A19861M01	A19861M01	N
<input type="checkbox"/>	001	A23692M02	A23692M02	N
<input type="checkbox"/>	001	A23697A01	A23697A01	N
<input type="checkbox"/>	003	A26459M01	A26459M01	N
<input type="checkbox"/>	000	A27439A03	A27439A03	N
<input type="checkbox"/>	001	A27665A02	A27665A02	N
<input type="checkbox"/>	001	A27842M02	A27842M02	N
<input type="checkbox"/>	001	A27848A03	A27848A03	N
<input type="checkbox"/>	001	A27848M03	A27848M03	N

Select the check boxes next to the User IDs which you want to clear and then click 'Clear' button.

3.4 Maintaining Function Descriptions

Any function that is a part of the system is defined through the 'Function Description Maintenance' screen before it is available for execution.

In the event of a function being added at your bank, you should define it through this screen. You can invoke the 'Function Description Maintenance' screen by typing 'SMDFNDSC' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Enter the following details:

Function Identification

Specify a Function ID for the function you wish to maintain.

Module

Click the adjoining option list to view a list of modules. Select the module for which the function will be used.

Type String

Indicate the type of the function – Maintenance, On-Line or Batch

Control String for Functions and Reports

You can then specify the rights to the different actions for the functions by checking against the action. These actions are listed under 'Control String for Functions and Reports':

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

- Hold (to put a contract on hold)
- Template (to save a contract as a template)
- View (to see the details of the contract)
- Generate (to generate reports)
- View (view the reports)
- Print (print the reports)

Auto authorization

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

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

Head Office Function

Select this check box to specify that the function can be used only by the Head Office branch.

3.5 Maintaining Codes for System Languages

You can assign a three character alphanumeric code for every language supported in the system. The 'Language Codes' maintenance screen is available under the Menu Browser.

Example

For English, you may specify the code as ENG

You can invoke the 'Language Code Maintenance' screen by typing 'SMDLNGCD' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Language Code Maintenance - Detailed

Language Code * _____

Language Name * _____

Display Direction _____

Language ISO Code _____

Input By _____ Date Time _____ Modification Number _____

Authorized By _____ Date Time _____

☐ Authorized ☐ Open

Exit

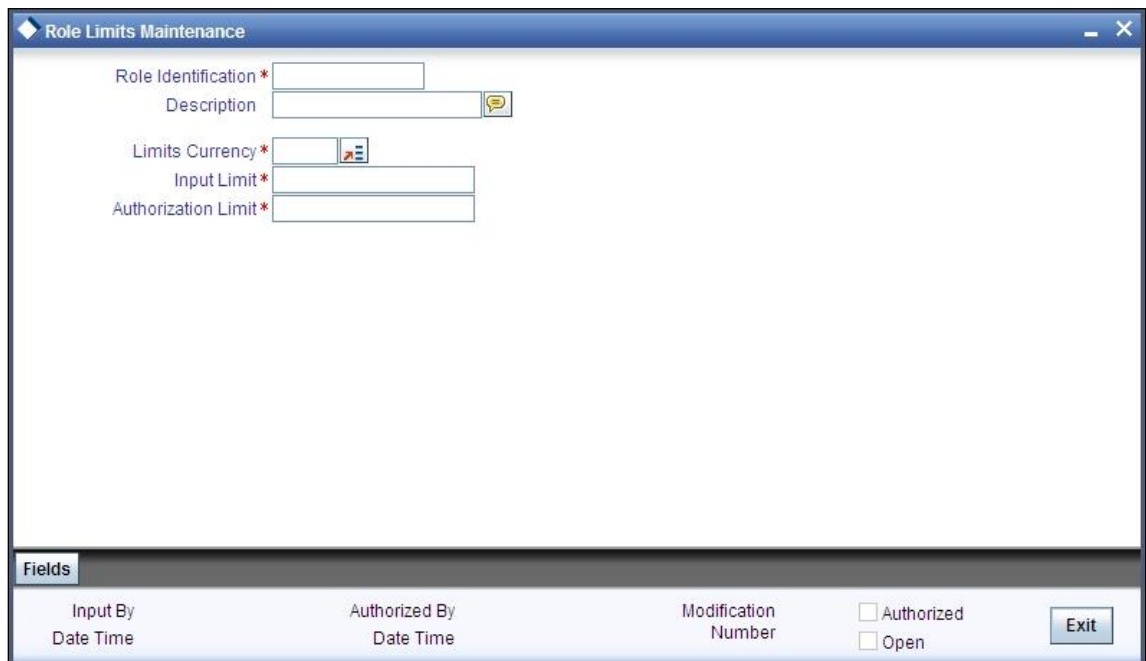
Specify the Language Code and the name of the language in the above screen.

3.6 Maintaining User Role Limits

You can 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.

Role Limits 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.

The Role Limits are maintained in the 'Role Limits Maintenance' screen. You can invoke the 'Role Limits Maintenance' screen by typing 'SMDRLMNT' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



Enter the following details here:

Role Identification


Specify here a Role ID that 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

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

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

Input Limit

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

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 proceed 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 proceed with authorizing the transaction.



The role limits (input and authorization) would apply to a user with which the limits role has been associated, for operations in any of the modules listed above.

3.7 Defining a User Roles

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

Roles Maintenance allows you to define a role profile that includes access rights to the functions that are common to a group of users. While creating a user you can specify a user role for the user. You can define and maintain Role Profiles in the 'Role Maintenance' screen. You can invoke the 'Role Maintenance' screen by typing 'SMDROLDF' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Specify a 'Role Identification' for the role profile. You may provide a brief description of the role too.

After you have defined the Role Identification and Description you should define the functions to which the role profile has access. The various functions in the system fall under different categories.

To assign a function to a role in the Role Description screen, you must use function categories in the Role Description screen:

- **Maintenance** - Functions relating to the maintenance of static tables
- **Batch** - Functions relating to the automated operations (like automatic liquidation of contract, interest, etc.)
- **On Line** - Functions relating to contract processing
- **Process**

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

Branch Restriction

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

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

- Allowed
- Disallowed

Choose the 'Allowed' option to maintain an allowed list, and the 'Branch Restrictions' list will show the list of allowed branches. Choose the 'Disallowed' option, to maintain a disallowed list of branches. If you maintain an 'allowed' list, then the role profile will be available only for those branches that you specify in the Branch Restrictions list. Similarly, if you maintain a 'disallowed' list, then the role profile will not be available only for those branches that you specify in the Branch Restrictions list.

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

Password Restriction

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

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

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

Click 'Password Restriction' button to define the list of Restrictive Passwords for the role profile you are defining. Any user, who is attached to the role, cannot use a password in this list.

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

3.8 Maintaining Single Sign on Details

You can maintain details for the Third Party or External System Sign On mechanism. This maintenance can be done in the 'Single Sign On Maintenance' screen. You can invoke the 'Single Sign On Maintenance' screen by typing 'SMDSOPRM' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

3.9 Defining and Maintaining System Users

You must define and maintain the details of every system user in the 'User Maintenance' screen. Here you can define the activities that a user can carry out on the system. You can set the User's ID and password. In addition you can also set the user role profile, password restrictions, branch restrictions and user access rights.

Note:

You can restrict the access group for the selected user ID using 'Access Group Restriction' screen. In case of data masking, if 'PII Allowed' check box is not selected in 'User Maintenance' screen (SMDUSERD), then PII values are masked.

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

The screenshot displays the 'User Maintenance' application window. It features a top menu bar with 'New' and 'Enter Query' options. The main content area is divided into two sections: 'User Details' and 'User Password'. The 'User Details' section includes fields for User ID, Name, User Reference, Language, Home Branch, Customer Number, LDAP DN, Time Level, Amount Format, Date Format, Auto Authorization, Supervisor Id, Show Dashboards, Alerts On Home, Debug Window Enabled, and LBL_PII_ALLOWED. The 'User Password' section includes fields for Password, Password Changed On, Force Password Change, User Email, Start Date, and End Date. A bottom navigation bar contains links for 'Restricted Password', 'Roles', 'Functions', 'User Branches Restrictions', 'Disallowed Functions', and 'Access Group Restriction'. The bottom status bar shows 'Maker', 'Checker', 'Date Time', 'Mod No', 'Record Status', 'Authorization Status', and an 'Exit' button.

User Details

User Identification

A unique Id having minimum six and maximum twelve characters has to be created for a user in Oracle FLEXCUBE ELCM. Specify the ID here.

Home Branch

Specify the User Login branch. It is treated as home branch.

LDAP DN

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

PII Allowed

Check this box to allow the users to view Personally Identifiable Information.

User Password

Password

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



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

Password Changed On

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

Email

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

Language

Specify the language preference of the User. English is the normal specification here.

Status Changed On

Specify the date when the status is changed from enabled to disabled or disabled to enabled

Last Signed On

Specify the last date timestamp of the user logged.

User Status

Indicate one of the following statuses for the user:

- Enabled - Users who can do transactions. This is the default.
- Hold - User doesn't have the privileges to do, or has been put on hold from doing, any kind of transaction
- Disabled – Users is disabled in Oracle FLEXCUBE ELCM. The user cannot do any transaction.

Password Changed On

The date the user changed his password.

Start Date

Indicates the starting date of the user's login privilege

End Date

Indicates the ending date of the user's login privilege

Classification

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

Staff	A user of the system who is an employee of your bank. You can include any of the functions available in the system in the user profile. Ideally, you should not include functions that are part of End of Cycle operations in the profile of a Staff user.
Customer	A customer who would want to log into the system from a remote terminal. You can include only those functions through which the customer can inquire into balances and transactions.
Auto EOD	A user at the bank who is responsible for running the automated End of Day operations. You can include any of the functions available in the system in the user profile. Ideally, you should include only functions that are part of End of Cycle operations in the profile of a AEOD user.
Branch	This provides a single login and change password rights for both the system and branch system. You can specify the vacation start date, vacation end date and dual password.

Propagate Detailed to Workflow

You can propagate the User Id and Password defined for a user of the system to the Workflow system as well. In other words, a user can use the same id and password to log into both the systems. To enable this feature select the 'Propagate Detailed to Workflow' option.

The following basic details will be sent to the Workflow system:

- User ID
- User Description
- User Password
- Record Status

The Password will be sent in an encrypted form and the encryption will be done based on the Workflow encryption logic.

Any modifications that you make in the above mentioned fields would be transmitted to the Workflow system. Whenever any modification (to the above mentioned fields) takes place in the system, it will first verify whether the user record exists in the Workflow system also. If the record is not present, a new record will be created in the Workflow database. If the record already exists in the system, the changes will be updated accordingly.

Auto Authorize

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

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

Customer Number

For User Profiles of users/employees who also happen to be your bank's customers, you can restrict the viewing and printing of Balances (in case of accounts) and financial details of contracts. To enable this, while creating the User Profile of the employee, specify the Customer Number of the employee here.

3.9.1 Roles

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

<input checked="" type="checkbox"/>	Branch Code *	Role *	Role Description
<input checked="" type="checkbox"/>			

Click 'Plus' button to add a record under the 'Roles' list. Into each added record's field select the required role by clicking the field's option list. Repeat this procedure to attach more roles.

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

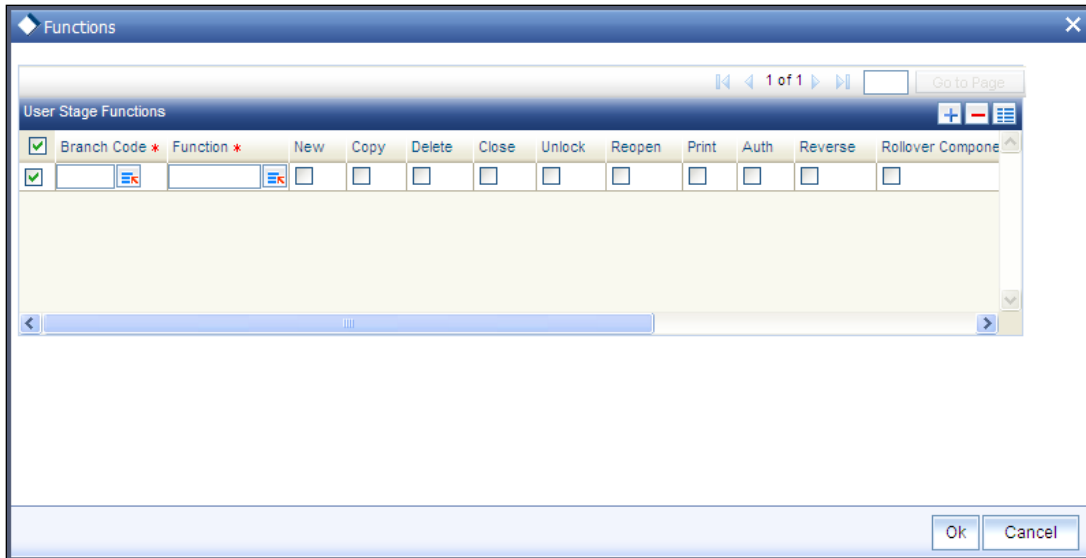
3.9.2 Functions

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

- Attached one or more roles to a user profile
- Given access to individual functions to a profile to which roles are attached

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

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

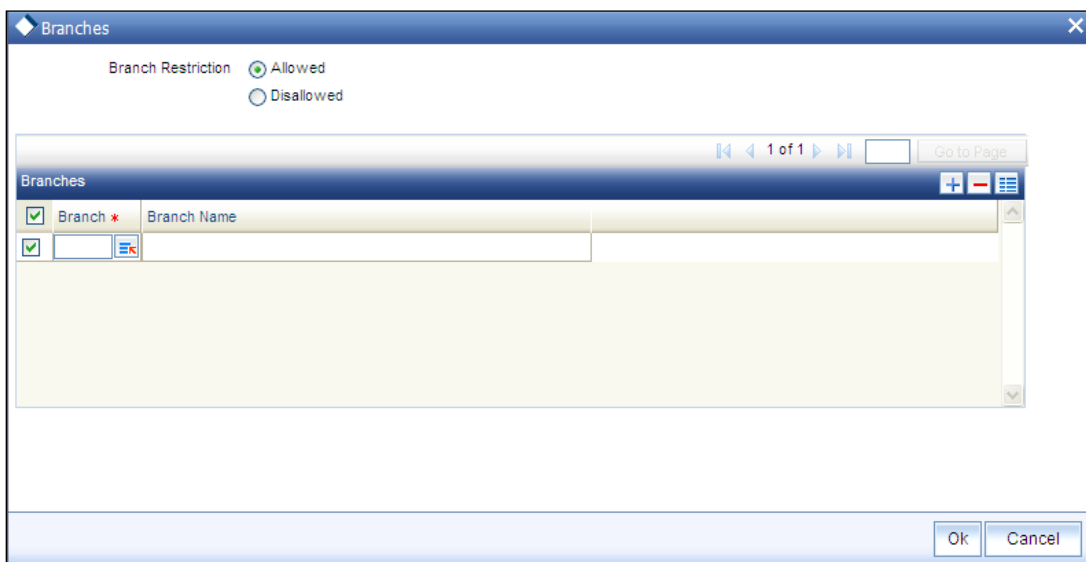


The various functions in the system fall under different categories.

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

3.9.3 Branches

To specify the branches from which the Staff and End of Day users of the bank can operate, you must use the 'Branches' screen. Click 'Branches' button in the User Maintenance screen and 'Branches' screen will be displayed as shown below.



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

- Allowed
- Disallowed

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

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

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



Note the following:

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

3.9.4 Restricted Passwords

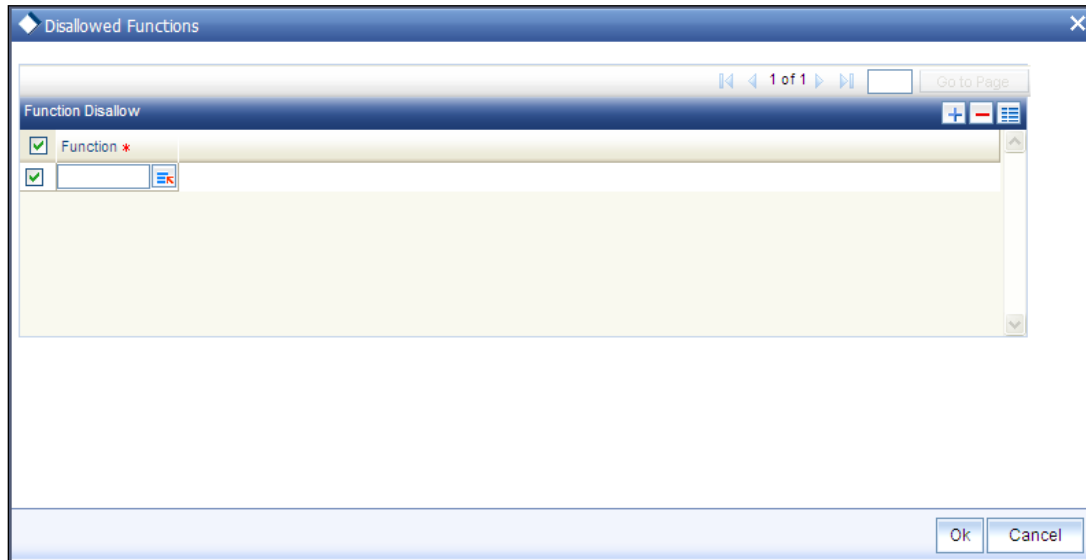
You can maintain a list of passwords that the user is most likely to use. For example, a user may tend to use the names of loved ones, the bank, department, etc. as a password as they are easy to remember. This might be a security risk as it will be easy for another person to guess a password. To prevent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

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

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

3.9.5 Disallowed Functions

You can restrict the user from operating certain functions by maintaining the functions in the Disallowed Functions screen. To invoke this screen, click 'Disallowed Functions' button.

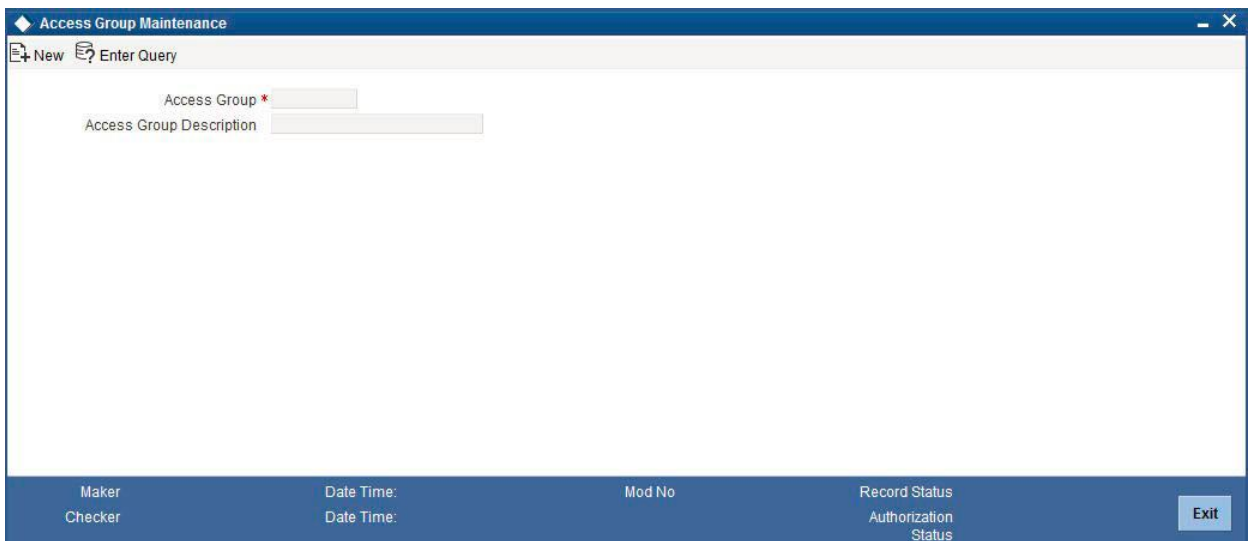


The screenshot shows a window titled "Disallowed Functions". Inside, there is a "Function Disallow" section with a table. The table has a column labeled "Function *" and a checkbox. The first row has a checked checkbox and a text input field. Below the table is a large empty text area. At the bottom right, there are "Ok" and "Cancel" buttons. The top right of the window has navigation controls and a "Go to Page" button.

3.10 Access Group Maintenance

3.10.1 Maintaining Access Group

You can maintain the access group for retail and corporate customers in the 'Access Group Maintenance' screen. You can invoke this screen by typing 'CODACGRP' in the top right corner of the Application tool bar and clicking the adjoining arrow button.



The screenshot shows a window titled "Access Group Maintenance". At the top, there are buttons for "New" and "Enter Query". Below these, there are two input fields: "Access Group *" and "Access Group Description". At the bottom, there is a status bar with fields for "Maker", "Checker", "Date Time:", "Mod No", "Record Status", "Authorization", and "Status". An "Exit" button is located at the bottom right.

Access Group

Specify the access group code.

Access Group Description

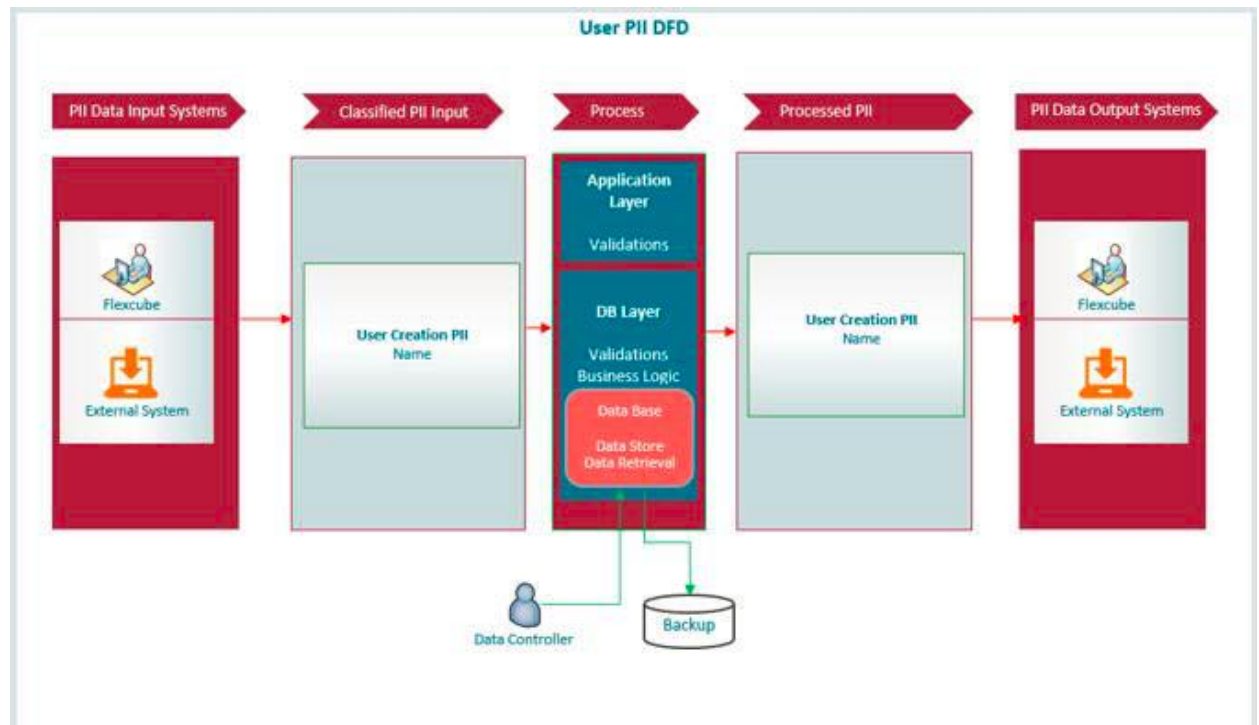
Give a brief description on the access group specified.

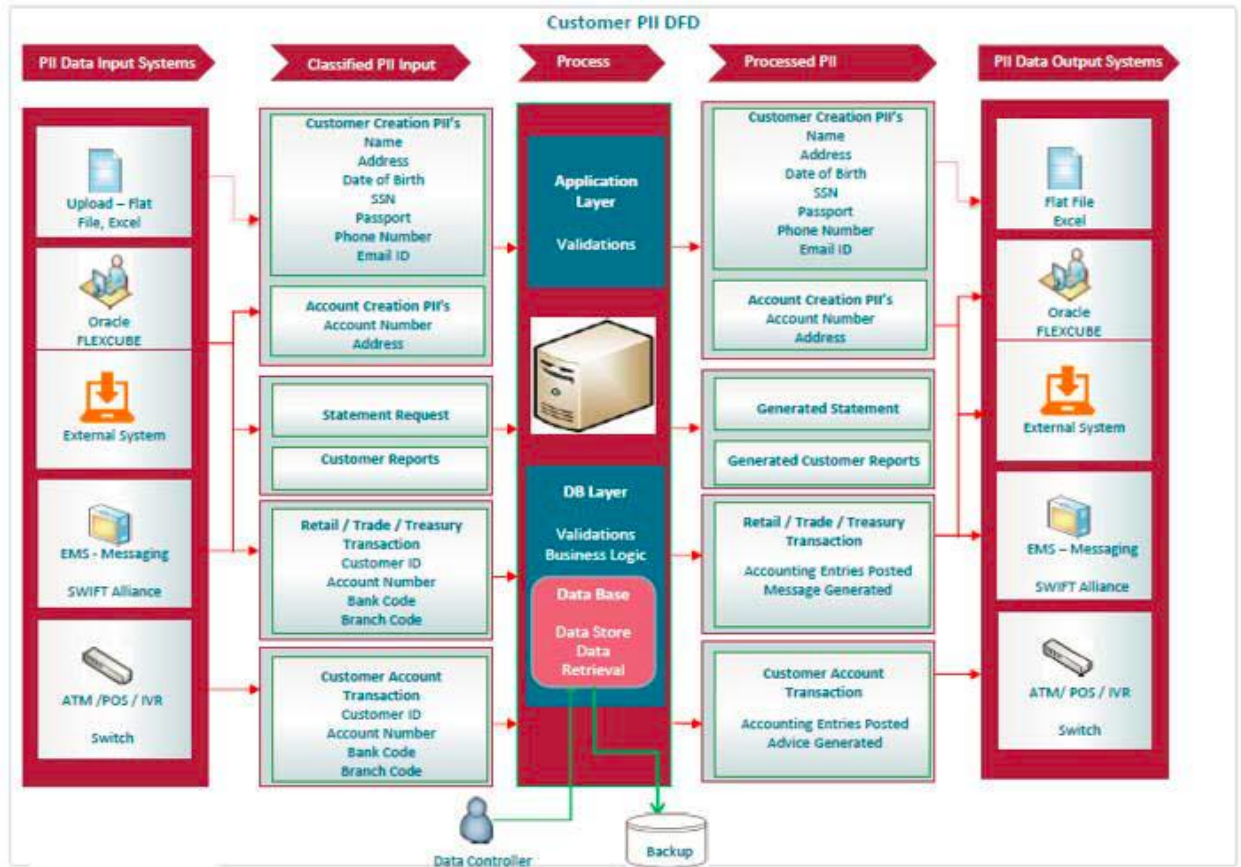
For unauthorized tanked Maintenances, access restriction is not applicable at query time.

3.11 Personally Identifiable Information

Personally Identifiable Information (PII) is the information that can be used on its own to identify a person. Any information that is used to distinguish one person from another can be a personally identifiable information. It can be any information like name, contact information, demography information, financial information, SSN, Passport number etc. Oracle FLEXCUBE allows you to mask, forget or restrict access to personally identifiable information of a user. You can forget the PII based on the maintenance in Forget Customer PII Maintenance screens.

The following flow diagrams explains the data flow of Personally Identifiable Information (PII).





Personally Identifiable Information captured in the system are categorized as below:

User Personal Information

Personal Information Category	Personal Information Data
Customer Name	User Name

Customer Personal Information

Personal Information Category	Personal Information Data
Customer Name	First, Middle, Last Name Father Name Spouse Name Guardian Name Mothers Maiden Name Joint Holder Name

Customer Contact Information	E-mail ID Postal/Zip Code Work Phone Number International Dialling Code Home Phone Number Mobile Number Fax Number Mailing Address Correspondence Address Permanent Address Domicile Address
Demography Information	Gender Birth Place Birth Country Date of Birth City State Country Nationality Language Location
Financial Information	Bank Name Branch Name Account Name Credit Card number Name on Card
Unique Identifiers	Social Security Identifier Passport Details National ID Tax Identification Number Visa Details
Other Information	KYC reference Power Of Attorney Details Nominee details Guardian Details

3.12 Masking

The system masks the personally identifiable information based on the credentials of the logged in user. You can mask personally identifiable information based on the PII field's data. When the user logs into the Application, the system checks 'PII Allowed' value maintained in the 'User Maintenance' screen against a user role and then displays masked or unmasked data. Any user with 'PII Disallowed' cannot view masked data and change log records. PII disallowed users should have the role where only querying the data is allowed.

3.13 Forgetting Customer Process

You can forget a specific customer by using the 'Forget Customer Process' screen. You can invoke the screen by typing 'CODCSFRT' in the top right corner of the application toolbar and clicking adjoining arrow button.

Forget Customer Process

New Enter Query

Forget Customer Process ID

Forget Customer Process Type ☒ Customer Initiated ☐ Bank Initiative

1 Of 1 Go

Customer No *	Process Status
---------------	----------------

Maker Date Time: Mod No Record Status
Checker Date Time: Authorization Status

Ok Exit

Following details are maintained in the screen:

Forget Customer Process ID

The system generated ID for processing the customer details. You can also enter manually while searching for forgotten customers.

Forget Customer Process Type

Select the type of request for forgetting the customers.

You can select 'Customer Initiated', when the customer has requested for forgetting their details immediately. You can select 'Bank Initiated' process type to process the closed customers in a bulk, as per the bank's requirement. The process is a non EOD batch process. For customer initiated process, you can select the list of closed customers. But for bank initiated process, the system picks all the closed customers based on the bank parameter maintenance and not individual customers.

Customer Number

Select the customer number from the option list.

Process Status

The system generated status, when you submit the request status is 'U'. Once the process is authorized the status changes to 'P'. Once authorized, the data of the customer will be updated with the respective masked value that you have entered in the CODBNKPR screen.

After the customer is forgotten in the system, the customer's data will not be available for any operations in any 'Detail' and the 'Summary' screens.

3.14 Forgetting Users

Oracle FLEXCUBE allows you can sanitize the data by forgetting the user's personally identifiable information (PII) once their accounts are closed. This is useful when data cannot be deleted due to referential integrity.

You can forget a specific customer by using the 'Forget User Process' screen. You can invoke the screen by typing 'SMDUSFRT' in the top right corner of the application toolbar and clicking adjoining arrow button.

Forget User Process

New Enter Query

Forget User Process ID Forget User Process Type ☒ User Initiative ☐ Bank Initiative

1 Of 1 Go

User ID	Process Status
---------	----------------

Maker Checker Date Time: Mod No Record Status Authorization Status Status Ok Exit

Following details are maintained in the screen:

Forget User Process ID

The system generated ID for processing the user details. You can also enter manually while searching for forgotten users.

Forget User Process Type

Select the type of request for forgetting the users.

You can select 'User Initiated', when the user has requested for forgetting their details immediately. You can select 'Bank Initiated' process type to process the closed users in a bulk, as per the bank's requirement. The process is a non EOD batch process. For user initiated process, you can select the list of closed users. But for bank initiated process, the system picks all the closed users based on the bank parameter maintenance and not individual users.

User ID

Select the users ID from the option list.

Process Status

The system generated status, when you submit the request status is 'U'. Once the process is authorized the status changes to 'P'. Once authorized, the data of the user will be updated with the respective masked value that you have entered in the 'SMDBNKPR' screen.

After the user is forgotten in the system, the user's data will not be available for any operations in any 'Detail' and the 'Summary' screens, including 'SMDUSERD' screen.

3.15 Log Access

Customer's can access logs based on the access rights set by the system administrator. They can have limited or full access, and accordingly they can view, generate, or purge logs.

3.15.1.1 Application Logs

The application log consists of the application or the front-end layer logs.

- Application Log path can be configured in fcubs.properties (Parameter APPLICATION_WORK_AREA) file, at the time of the property file creation.
- Application logs can be enabled /disabled based on fcubs.properties (Debug = 'Y' Or 'N').
- The storage mainly is in application server. The data controller control the access to the storage.

The section of fcubs.properties will looks like below

```
##### COMMON PROPERTIES #####
APPLICATION_NAME=FCJ
APPLICATION_EXT=FCROFC
APPLICATION_SERVER=WL
APPLICATION_WORK_AREA=/scratch/work_area/DEV/FC125R2/APPLLOGS
DEBUG=Y
SSL_ENABLED=Y
OPSS_AVAILABLE=N
BRANCH_CENTRALIZED=Y
REQUEST_TIME_OUT=1800000
```

3.15.2 Back-end Logs

Back end log consists of the back end layer debug logs.

- Database directories are created with the back end debug path by the data controller.
- Database directory has to be specified at the time of day 0 setup.

- The data controller can give module wise access of the back-end logs to the user.

3.15.3 Audit Logs

Audit Logs are used to see history of all changes that has happened. The user can view the changes made, along with the Maker and Checker Id as well as time stamp information.

In the STDCIF screen, click the Change log button to view the modification details.

3.15.4 Purging Logs

Logs are purged in both Application and DB server by the data controller.

3.16 User Administration - Branch Restrictions

In the Branch Restrictions maintenance under Bank Parameters, you have identified those applications and operations, for which you intend to maintain branch restrictions. Having done this, you must proceed to create the appropriate common branch restrictions for each branch administrator.

You can maintain common branch restrictions in the 'Branch Restrictions' screen. This can be done only at the head office branch. You can invoke the 'Branch Restrictions' screen by typing 'SMDBRRES' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows the 'Branch Restrictions' application window. It includes the following elements:

- Title Bar:** Branch Restrictions
- Form Fields:**
 - User Branch * (text box with a dropdown arrow)
 - Description (text box with a help icon)
 - Restriction type * (text box with a dropdown arrow)
 - Description (text box with a help icon)
 - Branch Restriction: Radio buttons for 'Allowed' and 'Disallowed' (selected).
- Restricted Branches Table:**

Branch Code *	Description
[Empty text box with dropdown arrow]	
- Fields Section:**
 - Input By Date Time
 - Authorized By Date Time
 - Modification Number
 - Authorized (checkbox)
 - Open (checkbox)
 - Exit button

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

User Branch

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

Restriction Type

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

Branch Restriction

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

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



Note the following:

The following must be borne in mind while creating common branch restrictions:

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

3.17 Maintaining User Data Restriction

Apart from the restrictions on the operations like: creating new, modifying, deleting, closing, and reopening the function ID, you can also maintain the user restrictions for,

- Category
- Liability Number
- Source
- Currency.

When the user tries to perform any operation like: New, Modify, Delete, Close, Reopen, Query on facility or collateral maintenance, before performing transaction in ELCM, system will check whether the user has the rights to perform the transaction for the data and if the user does not have rights, then the system will raise the following error message:

User does not have rights to perform transaction on this data.

You can maintain user restrictions in the 'User Restriction Maintenance' screen. You can invoke this screen by typing 'GEDUSRES' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

3.17.1 Category Restrictions Tab

You can maintain the category restriction from the 'Category Restrictions' tab.

Capture the following data to maintain user restriction for specific category:

User ID

Specify the user ID for which you want to set the category restriction.

Restriction Type

Choose the 'Allowed' option, to maintain an allowed list of category restrictions. Choose 'Disallowed' option to maintain a disallowed list of category restrictions.

Default value of this field will be 'Disallowed'. If you select restriction type as 'allowed', then you need to input at least one record.

Category Restrictions

Category Name

Specify the category for the restriction from the adjoining option list.

3.17.2 Liability Restrictions Tab

You can maintain the liability restriction from the 'Liability Restrictions' tab.

The screenshot shows the 'User Restrictions' application window. The 'Liability Restrictions' tab is active. The 'Restriction Type' is set to 'Disallowed'. The 'Liability Restrictions' table is currently empty. The bottom section contains fields for 'Input By', 'Authorized By', and 'Modification Number', along with checkboxes for 'Authorized' and 'Open', and an 'Exit' button.

Capture the following data to maintain the user restriction for specific liability:

User ID

Specify the user ID for which you want to set the liability restriction.

Restriction Type

Choose the 'Allowed' option, to maintain an allowed list of category restrictions. Choose 'Disallowed' option to maintain a disallowed list of category restrictions.

Default value of this field will be 'Disallowed'. If you select restriction type as 'allowed', then you need to input at least one record.

Liability Number

Specify the liability number for the restriction from the adjoining option list.

3.17.3 Source Restrictions Tab

You can maintain the source restriction from the 'Source Restrictions' tab.

Capture the following data to maintain the user restriction for specific source:

User ID

Specify the user ID for which you want to set the source restriction.

Restriction Type

Choose the 'Allowed' option, to maintain an allowed list of category restrictions. Choose 'Disallowed' option to maintain a disallowed list of category restrictions.

Default value of this field will be 'Disallowed'. If you select restriction type as 'allowed', then you need to input at least one record.

Source Code

Specify the source code for the restriction from the adjoining option list.

3.17.4 Currency Restrictions Tab

You can maintain the currency restriction from the 'Currency Restrictions' tab.

Capture the following data to maintain the user restriction for specific currency:

User ID

Specify the user ID for which you want to set the currency restriction.

Restriction Type

Choose the 'Allowed' option, to maintain an allowed list of category restrictions. Choose 'Disallowed' option to maintain a disallowed list of category restrictions.

Default value of this field will be 'Disallowed'. If you select restriction type as 'allowed', then you need to input at least one record.

Currency

Specify the currency for the restriction from the adjoining option list.

3.18 Viewing User Data restriction

You can view all the user data restrictions for Category, Liability, Source and Currency that have been maintained, and their status in the 'User Restriction Summary' screen. You can invoke this screen by typing 'GESUSRES' In the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.

The screenshot shows a web application window titled "Summary". It contains the following elements:

- Search Filters:**
 - Authorization Status:** A dropdown menu.
 - Record Status:** A dropdown menu.
 - User Id:** A text input field.
- Buttons:** "Search", "Advanced Search", and "Reset" are located on the right side.
- Pagination:** A bar showing "Records per page" set to 15, "1 Of 1" records, and a "Go to Page" input field.
- Table Header:** A single row with the following columns: "Authorization Status", "Record Status", "Id", and "User Id".
- Legend:**
 - Authorization Status:** A - Authorized, U - Unauthorized
 - Record Status:** C - Closed, O - Open
- Exit Button:** Located at the bottom right of the window.

You can base your queries on any or all of the following parameters and fetch records:

- Authorization Status
- Record Status
- User ID

Select any or all of the above parameters for a query and click 'Search' button. The records meeting the selected criteria are displayed.

System displays the following details pertaining to the fetched records:

- Authorization Status
- Record Status
- Id
- User Id

4. Core Maintenances

4.1 Introduction

The Core Maintenances section explains maintaining information related the core processes in the system. Core Maintenances include the following:

- Maintaining bank related parameters
- Creating and maintaining Branch details
- Creating and maintaining Liability records
- System related maintenances

4.2 Maintaining Your Bank Parameters

You can maintain information about your bank in the 'Bank Parameters Maintenance' screen. The information maintained here includes the bank name, head office, account number structure, local currency, spread and other preferences.

Details maintained in the 'Bank Parameters Maintenance' screen are applied to all branches of your bank.

For example the account number structure that you define in this screen will be a common format for customer accounts in all branches of your bank.

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

Bank Parameter Maintenance

Enter Query

Bank Code * Bank Name

Head Office Branch

Home Branch * Branch Name

Def

Discount Currency * Description

Reporting Currency * Description

Home Branch Currency * Description

Local Currency * Description

☐ Exchange Rate Copy

LBL_FRT_CUS_DET

No. of Days to Forget Customer

Masking Character

Fields

Maker Date Time: Mod No

Checker Date Time: Record Status

Authorization Status

Exit

Bank Code

Specify a unique character code for identifying your bank. You can follow your own convention in devising this code. In all inter-bank transactions this code identifies your bank.

Bank Name

Specify the detailed name of your bank. This name will always be displayed whenever the bank code is used.

Head Office Branch Code

From the list of the branches you have already maintained for your bank, select your Head Office code. The description of the branch designated as Head Office is displayed on selecting the code.

Default Currencies Code

You can indicate currency preferences for your bank. You can specify preferences to indicate the default currencies for the following purposes:

- **Local Currency**— Specify the local currency for all branches of your bank. This will be the default currency for all transactions. The income and expense balances of your bank will also be maintained in this currency.
- **Discount Currency** — If the discount rate for a particular currency is not maintained the discount rate of the currency specified here will be picked up for discounting profits on forward foreign exchange contracts.
- **Head Office Currency** — Specify the default currency for the Head Office.

- **Reporting Currency** — Specify the default currency in which all financial reporting should be done.



You cannot modify the currencies you specify here once the Bank Parameters record has been stored and authorized.

Propagate Exchange Rates to Branches

Specify whether the currency exchange rates maintained here must be propagated to all the bank branches as well. Select this check box to propagate rates to all branches.

Specifying Forget Customer Details

No of Days to Forget Customer

Enter the number of days, after which the system will forget the user after they close their account. Once the user is forgotten you can't view the details of the user.

Mask Character

Enter the character that you want to use to mask the user information, so that it is not visible to anyone.

4.3 Maintaining Branch Parameters

You can create and define various parameters for your bank's branches using the 'Branch Maintenance' screen. Here you can record the details of your bank's branches, define their reporting hierarchy, and maintain parameters such as their names and addresses including SWIFT, TELEX, and HOST addresses.

You can create the branch records only at the Head Office. All subsequent modifications on the records can be done at the branches only.

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

Branch Maintenance

Branch Details

Branch Code *

Branch Name *

Parent Branch *

Regional office *

Country Code

Customer Identity

Local Currency *

Weekly Holiday Sunday

Weekly Holiday Saturday

Time Zone Offset

Hours

Minutes

EOC Status N

Time Level 9

CutOff Offset Time

Hours

Minutes

☐ Auto Authorization

Address

Branch Address *

Fields

Input By DOC003
Date Time

Authorized By
Date Time

Modification
Number

☐ Authorized

☒ Open

Cancel

You can maintain the following details in the above screen.

Branch Code

Assign a code to the bank branch. The code acts as an identifier in the system for the particular office / branch.

Branch Name

Specify the name of the branch.

Local Currency

Specify the currency of operation for your branch and the default currency for all transactions of your branch. The income and expense balances of your branch will also be maintained in this currency.

GL Class

Specify the GL Class. The adjoining option list displays a list of all the valid GL codes and their description. You can choose the appropriate one.



You can also select 'ALL' as an option. This indicates that all the GL codes are allowed for this branch.

Parent Branch

Parent Branch is to define an alternate reporting line, other than the three level 'Head Office – Regional Office –Branch' structure. The 'Parent' for all the branches you create is the Head Office. You may specify a Parent, other than the Head Office, here. The name of the parent branch is displayed on selection.

Regional Office

This is the branch code of the Head Office or Regional Office (RO) to which the branch reports to.

For a Head Office or a Regional office, this code should be the Head Office branch code, which is also the default for this field. For the branches, specify that branch as the RO, to which the branch reports. Select from the list of options available here.

Country Code

Specify the code of the country in which the branch operates. Select from the list available here.

Branch Address

Enter the address of location of the branch here.

Telex Address

Specify the branch's TELEX address here.

Host Name

Enter the name of the Host server for this branch.

Time Level

This field displays the system time level status, represented by a number between 0 and 9.

User access to the system can be controlled by assigning each user and the system, a time level. Both the system and the users are set to different time levels. Only those users who have a time level equal to or greater than the system time level can log into the system. A control clerk, during the EOC process, does the change in time level status.

EOC Status

Under EOC status one of the following will be displayed:

B - Beginning of financial input; indicates system transactions in progress

I -- Indicates that user transactions are in progress

T-- End of user transaction input; indicates system transactions in progress

F -- End of financial input; system transactions also completed

E -- End of Day, Branch awaiting date change

The values are updated by EOC process.

Time Zone Offset – Hours and Minutes

For branches with different time zones, you can define the Offset Time that has be displayed in maker/authorizer time stamps and also in all the reports generated for the branch.

The offset time is specified in terms of hours and minutes. The time will be added/ subtracted from the Server Time maintained for the bank.

Specify the number of 'hours' to be offset from Server Time to arrive at the local branch time. This is the number of hours by which the branch leads or lags behind the Server Time.

Specify the additional 'minutes' by which the branch leads or lags behind the Server Time.

Weekly Holiday

Specify the weekly holiday days of the branch. You can specify up to two weekly holidays.



The reference time is always the System Time (System Server Time).

4.4 Maintaining ELCM Branch Parameters

You can maintain ELCM branch parameters by capturing the information related to customer number generation in 'ELCM Branch Parameter Maintenance' screen.

You can invoke the 'ELCM Branch Maintenance' screen by typing 'CODBRPRM' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

A screenshot of the 'Branch Parameter Maintenance' window. The window has a title bar with a diamond icon and the text 'Branch Parameter Maintenance'. Inside the window, there are three input fields: 'Branch Code', 'Start Customer Number', and 'End Customer Number'. At the bottom of the window, there is a footer area with labels for 'Input By', 'Authorized By', and 'Modification Number', each followed by a 'Date Time' label. To the right of these labels are two checkboxes labeled 'Authorized' and 'Open'. An 'Exit' button is located in the bottom right corner of the window.

If the check box 'Generate Customer Number' in 'Global Exposure Parameter Details' screen is checked, then you need to define the following fields in this screen.

Branch Code

System defaults the branch code for which the ELCM maintenance is being performed. System displays the transaction branch code

Start Customer Number

Specify the minimum number for which the ELCM customer number can be generated. Default value in this field will be 1.

End Customer Number

Specify the maximum number for which the ELCM customer number can be generated. Default value in this field will be 999999999.

4.5 Maintaining Your Branch Holidays

You can specify the weekly and annual holidays for your bank branch in the 'Branch Holiday Maintenance' screen.

The system uses the information maintained in this screen to do the following:

- For checking whether the start date, maturing date and schedule date for Limits does not fall on a holiday
- To display and record today's date and the next working date.

You can invoke the 'Branch Holiday Maintenance' screen by typing 'CODBRHOL' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows the 'Branch Holiday Maintenance' window. It features a grid for entering holidays for each month of the year. The grid has columns for days of the week (S, M, T, W, Th, F, Sa) and rows for each month (January, February, March, April, May, June, July, August, September, October, November, December). At the bottom, there is a 'Fields' section with input fields for 'Input By', 'Authorized By', 'Modification Number', and checkboxes for 'Authorized' and 'Open'. An 'Exit' button is also present.

This maintenance must be done at each branch of your Bank. You can thus have different sets of holidays for different branches of the bank.

Branch Code

Specify the branch code of the Branch for which you are maintaining the holidays.

Year

Select the year for which you are performing the maintenance. You can specify both weekly and annual holidays for the branch up to the year 9999 AD.

Click 'Refresh' after specifying the Year. The calendar will be displayed of the specified year. Click a date in the calendar to record it as a holiday. Holidays appear in red.



Future dates for future schedules can be maintained only if the holidays for the corresponding year have been maintained here.

4.6 Maintaining Country Codes

You can specify codes for countries in the 'Country Code Maintenance' screen. You can invoke the 'Country Code Maintenance' screen by typing 'STDCNTRY' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Enter the following details:

Country Code

Give a unique three-character alpha numeric code to identify the country. For example you can maintain 'USA' as the country code for the United States of America.

Country Name

Specify the name of the country whose details are being maintained.

Alternate Country Code

You can also associate an alternate country code. This is for information purposes only and will not be printed on any customer correspondence. For example you can have US as the alternate code for USA.

Blacklisted

Select this checkbox if the country has been blacklisted for any reason with regard to banking.

EU Member

Select this checkbox to specify that the country is a member of the European Union.

4.7 Maintaining Customer Information Details

You can maintain all basic information about a customer can be maintained via the 'Customer Maintenance' screen. These details are maintained at the branch level and are accessible to all branches. Duplicate customer records are hence not maintained at different branches.

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

The screenshot displays the 'Customer Maintenance' application window. At the top, there are buttons for 'New' and 'Enter Query'. Below these, the 'Type' section has radio buttons for 'Individual' (selected), 'Corporate', and 'Bank'. To the right, there are input fields for 'Full Name', 'Short Name *', and 'Branch Code *'. Further right is a 'Customer Category *' dropdown. Below the 'Type' section is a 'Customer No *' input field. A tabbed interface shows 'Personal', 'Corporate', 'Additional' (selected), and 'Director' tabs. Under the 'Additional' tab, there are two main sections: 'Status' and 'Identifier'. The 'Status' section contains a list of checkboxes: 'Frozen', 'Deceased', 'Whereabouts Unknown', 'UnAdvised', 'CRM Customer', 'Issuer Customer', 'Customer Treasury', and 'Blacklist Customer'. The 'Identifier' section has input fields for 'Name' and 'Unique Id Value'. Below these is a 'Relationship Manager' section with an 'RM ID' input field. At the bottom of the main form area is an 'Additional Details' section with input fields for 'Credit Rating', 'Access Group', 'Exposure Country', 'External Ref. No.', 'SSN', and 'Sector Code'. The bottom of the window features a 'Customer Source Details' tab and a 'Fields' section with labels for 'Maker', 'Checker', 'Date Time:', 'Mod No', 'Record Status', and 'Authorization Status'. An 'Exit' button is located in the bottom right corner.

Enter the following details:

Customer Number

Specify the Customer Number to uniquely identify a customer. This number should be unique across branches.

Short Name

Specify a short name for the customer here.

Customer Type

You have to indicate the Type to which the customer belongs. The options available are:

- Bank
- Corporate
- Individual

Country

Specify the country as given in the address of correspondence of this customer.

Nationality

Specify the nationality of the customer.

Language

As part of maintaining customer accounts and transacting on behalf of your customer you will need to send periodic updates to your customers in the form of official bank documents.

You have to indicate the language in which your customer wants the communication from the Bank to be in.

Exposure

Specify the country of exposure of this customer.

Customer Category

Specify the Customer Category here.

Credit Rating

Specify the credit worthiness of the customer using a credit rating.

Access Group

Specify the access group. Alternatively, you can select the access group from the option list. The list displays all valid access groups allowed to the user based on the maintenance at 'Access Group Restriction' screen under 'User Maintenance' screen.

Revision Date

Specify the revision date for the credit rating for the customer.

Source

Specify the source of the credit rating of the customer.

Customer Name

Enter the name of the customer. The customer will be addressed by this name in all correspondences sent from the bank

Address Line 1 - 4

You can specify the mailing address of the customer in the fields that are provided. You can specify the details of the address in each appropriate field, such as City, State, Country and Zip Code.

Fax

Specify the FAX number for the customer.

SSN

Specify the Social Security Number of the customer.

Frozen

Select the check box if the customer account is supposed to be frozen.

Deceased

If the customer whereabouts are unknown, then select this check box.

Unadvised

Select to indicate that the customer account is unadvised.

CRM Customer

If the customer is not of Oracle FLEXCUBE ELCM, then the customer will be treated as a CRM Customer. Select this check box to indicate this.

Issuer Customer

If the customer is not directly a part of Limits transaction, but is providing guarantees to other customer(s) in Oracle FLEXCUBE ELCM, such as in the case of Collateral Guarantees, then select this check box.

Treasury Customer

Select this checkbox to specify that the customer is a treasury customer.

4.7.1 Maintaining Customer Source Details

You can capture the source details for the customer in 'Customer Source Details' screen. To invoke this screen, click on 'Customer Source Details' button in the 'Customer Maintenance' screen.

Customer Source Details

Customer No *

Customer Name

Customer Source Details

Source Code	Source Customer Number
<input type="checkbox"/>	<input type="text"/>

Ok Exit

Customer No

Specify the customer number for which you want to capture the source code details.

Customer Name

System defaults customer name associated with the customer number.

Source Code

System defaults source code.

Source Customer Number

System defaults source customer number from Oracle FLEXCUBE.

4.8 Static Maintenances

Data that remains constant over a period of time is called static data. Usually, such data will be commonly accessed by more than one module. Such data is maintained in tables. Once the data is entered in a table, it has to be authorized before it can be used by any function. Each item in a table is called a record. Each record has a key that uniquely identifies it.

The following static values can be maintained as part of the ELCM system.

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

Category Maintenance

Category Name *

Description

Fields

Input By
Date Time

Authorized By
Date Time

Modification
Number

☐ Authorized
☐ Open

Exit

Here you can maintain the Category Name and its display value.

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

Exposure Maintenance

Exposure Name *

Description

Fields

Input By
Date Time

Authorized By
Date Time

Modification
Number

☐ Authorized
☐ Open

Exit

Here you can maintain an Exposure Name and its display value.

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

Here you can maintain Group Names and their values.

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

This screen allows Haircut Type Maintenance. This Haircut type would be required in the credit risk mitigation process and this is as part of BASEL II standards. Haircut Type maintained here will be utilized in Collateral category Maintenance.

This maintenance is at bank level and all branches would be able to access this information.

- Haircut Name

- Haircut Description

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

Here you can maintain Liability Names and their values.

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

Here you can maintain Location Codes and values.

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

The screenshot shows a window titled "Restriction Maintenance". It contains two input fields: "Restriction Name *" and "Description", each with a small yellow speech bubble icon to its right. Below the input fields is a "Fields" tab. Under the "Fields" tab, there are four columns of data: "Input By", "Authorized By", "Modification", and "Number". Each column has a "Date Time" label below it. To the right of these columns are two checkboxes: "Authorized" and "Open". An "Exit" button is located in the bottom right corner.

Here you can maintain Restriction names and their values.

You can invoke the 'Unique Identifier Maintenance' screen by typing 'CODUIDN' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows a window titled "Unique Identifier Maintenance". It contains two input fields: "ID Name *" and "ID Description". Below the input fields is a "Fields" tab. Under the "Fields" tab, there are four columns of data: "Date Time", "Authorized By", "Modification", and "Number". Each column has a "Date Time" label below it. To the right of these columns are two checkboxes: "Authorized" and "Open". An "Exit" button is located in the bottom right corner.

Here you can maintain Name and values for Unique Identifiers.

4.9 Static Type Maintenance

Maintenance of Static Types can be done via the Static Type Maintenance screen. You can invoke the 'Static Type Maintenance' screen by typing 'CODTYPES' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows a window titled "Static Type Maintenance". Inside the window, there are three input fields labeled "Type *", "Type Name", and "Value". Below these fields is a tab labeled "Fields". At the bottom of the window, there is a footer area containing the following fields: "Input By", "Date Time", "Authorized By", "Date Time", "Modification Number", and two checkboxes labeled "Authorized" and "Open". An "Exit" button is located on the right side of the footer.

4.10 Maintaining the System Date

You can set/ re-set the Oracle FLEXCUBE ELCM system date in the 'System Date Maintenance' screen. You can invoke the 'System Date Maintenance' screen by typing 'STDDATE' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows a window titled "System Dates Maintenance". Inside the window, there are four input fields labeled "Branch Code *", "Todays Date", "Previous Working Date", and "Next Working Date". Below these fields is a tab labeled "Fields". At the bottom of the window, there is a footer area containing the following fields: "Input By", "Date Time", "Authorized By", "Date Time", "Modification Number", and two checkboxes labeled "Authorized" and "Open". An "Exit" button is located on the right side of the footer.

Select the 'Branch Code' of branch to view its Today (current date), Next Working Date (next working day), and Next Working Date (the working day after the next working day) dates. You can modify the Next Working Date and the Next Working Date before EOD.

5. Maintenance

5.1 Introduction

The Maintenance section deals with the following details:

- Maintaining Product details
- Maintaining currency codes
- Maintaining common currency pairs to quote exchange rates
- Maintaining the currency holidays
- Maintaining exchange rates and rate types

5.2 Maintaining Product Details

You can maintain Product details for ELCM in the 'Product maintenance' screen.

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

Product Maintenance

Source *

Module *

Product Code *

Product Type

Description

Input By DOC003 Authorized By Modification ☐ Authorized
Date Time Date Time Number ☒ Open

Enter the following details:

Source

Specify the associated source for the product processor from the adjoining option list.

Module

Specify the associated module for the product from the adjoining option list.

Product Code

Specify the associated product code.

Product Type

Specify the type of the product.

Description

Describe the product.



Product code and source code is used in a product validation as a part of product maintenance.

5.3 Defining and Maintaining Currency Details

In the 'Currency Definition' screen you can define and maintain the attributes of currencies which your bank deals in. The attributes include the SWIFT code for the currency, the country to which the currency belongs, the interest method, the spot days, the settlement days, and many others.

You can define and maintain currency details only at your bank's Head Office. The maintained details will then be available to all the branches of your bank. You can invoke the 'Currency Definition' screen by typing 'CODCDEFN' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Enter the following details:

Code

Specify the currency code of the currency being defined.

Alternate Code

Specify the alternate code used to identify the currency.

Country

Select the country, to which the currency belongs to, from the list available here.

Cut-Off Time

Transactions received before the cut-off times for the transaction currency will be processed on the same day. Transactions received after the currency cut-off time will be processed the next working day. Specify the Cut-Off Time for the currency using the following fields:

- Days
- Hour
- Minute

Index Currency

Indicates that the maintained currency is a Notional Currency

Euro Conversion

Indicates that the maintained currency falls under Euro Conversion Required

Rounding

If you have selected Round Up or Round Down in the Rounding Rule field, you need to indicate the nearest unit to which the rounding should take place. The number of units specified here should not be greater than the number of decimals allowed for the currency.

Example

The decimal points specified for currency 'A' is 2. Rounding unit is .05

Amount for transaction is USD 100.326, which will be rounded off depending upon the decimals specified and the rounding rule and rounding unit.

For Rounding Rule 'Up', the amount available for transaction would be USD 100.35. For rounding rule 'Down', the transaction amount would have been rounded down to 100.30

If the rounding rule was specified as 'truncate' then, the amount would have rounded off to 100.32 (simply, knock off all decimal points beyond the stated decimals places to be rounded off). Thus whenever you specify a 'truncate' option you need not state the 'Rounding unit'.

Amount Format Mask

Specify the format in which amounts in this currency are to be displayed for contracts in this currency. Two options are available:

- 999,999,999
- 9,999, 999, 99

The system defaults to the 999,999,999 format.

Euro Type

By choosing the appropriate option, you can indicate if the currency is one of the following:

- The Euro
- An 'In' currency
- An 'Out' currency
- 'Euro Closed'

National currencies of 'In' countries are referred to as 'In' currencies. When maintaining other currencies, you have to choose the 'Out Ccy' option under Euro Type.

When the transition period ends, the national currencies of the participating countries would cease to exist as valid legal tenders. The Euro would be the only legal tender in the participating countries. Consequently, the Euro changes made to Oracle FLEXCUBE ELCM will no longer be required.

You can turn off the changes at the end of the transition period by:

- Closing all 'In' currencies, and
- Choosing the 'Euro Closed' option (for the Euro)

5.3.1 **Performing Currency Country Mapping**

You can do mapping of currency countries to the currency using the Currency Country Mapping screen. To invoke this, click 'Currency Country Mapping' button.

For each record, select a Country Code and then give its name/description.

5.4 **Maintaining Currency Pairs for Foreign Exchange**

Certain currency pairs are frequently traded in foreign exchange (ForEx) markets. The exchange rates for such common currency pairs - like USD & GBP or USD & JPY - are easily obtainable. For currency pairs wherein a currency is not traded in often – like ZAR-INR (South African Rand - Indian Rupee) – the ForEx rate is determined through a third currency. This third currency is called the 'Through Currency' and is usually a commonly quoted currency like the US dollar.

You can maintain the ForEx currency pairs common to your business in the 'Currency Pair Maintenance' screen. This maintenance is done at the Bank Head Office level. Invoke this screen from the Menu Browser. You can invoke the 'Currency Pair Maintenance' screen by typing 'CODCPAIR' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

In the above screen you can maintain commonly traded currency pairs (for which a regular market quote is readily available) and their details. For un-common pairs you can specify and maintain a 'Through Currency'.

Currency 1 and Currency 2

Here specify the currency pairs by their currency codes. You can also give brief descriptions/names of the currencies.


Through Currency

Select this check box to maintain a Through Currency for the currency pair.

For commonly traded currency pairs a regular market quote is readily available. For un-common pairs you must specify and maintain a 'Through Currency' to calculate the market quotes.

For the Through Currency you must specify the following:

- Currency Code
- Description or name of the currency
- Quotation Method – Direct or Indirect
- Number of Units for the quotation
- Spread Definition for the quotation
- Points Multiplier

 You need not maintain currency pairs whose through currency is the local currency as defined in the Bank-wide Parameters. This is because during exchange rate computation the local currency is taken as the through currency, unless specified otherwise.

5.5 Specifying Exchange Rates

In the rates input screen you can maintain the following parameters for each rate type and currency pair:

- Mid rate
- Buy spread and sell spread
- Buy rate and sell rate

You can specify the exchange rate and spread details for a currency pair and Rate Type combination in the 'Currency Exchange Rates Maintenance' screen. You can invoke the 'Currency Exchange Rates Maintenance' screen by typing 'CODRATES' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Rate Type	Mid Rate	Buy Spread	Sale Spread	Buy Rate	Sale Rate
-----------	----------	------------	-------------	----------	-----------

Currency 1 and 2

Specify the currency pair for which you are specifying the exchange rates. Specify the pair with regard to the ForEx market quotation method for exchange rates.

Currency Rates

You can specify the following rate and spread details for a currency pair and Rate Type combination:

- Rate Type
- Mid Rate
- Buy Spread
- Sale Spread
- Buy Rate
- Sale Rate
- Rate Date
- Rate Serial

5.6 Viewing Exchange Rates History

You can query for and view a history of all exchange rate maintained for a branch using the 'Exchange Rates History' screen. You can invoke the 'Exchange Rates History' screen by typing 'COSQRATE' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Exchange Rates Query

Branch Code Currency1

Currency2 Rate Type

From Date To Date

Records per page 15 1 Of 1 Go to Page

Branch Code	Currency1	Currency2	Rate Type	From Date	To Date	Mid Rate	Buy Rate	Sale Rate	Rate Sequence
-------------	-----------	-----------	-----------	-----------	---------	----------	----------	-----------	---------------

To query for a rate history, specify the following details first:

- Branch Code of the branch for which the rate history must be displayed
- Currency 1 and 2 involved in the foreign exchange transaction
- Rate type applied to the transaction
- To Date to specify the date till when the rates history must be shown

Once you specify the above details, click 'Query' button to view the results.

5.7 Maintaining Currency Rate Types

Your bank may quote different exchange rates for different ForEx transaction types. This means that the quote for currency exchange maybe different from that for Travellers Cheques.

To maintain currency rate types, use the 'Currency Rate Type Maintenance' screen. You can invoke the 'Currency Maintenance' screen by typing 'CODCRTYP' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Currency Rate Type				
Type*				
Description*				
Fields				
Input By	Authorized By	Modification	<input type="checkbox"/> Authorized	Exit
Date Time	Date Time	Number	<input type="checkbox"/> Open	

In the above screen you can maintain the rate types applicable to different transaction categories of your bank. The exchange rate corresponding to each maintained rate type can be specified in the Rate Definition screen.

Type

Assign a name to the rate type you wish to maintain here.

Description

Give a brief description of the rate type maintained.

Example

You can define a rate type called CASH. This rate type can be applied to all cash transactions in foreign currency. Another rate type called TRAV-CHKS can be used for traveller's cheques.

On defining a product for transaction type, you can also assign a rate type to the product. This rate type will then be applied to all contracts of the product. The Currency Rate Type maintenance is done for each bank branch at the Bank Head Office.

6. Gateway Maintenance

6.1 Introduction to Oracle FLEXCUBE ELCM Gateway

The Oracle FLEXCUBE ELCM Gateway processes allow seamless communication and integration of the Oracle FLEXCUBE ELCM system with a variety of other specialized applications. These other systems maybe deployed on different platforms and may use different infrastructure. The Gateway bridges the external system and the Oracle FLEXCUBE ELCM system.

Oracle FLEXCUBE ELCM Gateway provides two main kinds of processes:

- Gateway Online process
- Gateway Batch process

6.2 Defining an External System

To define an external system that will communicate via the Oracle FLEXCUBE ELCM Gateway, you need to use the 'External System – Detailed' screen. You can invoke the 'External System - Detailed' screen by typing 'GWDEXTSY' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows the 'External Systems - Detailed' window. It includes the following elements:

- External System:** Fields for 'External System*' and 'Description'.
- Correlation Pattern:** A 'Request' dropdown menu currently showing 'Message ID'.
- Message Exchange Pattern:** 'Request Message' dropdown set to 'Input Only' and 'Response Message' dropdown set to 'Full Screen'.
- Queue:** Text boxes for 'Default Response Queue' and 'Dead Letter Queue'.
- Validation and Registration:** Checkboxes for 'XSD Validation Required' and 'Register Response Queue Message Id'.
- External System Queues:** A table with two columns: 'In Queue*' and 'Response Queue'. It contains one row with empty text boxes and a small icon.
- Fields:** A bottom section with 'Input By', 'Authorized By', 'Modification Number', and checkboxes for 'Authorized' and 'Open', followed by an 'Exit' button.

Enter the following details:

External System

Specify a name for the external system. This should be the same as the Source in an incoming message.

Description

Specify a brief description for the External System.

Correlation Pattern - Request

You can define a way in which the external system should correlate its request message with the response message. You can choose Message ID of a request message as the Correlation ID in the response message. Alternatively, you can choose Correlation ID of a request message and maintain it as the Correlation ID of the corresponding response message.

Message Exchange Pattern - Request Message

You can choose the Request message to be 'Full Screen' or 'Input Only'.

Message Exchange Pattern - Response Message

You can choose the Response message to be 'Full Screen' or 'Primary Key'.

Queue - Default Response Queue

You can define a response queue for each of the In Queue's through which the External System will communicate with the system. Define a valid queue name as the Default Response Queue.

Queue - Dead Letter Queue

If the messages received are non-readable, such messages are directed to Dead Letter Queue defined for the external system.



If the Dead Letter Queue is not defined, such messages will be redirected to a queue with the name of the request queue appended with '_E'.

XSD Validation Required

Check this box to indicate if the request message should be validated against its corresponding XSD.

Register Response Queue Message ID

Check this box to indicate if the message ID provided by the Response Queue should be logged when a response message is posted into the queue.

6.2.1.1 Maintaining External System Queues

The 'External System Queues' list contains the 'In Queue' and 'Response Queue' lists. To add a record to the 'External System Queues' list click 'Plus' button. To delete a record from the list, you need to select the record using its check box and then click 'Minus' button. To view the details of a selected record click 'Details' button.

In Queue

Specify the name of the queue from which the messages were received. The name of the queue will help identify the external system.



This is required only if an incoming message does not display the source of the message. An In Queue is mapped to only one External System.

You can map multiple queues to a source. System will allow a source to post messages to multiple queues.

Response Queue

You can define Response Queue for every In Queue. This is required only when the External System fails to display the queue name on posting a request message into the In Queue.

6.3 Defining Access Rights to an External System

You can define access rights to an external system using the 'External System Functions – Detailed' screen. You can invoke the 'External System Functions - Detailed' screen by typing 'GWDEXTFN' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

External System Functions - Detailed

External System * [List Icon] Description

Function * [List Icon]

Action * [List Icon]

Service Name [List Icon]

Operation Code [List Icon]

Fields

Input By Date Time Authorized By Date Time Modification Number ☐ Authorized ☐ Open Exit

In the screen above, you need to specify the following details:

External System

Select an external system for which you wish to provide access rights. Click on the adjoining option list to display the list of values. The list displays all the external systems you have maintained in the 'External Systems – Detailed' screen.

Function ID

Select a Function ID from the list of values by clicking on the adjoining option list. The function ids are invoked from Gateway Functions.

Action

Select an action for the external system.

The following fields will be displayed in the screen:

Service Name

This displays the service name based on the Function ID and Action you select.

Operation Code

This displays the Operation Code based on the Function ID and Action you select.

6.4 External Communicator

You can maintain the details of the communication channel used by the Oracle FLEXCUBE ELCM Gateway system to communicate with the external system. This maintenance can be done in the 'External Communicator Maintenance' screen.

You can invoke the 'External Communicator Maintenance' screen by typing 'GWDECOMM' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

External Communicator Maintenance

Interface Id *

External System *

Communication Channel

☒ Web Service

☐ Available Queues

☐ HTTP

☐ EJB

Request Queue

Reply Queue

Request XSLT *

Reply XSLT *

Timeout Interval

Retry Count

☐ Response Required

Fields

Input By
Date Time

Authorized By
Date Time

Modification
Number

☐ Authorized

☐ Open

Exit

Enter the following details:

Interface ID

Specify the interface ID here.

External System

Specify the External System here.

Communication Channel

Indicate the kind of communication channel for which this maintenance is being done. The available channels are:

- Web Service

- Queue
- HTTP
- EJB (Enterprise Java Beans, the default value)

Request Queue and Reply Queue

Specify the queues for the Request and Reply messages.

Request XSLT and Reply XSLT

Specify the names of the Request and Reply XSLTs. Add the extension '.xml' to the names.

Timeout Interval

Specify in seconds the maximum time interval before which the communication must be timed out.

Retry Count

Specify the number of times the communication should be re-tried upon time out.

Response Required

Specify whether a response is required for your communication.

6.5 Interface Definition

After you maintain the names of external systems, you can define the actual external system interface related details. You can maintain these details through the 'Interface Definition Maintenance' screen. You can invoke the 'Interface Definition Maintenance' screen by typing 'GWDINTDF' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Enter the following details:

Interface ID

Specify the unique Interface ID to identify the interface between the external system and Oracle FLEXCUBE ELCM.

Function ID

Specify the function ID related to the interface.

Description

Briefly describe what the interface is all about. The description that you enter is for information purposes only and will not be printed on any correspondence with your customer.

File Type

Specify whether the file is used for the interface will be of Fixed or Delimited type.

Delimiter

Specify the Delimiter, if any, used in the interface file. If no delimiter is specified, the '\$' symbol is taken as the delimiter by default.

Interface Type

Indicate whether the interface is an Outbound Interface or an Inbound Interface.

An Outbound Interface is one, which results in the transfer of data from Oracle FLEXCUBE ELCM to an external system. When data is received into Oracle FLEXCUBE ELCM from an external source it is called an Inbound Interface.

Date Format

Indicate the filename mask from which data is to be read. For outgoing interfaces data is written according to the filename mask parameters that you set.

An example of the filename mask would be 'YYYYMMDD'.

File Name

Click the 'File Name' to specify the details of the input file and its directory path.

6.6 Defining the Notifications Enroute

You can invoke the 'Notification Enroutes - Detailed' screen by typing 'GWDNTFEN' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Input By	Authorized By	Modification Number	<input type="checkbox"/> Authorized
Date Time	Date Time		<input type="checkbox"/> Open

In 'Notification Enroutes - Detailed' screen, you define the following details:

Branch Code

Specify a branch for which you wish to define a topic. If you want to use a single topic for all branches and for a given notification code, you can use a wildcard '***'. Once you select a Branch Code, the corresponding description is displayed.

Notification Code

Select a notification code from the list of notification codes provided. You can indicate a wildcard '***' if a single topic needs to be used for all notifications in a branch.

Destination Name

Define a topic or a queue here. If you define a topic, you can assign multiple notification codes for a branch. In case of a queue, you can define only one notification code for each branch.

6.7 Defining Notifications Installed Messages

At the branch level, you can maintain notification codes for each branch. You can do this using the 'Notifications Installed' screen. You can invoke the 'Notification Installed Detailed' screen by typing 'GWDNTFIN' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Notifications Installed - Detailed

Branch Code * [dropdown]
Notification Code * [dropdown]
Branch Name [dropdown]
Description [dropdown]

Fields

Input By [dropdown] Authorized By [dropdown] Modification Number [dropdown] ☐ Authorized
Date Time [dropdown] Date Time [dropdown] ☐ Open

Exit

In this screen, you need to specify the following details:

Branch Code

Select a branch code for which you wish to assign a notification code. Once you select the branch code, the corresponding description is displayed.

Notification Code

From the list of values, select a notification code you wish to link with the branch. This will be used to generate notifications for the entire branch. Once you select the notification code, the corresponding description is displayed.

In addition to maintaining a notification code for a given branch, you can also specify a topic or a queue to which the notification messages should be sent.

You can define a topic/queue for a given branch and notification code in the 'Notifications Enroute' screen.

6.8 Incoming Message Browser

The messages received from the external system can be queried for in the 'Incoming Message Browser Summary' screen. You can invoke the 'Incoming Message Browser Summary' screen by typing 'GWSINBRW' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows the 'Incoming Message Browser - Summary' window. It features a search interface with two columns of criteria fields. The first column includes Message Reference Number, External System, Correlation Identification, Service Name, User Identification, Branch Date, and Message Status. The second column includes Branch, Message Identification, Request Queue Message Identification, Operation Code, Their User Identification, Server Date Stamp, and Flexcube Reference Number. Below the fields is a search bar with 'Search', 'Advanced Search', and 'Reset' buttons. To the right of the search bar are 'Records per page' (set to 15), '1 of 1' pages, and a 'Go to Page' field. Below the search bar is a table with columns: Message Reference Number, Branch, External System, Message Identification, Correlation Identification, and Request Queue Message Identification. The table is currently empty. At the bottom right is an 'Exit' button.

This summary screen can be used to search for incoming messages which match the any of the following criteria:

- Transaction Code
- External System
- Operation Code
- Action
- Branch
- Service Name
- Function
- User ID

The 'Result' list shows the messages which match your query.

The following details of the messages received from the external systems are displayed in the summary screen results.

- Transaction Code
- Branch
- External System
- Service Name
- Operation Code
- Function
- Action
- User ID
- Transaction Status

The search functions available are:

Advanced

Click 'Advanced' to specify queries with logical operators such as AND, OR and NOT.

Reset

Click 'Reset' to empty the values in the criteria fields, so that you may begin a new search.

Query

After specifying your search criteria click 'Query' to view the list of results which match your search criteria.

Refresh

Click 'Refresh' to refresh the list of results.

6.9 Outgoing Message Browser

Once the incoming messages have been processed, a response message will be sent to the external systems along with the status of the processed messages. You can query for these response messages in the 'Outgoing Message Browser Summary' screen. You can invoke the 'Outgoing Message Browser Summary' screen by typing 'GWSOTBRW' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Outgoing Message Browser - Summary

Message Reference Number

Related Message Reference

Service Name

Message Identification

Response Queue Message Identification

Their User Identification

Server Date Stamp

Branch

External System

Operation Code

Correlation Identification

User Identification

Branch Date

Message Status

Search Advanced Search Reset Records per page 15 1 of 1 Go to Page

<input type="checkbox"/>	Message Reference Number	Branch	Related Message Reference	External System	Service Name	Operation Code	Message Identification
--------------------------	--------------------------	--------	---------------------------	-----------------	--------------	----------------	------------------------

Exit

This query screen can be used to search for outgoing messages which match the criteria you specify. You can specify any or all of the following criteria:

- Transaction Code
- Related Message Reference
- Service Name
- User ID
- Branch
- External System
- Operation Code

The 'Result' list shows the messages which match your query.

The search functions available are:

Advanced

Click on 'Advanced' to specify queries with logical operators such as AND, OR and NOT.

Reset

Click on 'Reset' to empty the values in the criteria fields, so that you may begin a new search.

Query

After specifying your search criteria click on 'Query' to view the list of results which match your search criteria.

Refresh

Click on 'Refresh' to refresh the list of results.

6.10 Input File Processing

The processing of input files for the interface can be done via the 'Input File Processing' screen.

You can invoke the 'Input File Processing' screen by typing 'GWDINFUP' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows a window titled "Input File Processing". It contains the following fields and controls:

- Interface Id ***: A text input field.
- File Name ***: A text input field.
- Process Status**: A dropdown menu.
- Execute Button**: A button located below the Process Status dropdown.
- Description**: A text input field.
- Path**: A text input field.
- Force Run**: A checkbox.
- Exit**: A button located at the bottom right of the window.

Enter the following details:

Interface Identification

Specify the Interface for which the input file is being processed. Select the Interface ID from the list available here. On selecting an ID, the interface description is displayed in the field alongside.

File Name

Specify the input file name here. The file name should have the extension '.txt'. This means that only text files are allowed. Select the File name from the list available. On selecting a file name, the directory path (storage location) of the file is displayed in the field alongside.

Status

Specify the status of the file processing – File To Upload or Upload to Master.

Click 'Execute' button to execute the processing of the Input File.

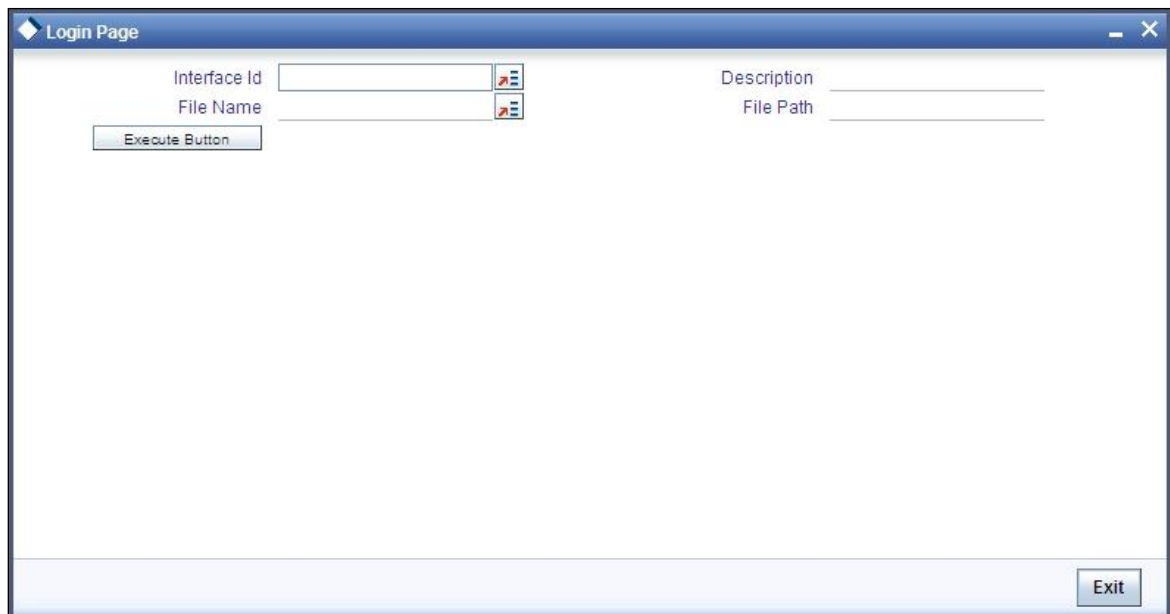
Force Run

If the file processing fails, you must re-enter the above details in the screen. Then select the Force Run check box before clicking 'Execute' button.

6.11 Output File Processing Screen

The processing of output files for the interface can be done via the 'Output File Processing' screen.

You can invoke the 'OutPut File Processing' screen by typing 'GWDOUFUP' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



The screenshot shows a window titled 'Login Page' with a blue header bar. Inside the window, there are four input fields arranged in a 2x2 grid. The top-left field is labeled 'Interface Id', the top-right is 'Description', the bottom-left is 'File Name', and the bottom-right is 'File Path'. Each field has a small icon to its right. Below the 'Interface Id' and 'File Name' fields is a button labeled 'Execute Button'. In the bottom right corner of the window is an 'Exit' button.

Enter the following details:

Interface Identification

Specify the Interface for which the output file is being processed. Select the Interface ID from the list available here. On selecting an ID, the interface description is displayed in the field alongside.

File Name

Specify the output file name here. Select the name from the list available. On selecting a file name, the directory path (storage location) of the file is displayed in the field alongside.

Click 'Execute' button to initiate the processing of the Output File.

6.12 Input File Process and Output File Process Monitor

You can query for and view the status of input and output file processing in the 'Input File and Output File Process Monitor' screen. You can invoke the 'Input File and Output File Process Monitor' screen by typing 'GWSIOSTS' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

File Name	Process ID	Interface ID	Start Time	End time	Process Status	Error Code	Remarks
-----------	------------	--------------	------------	----------	----------------	------------	---------

You can specify any or all of the following criteria for your query here:

- Authorization Status
- File Name
- Record Status
- Interface ID

The following details will be displayed in the results displayed

- Authorization Status
- Record Status
- File Name
- Process ID

- Interface ID
- Start Time
- End Time
- Status
- Error Code
- Remarks

The search functions available are:

Advanced

Click 'Advanced' to specify queries with logical operators such as AND, OR and NOT.

Reset

Click 'Reset' to empty the values in the criteria fields, so that you may begin a new search.

Query

After specifying your search criteria click 'Query' to view the list of results which match your search criteria.

Refresh

Click 'Refresh' to refresh the list of results.

6.13 Maintaining Upload Sources

Sources, from where file upload has to be performed for the gateway, can be maintained in the 'Upload Source Maintenance' screen. You can invoke the 'Upload Source Maintenance' screen by typing 'CODSORCE' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows the 'Upload Source Maintenance' window. It contains the following elements:

- Title Bar:** 'Upload Source Maintenance' with a close button (X).
- Form Fields:**
 - 'Source Code *' with a red asterisk indicating a required field.
 - 'Description' with a help icon (question mark in a circle).
 - A checkbox labeled 'Base Data From Flexcube'.
- Fields Section:** A tab labeled 'Fields' is active, showing a list of fields: 'Input By DOC2', 'Date Time', 'Modification Number', 'Authorized By', 'Date Time', 'Authorized', and 'Open'. The 'Open' checkbox is checked.
- Buttons:** A 'Cancel' button is located at the bottom right.

In the above screen, specify a 'Source Code' for the source. You may also give a brief description of the source.

7. End of Day Process

7.1 Introduction

The objective of the End of Day (EOD) cycle and processes is to perform the revaluation of operation and system date changes i.e. moving the Limit Server application date to the next working date.

EOD cycles in Oracle FLEXCUBE ELCM have a certain predefined stages/status which happens in the order given below:

- Mark End of Transaction Input (Mark EOTI)
- Post End of Transaction Input (Post EOTI)
- Facility Batch
- Date Change (DTCHG)
- Post Beginning of day (Post BOD)
- Mark Transaction Input (Mark TI)
- Post Mark Transaction Input (Post MarkTI)

Before running an EOD cycle there are some basic maintenances which you must do. These maintenances are explained below.

7.2 System Date Maintenance

The next working day for a particular branch has to be maintained in the 'System Date Maintenance' screen.

For details on System Date Maintenance, refer the section in the Core chapter of this User Manual

7.3 Maintaining Mandatory Batch Programs

Batch operations like Facility Batch, Reval (Collateral, currency) batch etc to be run during EOD cycle, their details must to be maintained using the 'Mandatory Batch Program Maintenance' screen. You can invoke the 'Mandatory Batch Program Maintenance' screen by typing 'EIDMANPR' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

The screenshot shows the 'Mandatory Batch Program Maintenance' window. It contains the following fields and controls:

- Branch ***: Text input field.
- Module ***: Text input field.
- End Of Cycle Group ***: Dropdown menu with 'End Of Day' selected.
- Function Identification ***: Text input field.
- Description**: Text input field.
- Sequence Number ***: Text input field.
- Error Handling**: Two radio buttons.
 - ☒ Stop Automatic End Of Day and Run Emergency Program
 - ☐ Continue with Automatic End Of Day
- Fields**: A tab at the bottom.
- Summary Section**:
 - Input By: [blank]
 - Date Time: [blank]
 - Authorized By: [blank]
 - Date Time: [blank]
 - Modification Number: [blank]
 - Authorized: ☐
 - Open: ☐
 - Exit button

Enter the following details:

Branch

Specify the Branch Code for which the batches need to be maintained.

Function Identification

Specify the Batch Name / function Id of the batch needs to be specified by using the list available here.

End of Cycle Group

The end of cycle (EOC) group that the batch needs to be run during EOD cycle has to be indicated here.

Error Handling

Indicate the action that must be taken if the EOD process runs into an error. You can indicate either of the following:

- Stop automatic EOD and run emergency program
- Continue with the Automatic EOD program

Module

Specify the module with regard to which the batch process is executed.

Sequence Number

Specify the sequence number of the batch process.

7.4 Running the End of Day Batch Process

After the above maintenances, the End of Day Batch Process - AEOD can be run using the 'End of Day Batch Start' screen. You can invoke the 'End of Day Batch Start' screen by typing 'AEDEODST' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.

Branch Code	Current Status	Run Till
<input type="checkbox"/>		

All the branches that are maintained in Oracle FLEXCUBE ELCM will be displayed under 'Branch Code' in this screen.

To run a branch/branches select the check box for each branch. This action displays the current status of the branch. Then, under 'Run Till', specify the Stage/status till which the EOD cycle has to be run.

Once you have selected all the required branches, click 'Ok' to start the AEOD cycle.

On starting of the AEOD cycle the following process stages will occur in a sequential order:

1. **Mark End of Transaction Input (Mark EOTI):** This process will check for unauthorized Transactions, Holiday Maintenance checks and Process that has been pending as a part of Post MarkTI.
This process also checks if all the batches as a part of POST MarkTI have been run successfully. If not, then all the unsuccessful batches as part of POST MarkTI are re-run. Once the Mark EOTI is processed and successful, the branch status will be changed to 'EOTI'. After this stage and until MARK TI stage is completed no transactions will be allowed to process.
2. **Post End of Transaction Input (Post EOTI):** All batches, which are maintained for the branch under EOC process, are run as a part of this stage.
As a part of EOD batch processing in POST EOTI there are certain batches to be run in a specific order. These are explained under the 'EOD Batch Processing Post EOTI' section.

3. Date Change (DTCHG): In this stage, the system date / branch date/Branch Application date is changed to the next working date. If the Next Working Date falls in the next Period Code then the branch will be updated accordingly.
4. Post Beginning of day (Post BOD): All batches, which are maintained for the branch under EOC process, are run as a part of this stage.

The batches that can be maintained as a part of Post BOD are as follows:

- Facility Batch (Fast Path: GEBFACLT) - As part of this batch all the tanked utilization which has happened as part of utilization transaction will be un-tanked and the tanked amount for the facility of that branch will be set back to Zero.
 - Archival Batch (Fast Path : ARCBATCH) - This batch involves the process where in all the Records in the upload tables incase of input file processing will be migrated to Respective Archive Tables.
5. Mark Transaction Input (Mark TI): Checks if all the batches as a part of Post BOD have been run successfully .If not they are re-run as part of POST BOD. It will change the status of the Branch Transaction Input: Post Mark Transaction Input (Post MarkTI)

All batches, which are maintained for branch under EOC process, will be run as a part of this stage.

7.5 Viewing the AEOD Process Details

All the above process flow stages can be viewed using AEOD Monitor Screen as shown below:

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

Summary

Branch Status

Process Event Sequence Number

Records per page 1 Of 1

Branch	Status	Process	Event Sequence Number	Error Code	Reason	Start Time	End Time	End of Cycle	User Id	Terminal ID
--------	--------	---------	-----------------------	------------	--------	------------	----------	--------------	---------	-------------

Status S - Success X - Running E - Error

Flag N - Transaction Input T - End Of Transaction Input E - End Of Day B - Beginning Of Day

All errors and successful processes can be viewed in the AEOD Monitor.

7.6 EOD Batch Processing Post EOTI

As a part of EOD batch processing in POST EOTI there are certain batches to be run in a specific order as mentioned below.

7.6.1 Market Revaluation Batch (Screen Code: GEBMAREV)

The price of the security changes every day. This price change should effect the market value based collateral, and in turn the collateral contribution to line code. This process of recalculation due to security price change is called Security Revaluation.

Currency Revaluation - Due to exchange rate variation every day, the value of the limit available amount will be made recalculated. This process of recalculation due to exchange rate variation is Currency Revaluation.

7.6.2 Currency Revaluation Batch (Screen Code: GEBCYREV)

This batch takes care of the revaluation of Limit Contribution as a part of collateral due to change in Exchange rates. This is only if the collateral currency and collateral pool currency are different and there is a change in exchange rate between the two pairs maintained for Collateral and Collateral Pool.

This batch also takes care of revaluation of Collateral Contribution as a part of Facility maintenance due to change in Exchange rates. This is only if the Collateral Pool currency and Facility currency are different and there is a change in exchange rate between the two pairs maintained for Collateral Pool and Facility.

7.6.3 Utilization Batch (Screen Code: GEBUTILS)

As a part of this batch, Value Date Balances will be updated if the value date updating is a part of batch processing (according to Gems Parameters). Also Exposures Update will be updated if the Exposures updating is a part of batch processing (according to Gems Parameters).

7.6.4 Facility Batch (Screen Code: GEBFACTL)

- As a part of this batch all the Line Code, Collaterals and Securities which have crossed their Expiry date will be made Unavailable.
- Freeing of limits.
- If the covenants for the particular collateral or facility are not submitted with the defined covenant renewal date.
- If Facility Review date is crossed
- If User Defined Status for the facility is in bad status.
- Availment expiry date
- If the limit amount assigned to the facility is not utilized with in the specified expiry date then available flag will be turned off. Hence freezing the line for respective liability.
- Recalculation of Rolling Tenors
- Handles Limit Transfer Expiry
- Intra Day utilization for each facility will be set to zero.
- Back Up of line code, utilization and liability details into history/Archival will be done.
- End of cycle group: This batch has to run during the EOTI (End of Transaction Input)

7.6.5 Collateral Batch (Screen Code: GEBCOLAT)

As a part of collateral batch all the expired collaterals will be taken up and the their respective limit contribution will be made to zero and the corresponding linked Collateral Pools and Facility will be updated with the latest value.

7.7 **Integrating Oracle FLEXCUBE EOD Process with ELCM**

Oracle FLEXCUBE facilitates integrating EOD process of Oracle FLEXCUBE and ELCM. It allows you to maintain all the batches of ELCM in Oracle FLEXCUBE. After integrating there will be only one EOD process of Oracle FLEXCUBE and ELCM. And you have to link all the batches associated to ELCM as part of Oracle FLEXCUBE EOD maintenance.

The table below lists the batches that are ELCM batches maintained as part of Oracle FLEXCUBE EOD mandatory programs and which are executed before Post EOTI stage of Oracle FLEXCUBE

SI No	Batch Name	Description
1	ELBCOMNT	Commitment Batch

7.7.1 **Commitment Batch (Screen Code: ELBCOMNT)**

During EOD, as part of commitment batch (ELBCOMNT), commitment contracts are created where commitment products are linked to a facility. When utilizations or payments are triggered for the facility, the batch will also fire the LINK/DLINK events for the commitment contract. Whenever amendments are done to the facility, corresponding changes will be done to the commitment contracts. During this batch, charges will be calculated as part of events triggered for the commitment contract, for instance when there is a change in the facility limit amount or when an unadvised facility is utilized.

Refer the chapter 'Maintenances and Operations' in the Retail Lending User Manual for details on the SDEs used to calculate the charges.

The table below explains ELCM batches maintained as part of Oracle FLEXCUBE EOD mandatory programs and these batches are executed before Mark EOFI stage of Oracle FLEXCUBE.

SI No	Batch Name	Description
1	ELBCOLAT	Collateral Batch
2	ELBFACTL	Facility Batch
3	ELBCYREV	Currency Revaluation Batch
4	ELBMRKAT	Market Revaluation Batch
5	ELBUTILS	Utilization Batch

Oracle FLEXCUBE EOD framework is used to trigger the EOD process for both system Oracle FLEXCUBE and ELCM. The ELCM batches are maintained as part of Oracle FLEXCUBE batch maintenance.

During EOD process, if the processing batch is of ELCM then batch process invokes ELCM batch process. After completing ELCM batch process, ELCM updates the batch status in Oracle FLEXCUBE.

7.7.2 **Running EOD Process**

The common EOD process triggers from Oracle FLEXCUBE. Oracle FLEXCUBE triggers the EOD process in ELCM only for the branches for which 'ELCM replication' option is selected.

Before running EOD process in Oracle FLEXCUBE, you need to check the unauthorized transactions in both Oracle FLEXCUBE and ELCM system.

On starting the common EOD cycle the following stages will occur:

1. As a part of MarkEOTI process,
 - Oracle FLEXCUBE triggers MarkEOTI process in ELCM system.
 - If there are any errors in marking the EOTI in ELCM, then ELCM will send the error details to Oracle FLEXCUBE and Oracle FLEXCUBE will abort the EOD process with the ELCM error.
 - If ELCM MarkEOTI is completed, then Oracle FLEXCUBE will continue with its process.
2. After marking the EOTI,
 - Oracle FLEXCUBE EOD process will continue with the Post EOTI batches.
 - If any batches are related to ELCM, then Oracle FLEXCUBE triggers batch processing in ELCM.
 - If any error occurs as part of ELCM batch process, then ELCM process will send the error details to Oracle FLEXCUBE and Oracle FLEXCUBE will mark ELCM batch as aborted and will resubmit ELCM batch.
3. As part of MarkEOF1 process, Oracle FLEXCUB does not trigger any process in ELCM.
4. If any ELCM batches are attached as part of post EOF1, then system triggers ELCM batch.
5. As a part of MarkEOD process, Oracle FLEXCUBE will not trigger any process in ELCM.
6. As part of 'Date Change' process, Oracle FLEXCUBE triggers 'Date Change' process in ELCM.
7. If any ELCM batches are attached as part of BOD, then system triggers ELCM batch.
8. As part of 'MarkTI' process, Oracle FLEXCUBE would trigger "MarkTI" process in ELCM.



If there are any separate branches maintained as a part of ELCM, then it is not linked to any Oracle FLEXCUBE instances therefore separate EOD process has to be executed in ELCM standalone system.

8. Annexure 1- Personally Identifiable Information

8.1 Creating/Querying Customers of Restricted AccessGroup

Oracle FLEXCUBE allows granular access to customers and accounts. You can define access groups for the retail and corporate customers and restrict the access to these groups based on the maintenance in 'Access Group Restriction' in 'User Maintenance' screen.

If the access group is maintained as 'Disallowed' in the Access Group Restriction screen, then you cannot create and query the customer and account details of the group from the following screens:

Function ID	Description
GEDCOLLT	Collateral Maintenance
GEDCULIK	Customer to Liability Link Maintenance
GEDFACTL	Facilities Maintenance
CODCIFDF	Customer Maintenance
COSCIFDF	Customer Maintenance Summary screen

8.2 Masked/Unmasked PII

If 'PII Allowed' flag is unchecked in User Maintenance (SMDUSERD) screen, then you will be able to view only the masked PII information from the following screens:

Function ID	Description
GEDCOLLT	Collateral Maintenance
GEDCULIK	Customer to Liability Link Maintenance
GEDFACTL	Facilities Maintenance
CODCIFDF	Customer Maintenance
COSCIFDF	Customer Maintenance Summary screen

9. Screen Glossary

9.1 Function ID List

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

Function ID	Function Description
AEDEODST	Login Page
AESEODMR	Summary
CODCATGY	Category Maintenance
CODCIFDF	Customer Details
CODEXPTY	Exposure Maintenance
CODGROUP	Group Maintenance
CODHCUTT	Haircut Maintenance
CODLOCCD	Location Maintenance
GEDMLIAB	Liability Maintenance
CODRESTY	Restriction Maintenance
CODSORCE	Upload Source Maintenance
CODTYPES	Static Type Maintenance
CODUIDN	Unique Identifier Maintenance
CODCDEFN	Currency Definition
CODCPAIR	Currency Pair Maintenance
CODCRTYP	Currency Rate Type Maintenance
COSQRATE	Exchange Rates History
CODRATES	Currency Exchange Rates Input
CODACGRP	Access Group Maintenance
CODCSFRT	Forget Customer Process
EIDMANPR	Mandatory Batch Program Maintenance
GWDECOMM	External Communicator Maintenance

Function ID	Function Description
GWDEXTFN	External System Functions - Detailed
GWDEXTSY	External System Maintenance
GWDINFUP	Input File Processing
GWDINTDF	Interface Definition Maintenance
GWDNTFEN	Notifications Enroute Maintenance
GWDNTFIN	Notifications Installed - Detailed
GWDOUFUP	OutPut File Processing
GWSINBRW	Incoming Message Browser
GWSIOSTS	Summary
GWSOTBRW	Outgoing Message Browser
SMDBNKPR	SMS Bank Parameters Maintenance
SMDBRRES	Branch Restrictions
SMDFNDS	Function Description Maintenance
SMDLNGCD	Language Code Maintenance
SMDRLMNT	Role Limits Maintenance
SMDROLDF	Role Maintenance
SMDSOPRM	Single Sign On Maintenance
SMDUSERD	User Maintenance
CODBNKPR	Bank Parameters Maintenance
SMDBRANH	Branch Parameters Maintenance
SMDUSFRT	Forget User Process
STDCNTRY	Country Code Maintenance
STDDATE	System Dates Maintenance
CODBRHOL	Local Holiday Calendar Maintenance
UDDFNMNT	User Defined Fields Function Field Mapping Maintenance
UDDMNTFN	User Defined Fields Maintenance

Function ID	Function Description



Enterprise Limits and Collateral Management
[May] [2018]
Version 12.1.0.0.1

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
[www.oracle.com/ financial_services/](http://www.oracle.com/financial_services/)

Copyright © [2018] Oracle Financial Services Software Limited. All rights reserved.

No part of this work may be reproduced, stored in a retrieval system, adopted or transmitted in any form or by any means, electronic, mechanical, photographic, graphic, optic recording or otherwise, translated in any language or computer language, without the prior written permission of Oracle Financial Services Software Limited.

Due care has been taken to make this document and accompanying software package as accurate as possible. However, Oracle Financial Services Software Limited makes no representation or warranties with respect to the contents hereof and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this document and the accompanying Software System. Furthermore, Oracle Financial Services Software Limited reserves the right to alter, modify or otherwise change in any manner the content hereof, without obligation of Oracle Financial Services Software Limited to notify any person of such revision or changes.

All company and product names are trademarks of the respective companies with which they are associated.