Security Management System User Guide

Oracle FLEXCUBE Universal Banking

Release 14.7.1.0.0

Part No. F77194-01

May 2023

ORACLE

Security Management System User Guide
Oracle Financial Services Software Limited
Oracle Park

Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India
Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
https://www.oracle.com/industries/financial-services/index.html

Contents

1. Preface

1.1 Introduction

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

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

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

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

1.2 Audience

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

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

1.3 Documentation Accessibility

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

1.4 Organization

This manual is organized into the following chapters:

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

Chapter 2	*Security Management* explains how to define and maintain the security of the banking system in terms of users access and roles.
Chapter 3	*Associated Functions* discusses on the details pertaining to defining and maintaining additional security options such as clearing user profile, changing system time level, maintaining SSO parameters, error Messages, and viewing user activity, branch status, and so on.
Chapter 4	Annexure A - Personally Identifiable Information has customer's information.
Chapter 5	*Function ID Glossary* has alphabetical listing of Function/Screen IDs used in the module with page references for quick navigation.

1.5 Abbreviations

Abbreviation	Description
FC	Oracle FLEXCUBE
AEOD	Auto End of Day
BOD	Beginning of Day
EOD	End of Day
EOTI	End of Transaction Input
EOFI	End of Financial Input
The System	This term is always used to refer to Oracle FLEXCUBE
SI	Standing Instructions
MM	Money Market
RM	Relationship Manager

1.6 Glossary of Icons

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

Icons	Function
	Exit
	Add row
	Delete row

Icons	Function
	Option List

1.7 Related Documents

- The Procedures User Manual
- Common Core - Security Management System User Guide

2. Security Management

2.1 Introduction

This chapter contains the following sections:

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

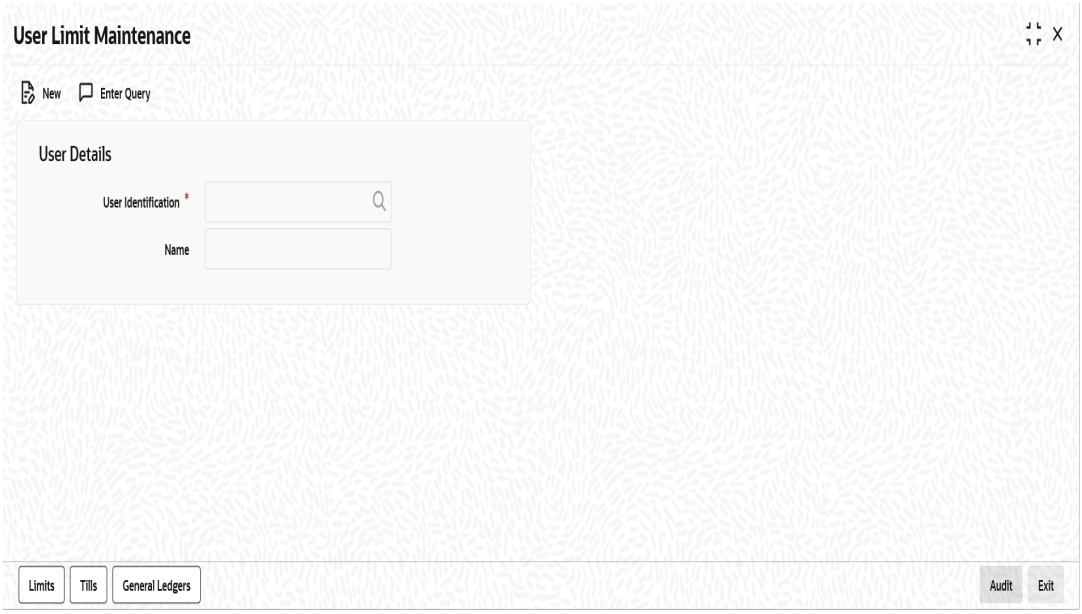
2.2 User Limit Maintenance

This section contains the following topics:

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

2.2.1 Invoking User Limit Maintenance Screen

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



User Identification

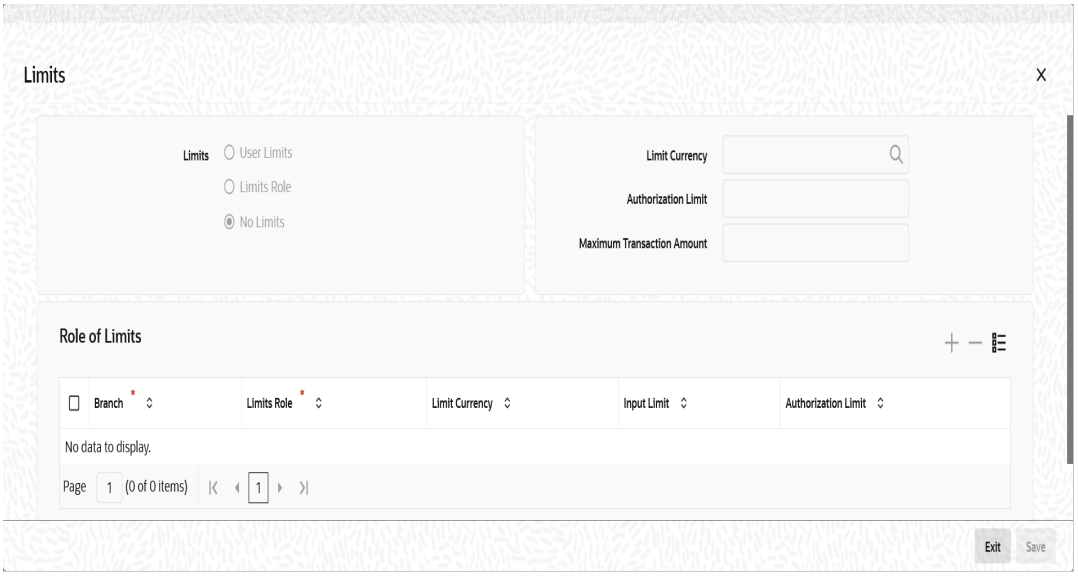
Specify the user identification code. Alternatively, you can select the user identification code from the option list. The list displays all valid values.

Name

The system displays the name of the user.

2.2.2 Limits Button

Click ‘Limits’ button to invoke the Limits screen.



Limits

Select the limits from the following options:

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

Limit Currency

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

Authorization Limit

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

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

Maximum Transaction Amount

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

Role of Limits

Branch

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

Limits Role

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

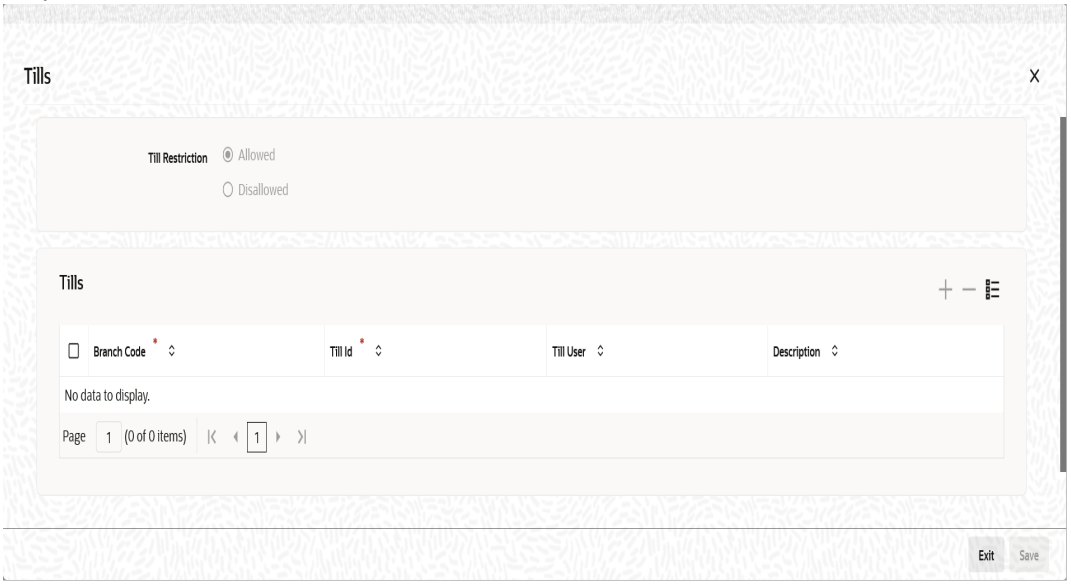
- Limits Currency
- Input Limit
- Authorization Limit

Note

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

2.2.3 Tills Button

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



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

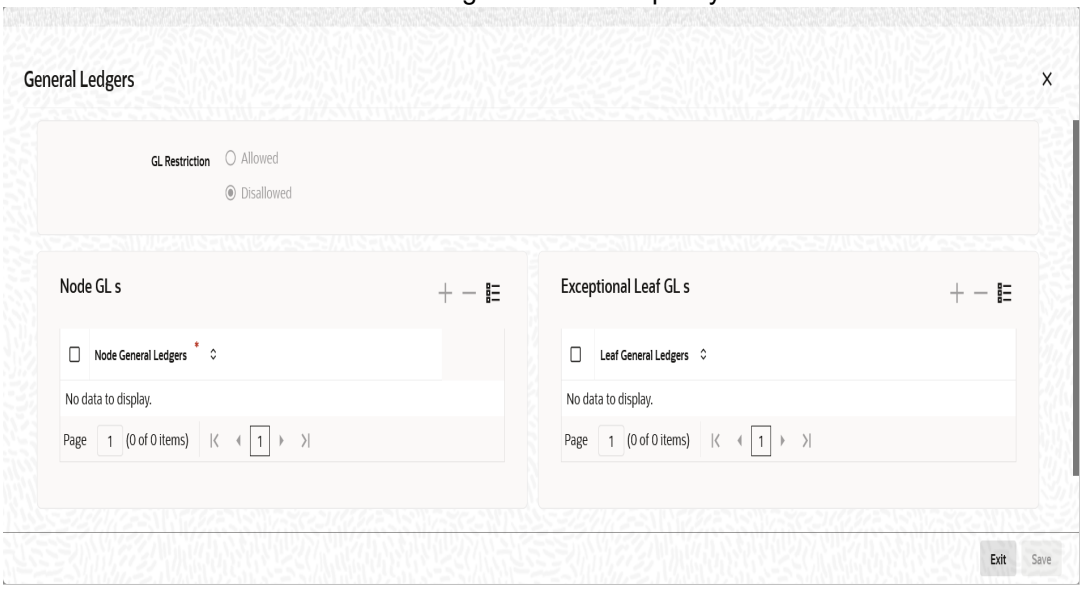
- Select the option 'Allowed' if you want to allow the user to manage certain tills
- Select the option 'Disallowed' to disallow the user to manage certain tills

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

2.2.4 General Ledgers Button

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

GLs and Leaf GLs. Leaf GLs maintained in the section ‘Exception Leaf GLs’ will be excluded from this restriction. Click ‘General Ledgers’ button to specify the GL restrictions.



You can either allow or disallow the user from using certain GLs. Select the node GLs that you want to restrict. If you want to allow/disallow posting to some leaf GLs from the selected node GL, specify them in the Exception Leaf GLs list.

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

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

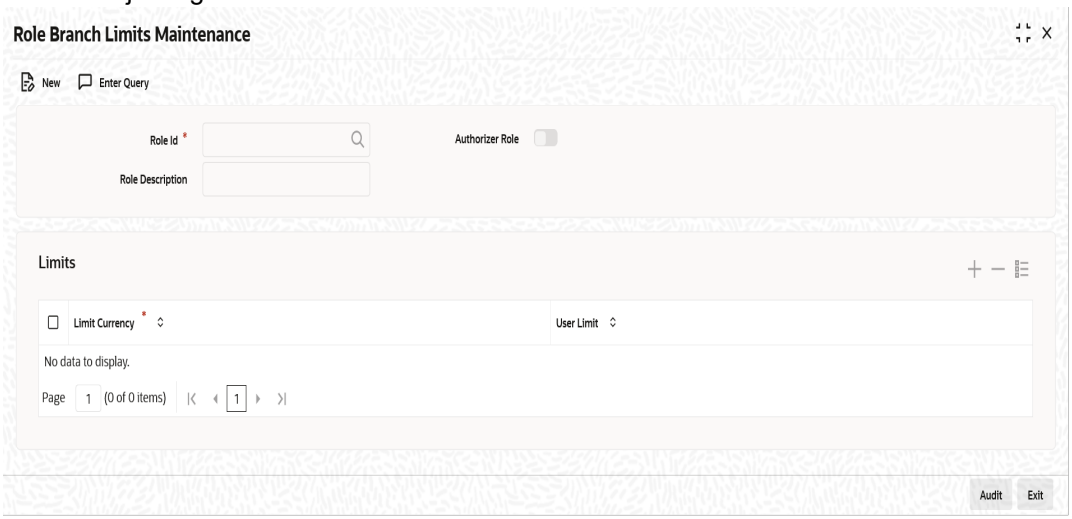
2.3 Role Branch Limits Maintenance

This section contains the following topics:

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

2.3.1 Invoking Role Branch Limits Maintenance Screen

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



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

Role ID

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

Role Description

The system displays the role description.

Authorizer Role

Check this box to enable authorizer role.

Limit Currency

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

User Limit

Specify the user specific limit.

2.4 Limits Role Maintenance

This section contains the following topics:

- Section 2.4.1, "Invoking Limits Role Maintenance"

2.4.1 Invoking Limits Role Maintenance

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

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

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

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

Role Identification

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

Description

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

Limits Currency

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

Note

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

Input Limit

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

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

Authorization Limit

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

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

Note

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

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

2.5 Multi-Factor Authentication

This section contains the following topic:

2.5.1 Logging into Oracle FLEXCUBE by Multi-Factor Authentication

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

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

You can specify the following details:

Multi-Factor Id

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

Multi-Factor PIN

Specify the Multi-Factor PIN for MFA.

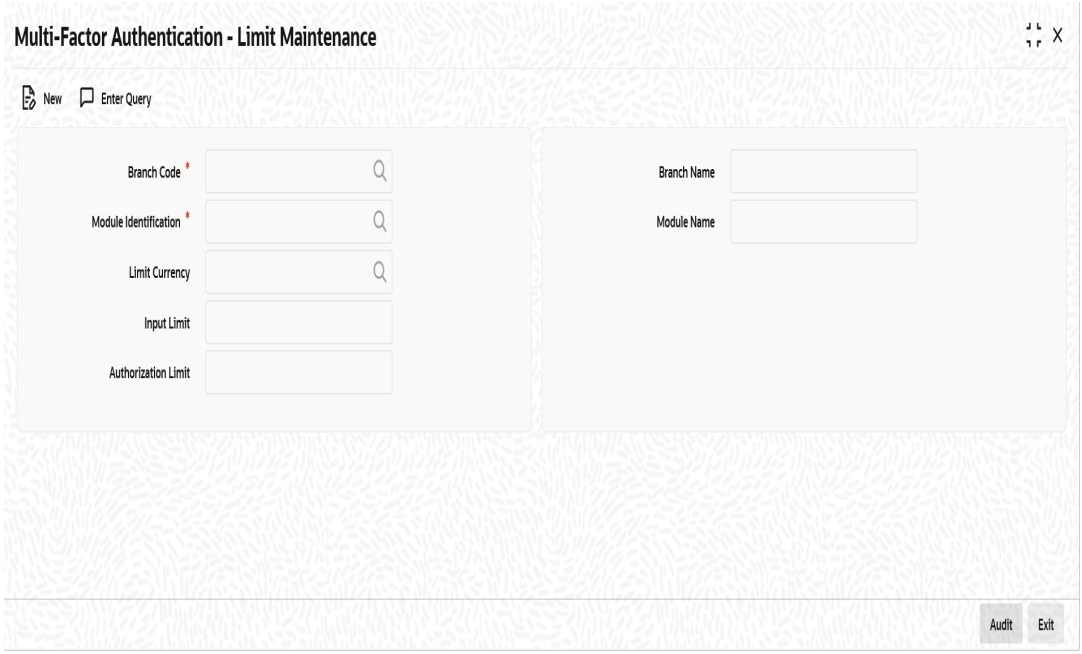
The system generates the MFA PIN just before the authentication, which expires in a short time. The generated MFA PIN is communicated to the user in multiple ways, such as text messages sent to the user's mobile phone or electronic devices.

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

2.5.2 Maintaining Multi-Factor Authentication Limits

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

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



You can specify the following details here:

Branch Code

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

Branch Name

The system displays the name of the branch code.

Module Identification

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

Module Name

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

Limit Currency

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

Input Limit

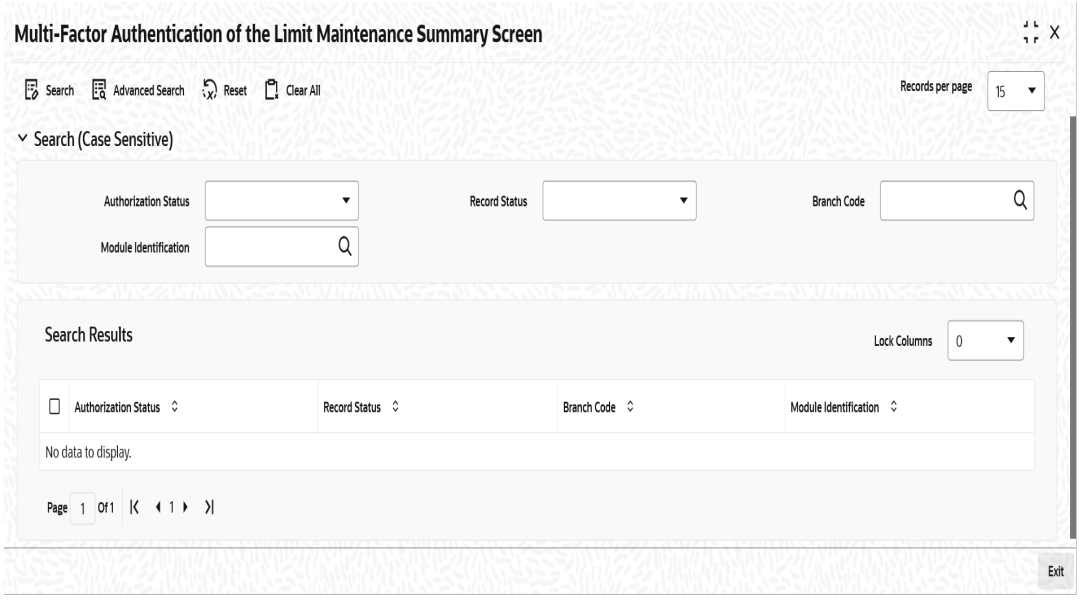
Specify the limit amount for input.

Authorization Limit

Specify the authorization limit amount for authorizer.

2.5.3 Viewing Multi-Factor Authentication - Limit Maintenance Summary

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



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

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

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

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

3. Associated Functions

This chapter contains the following sections:

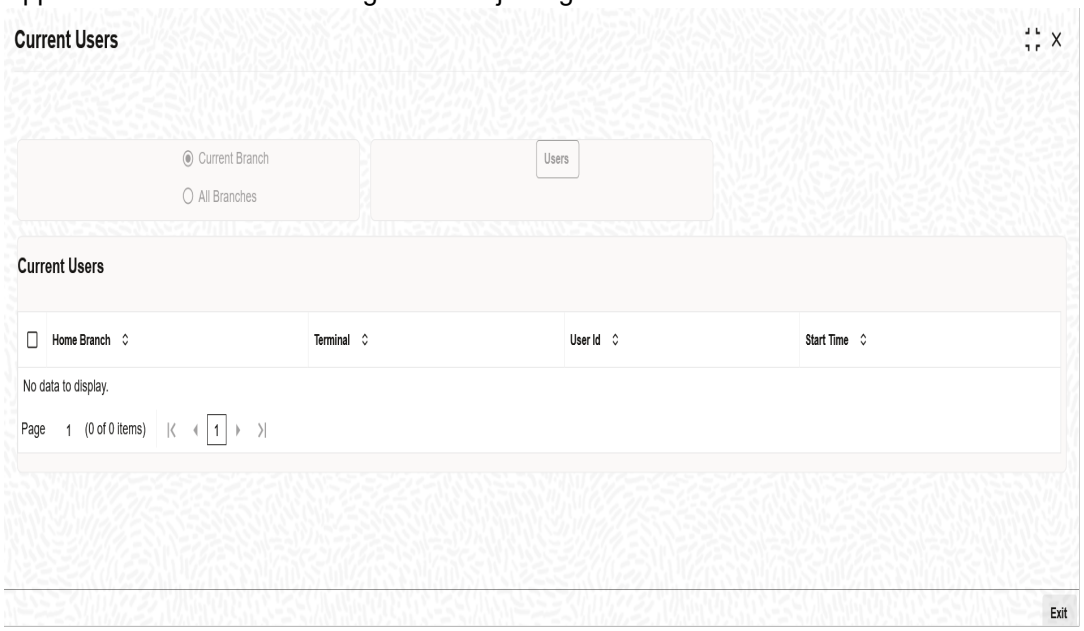
3.1 Current Users

This section contains the following topics:

3.1.1 View Current Users

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

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



The following details are captured here:

Branch

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

- Current Branch
- All Branches

The following user details are displayed here:

- Branch – The branch from which the user has logged in

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

Note

Current user database logs are enabled based on the work area maintained in Day 0 set-up.

3.2 Error Messages

This section contains the following topics:

- Section 3.2.1, "Maintaining Error Messages"

3.2.1 Maintaining Error Messages

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

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

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

The following details are captured here:

Error Code

Specify a code for the error message here.

Language

Specify the language code of the error message.

Description

Specify the description for the language code.

Message

Specify the error message that has to be displayed.

3.3 Branch Status

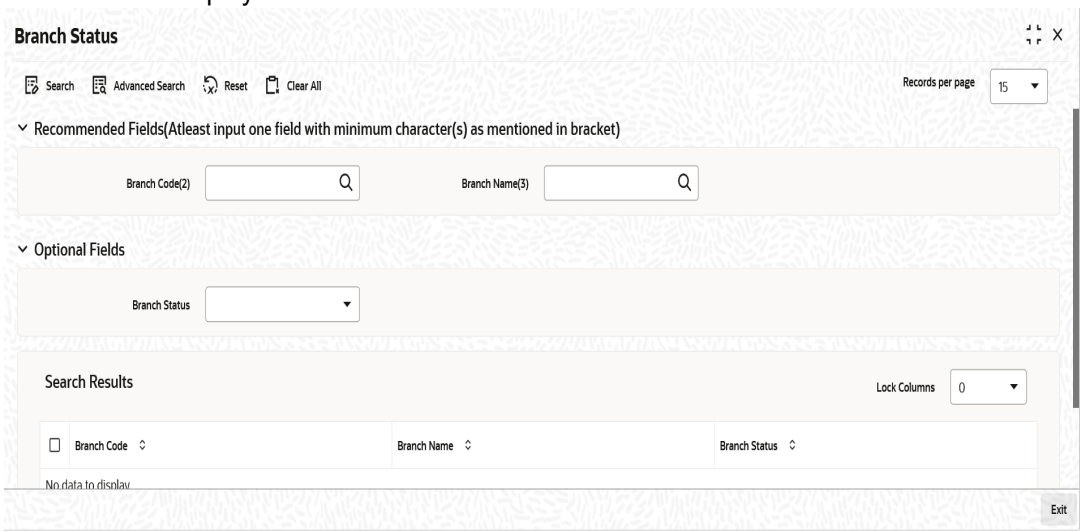
This section contains the following topics:

- Section 3.3.1, "Viewing Branch Status"

3.3.1 Viewing Branch Status

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

The screen is displayed as below:



You can query for records based on the following criteria:

- Branch Code
- Branch Name
- Branch Status

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

- Branch Code
- Branch Name
- Branch Status

4. Annexure A - Personally Identifiable Information

4.1 Querying Forgotten Customers

Oracle FLEXCUBE allows forgetting the personal identifiable information (PII) of a customer who has closed an account. If the personal identification information of a customer is forgotten, then you cannot query the PII details of forgotten customers from the following screens:

Function ID	Screen Description
IADCUSAC	Islamic Customer Accounts Detailed
IADCUSTD	Islamic TD Accounts Maintenance
ICDREDMN	Term Deposits Redemption Input
MSDCACAD	Account Address Maintenance
MSDCUSAD	Customer Address Maintenance
STDCASAC	Quick Customer Account Input
STDCIF	Customer Maintenance
STDCIFAD	Quick Customer Addition
STDCIFIS	Customer Signature and Image Upload
STDCIFNT	Customer Name Maintenance
STDCSHIS	Customer Signature and Image History
STDCUSAC	Customer Accounts Maintenance
STDCUSTD	Deposit Account Booking
STDCUSVW	360 Degree Corporate Customer View
STDFIACC	Financial Inclusion Customer Account Creation
STDJHMNT	Joint Holder Maintenance
STDSEGAS	Customer Segment Association

SVDCIFOL	Signature Verifications
IASCUSAC	Islamic Customer Accounts Summary
IASCUSTD	Islamic TD Accounts Summary
ICSREDMN	Term Deposits Redemption Input - Summary
MSSCACAD	Account Address Summary
MSSCUSAD	Customer Address Summary
STSCASAC	Quick Customer Account Summary
STSCIF	Customer Summary
STSCIFAD	Quick Customer Addition Summary
STSCIFIS	Customer Signature and Image Upload
STSCIFNT	Customer Name Summary
STSCUSAC	Customer Accounts Summary
STSCUSTD	Deposit Account Summary
STSCUSVW	360Degree Customer View Entry Point
STSFIACC	Financial Inclusion Customer Account Summary
STSJHMNT	Joint Holder Summary
STSSEGAS	Customer Segment Association Summary
SVDIMGVW	Customer Signature and Image View

4.2 Creating/Querying Customers of Restricted Access Group

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
MSDCACAD	Account Address Maintenance
MSSCACAD	Account Address Summary
STDCASAC	Quick Customer Account Input
STSCASAC	Quick Customer Account Summary
STDCIFAD	Quick Customer Addition
STSCIFAD	Quick Customer Addition Summary
STDCIFIS	Customer Signature and Image Upload
STSCIFIS	Customer Signature and Image Uplaod
STDCIFNT	Customer Name Maintenance
STDCRACC	External Customer Account Input
STSCRACC	External Customer Account Input Summary
STDCSHIS	Customer Signature and Image History
STDFIACC	Financial Inclusion Customer Account Creation
STSFIACC	Financial Inclusion Customer Account Creation Summary
STDJHMNT	Joint Holder Maintenance
STSJHMNT	Joint Holder Summary
STDKYCMN	KYC Maintenance
STSKYCMN	KYC Maintenance Summary
STDSEGAS	Customer Segment Association
STSSEGAS	Customer Segment Association Summary
SVDCIFOL	Signature Verifications
SVDIMGVW	Customer Signature and Image View
ACDOPTN	Account Statement Report
CSDOPTN	Customer Interest Statement
IADCUSAC	Islamic Customer Accounts Detailed
IASCUSAC	Islamic Customer Accounts Summary
IADCUSTD	Islamic TD Accounts Maintenance
IASCUSTD	Islamic TD Accounts Summary

ICDCALAC	Interest & Charges Single Account Online Calculation
ICDLIQAC	Interest & Charges Single Account Online Liquidation
ICDOLIQ	Interest & Charges Multiple Account Online Liquidation
ICDREDMN	Term Deposits Redemption Input
ICSREDMN	Term Deposits Redemption Summary
MSDCUSAD	Customer Address Maintenance
MSSCUSAD	Customer Address Summary
STDACCDT	Customer Accounts
STDCIF	Customer Maintenance
STSCIF	Customer Summary
STDCUSAC	Customer Accounts Maintenance
STSCUSAC	Customer Accounts Summary
STDCUSTD	Deposit Account Booking
STSCUSTD	Deposit Account Summary
STDCUSVW	360 Degree Corporate Customer View

4.3 Masked/Unmasked PII

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

Function ID	**Description**
CSDOPTN	Customer Interest Statement
IADCUSAC	Islamic Customer Accounts Detailed
IADCUSTD	Islamic TD Accounts Maintenance
ICDREDMN	Term Deposits Redemption Input
MSDCACAD	Account Address Maintenance
MSSCACAD	Account Address Summary
MSDCUSAD	Customer Address Maintenance
MSSCUSAD	Customer Address Summary
STDACCDT	Customer Accounts
STDCASAC	Quick Customer Account Input

STDCIF	Customer Maintenance
STSCIF	Customer Summary
STDCIFAD	Quick Customer Addition
STSCIFAD	Quick Customer Addition Summary
STDCIFCR	External Customer Input
STSCIFCR	Customer Summary
STDCIFIS	Customer Signature and Image Upload
STSCIFIS	Customer Signature and Image Uplaod
STDCIFNT	Customer Name Maintenance
STDCRACC	External Customer Account Input
STDCSHIS	Customer Signature and Image History
STDCUSAC	Customer Accounts Maintenance
STDCUSTD	Deposit Account Booking
STDCUSVW	360 Degree Corporate Customer View
STDFIACC	Financial Inclusion Customer Account Creation
STSFIACC	Financial Inclusion Customer Account Creation Summary
STDJHMNT	Joint Holder Maintenance
STSJHMNT	Joint Holder Summary
STDKYCMN	KYC Maintenance
STSKYCMN	KYC Maintenance Summary
STDSEGAS	Customer Segment Association
SVDCIFOL	Signature Verifications
SVDIMGVW	Customer Signature and Image View
SMDUSRDF	User Maintenance

5. Function ID Glossary