Oracle® Database

Common Core - Security Management System User Guide

Release 14.7.5.0.0

G24984-01

September 2024

Oracle Database Common Core - Security Management System User Guide, Release 14.7.5.0.0

G24984-01

Primary Authors: (primary author), (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

Contents

Preface

Purpose

This user manual is designed to get familiar with the Common Core - Security Management System (SMS) module of the Oracle FLEXCUBE Universal Banking. It provides an overview of the module and describes the various stages in setting- up and using the security features that Oracle FLEXCUBE Universal Banking offers.

Audience

Table Audience

Role	Function
Oracle FLEXCUBE Universal Banking Implementers	To set up the initial startup parameters in the individual client workstations and to set up security management parameters for the bank
SMS Administrator for the Bank	To set up the SMS bank parameters and to identify the branch-level SMS Administrators.
SMS Administrator for the Branch	To create a user and Rsddole profiles for the branches of the bank and to grant access to the various functions to the users.
A Oracle FLEXCUBE Universal Banking user	Any user of Oracle FLEXCUBE Universal Banking whose activities are traced by the Security Management System module.

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.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documents

Refer to the following documents for more information:

1. Procedures User Guide
2. Security Management System User Guide

Conventions

The following text conventions are used on this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
Italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

Acronyms and Abbreviations

Table Acronyms and Abbreviations

Abbreviation	Description
FC	Oracle FLEXCUBE Universal Banking
AEOD	Auto End of Day
BOD	Beginning of Day
EOD	End of Day
EOTI	End of Transaction Input
EOFI	End of Financial Input
System	Oracle FLEXCUBE Universal Banking
SI	Standing Instructions
MM	Money Market
RM	Relationship Manager

List of Topics

Table List of Topics

Topics	Description
#unique_12	This topic explains how to define and maintain the security of the banking system in terms of user access and roles.

Table (Cont.) List of Topics

Topics	Description
#unique_13	This topic describes the details about defining and maintaining additional security options such as clearing user profiles, changing system time levels, maintaining SSO parameters, and viewing user activity, branch status, and so on.
#unique_14	This topic lists all the error codes with the associated messages that can encounter while working with this module.
Glossary	This topic describes the alphabetical listing of Function/Screen ID's used in the module with page references for quick navigation.

List of Icons

Refer to the Icons topic in the Procedures User Guide for the commonly used icons and their uses.

Commonly Used Symbols and Icons

Table Commonly Used Symbols and Icons

Symbols	Description
Cancel	Click **Cancel** to cancel the performed action.
Change Log	When the authorizer clicks **Change Log**, the system displays the changes made to the transaction in a pop-up window. By default, the change log is set to display only modified values. The **Change Log** has two options, **All** and **Updated**. **All** displays both modified and non-modified fields and **Updated** displays only the modified fields. All the modified values are displayed in red which helps the authorizer to compare and simplify the authorization process.
Close	Click **Close** to close a record. This action is available only when a record is created.
Enter Query	Click **Enter Query** to enter a query.
Exit	Click **Exit** to cancel the performed action.
Exit Query	Click **Exit Query** to close a record. This action is available only when a record is created.
Fetch	Click **Fetch** to fetch the records based on given inputs.
First	Click **First** to view the first set of records.
Go	Click **Go** to view a set of records, post entering the mandatory inputs/ details.
Last	Click **Last** to view the last set of records.
Next	Click **Next** to view the next set of records.
New	Click **New** to add a new record. When the user clicks **New**, the system displays a new record enabling to specify the required data.
Ok	Click **Ok** to confirm the details on the screen.
Previous	Click **Previous** to view the previous set of records.

Symbols and Icons

This guide has the following list of symbols and icons.

Table Symbols and Icons - Common

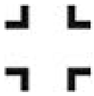
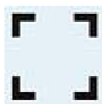
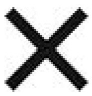
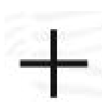
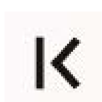
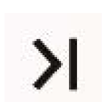
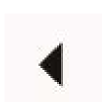
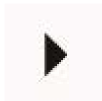
Symbol/Icon	Function
	Minimize
	Maximize
	Close
	Perform Search
	Open a list
	Add a new record
	Navigate to the first record
	Navigate to the last record
	Navigate to the previous record

Table (Cont.) Symbols and Icons - Common

Symbol/Icon	Function
	Navigate to the next record

Pre-requisite

Specify **User ID** and **Password** and login to the **Home** screen of an application.

- Purpose
- Audience
- Documentation Accessibility
- Critical Patches
- Diversity and Inclusion
- Conventions
- Screenshot Disclaimer
- Acronyms and Abbreviations
- Basic Actions
- Symbols and Icons
- Prerequisite

Purpose

This user manual is designed to get familiar with the Common Core - Security Management System (SMS) module of the Oracle FLEXCUBE Universal Banking. It provides an overview of the module and describes the various stages in setting- up and using the security features that Oracle FLEXCUBE Universal Banking offers.

Audience

Table Audience

Role	Function
Oracle FLEXCUBE Universal Banking Implementers	To set up the initial startup parameters in the individual client workstations and to set up security management parameters for the bank
SMS Administrator for the Bank	To set up the SMS bank parameters and to identify the branch-level SMS Administrators.
SMS Administrator for the Branch	To create a user and Rsddole profiles for the branches of the bank and to grant access to the various functions to the users.

Table (Cont.) Audience

Role	Function
A Oracle FLEXCUBE Universal Banking user	Any user of Oracle FLEXCUBE Universal Banking whose activities are traced by the Security Management System module.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Table Conventions

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

Acronyms and Abbreviations

Table Acronyms and Abbreviations

Abbreviation	Description
FC	Oracle FLEXCUBE Universal Banking
AEOD	Auto End of Day
BOD	Beginning of Day
EOD	End of Day
EOTI	End of Transaction Input
EOFI	End of Financial Input
System	Oracle FLEXCUBE Universal Banking
SI	Standing Instructions
MM	Money Market
RM	Relationship Manager

Basic Actions

Table Basic Actions

Action	Description
Approve	Used to approve the initiated report. This button is displayed, once the user click **Authorize**.
Audit	Used to view the maker details, checker details, and report status.
Authorize	Used to authorize the report created. A maker of the screen is not allowed to authorize the report. Only a checker can authorize a report, created by a maker.
Close	Used to close a record. This action is available only when a record is created.
Confirm	Used to confirm the performed action.
Cancel	Used to cancel the performed action.
Compare	Used to view the comparison through the field values of old record and the current record. This button is displayed in the widget, once the user click **Authorize**.
Collapse All	Used to hide the details in the sections. This button is displayed, once the user click **Compare**.
Expand All	Used to expand and view all the details in the sections. This button is displayed, once the user click **Compare**.
New	Used to add a new record. When the user click **New**, the system displays a new record enabling to specify the required data.

Table (Cont.) Basic Actions

Action	Description
OK	Used to confirm the details in the screen.
Save	Used to save the details entered or selected in the screen.
View	Used to view the report details in a particular modification stage. This button is displayed in the widget, once the user click **Authorize**.
View Difference only	Used to view a comparison through the field element values of old record and the current record, which has undergone changes. This button is displayed, once the user click **Compare**.
Unlock	Used to update the details of an existing record. System displays an existing record in editable mode.

Symbols and Icons

The following symbols and icons are used in the screens.

Table Symbols and Icons - Common

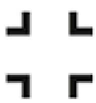
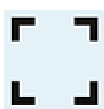
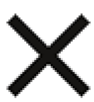
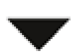
Symbol/Icon	Function
	Minimize
	Maximize
	Close
	Perform Search
	Open a list

Table (Cont.) Symbols and Icons - Common

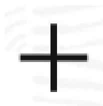
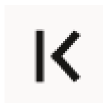
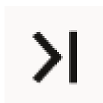
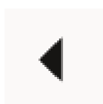
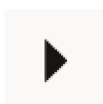
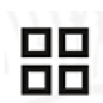
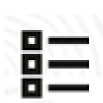
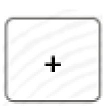
Symbol/Icon	Function
	Add a new record
	Navigate to the first record
	Navigate to the last record
	Navigate to the previous record
	Navigate to the next record
	Grid view
	List view
	Refresh
	Click this icon to add a new row.

Table (Cont.) Symbols and Icons - Common

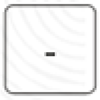
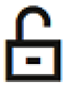
Symbol/Icon	Function
	Click this icon to delete an existing row.
	Click to view the created record.
	Click to modify the fields.
	Click to unlock, delete, authorize or view the created record.

Table Symbols and Icons - Audit Details

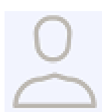
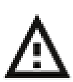
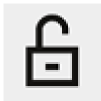
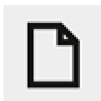
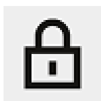
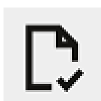
Symbol/Icon	Function
	A user
	Date and time
	Unauthorized or Closed status
	Authorized or Open status

Table Symbols and Icons - Widget

Symbol/Icon	Function
	Open status
	Unauthorized status
	Closed status
	Authorized status

Prerequisite

Specify the **User ID** and **Password**, and login to **Home** screen.

1

Security Management

This topic explains how to define and maintain the security of the banking system in terms of user access and roles.

Controlled access to the system is a basic parameter that determines the robustness of the security in banking software. In Oracle FLEXCUBE Universal Banking, we have employed a multi-pronged approach to ensure that these parameters are in place.

Table 1-1 Security Management Parameters

Security Management Parameters	Description
Only Authorized Users Access the System	First, only authorized users can access the system with the help of a unique User ID and a password. Secondly, a user should have access rights to execute a function.
User Profiles	The user profile of a user contains the User ID, Password, and Functions to which the user has access.
Restricted Number of Unsuccessful Attempts	Define the maximum number of unsuccessful attempts after which a User ID should be disabled. When a User ID has been disabled, the administrator should enable it. The password of a user can be made applicable only for a fixed period. This forces the user to change the password at regular intervals thus reducing security risks. Further, define passwords that could be commonly used by a user as Restrictive Passwords at the user, user role, and bank level. A user cannot use any password that is listed as a Restrictive Password at any of these levels.
Restricted Access to Branches	Indicate the branches from where a user can operate in the **Restricted Access** screen.
All Activities Tracked	An extensive log is kept of all the activities on the system. The user can generate reports on the usage of the system anytime. These reports give details of unsuccessful attempts at accessing the system along with the nature of these attempts. It could be an invalid password attempt, the last login time of a user, etc.
Audit Trail	Whenever a record is saved in the module, the ID of the user who saved the record is displayed in the **Input By** field at the bottom of the screen. The date and time at which the record is saved are displayed in the **Date/Time** field. A record that is entered should be authorized by a user, bearing a different login ID, before the EOD is run. Once the record is authorized, the ID of the user who authorized the record will be displayed in the **Authorized By** field. The date and time at which the record was authorized are displayed in the **Date/Time** field positioned next to the **Authorized By** field. The number of modifications that have happened to the record is stored in the field **Modification Number**. The status of the record whether it is **Open** or **Closed** is also recorded in the **Open** check box.

Bank Level Parameter Setup

Refer to the following topics for detailed information:

- #unique_27
- #unique_28

Bank Restriction

Refer to the topic #unique_29 for detailed information.

User Details Modification in Bulk

Refer to the topic #unique_30 for detailed information.

Common Branch Restrictions

Refer to the topic #unique_31 for detailed information.

Function Maintenance

Refer to the following topics for detailed information:

- #unique_32
- #unique_33

Defining Password Restriction

Refer to the topic #unique_34 for detailed information.

User Role Maintenance

Refer to the following topics for detailed information:

- #unique_35
- #unique_36
- #unique_37
- #unique_38
- #unique_39
- #unique_40
- #unique_41
- #unique_42
- #unique_43
- #unique_44

User Holidays Maintenance

Refer to the following topics for detailed information:

- #unique_45
- #unique_46

User Creation

Refer to the following topics for detailed information:

- #unique_47
- #unique_48

User Profile Entitlements

Refer to the following topics for detailed information:

- #unique_49
- #unique_50
- #unique_51
- #unique_52
- #unique_53
- #unique_54
- #unique_55
- #unique_56
- #unique_57
- #unique_58
- #unique_59

Customer Access Group Maintenance

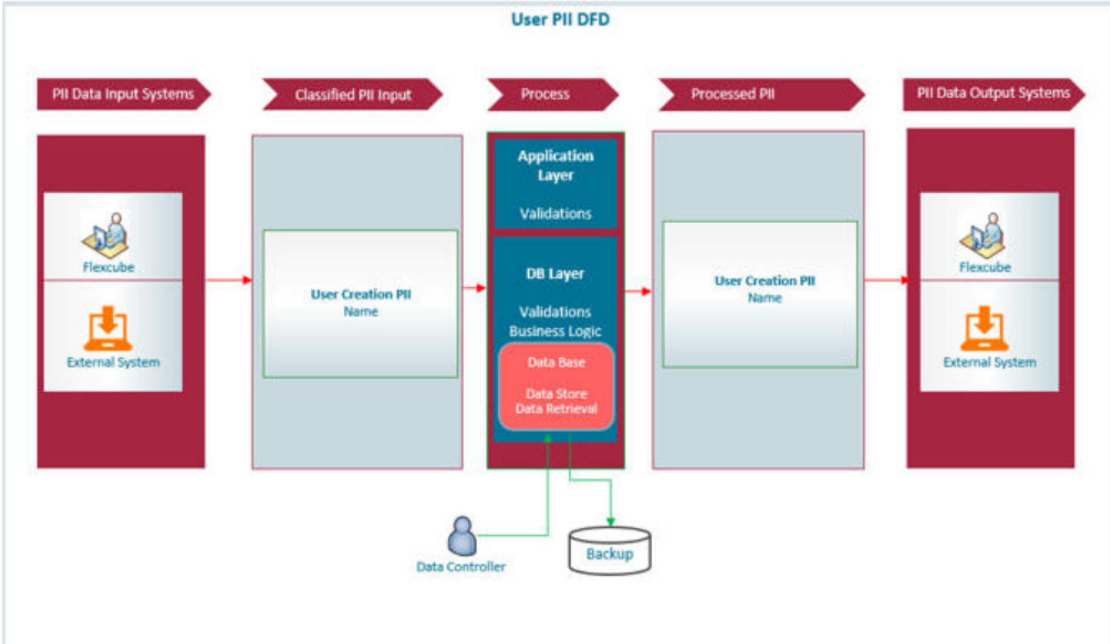
Refer to the topic #unique_60 for detailed information.

Personally Identifiable Information

Personally Identifiable Information (PII) is 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 personally identifiable information. It can be any information like Name, Contact Details, Demography Information, Financial Information, SSN, Passport Number, etc. Oracle FLEXCUBE Universal Banking allows masking, forgetting or restricting access to Personally Identifiable Information of a user. It is possible to mask or forget the PII based on the maintenance in **Masking Maintenance** and **Forget Customer PII Maintenance** screens.

The following flow chart explains the data flow of Personally Identifiable Information (PII):

Figure 1-1 Personally Identifiable Information (PII)



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

Table 1-2 Personally Identifiable Information (PII)

User Personal Information Category	Personal Information Data
Customer Name	User Name

Mask Maintenance

Refer to the topic #unique_61 for detailed information.

Forget Customer

Oracle FLEXCUBE Universal Banking allows to sanitize the data by forgetting the customer's Personally Identifiable Information (PII) once their accounts are closed. This is useful when data cannot be deleted due to referential integrity. The following are the screens through which the user can query the details of a customer:

- **STDCIFCR (External Customer Input)**
- **STDCRACC (External Customer Account Input)**

However, while viewing the details of a customer whose data is forgotten, the system displays a message that says the details of the forgotten customer can't be viewed.

The topic contains following sub-topics:

- #unique_62
- #unique_63

Log Access

Refer to the topic #unique_64 for detailed information.

Department Details

Refer to the topic #unique_65 for detailed information.

Process Codes

Refer to the topic #unique_66 for detailed information.

Single Sign On (SSO) Enabled Environment

Refer to the topic #unique_67 for detailed information.

Defining Entity Maintenance

Refer to the topic #unique_68 for detailed information on entity maintenance.

- Maintain SMS Banks Parameters
  This topic explains systematic instructions to maintain SMS bank parameters.
- Maintain Password Restriction Details in SMS Banks Parameters
  This topic explains systematic instructions to process password restrictions.
- Maintain Bank Restriction
  This topic explains systematic instructions to maintain bank restrictions.
- Maintain User Credential Change Details
  This topic explains systematic instructions to process the **User Credentials Change** screen.
- Maintain Branch Restrictions
  This topic explains systematic instructions to maintain the branch restrictions.
- Maintain Function Description
  This topic explains systematic instructions to maintain function descriptions.
- Define Menu
  This topic describes the process of defining the main and sub-menus for the Oracle FLEXCUBE Universal Banking.
- Define Password Restriction
  This topic explains systematic instructions to define password restrictions.
- Maintain Roles
  This topic explains systematic instructions to maintain the role profiles.
- Process Role Maintenance Details
  This topic explains systematic instructions to process role maintenance details.
- Maintain Report Details for Role
  This topic provides systematic instructions to maintain report details in the **Role Maintenance** screen.
- Maintain Batch Details for Role
  This topic provides systematic instructions to maintain batch details in the **Role Maintenance** screen.
- Maintain Online Details for Role
  This topic provides systematic instructions to maintain online details in the **Role Maintenance** screen.
- Maintain Access Rights for Role
  This topic explains systematic instructions to maintain access stage rights for the function ID.

- Maintain Account Class Restrictions for Role
  This topic explains systematic instructions to maintain account class restrictions.
- Maintain Branch Restriction Details for Role
  This topic explains systematic instructions to maintain branch restrictions for the role profile.
- Maintain Rights for Role
  This topic explains systematic instructions to process the necessary rights to perform various operations in respect of incoming and outgoing messages.
- Define Roles for Oracle FLEXCUBE Universal Banking Branch Users
  This topic explains systematic instructions to define roles for Oracle FLEXCUBE Universal Banking branch users.
- Maintain User Holidays
  This topic explains systematic instructions to maintain user holidays.
- Process User Holiday Summary
  This topic explains systematic instructions to process user holiday summary details.
- Maintain Users
  This topic explains systematic instructions to create user profiles.
- Maintain Roles for Users
  This topic explains systematic instructions to attach a user profile to a role in the **Roles** screen.
- Maintain Rights for Users
  This topic explains systematic instructions to maintain rights in the **User Maintenance** screen.
- Maintain Functions for Users
  This topic explains systematic instructions to maintain functions in the **User Maintenance** screen.
- Maintain Account Class Restrictions for Users
  This topic explains systematic instructions to specify account class restrictions.
- Maintain Branch Details for Users
  This topic explains systematic instructions to maintain branch details in the **User Maintenance** screen.
- Maintain Product Restrictions for Users
  This topic explains systematic instructions to maintain product details in the **User Maintenance** screen.
- Maintain Disallowed Functions for Users
  This topic explains systematic instructions to maintain disallowed functions in the **User Maintenance** screen.
- Maintain Centralized Role Details for Users
  This topic explains systematic instructions to maintain centralized role details in the **User Maintenance** screen.
- Maintain Dashboard Mapping Details for Users
  This topic explains systematic instructions to maintain dashboard mapping details in the **User Maintenance** screen.
- Maintain Access Group Restrictions for Users
  This topic explains systematic instructions to maintain the access group restrictions in the **User Maintenance** screen.

- Maintain Customer Access Group
  This topic explains systematic instructions to maintain customer access groups for retail and corporate customers.
- Maintain Masking Details
  This topic explains systematic instructions to maintain masking details.
- Maintain Forget Customer Personal Identifiable Information (PII)
  This topic explains systematic instructions to maintain the **Forget Customer PII Maintenance** screen.
- Forget Customer Process
  This topic explains systematic instructions to forget the specific customer.
- Log Access
  This topic describes an overview of the different logs and their access.
- Maintain Department Details
  This topic explains systematic instructions to maintain department details.
- Maintain Process Codes
  This topic explains systematic instructions to maintain process codes.
- Single Sign On Enabled Environment
  This topic describes an overview of the Single Sign On enabled environment.
- Maintain Entities
  This topic explains systematic instructions to maintain entities.

1.1 Maintain SMS Banks Parameters

This topic explains systematic instructions to maintain SMS bank parameters.

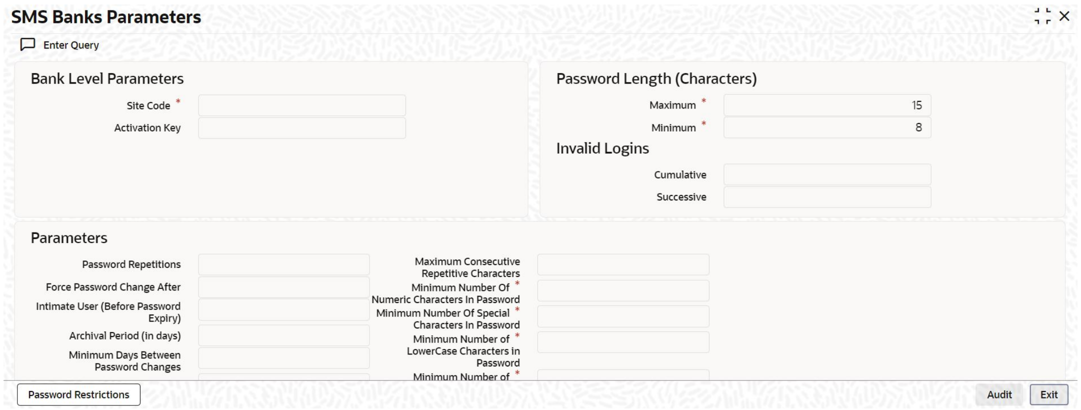
Certain parameters related to security management should be defined at the bank level. These parameters will apply to all the users of the system. Examples of such parameters are the number of invalid login attempts after which a user ID should be disabled, the maximum and minimum length for a password, the number of previous passwords that should not be used, the interval at which the password should be changed by every user, and so on.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDBANKP** in the text box, and click **Next**.

   The **SMS Banks Parameters** screen displays.

Figure 1-2 SMS Banks Parameters



> **Note:**
>
> The bank parameters can be modified only when the Head Office branch is in the transaction input stage.

2. On the **SMS Banks Parameters** screen, specify the fields.

> **Note:**
>
> The fields, which are marked with an asterisk, are mandatory.

For more information on fields, refer to the field description table.
Bank Level Parameters

Table 1-3 Bank Level Parameters - Field Description

Field	Description
Site Code	Specify the **Site Code**.
Activation Key	The system displays the activation key.

Password Length (Characters) - Indicate the range of length (in terms of the 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 is specified here.

Table 1-4 Password Length - Field Description

Field	Description
Maximum and **Minimum**	The minimum length defaults to 8, and the maximum length to 15. If required, change the default values and specify the required range. In this case, the user can specify a minimum length between 8 to 11 characters, and a maximum length between 12 to 30 characters. The minimum specified length must not exceed the maximum length.

Invalid Logins - Specify the allowable number of times an invalid login attempt is made by a user. Each user accesses the system through a unique **User ID** and **Password**. While logging on to the system, if either the **User ID** or the **Password** is wrong, it amounts to an invalid login attempt.

Table 1-5 Invalid Logins - Field Description

Field	Description
Cumulative and **Successive**	The user can stipulate the allowable number of cumulative invalid attempts made during a day as well as the allowable number of consecutive or successive invalid attempts made at a time. In either case, if the number of invalid attempts exceeds the stipulated number, the user ID is disabled. By default, the allowable number of cumulative invalid attempts is six, and the allowable number of consecutive invalid attempts is three. If required, change the default value and specify the allowable number of attempts in each case. Specify an allowable number for cumulative attempts between 6 to 99, and for consecutive (successive) attempts, between 3 to 5. Once specified, the allowable number of cumulative or consecutive login attempts can be changed 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.

Parameters

Table 1-6 Parameters - Field Description

Field	Description
Password Repetitions	Stipulate the number of previous passwords that cannot be set as the new current password, when a password change occurs. The system defaults to a value of three (that is when a user changes the user password, the user’s previous three passwords cannot be set as the new password). The default value can be changed to a number between one and five, inclusive. For example, while setting up the Bank Level Parameters, a value of **2** is in the **Password Repetitions** field. Suppose that a user of the system has the user ID and password for login. If the user wants to change the password for the first time, process the **Change Password** screen. The user cannot select the current password again but has to enter a new password. The user wants to change the password for the second time. As the last two passwords cannot be used (Password Repetitions = 2 in the Bank Level Parameters table), the user cannot enter either of the old passwords. The user must enter a password that is different from the previous two passwords. The number specified here should be greater than or equal to 1 and less than or equal to 5.

Table 1-6 (Cont.) Parameters - Field Description

Field	Description
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, specify the number of calendar days for which the password should be valid. After the specified number of days has elapsed for the user's password, it is no longer valid and a password change is forced. The number of calendar days defined here will be applicable for a password change of any nature either through the **Change Password** function initiated by the user or a forced change initiated by the system. The system defaults to a value of 30, which can be changed. If it is changed, the number of days specified here should be between 15 to 180 days, inclusive.
Intimate User (Before Password Expiry)	The number of days for which a password is to be valid is defined in the **Force Password Change After** field. Indicate the number of working days before password expiry that a warning is to be issued to the user. When the user logs into the system (the stipulated number of days before the expiry date of the password), a warning message will continue to be displayed till the password expires or till the user changes it. By default, the value for this parameter is two (that is two days before password expiry). If required, change a field value to a number greater than zero and less than or equal to five. For example, if the value specified in the **Intimate User (Before Password Expiry)** field is 2 and a user's password is due to expire on January 31. The warning message is displayed on January 29 and January 30 whenever the user logs in.
Archival Period (In Days)	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, and so on.) should be maintained. The system defaults to a value of 30 which can be changed. Specify an archival period that is greater than or equal to 7 calendar days.
Minimum Days Between Password Changes	Specify the minimum number of calendar days that must elapse between two password changes. After a user has changed the user password, it cannot be changed again until the minimum number of days specified here has elapsed. By default, the minimum number of days between password changes is set to One. However, this can be modified. **Note:** • The **Minimum Days Between Password Changes** field value should not be more than the days defined in the field **Force Password Change After**. • It is recommended to not set the **Minimum Days Between Password Changes** field value to **0**.

Table 1-6 (Cont.) Parameters - Field Description

Field	Description
Dormancy Days	Oracle FLEXCUBE Universal Banking allows automatically disabling the profile of all the users who have not logged into the system for a pre-defined period. 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 is specified in this screen. This is reckoned in calendar days that are inclusive of holidays. All dormant users are disabled when attempting to log in to the post **Dormancy Days**.
Display Legal Notice	Check this box to display a legal notice.
Password External	The password external is enabled if the **PASSWORD_EXTERNAL** is maintained as **Y** in the property file. However, this check box cannot be edited. If the **Password External** box is checked, then the user and the password cannot be modified.
Number of Days to Forget User	Specify the number of days to forget the user by the system.
Maximum Consecutive Repetitive Characters	It is allowed to place restrictions on the number of alpha and numeric characters that can be specified for a user password. Specify 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. For example, the value specified in the **Maximum Consecutive Repetitive Characters** field is 3 and a user decides to change his password to STUDDDD123. The system will not allow this password change as the **Maximum Consecutive Repetitive Characters** value has exceeded the recurrence of D in the password.
Minimum Number of Special Characters in Password	Specify the 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 the limits are not specified, the following default value will be used: **Minimum Number of Special Characters = 1**
Minimum Number of Numeric Characters in Password	Specify 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 the limits are not specified, the following default value will be used: **Minimum Number of Numeric Characters = 1** **Note:** Specify any number between 0 to 11 in each of these fields. However, 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**.

Table 1-6 (Cont.) Parameters - Field Description

Field	Description
Minimum Number of Lowercase Characters in Password	Specify 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 the limits are not specified, the following default values will be used: • **Minimum Number of Lower Case Characters = 1** • **Maximum Number of Numeric Characters = Maximum Password Length**
Minimum Number of UpperCase Characters in Password	Specify the minimum number of upper case characters allowed in a user password. The allowed uppercase characters are from the US-ASCII character set only. The system validates these specifications only when a user chooses to change the password. If the limits are not specified, the following default values will be used: • **Minimum Number of Upper Case Characters = 1** • **Maximum Number of Numeric Characters = Maximum Password Length**
Mask Character	Enter a character that is used to mask personal information.

> **Note:**
>
> The fields, which are marked with an asterisk, are mandatory.

For more information on fields, refer to the field description table.

Table 1-7 Warning Screen Text - Field Description

Field	Description
Warning Screen Text	At bank level, a warning message containing legal requirements and security policy is to be displayed to all users before allowing them to log in to Oracle FLEXCUBE Universal banking. Specify the text (content) of such a message in the **Warning Screen Text** field. This message will be displayed soon after a user launches the Oracle FLEXCUBE Universal Banking login screen. The user will be allowed to continue with the login process only after clicking **Ok** on the message window. The contents of the message can be modified only during the transaction input stage. The changes will come into effect during the next login by a user. The maximum size of the warning message is 1000 characters. **Note:** It is allowed to specify the contents of the warning message only if the **Display Legal Notice** option is enabled.

Screen Saver Details - The Oracle FLEXCUBE Universal Banking application screen will be locked if there is no activity for some time, and can be logged in back only after specify the password of the user ID. For more information on fields, refer to the field description table.

> **Note:**
>
> The fields, which are marked with an asterisk, are mandatory.

For more information on fields, refer to the field description table.

Table 1-8 Screen Saver Details - Field Description

Field	Description
Screensaver Required	Check this box if a screensaver is required.
Screensaver Interval Modifiable at User level	Check this box to modify the screensaver interval at the user level.
Screensaver Interval (in seconds)	Specify the time in seconds, after which the screen should be locked. If both the **Screensaver Required** and **Screensaver Interval Modifiable at User level** boxes are checked at the bank level, then it will be visible at the user level. Otherwise, it will be hidden. The system defaults the screensaver time out from the bank parameter's screen. The administrator who creates a user will be allowed to change the same during user creation time. The screensaver interval maintained at the user level should always be less than or equal to that maintained at the bank level. If the screensaver interval is not specified in the user level, the system takes the interval from **SMS Banks Parameters** screen. The screensaver interval can be specified by the user only if the **Screensaver Interval Modifiable at User level** is checked in the **SMS Banks Parameters** screen.

3. Click **Exit** to end the transaction.

1.2 Maintain Password Restriction Details in SMS Banks Parameters

This topic explains systematic instructions to process password restrictions.

Through the **Password Restrictions** screen, define a list of passwords that cannot be used by any user of the system in the bank. This restrictive passwords list can be defined at three levels:

- At the bank level (applicable to all the users of the system)
- At the user role level (applicable for all the users assigned the same role)
- At the user level (applicable for the user)

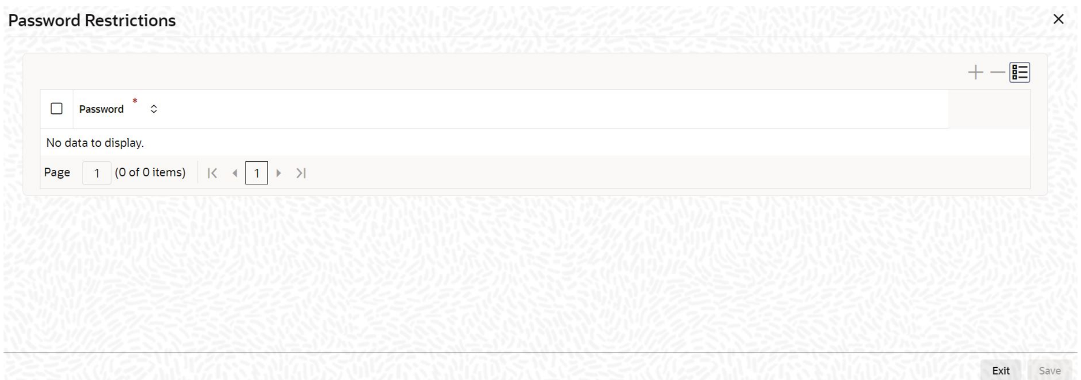
The list of restrictive passwords should typically contain the passwords the users are most likely to use such as Bank Name, City, Country, etc. For a user role, it could contain names or terms that are commonly used in the department. At the user level, it could contain the names of loved ones, and so on. By disallowing users from using such common passwords, the risk of somebody other than the user knowing the password can be reduced.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On the **SMS Banks Parameters** screen, click **Password Restrictions**.

   The **Password Restrictions** screen displays.

   Figure 1-3 Password Restrictions

2. On the **Password Restrictions** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-9 Password Restrictions - Field Description

Field	Description
Password	Click **Add** to add a new password record and specify restricted passwords at the bank level that should not be used by any user of the bank. To select a record in the list, use the check box beside it.

3. After listing restrictive passwords in the password list, click **Ok** to save the password restrictions.
4. Click **Exit** to end the transaction.

1.3 Maintain Bank Restriction

This topic explains systematic instructions to maintain bank restrictions.

Administrators of branches can be restricted from performing operations related to specific functions in branches other than their home branches. These are referred to as **Branch Restrictions for Specific Applications**. 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 maintained, 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 requirements, the implementers at installation configure a list of the specific functions or applications for which might wish to maintain such branch restrictions. The user can maintain branch restrictions for each of these applications, as required.

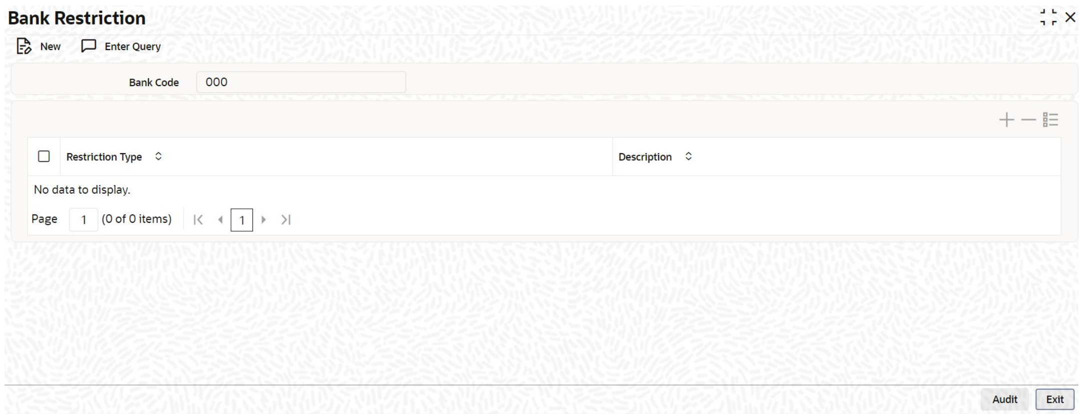
Note:

The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDBNKRT** in the text box, and click **Next**.

   The **Bank Restriction** screen displays.

Figure 1-4 Bank Restriction



2. On the **Bank Restriction** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-10 Bank Restriction - Field Description

Field	Description
Bank Code	The system displays the bank code.
Restriction Type	Specify the **Restriction Type**.
Description	The system displays the description of the restriction type.

3. Click **Exit** to end the transaction.

1.4 Maintain User Credential Change Details

This topic explains systematic instructions to process the **User Credentials Change** screen.

It is possible to change or reset user passwords in bulk if one has the system admin rights. After modification of the user list, click **Save**. The modified user list is stored in a temporary table. The lists of users which are modified and mapped with a unique sequence number is not available until the particular sequence number is authorized. When the particular sequence number is authorized those user details are changed and updated.

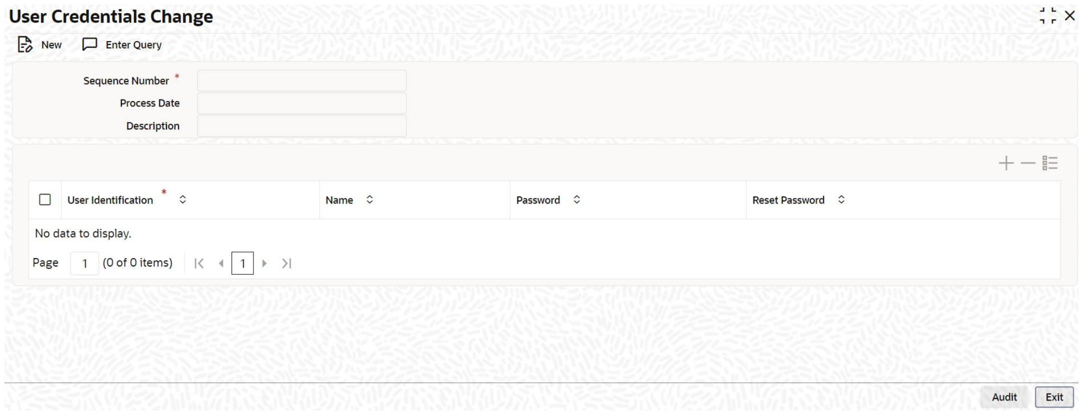
Note:

The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDCHPWD** in the text box, and click **Next**.

   The **User Credentials Change** screen displays.

   Figure 1-5 User Credential Change

2. On the **User Credentials Change** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-11 User Credentials Change - Field Description

Field	Description
Sequence Number	Click **New** to generate a new **Sequence Number**. The system displays the sequence number.
Process Date	Click **Calendar** and select the date. This field is generally useful for querying purpose.
Description	Specify a description of what modification is being done on selected user IDs.
User Identification	Select the **User Id** to be changed from the list of values.
Name	The system displays the name of the user specific to the selected user ID.
Password	The system displays the password of the selected user ID. This field is editable only if the **Auto Generation Required** option is not selected at the application level. If the **Auto Generation Required** option is checked, the password is auto-generated by the application.
Reset Password	Select this check box to reset the password in case of user IDs where the password needs to be auto-generated. If the external password is enabled in the bank parameters, then the **Password** and **Reset Password** fields are disabled for editing.

3. Click **Exit** to end the transaction.

1.5 Maintain Branch Restrictions

This topic explains systematic instructions to maintain the branch restrictions.

In the **Branch Restrictions** screen, the user has identified those applications and operations for which intend to maintain branch restrictions. Having done this, the user must proceed to create the appropriate common branch restrictions for each branch administrator.

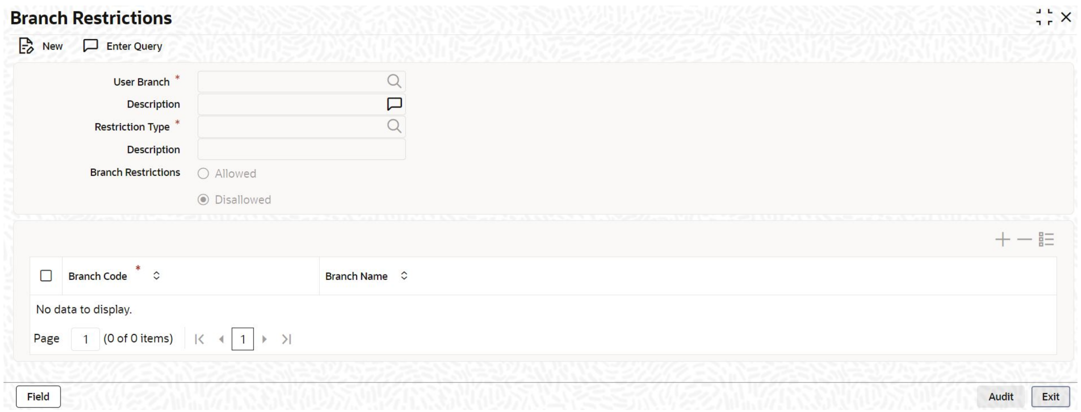
Note:

The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDBRRST** in the text box, and click **Next**.

   The **Branch Restrictions** screen displays.

   Figure 1-6 Branch Restrictions

   In this screen, common branch restrictions can be created only at the head office branch.

2. On the **Branch Restrictions** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-12 Branch Restrictions - Field Description

Field	Description
User Branch	Specify the home branch of the administrator for which maintaining common branch restrictions.
Description	The system displays the description of the selected user branch.
Restriction Type	Indicate the specific application for which wants to maintain common branch restrictions, for the administrator of the selected branch. Specify a restriction type that has been maintained in the SMS branch restriction type maintenance.
Description	The system displays the description of the selected restriction type.
Branch Code	Specify the **Branch Code**.
Branch Name	The system displays the branch name of the selected branch code.

Table 1-12 (Cont.) Branch Restrictions - Field Description

Field	Description
Branch Restrictions	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**). Select one of the following options: • **Allowed** • **Disallowed** The common branch restrictions 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.

For example, the following common branch restrictions are created:

Table 1-13 Common Branch Restrictions

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

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

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

Note:

- 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 that are specified in the SMS branch restriction types maintenance, the user must create the appropriate common branch restrictions in the **Branch Restrictions** screen. If no restrictions have been created in the **Branch Restrictions** screen for a specific branch for an application chosen in the SMS branch restriction types maintenance, operations pertaining to the application will not be allowed from that branch.
- To allow the administrator of a certain branch to perform operations pertaining to a specific application for all branches, you can either maintain an allowed list with all branches selected or maintain a disallowed list with none of the branches selected.

3. Click **Exit** to end the transaction.

1.6 Maintain Function Description

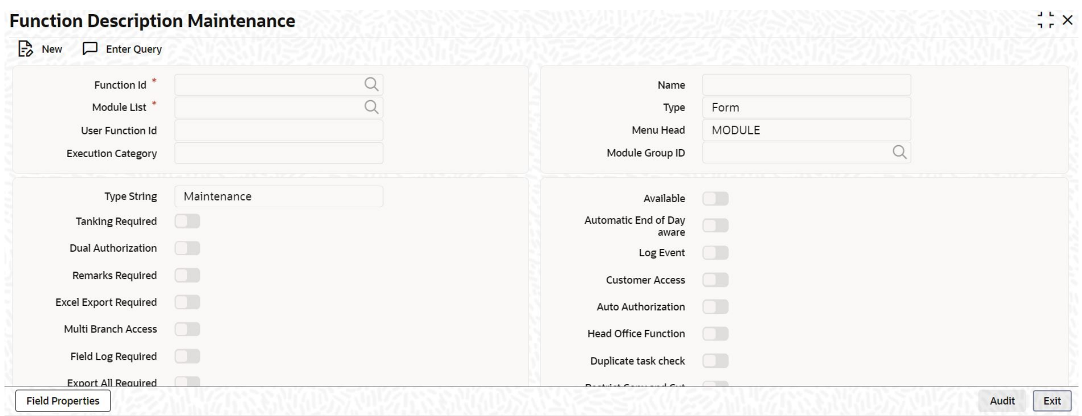
This topic explains systematic instructions to maintain function descriptions.

Any function that is a part of the system should be defined through the **Function Description Maintenance** screen before it is available for execution. Through this screen, the user can modify the description of the function that appears in the application browser.

1. On **Homescreen**, type **SMDFNDSC** in the text box, and click **Next**.

   The **Function Description Maintenance** screen displays.

Figure 1-7 Function Description Maintenance



2. On the **Function Description Maintenance** screen, specify the fields.

> **Note:**
>
> The fields, which are marked with an asterisk, are mandatory.

For more information on fields, refer to the field description table.

Table 1-14 Function Description Maintenance - Field Description

Field	Description
Function ID	Click **Search** and specify the function ID for which want to give access rights.
Module List	Click **Search** and specify the module to which the function ID has to be mapped. All functions are mapped to specific modules.
Name	Specify the executable to open the function Id.
Type	Select the type of function ID from the drop-down list: • **Form** • **Report 1** • **Stored Procedure**

Table 1-14 (Cont.) Function Description Maintenance - Field Description

Field	Description
Menu Head	Select the menu head from the drop-down list: • **Module** • **Report** Then specify the rights to the different actions for the functions by checking against the action. These actions can be: a. **Static Maintenance Functions** • **New** - Define a new record • **Copy** - Copy details of an existing record • **Delete** - Delete an existing record • **Close** - Close an existing record • **Unlock** - To amend an existing record • **Reopen** - Reopen an existing record • **Print** - Print the details of selected records • **Authorize** - Authorize any maintenance activity on a record b. **Contracts and on-line Transaction Processing** • **Reverse** - Reverse an authorized contract • **Rollover** - To manually roll over an existing contract into a new contract • **Confirm** - To indicate the counterparty or broker confirmation of a contract • **Liquidate** - To manually liquidate a contract • **Hold** - To put a contract on hold • **View** - To see the details of the contract c. **Reports** • **Generate** - To generate reports • **View** - View the reports • **Print** - Print the reports To delete the access rights given for a function, select the **Function ID** and click **Delete**.
Module Group ID	Click **Search** and specify the group ID of the module from the list of values.
User Function ID	Specify a custom function ID which can be used as an alias for the function ID selected. If the **User Function ID** is typed in the text box at the top right corner of the application **Homescreen** and clicked **Next**, the system checks for the mapped function id and launches that function id screen.
Execution Category	Select the execution category from the drop-down list: • **Java** • **PL/SQL** If the **Java** category is selected, the ODT screen processing logic is done through the application layer, and if the **PL/SQL** category is selected, then the ODT screen processing logic is done through the database layer.

Table 1-14 (Cont.) Function Description Maintenance - Field Description

Field	Description
Type String	Select the **Type String** from the drop-down list: • **Maintenance** • **Online** • **Batch** • **Reports** • **BO Reports** • **Web Branch** • **Process** • **Task** • **EL Maintenance** • **EL Reports** • **EL Online** • **SMS Maintenance** • **LBL_VAM_MAINTENANCE** • **Payments Online** • **Payments Maintenance** • **Dashboard**
Tanking Required	Check this box to indicate that the maintenance records that are created or modified in the system for the function Id specified here, need to be tanked till they get authorized. The new or modified records are written to the static tables only after authorization. For more details on tanking of maintenance records refer to the Core Services User Guide.
Dual Authorization	Check this box to enable dual authorization for records that are created or modified in the system for the specified function ID. If dual authorization is enabled then after the creation or modification of a maintenance record, an intermediate verifier (First Authorizer) has to verify the record before the record can actually be authorized. The user must not enable both **Dual Authorization** and **Auto Authorization** for a function ID at the same time, as they are mutually exclusive.
Remarks Required	Check this box to enable capturing of maker remarks on the actions like save, close and reopen of records belonging to the selected function id. If this box is checked then the system pops up a **Maker Remarks** window and forces the maker to save remarks while saving, closing, or reopening a record, The checker/authorizer can view the maker remarks entered and also enter remarks for each modification while authorizing the record.
Excel Export Required	Check this box to enable data export for the selected function id. If this box is checked, the system allows to export data from records belonging to the selected function id into an excel file.
Multi Branch Access	Check this box to configure a dual access framework for the function ID.**Note:** • If the function level check box is unchecked, the transactions will be posted in the current branch. • Dual access functionality is enabled only when the **Multi Branch Access** check boxes checked at **User ID** and **Function ID** levels.
Field Log Required	Check this box to enable file log for the selected function id.
Export All Required	Check this box to enable export for the selected function id.

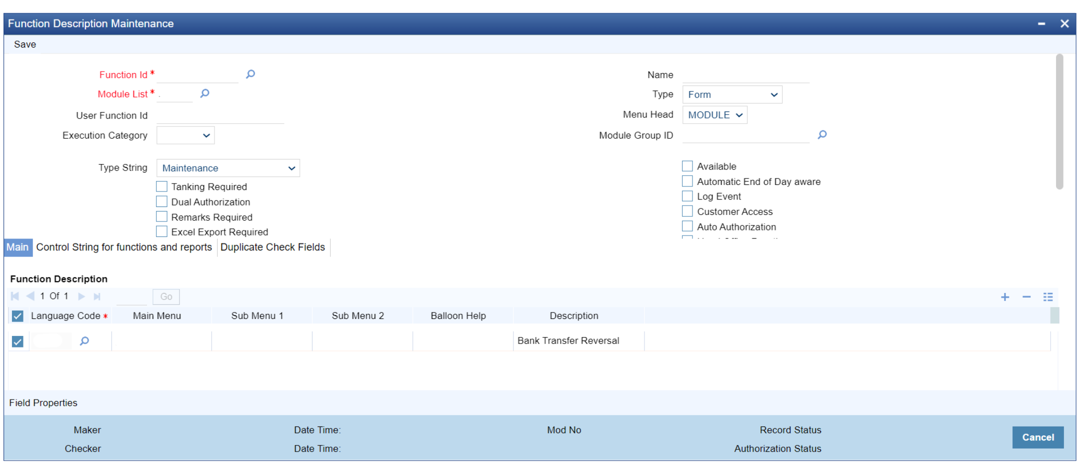
Table 1-14 (Cont.) Function Description Maintenance - Field Description

Field	Description
Allow Operations during End of Day	Check this box to allow operations during the end of day.
Available	Check this box to make the function accessible in the Oracle FLEXCUBE Universal Banking menu. The definition of the menu would be as specified in the column at the bottom of the **Function Description Maintenance** screen. If this box is unchecked, then this screen will not be accessible from the menu even if it is selected for the role that is assigned to the user.
Automatic End Of Day Aware	Check this box to consider the function for an AEOD run.
Log Event	Check this box to enable the event log for a particular Function ID, Oracle FLEXCUBE Universal Banking maintains an extensive log of the activities of every user. This can later be used for reporting on user activities.
Customer Access	Check this box to make the function available to users who are classified as customers.
Auto Authorization	As configured for the installation, automatic authorization is applicable for a pre-shipped list of functions. For those functions, revoke the applicability of automatic authorization, if required. It is not possible to indicate the applicability of automatic authorization for any other functions than those pre-shipped functions configured for your installation.
Head Office Function	Check this box to enable the function to be handled only by the users of the Head Office. Users of the other branches would be only allowed to view the Function.
Duplicate Test Check	Check this box to duplicate test check.
Restrict Copy and Cut	Check this box to restrict the copy and cut options.
Restrict Print	Check this box to restrict the printing option.

3. On the **Function Description Maintenance** screen, click **Main**.

   The **Main** tab displays.

Figure 1-8 Main



4. On the **Main** tab, specify the fields.

> **Note:**
>
> The fields, which are marked with an asterisk, are mandatory.

For more information on fields, refer to the field description table.

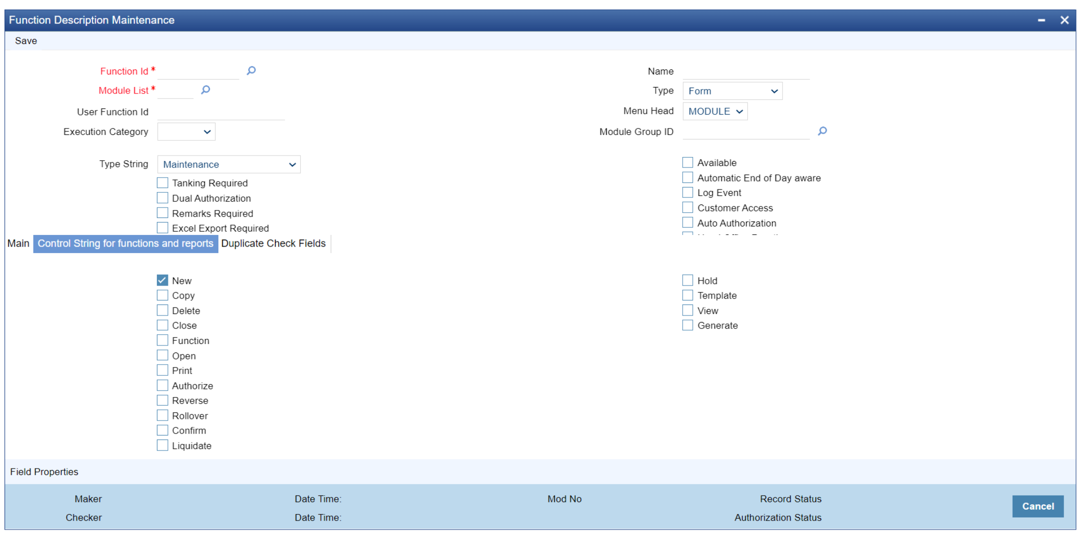
Table 1-15 Main - Field Description

Field	Description
Language Code	Click **Search** and specify the language code from the list of values.
Main Menu	Specify the **Main Menu**.
Sub Menu 1 and **Sub Menu 2**	Specify the sub menu details.
Balloon Help	Specify the **Balloon Help**.
Description	Specify the description.

5. On the **Function Description Maintenance** screen, click **Control String for Functions and Reports**.

   The **Control String for Functions and Reports** tab displays.

Figure 1-9 Control String for Functions and Reports



6. On the **Control String for Functions and Reports** tab, specify the fields.

> **Note:**
>
> The fields, which are marked with an asterisk, are mandatory.

For more information on fields, refer to the field description table.

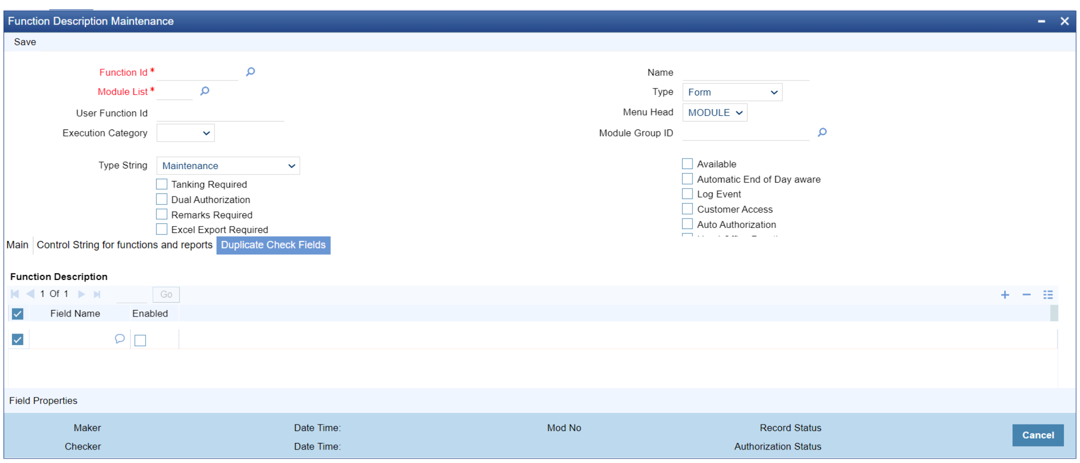
Table 1-16 Control String for Functions and Reports - Field Description

Field	Description
New	Check this box to add **New** action for the function being defined.
Copy	Check this box to add **Copy** action for the function being defined.
Delete	Check this box to add **Delete** action for the function being defined.
Close	Check this box to add **Close** action for the function being defined.
Function	Check this box to add **Function** action for the function being defined.
Open	Check this box to add **Open** action for the function being defined.
Print	Check this box to add **Print** action for the function being defined.
Authorize	Check this box to add **Authorize** action for the function being defined.
Reverse	Check this box to add **Reverse** action for the function being defined.
Rollover	Check this box to add **Rollover** action for the function being defined.
Confirm	Check this box to add **Confirm** action for the function being defined.
Liquidate	Check this box to add **Liquidate** action for the function being defined.
Hold	Check this box to add **Hold** action for the function being defined.
Template	Check this box to add **Template** action for the function being defined.
View	Check this box to add **View** action for the function being defined.
Generate	Check this box to add **Generate** action for the function being defined.

7. On the **Function Description Maintenance** screen, click **Duplicate Check Fields**.

   The **Duplicate Check Fields** tab displays.

Figure 1-10 Duplicate Check Fields



8. On the **Duplicate Check Fields** screen, specify the fields.

> **Note:**
>
> The fields, which are marked with an asterisk, are mandatory.

For more information on fields, refer to the field description table.

Table 1-17 Duplicate Check Fields - Field Description

Field	Description
Field Name	Type the field name in the text box.
Enabled	Check this box to enable the specified field.

9. Click **Exit** to end the transaction.

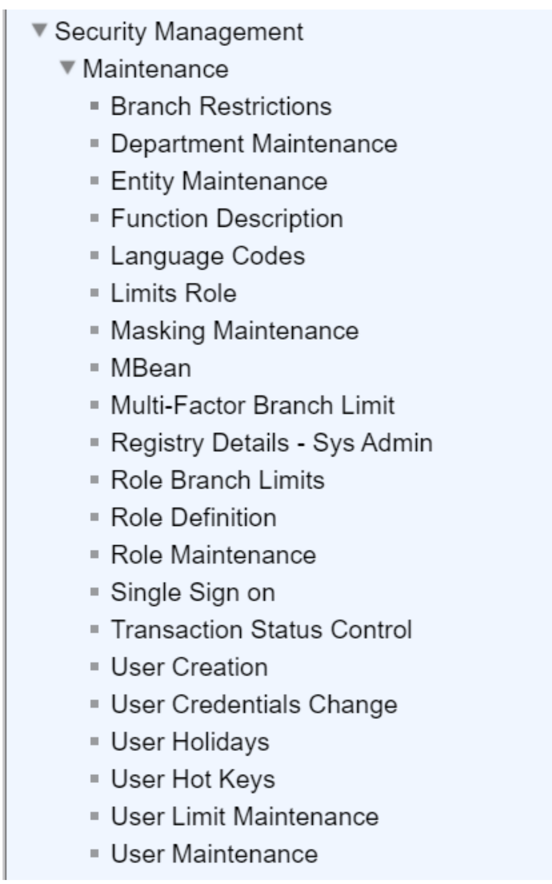
1.7 Define Menu

This topic describes the process of defining the main and sub-menus for the Oracle FLEXCUBE Universal Banking.

The Oracle FLEXCUBE Universal Banking menu can be defined in the topic #unique_32. The user can define the menu appearance for a given language. The menu can only be drilled down up to two sub-menu levels.

For example, For language code **ENG**, if the **Main Menu** value is given as **Security Management**, **Sub Menu 1** as **Maintenance**, and **Sub Menu 2** as **Function Description** for function ID **SMDFNDSC (Function Description Maintenance)**, then on the Oracle FLEXCUBE Universal Banking menu it would appear as follows:

Figure 1-11 Oracle FLEXCUBE Universal Banking Menu



1.8 Define Password Restriction

This topic explains systematic instructions to define password restrictions.

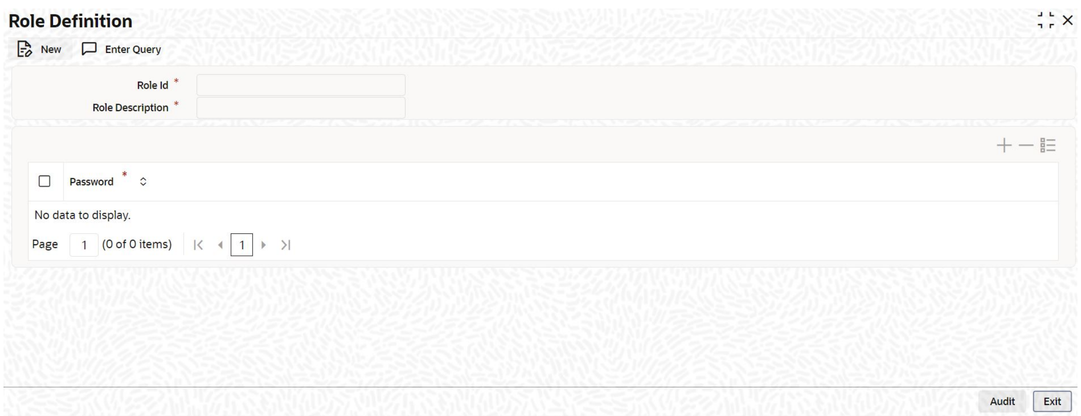
The system allows creation of a list of words that the users, having a certain Role are likely to use as passwords and on which restrictions can be placed. The list of Restrictive Passwords should contain those passwords that the users are most likely to use such as Bank Name, City, Country, and so on. 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, the risk of somebody other than the user knowing the password can be reduced.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SSDROLDF** in the text box, and click **Next**.

   The **Role Definition** screen displays.

   Figure 1-12 Role Definition

2. On the **Role Definition** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-18 Role Definition - Field Description

Field	Description
Role ID	Specify the **Role ID**.
Role Description	Specify the description of the selected **Role ID**.
Password	Specify a list of restrictive passwords for a role.

Any user who is attached to the role cannot use a password in this list. The user can define only the functions that apply to 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. Click **Exit** to end the transaction.

1.9 Maintain Roles

This topic explains systematic instructions to maintain the role profiles.

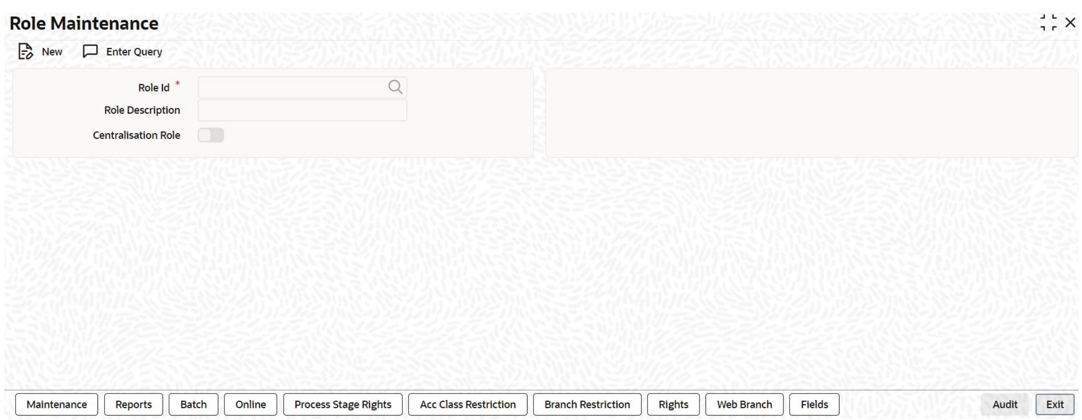
Likely, users working in the same department at the same level of hierarchy need to have similar user profiles. In such cases, define a Role Profile that includes access rights to the functions that are common to a group of users. A user can be linked to a Role Profile which gives the user access rights to all the functions in the Role Profile. The roles defined will be effective only after dual authorization.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDROLDF** in the text box, and click **Next**.

   The **Role Maintenance** screen displays.

Figure 1-13 Role Maintenance



2. On **Role Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-19 Role Maintenance - Field Description

Field	Description
Role ID	Specify the role identification code.
Role Description	The system displays the description of the selected **Role ID**.
Centralization Role	Check this box to centralize the role.

After defining the basic attributes of a role profile, define the functions to which the role profile has access. Check the **Centralization Role** box to specify that the role is applicable for centralized users. The role is automatically associated with all accessible branches if the multi-branch operational parameter is enabled. The various functions in the system fall under different categories.

To assign a function to a role in the **Role Maintenance** screen, click the function categories to which the function belongs. In the **Role Maintenance** screen, the following are the function categories:

Table 1-20 Role Maintenance - Function Category

Function Category	Description
Maintenance	Functions related to the maintenance of static tables
Reports	Functions related to the generation of reports in the various modules
Batch	Functions related to automated operations (like automatic liquidation of contracts, interest, etc.)
Online	Functions related to contract processing
Process Stage Rights	Functions related to workflow
Acc Class Restriction	Functions related to restricting the role from using certain account classes
Branch Restriction	Functions related to restricting the association of roles to certain branches
Rights	Functions related to giving necessary rights for perform various operations in respect of incoming and outgoing messages
Web Branch	Functions related to the Teller module for the role of branch users
Fields	Functions related to User Defined Fields

3. To create a Role profile that closely resembles an existing one, follow the below given steps:
   a. Select **Copy** from the application toolbar to copy the existing profile onto the new one.

      A list of existing role profiles displays.
   b. Click on the existing role profile that is to be copied.

      All the details of the profile except the Role ID are copied and displayed.
   c. Enter a unique **Role ID** and change any of the details of the profile before saving it.
4. To delete an existing role profile, follow the below given steps:

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

   - Select **Close** from the application toolbar to delete an existing role profile.

     If the role is linked to any user, a warning message displays.

     > **Note:**
     >
     > i. This message will bring your attention to the fact that the user profile to which the role is linked will not be the same if the role profile is closed.
     >
     > ii. The Role Profile will be closed only if the closure is confirmed.
5. Click **Exit** to end the transaction.

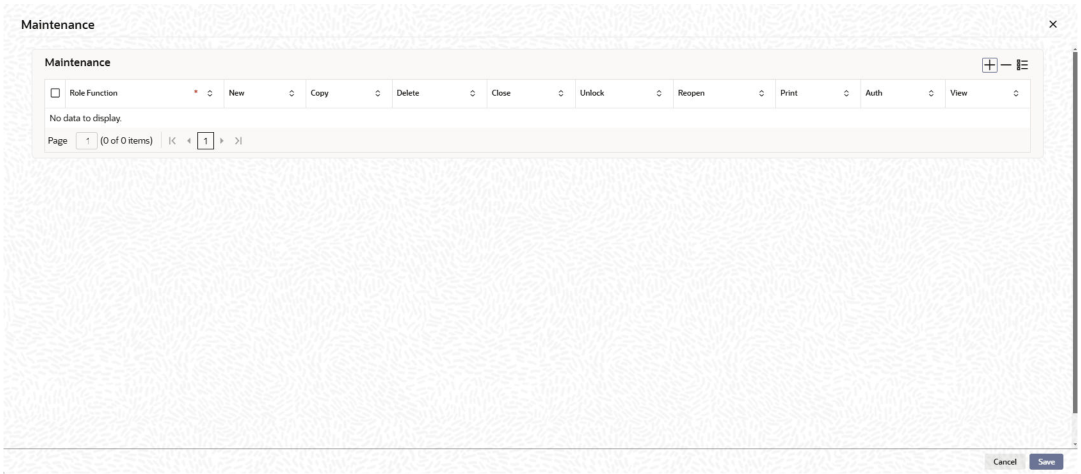
1.10 Process Role Maintenance Details

This topic explains systematic instructions to process role maintenance details.

1. On the **Role Maintenance** screen, click **Maintenance**.

   The **Maintenance** screen displays.

   Figure 1-14 Maintenance



2. On the **Maintenance** screen, specify the fields.

   > **Note:**
   >
   > The fields, which are marked with an asterisk, are mandatory.

   For more information on fields, refer to the field description table.

   Table 1-21 Maintenance - Field Description

Field	Description
Role Function	Click **Search** and specify the role function ID.
New	Check this box to add **New** action to the selected role profile.
Copy	Check this box to add **Copy** action to the selected role profile.
Delete	Check this box to add **Delete** action to the selected role profile.
Close	Check this box to add **Close** action to the selected role profile.
Unlock	Check this box to add **Unlock** action to the selected role profile.
Reopen	Check this box to add **Reopen** action to the selected role profile.
Print	Check this box to add **Print** action to the selected role profile.
Auth	Check this box to add **Auth** action to the selected role profile.
View	Check this box to add **View** action to the selected role profile.

3. Click **Ok** to save the details.

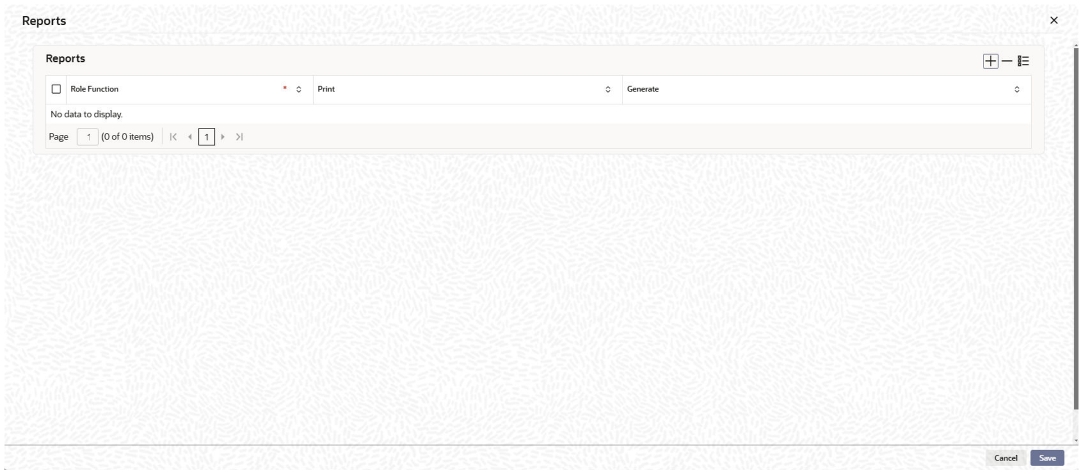
1.11 Maintain Report Details for Role

This topic provides systematic instructions to maintain report details in the **Role Maintenance** screen.

1. On the **Role Maintenance** screen, click **Reports**.

   The **Reports** screen displays.

   Figure 1-15 Reports

2. On the **Reports** screen, specify the fields.

   > **Note:**
   >
   > The fields, which are marked with an asterisk, are mandatory.

   For more information on fields, refer to the field description table.

   Table 1-22 Reports - Field Description

Field	Description
Role Function	Click **Search** and specify the role function ID.
Print	Check this box to add **Print** action to the selected role profile.
Generate	Check this box to add **Generate** action to the selected role profile.

3. Click **Ok** to save the details.

1.12 Maintain Batch Details for Role

This topic provides systematic instructions to maintain batch details in the **Role Maintenance** screen.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **Role Maintenance** screen.

1. On the **Role Maintenance** screen, click **Batch**.

The **Batch** screen displays.

Figure 1-16 Batch

2. On the **Batch** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-23 Batch - Field Description

Field	Description
Role Function	Click **Search** and specify the role function ID.

3. Click **Ok** to save the details.

1.13 Maintain Online Details for Role

This topic provides systematic instructions to maintain online details in the **Role Maintenance** screen.

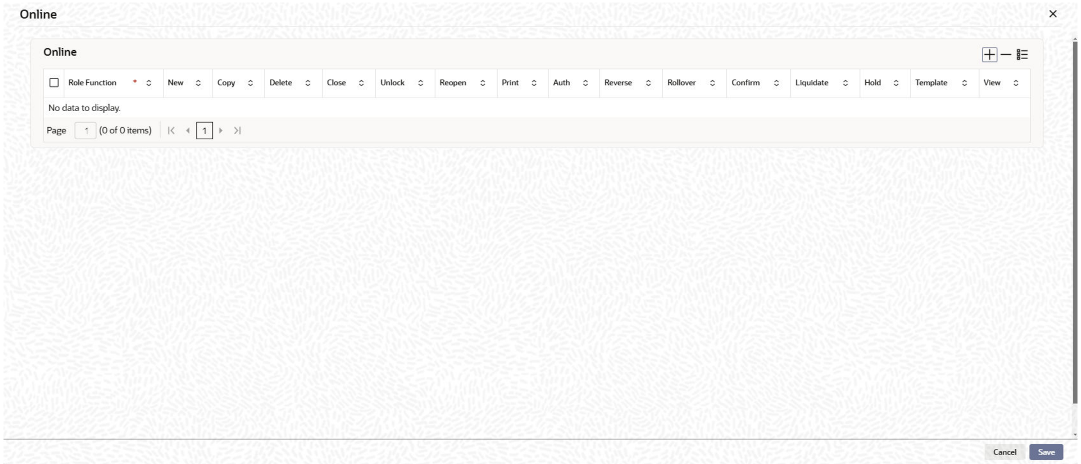
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **Role Maintenance** screen.

1. On the **Role Maintenance** screen, click **Online**.

   The **Online** screen displays.

Figure 1-17 Online



2. On the **Online** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-24 Online - Field Description

Field	Description
Role Function	Click **Search** and specify the role function ID.
New	Check this box to add **New** action to the selected role profile.
Copy	Check this box to add **Copy** action to the selected role profile.
Delete	Check this box to add **Delete** action to the selected role profile.
Close	Check this box to add **Close** action to the selected role profile.
Unlock	Check this box to add **Unlock** action to the selected role profile.
Reopen	Check this box to add **Reopen** action to the selected role profile.
Print	Check this box to add **Print** action to the selected role profile.
Auth	Check this box to add **Auth** action to the selected role profile.
Reverse	Check this box to add **Reverse** action to the selected role profile.
Rollover	Check this box to add **Rollover** action to the selected role profile.
Confirm	Check this box to add **Confirm** action to the selected role profile.
Liquidate	Check this box to add **Liquidate** action to the selected role profile.
Hold	Check this box to add **Hold** action to the selected role profile.
Template	Check this box to add **Template** action to the selected role profile.
View	Check this box to add **View** action to the selected role profile.

3. Click **Ok** to save the details.

1.14 Maintain Access Rights for Role

This topic explains systematic instructions to maintain access stage rights for the function ID.

Through the **Process Stage Rights** screen, specify the function ID to which the role profile is associated.

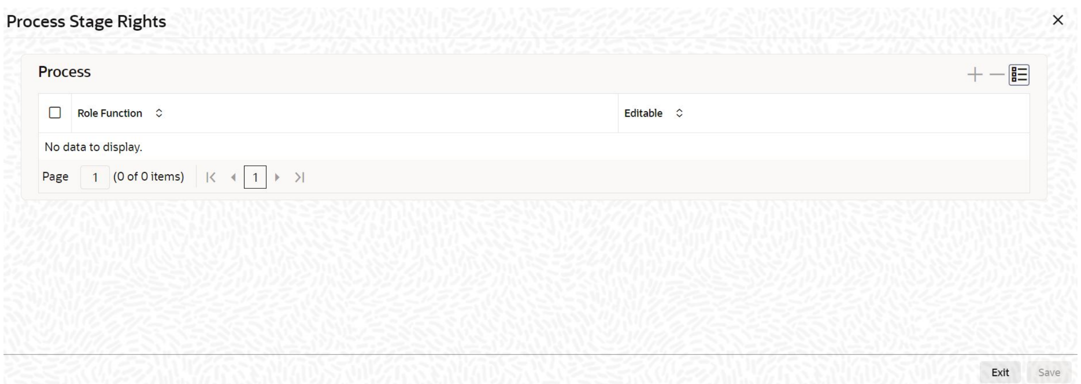
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **Role Maintenance** screen.

1. On the **Role Maintenance** screen, click **Process Stage Rights**.

   The **Process Stage Rights** screen displays.

   Figure 1-18 Process Stage Rights



2. On the **Process Stage Rights** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-25 Process Stage Rights - Field Description

Field	Description
Role Function	Click **Search** and specify the function ID for which access rights are to be provided.
Editable	Check this box to provide editing access for the selected function ID.

3. Click **Exit** to end the transaction.

1.15 Maintain Account Class Restrictions for Role

This topic explains systematic instructions to maintain account class restrictions.

Through the **Acc Class Restriction** screen, restrict the role from using certain account classes that are maintained in Oracle FLEXCUBE Universal Banking.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **Role Maintenance** screen.

1. On the **Role Maintenance** screen, click **Acc Class Restriction**.

   The **Acc Class Restriction** screen displays.

Figure 1-19 Acc Class Restriction

2. On the **Acc Class Restriction** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-26 Acc Class Restriction - Field Description

Field	Description
Account Class Restriction	Select one of the following options: • **Allowed** • **Disallowed** After choosing either the **Allowed** or **Disallowed** option, click **Add** to add a record under the **Account Class Restrictions** list.
Account Class	After selecting the **Account Class Restriction** field details, click **Add** to add a new record. Click **Search** and specify the account classes which have to be restricted for the role.
Description	The system displays the description of the account class.

   For more details about account class restriction, refer to the topic #unique_53.

3. Click **Ok** to save the details.

1.16 Maintain Branch Restriction Details for Role

This topic explains systematic instructions to maintain branch restrictions for the role profile.

Through the **Branch Restriction** screen, specify the branches to which the role profile is associated and for which it is available.

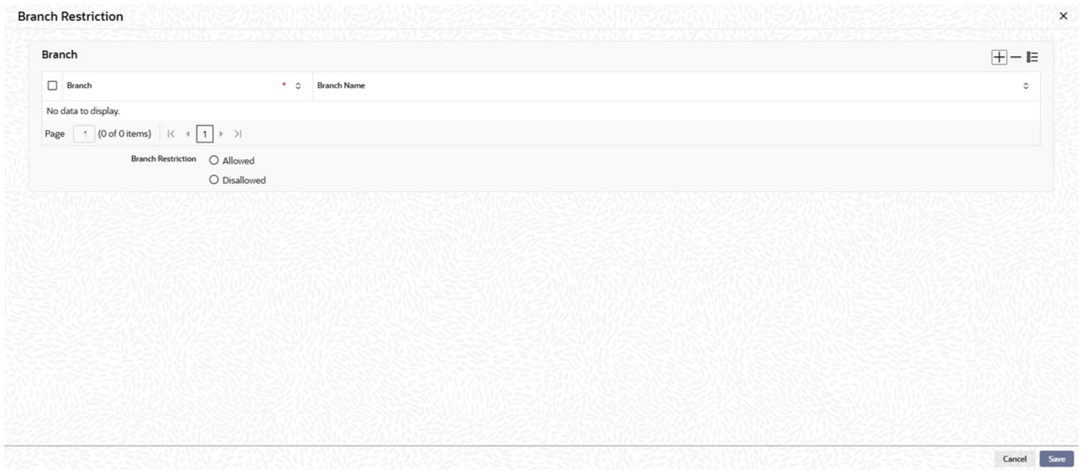
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **Role Maintenance** screen.

1. On the **Role Maintenance** screen, click **Branch Restriction**.

   The **Branch Restriction** screen displays.

Figure 1-20 Branch Restriction



2. On the **Branch Restriction** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-27 Branch Restriction - Field Description

Field	Description
Branch Restriction	Select one of the following options: • **Allowed** • **Disallowed** Select the **Allowed** option to maintain an allowed list, and the branch restrictions list shows the list of allowed branches. Select the **Disallowed** option to maintain a disallowed list of branches. If an allowed list is maintained, then the role profile will be available only for those branches that are specified in the Branch Restrictions list. Similarly, if a disallowed list is maintained, then the role profile will not be available only for those branches that are specified in the Branch Restrictions list.
Branch	Click **Search** and specify the list of branches for which the role is defined.
Branch Name	The system displays the name of the selected branch.

3. Click **Ok** to save the records.

1.17 Maintain Rights for Role

This topic explains systematic instructions to process the necessary rights to perform various operations in respect of incoming and outgoing messages.

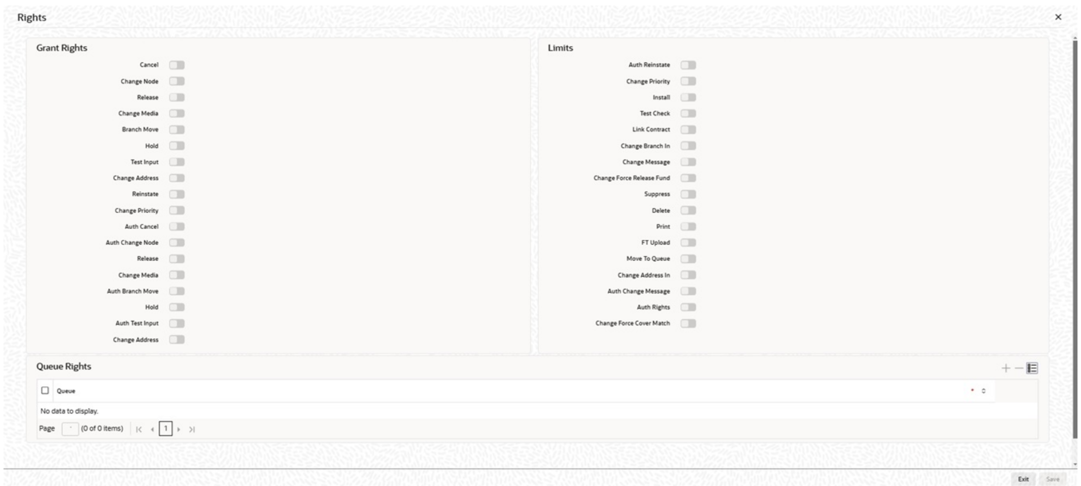
For a role profile, specify the necessary rights to perform various operations in respect of incoming and outgoing messages in the Messaging module of Oracle FLEXCUBE Universal Banking. The user can grant specific permissions for operations on messages as well as allocate the messaging queues to which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

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On the **Role Maintenance** screen, click **Rights**.

   The **Rights** screen displays.

   Figure 1-21 Rights

2. On the **Rights** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-28 Rights - Field Description

Field	Description
Grant Rights	Check against the messaging operations for which want to grant permission. Grant permissions for the following operations on outgoing messages: • Generating a message • Printing a message • Placing a message on hold • Releasing a message on hold • Canceling a message • Inserting a test word • Reinstating a message • Changing the priority of a message • Request information relating to the status of a message • Request cancellation of a message • Changing the media through which a message is transmitted • Changing the address to which a message is to be sent • Moving a message to another branch • Changing the node from which a message should be generated • Authorization of any of the operations listed above, in respect of outgoing message Grant permissions for the following operations on incoming messages: • Printing a message • Authorizing a test word • Routing a message to a queue • Associating a message with a contract • Uploading incoming messages • Making changes (edits) in incoming messages. It is also possible to grant permissions for changing the branch and the address in incoming messages • Authorizing changes made to incoming messages • **Force Release** payment message transactions with **Funding Exception** status and insufficient funds • Suppressing a message • Deleting a message Granting each of these permissions in the **Rights** screen enables the user having this role to perform the corresponding functions in the Incoming and Outgoing Message Browsers. The appropriate icon in the browser, in each case, is enabled for the users associated with the role. **Note:** For details regarding each of these operations in respect of both incoming and outgoing messages, refer the Messaging System user manual. Apart from these functions, the user can also grant permission for the cover matching function for incoming payment message transactions.

Table 1-28 (Cont.) Rights - Field Description

Field	Description
Limits	Check against the messaging operations for which want to grant limit details. • **Auth Reinstate** • **Change Priority** • **Install** • **Test Check** • **Link Contract** • **Change Branch In** • **Change Message** • **Change Force Release Fund** • **Suppress** • **Delete** • **Print** • **FT Upload** • **Move To Queue** • **Change Address In** • **Auth Change Message** • **Auth Rights** • **Change Force Cover Match**
Queue	Click **Search** and specify the queue from the list of values. The user can grant the message queues to which the role has access, and in which users associated with the role can perform messaging operations according to the messaging rights have assigned. The required queues can be selected and listed in the **Queues** list under the **Grant Queues** section.

3. Click **Exit** to end the transaction.

1.18 Define Roles for Oracle FLEXCUBE Universal Banking Branch Users

This topic explains systematic instructions to define roles for Oracle FLEXCUBE Universal Banking branch users.

Through the **Web Branch** screen, define a role with functions typically performed from the Oracle FLEXCUBE Universal Banking Branch system, also maintain the role **Teller** and select the branch function.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **Role Maintenance** screen.

1. On the **Role Maintenance** screen, click **Web Branch**.

   The **Web Branch** screen displays.

Figure 1-22 Web Branch

2. On the **Web Branch** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-29 Web Branch - Field Description

Field	Description
Role Function	Click **Search** and specify the role function from the list of values.

> **Note:**
>
> - To give access of host functions to the **Teller**, attach a role like **ALLROLES** or another role with host functions in addition to the **Teller** role. This can be done at the User Profile level for the allowed branch.
> - The system generates a notification on the authorization of any modification, addition, or deletion of a role.

3. Click **Exit** to end the transaction.

1.19 Maintain User Holidays

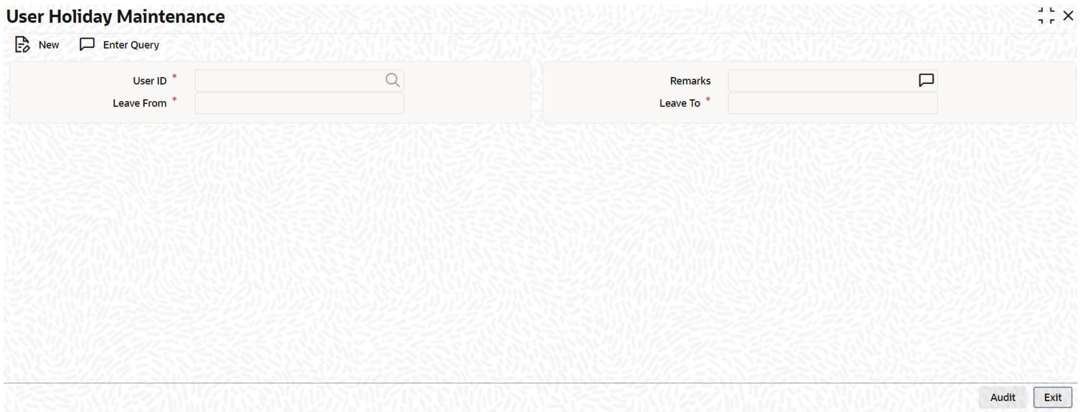
This topic explains systematic instructions to maintain user holidays.

Through the **User Holiday Maintenance** screen, block a specific user for a certain time frame by defining holiday slots for that user profile.

1. On **Homescreen**, type **SMDUSHOL** in the text box, and click **Next**.

   The **User Holiday Maintenance** screen displays.

Figure 1-23 User Holiday Maintenance



2. On the **User Holiday Maintenance** screen, specify the fields.

> **Note:**
>
> The fields, which are marked with an asterisk, are mandatory.

For more information on fields, refer to the field description table.

Table 1-30 User Holiday Maintenance - Field Description

Field	Description
User ID	Click **Search** and specify the user ID for whom want to define the holiday period. The adjoining list of values displays all the valid user profiles maintained in the system.
Leave From	Click **Calendar** and select the start date for the holiday period.
Leave To	Click **Calendar** and select the end date for the holiday period. The user is not allowed to log in within the specified holiday range.
Remarks	Specify a brief description for the holiday.

It is feasible to maintain multiple holiday slots for a user, but the system will not allow including as specific day in more than one slot.

3. Click **Exit** to end the transaction.

1.20 Process User Holiday Summary

This topic explains systematic instructions to process user holiday summary details.

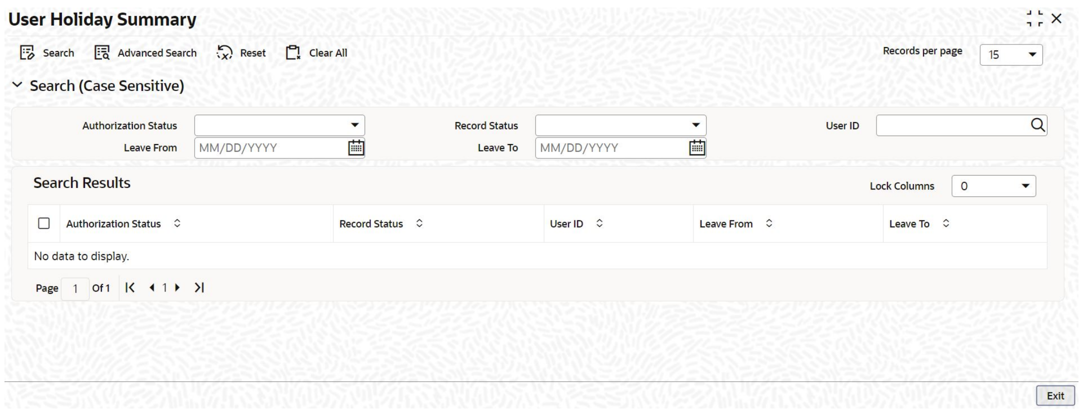
The **User Holiday Summary** screen allows one to view holiday periods maintained for any user profile.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMSUSHOL** in the text box, and click **Next**.

   The **User Holiday Summary** screen displays.

   Figure 1-24 User Holiday Summary



2. On the **User Holiday Summary** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-31 User Holiday Summary - Field Description

Field	Description
Authorization Status	Select the authorization status from the drop-down list: • **Authorized** • **Unauthorized** • **Rejected**
Record Status	Select the record status from the drop-down list: • **Open** • **Closed**
User ID	Click **Search** and specify the **User ID** from the list of values.
Leave From	Click **Calendar** and select **Leave From** date.
Leave To	Click **Calendar** and select **Leave To** date.

3. Click **Search** after specifying the search parameters.

   The system identifies all records satisfying the specified criteria and displays the following details for each one of them:

   - **Authorization Status**
   - **Record Status**
   - **User ID**
   - **Leave From**
   - **Leave To**
4. Click **Exit** to end the transaction.

1.21 Maintain Users

This topic explains systematic instructions to create user profiles.

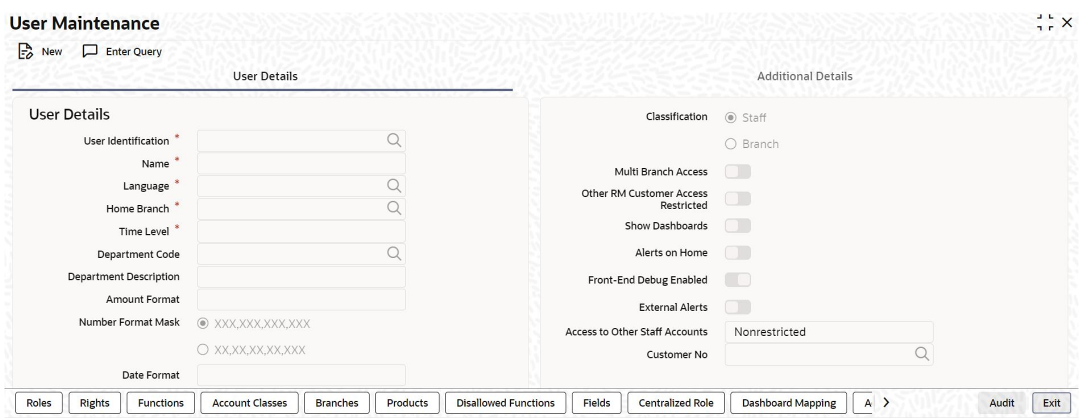
A User Profile defines the activities that a user can carry out on the system. It also contains the user ID, the name through which the user will access the system and the password. The user profiles will be effective only after dual authorization.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDUSRDF** in the text box, and click **Next**.

   The **User Maintenance** screen displays.

   Figure 1-25 User Maintenance

   > **Note:**
   >
   > The **User Details** tab displays default.

2. On the **User Details** tab, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-32 User Maintenance - Field Description

Field	Description
User Identification	Specify the user identification. This ID identifies the user whose profile is being defined. In a user ID, Use alphabets in upper or lower case, numbers 0 to 9, and _ (underscore). The number of characters in a User ID should be greater than or equal to six and less than 12.
Name	Specify the name of the user.

Table 1-32 (Cont.) User Maintenance - Field Description

Field	Description
Language	Click **Search** and specify the language in which the user's screen have to be defined from the list of values. The language codes maintained through the **Language Code Maintenance** screen are available for selection.
Home Branch	By default, the **Current Branch** displays here. All users have to be attached to a branch.
Time Level	The time level defaults to **Nine**. Specify the time level that is to be maintained at the User level if needed. Specify values between **Zero** to **Nine**. The **Time Level** can be specified at the Branch level and the User level. To log in, then the time level maintained at User Profile should be greater than or equal to that maintained at the Branch level. Time levels are maintained to prevent logging into the application when the system is processing the EOC batch. Before EOC Operations, the time level of the system is increased, so that it is higher than that maintained at the User level. However, if the user is not logged out when the **Time Level** is raised to the one higher than defined, then the user can continue to use the application. If required, modify the time level at the user profile level when the branch is at the **Transaction Input** stage. **Note:** After modifying the time level value to the value wanted to maintain, move the cursor to any other field and then click **Save**.
Department Code	Click **Search** and specify the department code. The adjoining list of values displays a list of all the valid department codes maintain in the system.
Department Description	The system displays the department description.
Amount Format	Select the amount format from the drop-down list. • **.,** • **,.** • **,**
Number Format Mask	Select the format of the mask number either in Million or Lakh from the following options: • **XXX,XXX,XXX,XXX** • **XX,XX,XX,XX,XXX**
Date Format	Select the date format from the drop-down list. • **MM/DD/YYYY** • **DD/MM/YYYY** • **YYYY-MM-DD** • **DD-MMM-YYYY** • **DD-MM-YYYY** • **DD.MM.YYYY**

Table 1-32 (Cont.) User Maintenance - Field Description

Field	Description
Auto Authorization	To indicate that a user is allowed to perform automatic authorization, check the **Auto Authorization** box. If automatic authorization has been enabled for a function, branch, and user profile, and a user has rights for both input and authorize operations, any record maintained by such user in the corresponding function (maintenance or online) screens will be automatically authorized when the **Save** operation is performed. For example of the automatic authorization enabled branches, refer to the #unique_49/unique_49_Connect_42_TABLE_PW1_1XP_SSB table. For example of the automatic authorization enabled functions, refer to the #unique_49/unique_49_Connect_42_TABLE_PYC_HXP_SSB table. For example of the Transaction access rights for the users, refer to the #unique_49/unique_49_Connect_42_TABLE_AVD_RXP_SSB. For example of the automatic authorization examples according to maintenance, refer to the #unique_49/ unique_49_Connect_42_TABLE_IBZ_GYP_SSB
Supervisor Identification	Specify the ID of the supervisor of the user. The list of values displays all valid supervisor identifications maintained in the system. In the case of relationship managers, also use this field to define the Relationship Manager hierarchy. For defining the Relationship Manager hierarchy in this method, select the RM user who is one level up in the hierarchical order as the supervisor. If the user is superior in the RM hierarchical order, specify their user ID as the supervisor ID. The supervisor ID list of values also shows the user ID of the user is maintained. This means it is possible to define an RM user as their own supervisor. **Note:** The RM hierarchy defined in this method is enabled only if the check box **RM Hierarchy Setup Required** is not checked in the **SMS Banks Parameters** screen.
Supervisor Name	The system displays the name of the supervisor based on the selected **Supervisor Identification**.
PII Allowed	Check this box to allow the users to view Personally Identifiable Information.
Classification	• **Staff** - All internal users of the bank can be classified as Staff. Include any of the functions available in the system in the user profile. • **Branch** - This indicates a branch user. This is used to identify a branch user and branch-specific user maintenance for the branch user.
Multi Branch Access	Check this box to configure a dual access framework for the specified **User ID**.

Table 1-32 (Cont.) User Maintenance - Field Description

Field	Description
Other RM Customer Access Restricted	The user’s access to the transactions of the customers who are assigned to a different relationship manager can be restricted. Check this box to restrict the user from viewing, creating, authorizing or amending the transactions of the customers who are not assigned. The customers who are not assigned to the relationship manager include the customers assigned to other relationship managers as well as those who are not assigned to any relationship manager. If this box is not checked, the user can view, create, authorize and amend the transactions of the customers assigned to other relationship managers. This is applicable to the users created with their role as relationship manager.
Show Dashboards	Check this box if want the system to display all the dashboards assigned to User Role on the landing page.
Alerts on Home	Check this box if want the system to display the Alerts on the landing page.
Front-End Debug Enabled	Check this box to enable the debug window for a user.
External Alerts	Check this box to enable the external alerts.

Table 1-32 (Cont.) User Maintenance - Field Description

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Access to Other Staff Accounts</td><td>Select Access to Other Staff Accounts from the drop-down list:
Restricted
Nonrestricted
A user with restricted access will not be able to view/print details of contracts involving the product in all Contract Functions and Contract Summary screens for the following modules:
Corporate Teller
Clearing
The Contract Online and Cycle Due screen of SI
Foreign Exchange (online and payment)
The Contract Online, Value Dated Amendments, and Payments Input screens of MM
The Contract Online put, Value Dated Amendments, Payments Input, and Loans
Note:
The view restriction does not apply to the transaction or contract screens in which the other staff accounts are involved.

The other functions to which the user will have restrictive rights are as follows:
Ad-hoc loan statement generation
Queries - Accounting Entries
Customer Based Information Retrieval
Limits Override showing account balances
Message Browser
If a balance exception has occurred, the balances are not displayed for the restricted user but will be replaced by **.

Note:
The restricted users will be able to:
View/print financial information of contracts they have initiated or view/ print balances of their accounts.
Post transactions to the staff accounts or create contracts for staff members, even if the user is restricted to view/print the balances/contract information of other colleagues.
In case of a balance exception during transaction posting, the balance will not be displayed. The Exception Message will only state that the account will be Overdrawn on account of the transaction.
Post transactions and view transaction information until the contract is authorized. After authorization, such users cannot access the contract.</td></tr>
</table>

Table 1-32 (Cont.) User Maintenance - Field Description

Field	Description
Customer Number	Click **Search** and specify the **Customer Number** from the list of values. It is feasible to link the customer number (CIF ID) of the employee with the User ID.

For example, if the automatic authorization is enabled for the following branches in the Branch Parameters:

Table 1-33 Automatic Authorization enabled Branches

Branch	Automatic Authorization Enabled
000	Yes
001	No
002	Yes

In the **Function Description Maintenance** screen, automatic authorization has been enabled for the following functions:

Table 1-34 Automatic Authorization enabled Functions

Function	Automatic Authorization Enabled
Customer Information Maintenance	Yes
LD Contract Online	Yes
Customer Account Maintenance	Yes

Automatic authorization rights are maintained for specific users in the User Maintenance as shown below:

Table 1-35 Automatic Authorization enabled Users

User	Automatic Authorization Enabled
Ronald	Yes
George	Yes
Smith	No

Transaction access rights for the users are maintained as shown below:

Table 1-36 Transaction access rights

User	Branch	Function	Input Access	Authorize Access
Ronald	000	Customer Information Maintenance	Yes	Yes
Ronald	001	Customer Information Maintenance	Yes	Yes

Table 1-36 (Cont.) Transaction access rights

User	Branch	Function	Input Access	Authorize Access
Ronald	000	Customer Account Maintenance	Yes	No
George	001	LD Contract Online	Yes	Yes
George	000	Customer Account Maintenance	Yes	Yes
Smith	000	LD Contract Online	Yes	Yes
Smith	000	Customer Account Maintenance	Yes	Yes

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

Table 1-37 Automatic Authorization - Maintenance

User	Branch	Function	Automatic Authorization on Save?	Reason
Ronald	000	Customer Information Maintenance	Yes	Input and Authorize rights are enabled for the user, as well as automatic authorization rights enabled for the user, branch, and function.
Ronald	001	Customer Information Maintenance	No	Automatic authorization is not enabled for branch 001.
Ronald	000	Customer Information Maintenance	No	Authorization access is not enabled for the user.
George	001	LD Contract Online	No	Automatic authorization is not enabled for branch 001.

Table 1-37 (Cont.) Automatic Authorization - Maintenance

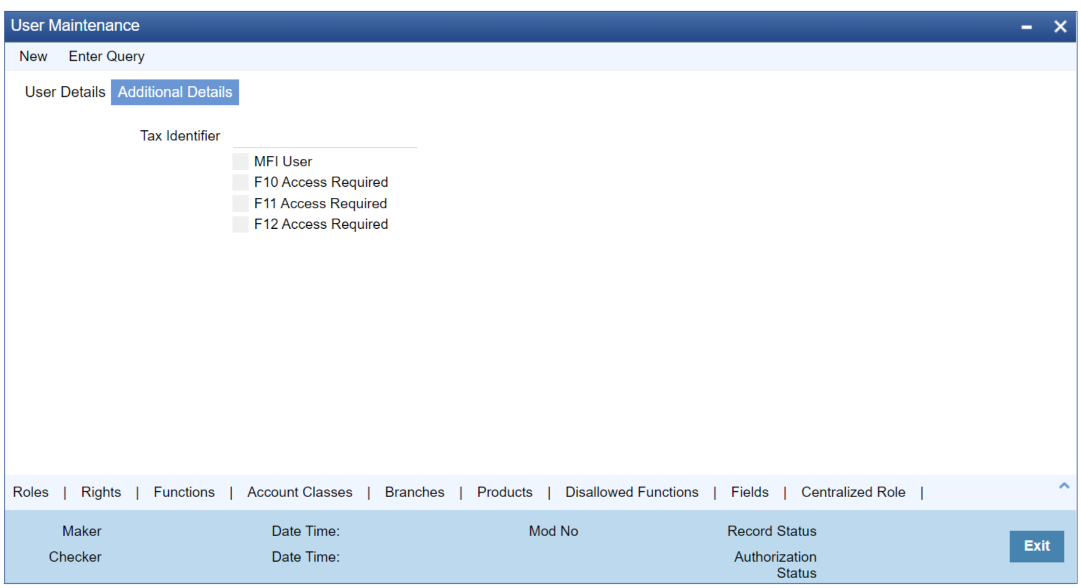
User	Branch	Function	Automatic Authorization on Save?	Reason
George	000	Customer Information Maintenance	Yes	Input and Authorize rights are enabled for the user, as well as automatic authorization rights enabled for the user, branch, and function. The user can also authorize any maintenance done by the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

For more details about automatic authorization, refer to the Procedures User Guide.

3. On the **User Maintenance** screen, click **Additional Details**.

   The **Additional Details** tab displays.

Figure 1-26 Additional Details



4. On the **Additional Details** tab screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-38 Additional Details - Field Description

Field	Description
Tax Identifier	Specify the tax identifier code of the customer to monitor Anti Money Laundering activities.
MFI User	Select the **MFI User** check box to indicate that the user is a Microfinance (Account Officer) user. By default, the system leaves this check box deselected to indicate that all users would be normal users. An account officer can book loan accounts for customers who are linked to him/her. **Note:** For more details, refer to topic (**Account Officer Maintenance** screen) Linking Customers to Account Officers in the Micro finance User Manual.
F10 Access Required	Select this check box to access **SVDIMGVW (Customer Signature and Image View)** screen.
F11 Access Required	Select this check box to access **STDCUSBL (Customer Account Balance View)** screen.
F12 Access Required	Select this check box to access **SVDIMGVW (Customer Signature and Image View)** screen.

5. Click **Exit** to end the transaction.

1.22 Maintain Roles for Users

This topic explains systematic instructions to attach a user profile to a role in the **Roles** screen.

A Role is always associated with a user for a specific Branch. The values set at the role level are directly inherited by the user for that branch, like Functions IDs, Account Class and Branch Restrictions, Input and Authorization Limits, and so on.

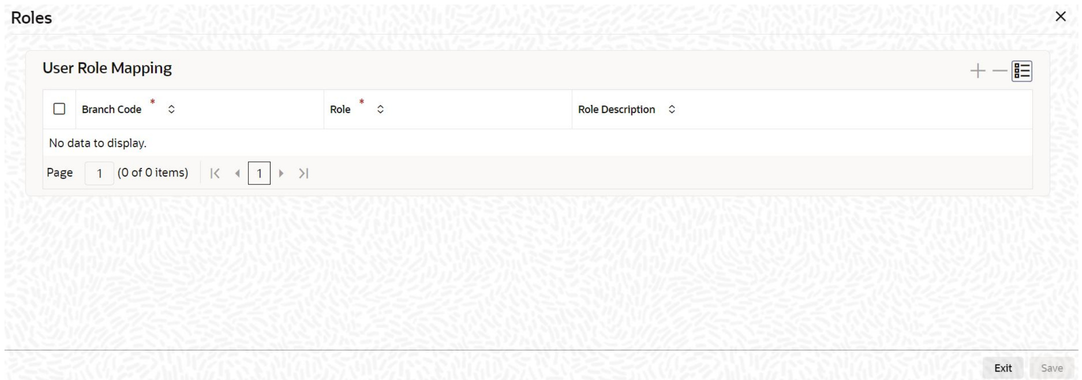
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Roles**.

   The **Roles** screen displays.

Figure 1-27 Roles



2. On the **Roles** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-39 Roles - Field Description

Field	Description
Branch Code	Click **Search** and specify the branch code assigned to the user role from the list of values. The list of values displays all the valid branch codes maintained in the system.
Role	Click **Search** and specify the role assigned to the user for the selected **Branch Code**. The list of values displays all valid roles maintained in the system. **Note:** One can assign the role of Relationship Manager to a user by selecting **RM-ROLE**.
Role Description	Based on the selected **Role** field, the system displays the role description.

3. Click **Add** to add a record under the **Roles** list.
4. To delete a role(s) that has been attached to a user profile, check the box beside the required record and click **Delete**.
5. Click **Exit** to end the transaction.

1.23 Maintain Rights for Users

This topic explains systematic instructions to maintain rights in the **User Maintenance** screen.

A user should have the necessary rights to perform various operations in respect of incoming and outgoing messages in the Messaging module of Oracle FLEXCUBE Universal Banking. The user can grant specific permissions for operations on messages, as well as allot the messaging queues to which the user has access.

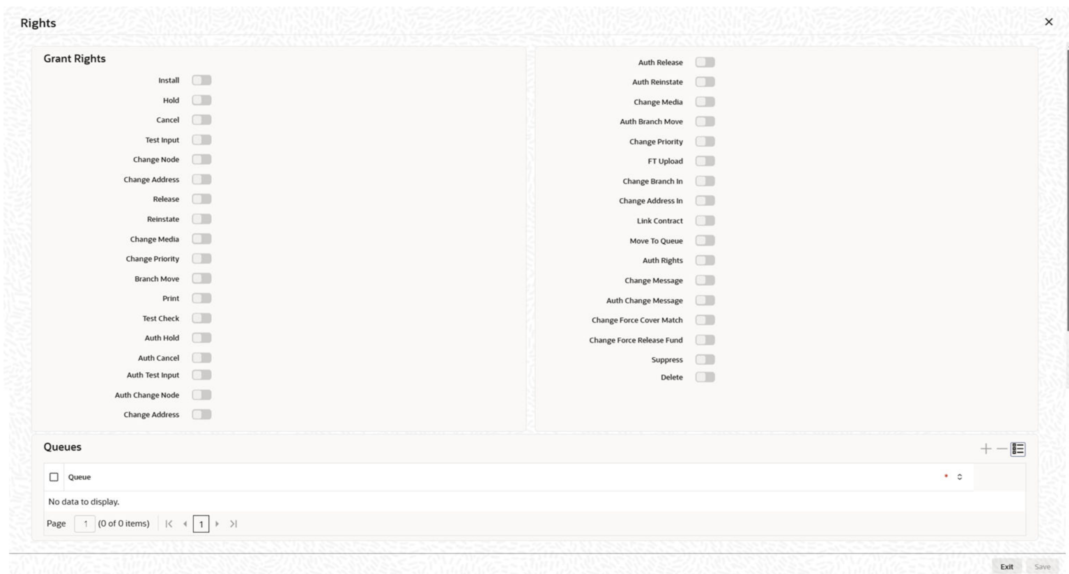
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Rights**.

   The **Rights** screen displays.

Figure 1-28 Rights



2. On the **Rights** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-40 Rights - Field Description

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Grant Rights</td><td>Check against the messaging operations for which want to grant permission. Grant permissions for the following operations on outgoing messages:

Generating a message
Printing a message
Placing a message on hold
Releasing a message on hold
Canceling a message
Inserting a test word
Reinstating a message
Changing the priority of a message
Request information relating to Status of a message
Request cancellation of a message
Changing the media through which a message is transmitted
Changing the address to which a message is to be sent
Moving a message to another branch
Changing the node from which a message should be generated
Authorization of any of the operations listed above, in respect of outgoing message

Grant permissions for the following operations on incoming messages:

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

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

Note:
For details regarding each of these operations in respect of both incoming and outgoing messages, refer to the Messaging System user manual.

Apart from these functions, the user can also grant permission for the cover matching function for incoming payment message transactions.</td></tr>
</table>

Table 1-40 (Cont.) Rights - Field Description

Field	Description
Queues	The message queues can be allocated to which the user has access, and in which the user can perform messaging operations according to the messaging rights have assigned. The required queues can be selected and listed in the **Queues**.

3. Click **Exit** to end the transaction.

1.24 Maintain Functions for Users

This topic explains systematic instructions to maintain functions in the **User Maintenance** screen.

In addition to attaching a user profile to a role, the rights can be given to individual functions. For a user profile to which no role is attached, access can be given to specific functions.

- If attached one or more roles to a user profile
- If access is given 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.
For example, The role profile **FXDP1** has access to **New**, **Copy**, **Delete**, **Close**, **Reopen**, **Unlock**, and **Print** for the Forward Rates table.

Attach the user profile of Tanya to the role **FXDP1**. While allotting rights to individual functions for Tanya, give rights to **New**, **Copy**, **Delete**, and **Close** for the Forward Rates table. The role has access rights to **Reopen**, **Unlock** and **Print** in addition to these. In such a case, the user profile of Tanya will have rights to only the functions to which rights are given at the user profile level (that is, **New**, **Copy**, **Delete**, and **Close**) even if the role **FXDP1** has rights to other functions.

Note:

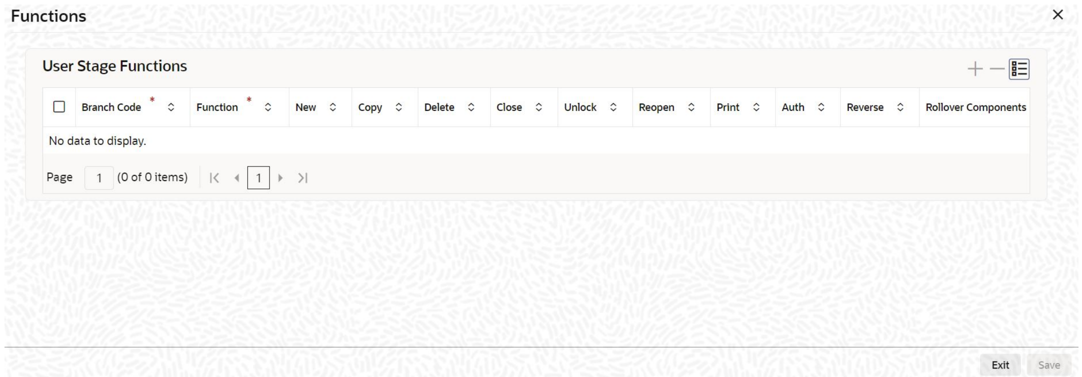
The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Functions** to give access to functions for the user profile.

   The **Functions** screen displays.

Figure 1-29 Functions



2. On the **Functions** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-41 Functions - Field Description

Field	Description
Branch Code	Click **Search** and specify the branch code.
Function	Click **Search** and specify the function for which want to give rights. The adjoining list of values displays a list of Function IDs belonging to the category along with their descriptions. Specify the rights to the different actions for the functions by checking against the action. **Note:** For more information on functions refer to the topic #unique_32.

The various functions in the system fall under different categories. To assign a function to a user profile in the **Functions** screen, select the tab of the function category to which the function belongs. The function categories and their respective tab in the **Functions** screen are as follows:

Table 1-42 Function category

Category (Tab)	Description
Maintenance	Functions relating to the maintenance of static tables.
Online	Functions relating to contract processing.
Batch	Functions relating to the automated operations (like automatic liquidation of contract, interest, etc.)
Reports	Functions relating to the generation of reports in the various modules.
Process	Functions relating to access rights for the tasks under a process.

Click the corresponding category tab to associate the required functions.

3. Click **Exit** to end the transaction.

1.25 Maintain Account Class Restrictions for Users

This topic explains systematic instructions to specify account class restrictions.

The user can be restricted from using certain account classes that are maintained in Oracle FLEXCUBE Universal Banking in two ways.

- A user role that has an account class restriction can be mapped at the User Role level, for an allowed branch in the **Roles** screen at the User Profile level. Restricted account classes can be viewed in the **Account Classes** list of values at the User Role level and not at the User Profile level.
- Select account classes from the **Account Classes** list of values and then select an option from the following at the User Profile level:
  - **Allowed**
  - **Disallowed**

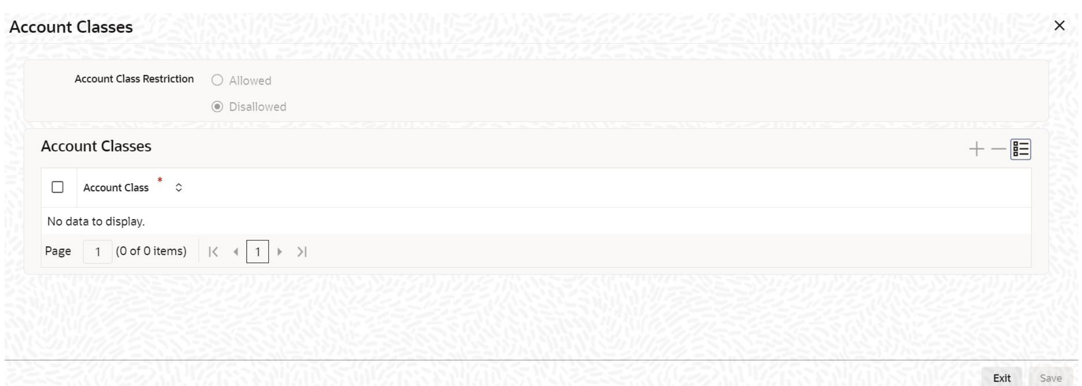
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Account Classes**.

   The **Account Classes** screen displays.

   Figure 1-30 Account Classes

2. On the **Account Classes** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-43 Account Classes - Field Description

Field	Description
Account Class Restriction	Specify either to allow or disallow the user from using certain account classes. Subsequently, specify the account classes, which have to be allowed or restricted for the user depending on the option selected. • **Allowed** - Select this option to allow selected account classes and disallow unselected account classes. • **Disallowed** - Select this option to disallow selected account classes and allow unselected account classes. In both cases, the user can query customer accounts belonging to a restricted account class. However, the system will not allow the creation and modification of an account under a restricted account class.
Account Class	Click **Search** and specify the account class from the adjoining list of values.

3. Click **Exit** to end the transaction.

1.26 Maintain Branch Details for Users

This topic explains systematic instructions to maintain branch details in the **User Maintenance** screen.

To specify the branches from which the staff and branch users of the bank can operate, use the **Branches** screen.

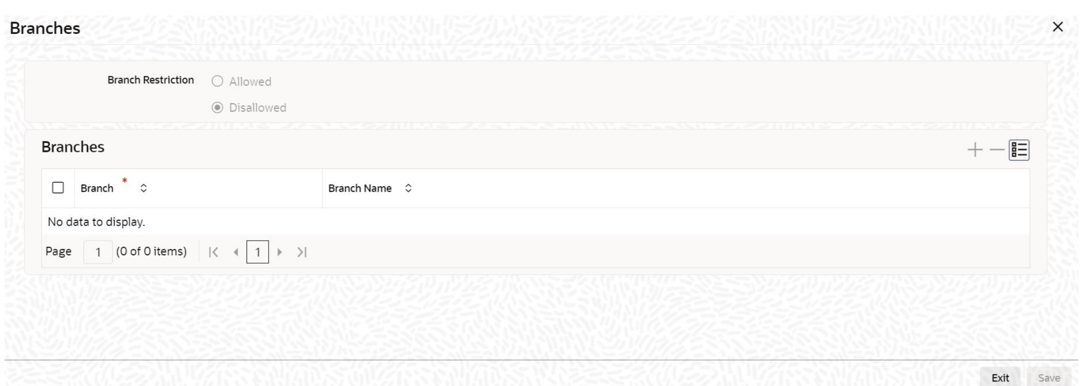
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Branches**.

   The **Branches** screen displays.

Figure 1-31 Branches



2. On the **Branches** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-44 Branches - Field Description

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Branch Restriction</td><td>Select one of the following options to maintain a list of branches for the user:
Allowed - To maintain an allowed list of branches, select Allowed. Then the Branch Restriction list shows the list of allowed branches.
Disallowed - To maintain a disallowed list of branches, select Disallowed.
If an Allowed list is maintained, then the user profile will be available only for branches that are specified in the Branch Restriction list. Similarly, if a Disallowed list is maintained, then the user profile will not be available only for branches that are specified in the Branch Restriction list. Any branch that is Disallowed will not appear to that user in change branch list.
If you maintain an allowed list, then the user profile will be available only for those branches that you specify in the Branch Restrictions list. Similarly, if you maintain a disallowed list, then the user profile will not be available only for those branches that you specify in the Branch Restrictions list. Any branch that is Disallowed will not appear to that user in his Change Branch list.</td></tr>
<tr><td>Branch</td><td>Click Add to add a record under the Branch Restriction list. Click Search and select the required branch from the adjoining list of values.

Note:
The branch in which the user profile is defined is known as the Home Branch. The branches that the user can access are known as the Host Branch.
The user should create an ID called GUEST in each branch. When a user belonging to the staff category changes the branch of operation, the user can perform the functions defined for the GUEST ID in the Host Branch.</td></tr>
<tr><td>Branch Name</td><td>The system displays the branch name.</td></tr>
</table>

3. Click **Exit** to end the transaction.

1.27 Maintain Product Restrictions for Users

This topic explains systematic instructions to maintain product details in the **User Maintenance** screen.

The user can be restricted from using certain products maintained in the Oracle FLEXCUBE Universal Banking. Such product restrictions for the user can be specified in the **Products** screen. In the **Products** screen, the following restrictions on the user profile can be placed:

- **Posting Restriction**
- **Access Restriction**

The users with **Posting Restriction** will not be able to process transactions involving restricted products, and the users with **Access Restriction** will not be allowed to view or print financial details of contracts involving restricted products.

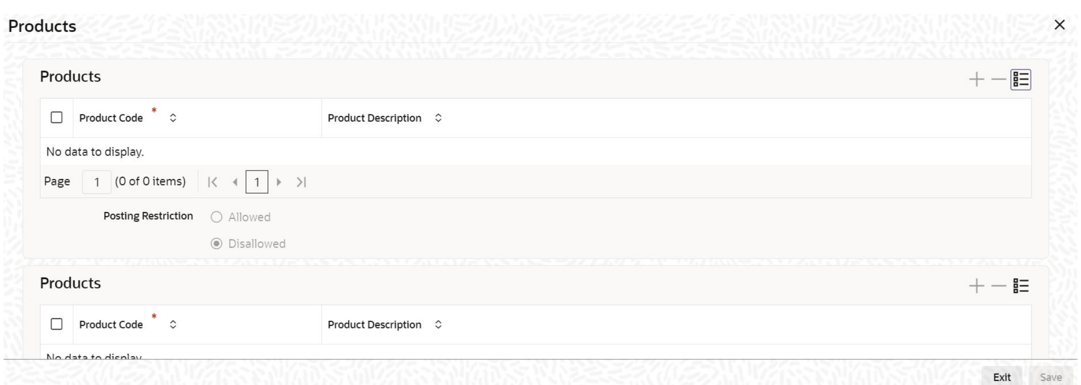
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Products**.

   The **Products** screen displays.

   Figure 1-32 Products

2. On the **Products** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-45 Products - Field Description

Field	Description
Posting Restriction and **Access Restriction**	Select one of the following options to allow or disallow the user from posting into/accessing certain products: • **Allowed** - Select the option **Allowed** to allow the user to post entries into/access certain products. • **Disallowed** - Select the option **Disallowed** to disallow the user from posting/accessing certain products.
Product Code	Click **Add** to add a record under the **Products** list. Click **Search** and specify the required product code from the adjoining list of values.
Product Description	The system displays the product description.

> **Note:**
>
> If for a product, the Access restriction has not been maintained but Posting is allowed the restricted user can post transactions for that product and can view the contract information until such time that the contract gets authorized.

3. Click **Exit** to end the transaction.

1.28 Maintain Disallowed Functions for Users

This topic explains systematic instructions to maintain disallowed functions in the **User Maintenance** screen.

Through the **Disallowed Functions** screen, restrict certain functions from being performed by a user.

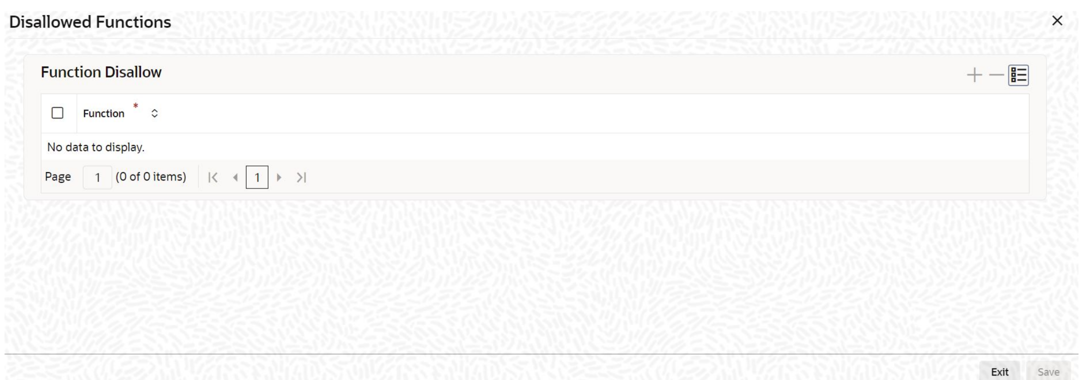
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Disallowed Functions**.

   The **Disallowed Functions** screen displays.

   Figure 1-33 Disallowed Functions

2. On the **Disallowed Functions** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-46 Disallowed Functions - Field Description

Field	Description
Function	Click **Search** and select the disallowed function from the list of values.

3. Click **Exit** to end the transaction.

1.29 Maintain Centralized Role Details for Users

This topic explains systematic instructions to maintain centralized role details in the **User Maintenance** screen.

In the **Centralized Role Mapping** screen, the centralization role can be linked to a user, and also can view the centralized role maintained for the user profile.

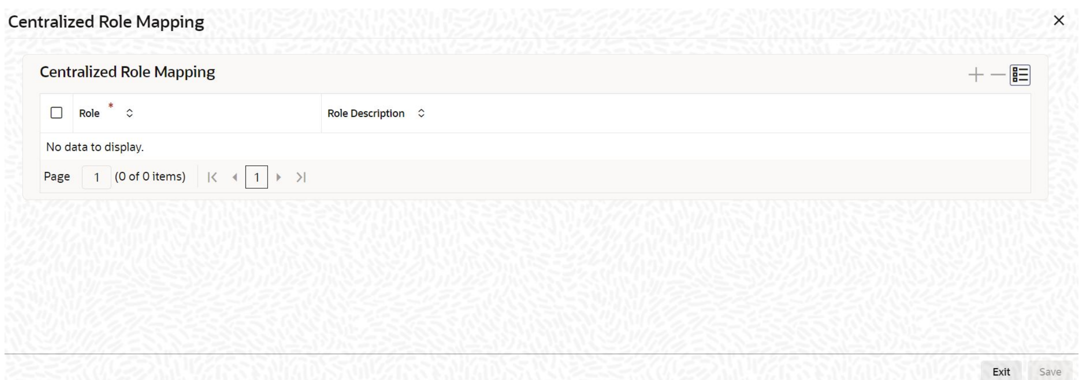
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Centralized Role**.

   The **Centralized Role Mapping** screen displays.

   Figure 1-34 Centralized Role Mapping



2. On the **Centralized Role Mapping** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-47 Centralized Role Mapping - Field Description

Field	Description
Role	Click **Search** and specify the centralized role from the adjoining list of values.
Role Description	The system displays the description of the role.

If the multi branch operational parameter is enabled and the centralization roles are defined, then the roles are automatically assigned to the branches based on the branch restriction details specified in the **User Maintenance** screen. Through the **Roles** screen, additional list of normal roles can be included.

> **Note:**
>
> A centralized role cannot be assigned to a subset of allowed branches of a user. The normal role must be assigned manually to each applicable branch.

3. Click **Exit** to end the transaction.

1.30 Maintain Dashboard Mapping Details for Users

This topic explains systematic instructions to maintain dashboard mapping details in the **User Maintenance** screen.

If the **Show Dashboards** box is checked in the **User Maintenance** screen, then the specified user can be mapped to one or more dashboards in the **Dashboard Maintenance** sub-screen.

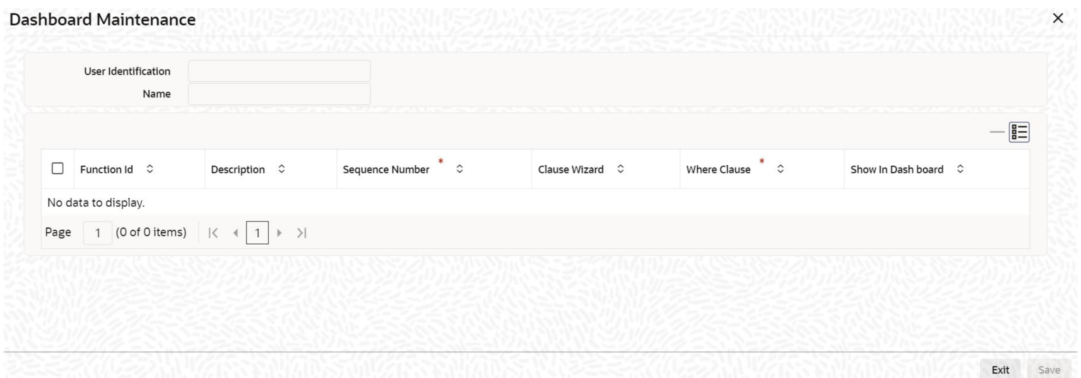
> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Dashboard Mapping**.

   The **Dashboard Maintenance** screen displays.

   Figure 1-35 Dashboard Maintenance



2. On **Dashboard Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-48 Dashboard Maintenance - Field Description

Field	Description
User Identification	The system defaults the user identification number from the **User Maintenance** screen.
Name	The system displays the user name from the **User Maintenance** screen.
Populate	Click **Populate** to display DFIs mapped to the specified user role.
Function ID	The system displays the function ID of the dashboard assigned to the user.
Description	The system displays the description of the dashboard.
Sequence Number	Specify the sequence number based on the user's preference.
Where Clause	The system defaults the values specified in the **Dashboard Condition** screen.

Table 1-48 (Cont.) Dashboard Maintenance - Field Description

Field	Description
Show in Dashboard	Check this box to display a specific dashboard assigned to the user. **Note:** The system generates a notification on the authorization of any modification, addition, or deletion of the user.

In this screen, the filter conditions can be maintained for each DFI the user is mapped to.

3. Click **Clause Wizard**.

   The **Dashboard Condition** screen displays.

4. On the **Dashboard Condition** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-49 Dashboard Condition - Field Description

Field	Description
Column Name	Specify the column name for which want to maintain filter conditions. The adjoining list of values displays all valid columns available in the Dashboard.
Condition	Select the filter condition from the drop-down list: • **AND** • **OR** • **(** • **)** • **=** • **>** • **<** Click **Add** to add the selected conditions to the **Where Clause** field.

5. Click **Exit** to end the transaction.

1.31 Maintain Access Group Restrictions for Users

This topic explains systematic instructions to maintain the access group restrictions in the **User Maintenance** screen.

Through the **Access Group Restriction** screen, restrict the group code for the selected user ID.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

Login to the **User Maintenance** screen.

1. On the **User Maintenance** screen, click **Access Group Restriction**.

   The **Access Group Restriction** screen displays.

   Figure 1-36 Access Group Restriction

2. On the **Access Group Restriction** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-50 Access Group Restriction - Field Description

Field	Description
Access Group	Select one of the following options to indicate whether the access group is allowed or disallowed for the user: • **Allowed** • **Disallowed**
Access Group	Click **Search** and specify the access group which is allowed or disallowed for the user from the list of values. The list of access groups displays the valid access group codes (Open/Authorized).
Access Group Description	The system displays the description of the selected group code.

   The user can query or modify the account details only for those customers whose group code is allowed. If a user tries to query or modify the account of the customer whose group code is restricted, the system displays the error message **User is restricted to query or modify the account**.

3. Click **Exit** to end the transaction.

1.32 Maintain Customer Access Group

This topic explains systematic instructions to maintain customer access groups for retail and corporate customers.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **STDACGRP** in the text box, and click **Next**.

   The **Access Group Maintenance** screen displays.

Figure 1-37 Access Group Maintenance

2. On the **Access Group Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-51 Access Group Maintenance - Field Description

Field	Description
Access Group	Specify the access group code.
Access Group Description	Type a description for the access group.

3. Click **Exit** to end the transaction.

1.33 Maintain Masking Details

This topic explains systematic instructions to maintain masking details.

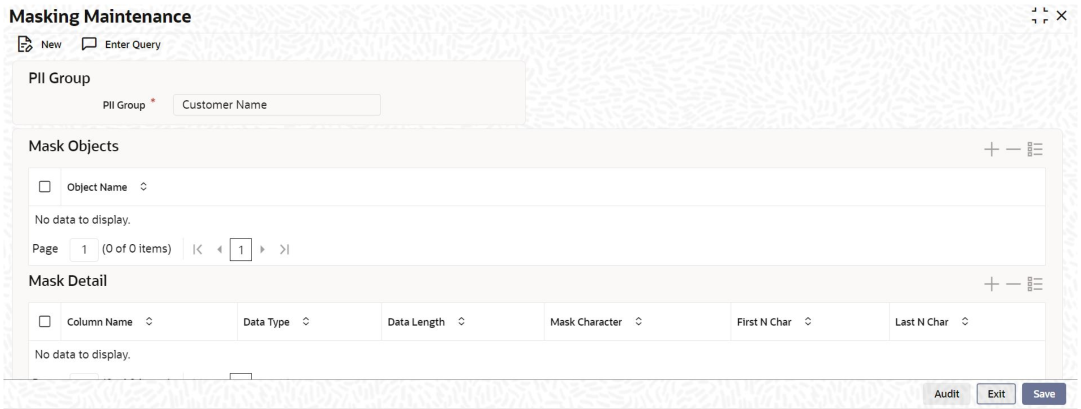
Through the **Masking Maintenance** screen, mask personally identifiable information based on the maintenance. The data for this screen is picked from the PII field's static data. However, the masking definitions defaulted on this screen can be modified.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDMASKD** in the text box, and click **Next**.

   The **Masking Maintenance** screen displays.

Figure 1-38 Masking Maintenance



2. On the **Masking Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-52 Masking Maintenance - Field Description

Field	Description
PII Group	Select the PII group from the drop-down list: • **Customer Name** • **Customer Contact Information** • **Demographic Information** • **Financial Information** • **Unique Identifiers** • **Other Information**
Object Name	The database objects **Table** or **View** that applies the masking policies. Select the object name from the list of values based on the chosen PII group.
Column Name	Select the name of the column from the list of values that displays the masked value.
Data Type	The data type is pre-populated based on the selected **Column Name**. Enter the new value, if required.
Data Length	Specify the length of the data. The value is pre-populated based on the selected **Column Name**. Enter the new value, if required.
Mask Character	Enter the character with which the information is masked. • If the **Data Type** is **Alphanumeric**, use alphabets and numerals. • If the **Data Type** is **Date**, leave the mask character blank. By default, the system displays the date **01-Jan-1970**. • If the **Data Type** is **Numeric**, maintain any number from 1-9.
First N Character	Enter the number of characters at the start of the string that has to be masked as per the chosen masking character.
Last N Character	Enter the number of characters at the end of the string that has to be masked as per the chosen masking character.

After maintaining masking details, when the user logs in to the application, the system checks **PII Allowed** value maintained in the **User Maintenance** screen against a user role and then displays the masked or unmasked data.

> **Note:**
>
> PII disallowed users cannot view tanked and change log records

3. Click **Exit** to end the transaction.

1.34 Maintain Forget Customer Personal Identifiable Information (PII)

This topic explains systematic instructions to maintain the **Forget Customer PII Maintenance** screen.

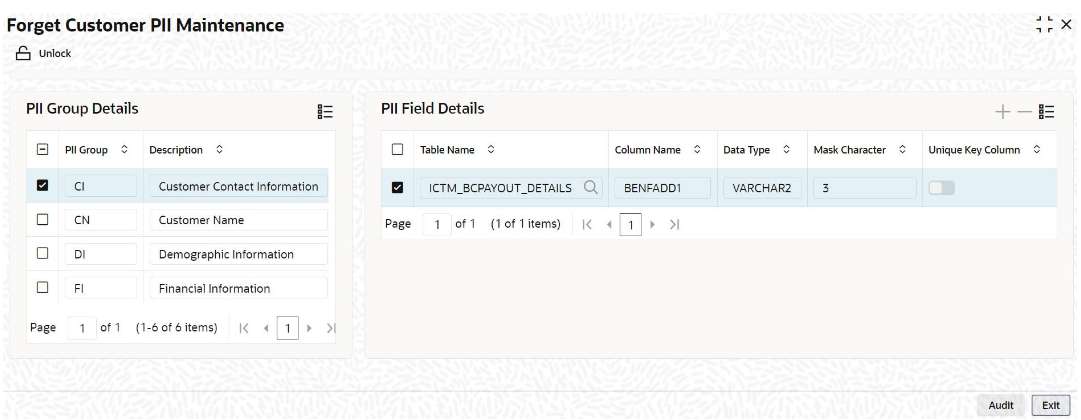
Through the **Forget Customer PII Maintenance** screen, maintain the customer or user PII that is to be forgotten by the system in Oracle FLEXCUBE Universal Banking.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDPIFRT** in the text box, and click **Next**.

   The **Forget Customer PII Maintenance** screen displays.

Figure 1-39 Forget Customer PII Maintenance



2. On the **Forget Customer PII Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-53 Forget Customer PII Maintenance - Field Description

Field	Description
PII Group	Select the PII group for which the data is to be forgotten.
Description	The system displays the description for each PII group.

Table 1-53 (Cont.) Forget Customer PII Maintenance - Field Description

Field	Description
Table Name	The name of the table in the database contains the customer information that the system has to be forgotten. Specify the table name from the list of values.
Column Name	The system displays the column name in the table.
Data Type	The system displays the data type of customer information.
Mask Character	Enter the character that is to be used to mask the customer information, so that it is not visible to anyone.
Unique Key Column	The **Unique Key Column** box is checked so that the user can easily select the unique key columns as indices for the table.

3. Click **Exit** to end the transaction.

1.35 Forget Customer Process

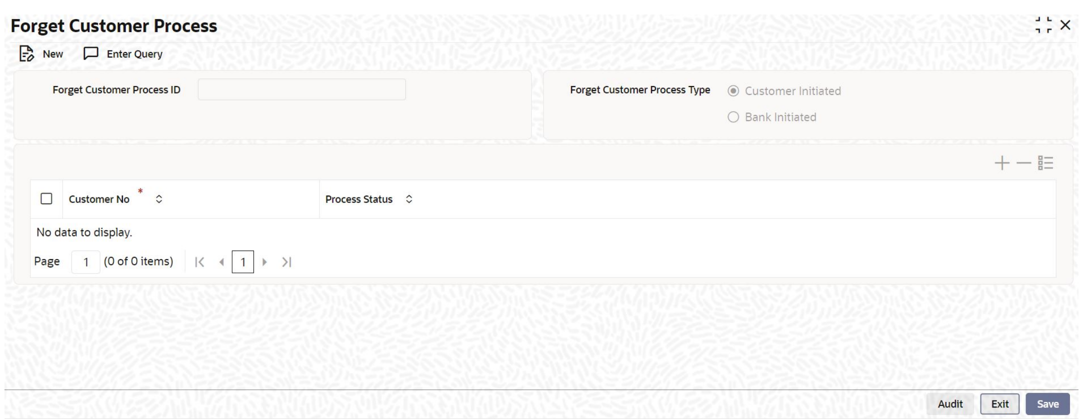
This topic explains systematic instructions to forget the specific customer.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **STDCSFRT** in the text box, and click **Next**.

   The **Forget Customer Process** screen displays.

Figure 1-40 Forget Customer Process



2. On the **Forget Customer Process** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-54 Forget Customer Process - Field Description

Field	Description
Forget Customer Process ID	This field displays the system-generated ID for processing the customer details. Alternatively, enter **Forget Customer Process ID** manually while searching for forgotten customers.
Forget Customer Process Type	Select the type of request for forgetting the customers from the following option: • **Customer Initiated** - Select this option, when the customer has requested for forgetting their details immediately. • **Bank Initiated** - Select this option to process the closed customers in a bulk, as per the bank's requirement. The process is a non-EOD batch process. For the **Customer Initiated** process, select the list of closed customers. But for the **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 list of values.
Process Status	This field displays the system-generated status. On submission of the request, the status is **U**, whereas once the process is authorized the status changes to **P**.

Once authorized, the data of the customer is updated with the respective masked value that is entered in the **Forget Customer PII Maintenance** screen.

> **Note:**
>
> After the customer is forgotten in the system, the customer's data is not available for any operations in any detail/maintenance and the summary screens.

3. Click **Exit** to end the transaction.

1.36 Log Access

This topic describes an overview of the different logs and their access.

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

Application Logs

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

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

The section of the **fcubs.properties** is shown below:

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

Back-end Logs

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

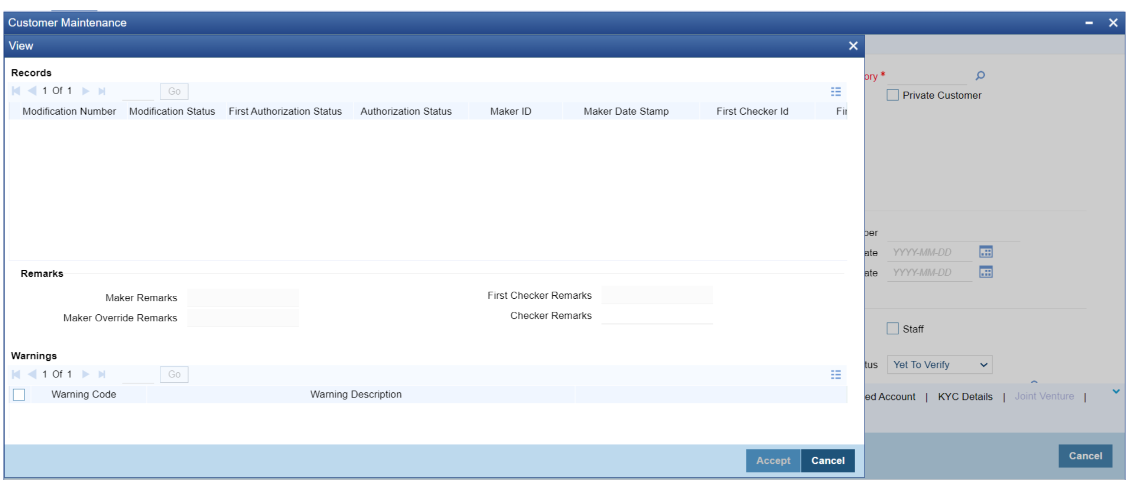
- Database directories are created with the back-end debug path by the data controller. Database directory has to be specified at the time of day 0 setup.
- The data controller can give module-wise access to the back-end logs to the user.

Audit Logs

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

In the **Customer Maintenance** screen, click **Change log** to view the modification details as follows:

Figure 1-41 Customer Maintenance - Change Log



Purging Logs

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

1.37 Maintain Department Details

This topic explains systematic instructions to maintain department details.

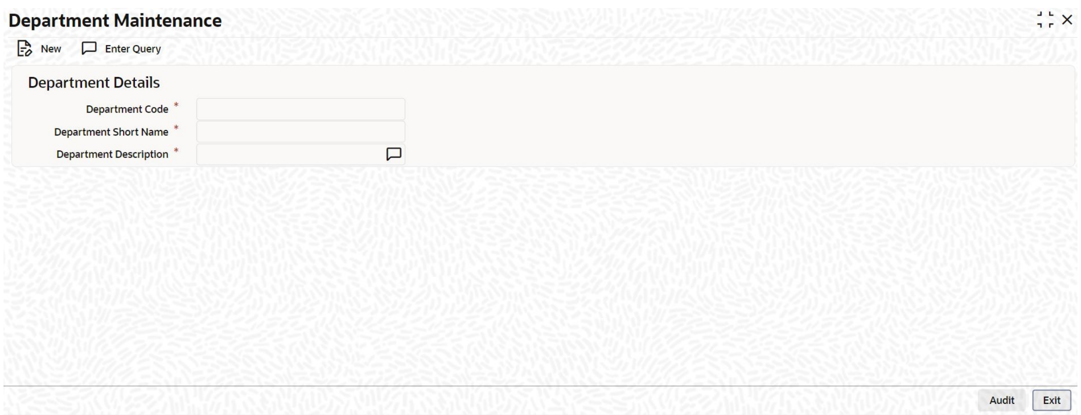
Through the **Department Maintenance** screen, Oracle FLEXCUBE Universal Banking allows capturing department's details. However, only privileged administrative users can edit the department details.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDDPTMT** in the text box, and click **Next**.

   The **Department Maintenance** screen displays.

   Figure 1-42 Department Maintenance

2. On the **Department Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-55 Department Maintenance - Field Description

Field	Description
Department Code	Specify the department code of a maximum of 3 alphanumeric characters.
Department Short Name	Specify the department's short name of a maximum of 10 alphanumeric characters.
Department Description	Specify the department description of a maximum of 225 alphanumeric characters.

3. Click **Exit** to end the transaction.

1.38 Maintain Process Codes

This topic explains systematic instructions to maintain process codes.

> **Note:**
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDPRCDE** in the text box, and click **Next**.

   The **Process Definition** screen displays.

   Figure 1-43 Process Definition

2. On the **Process Definition** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-56 Process Definition - Field Description

Field	Description
Process Code	Specify a unique code for the process.
Description	Type a description of the process.

3. Click **Save** to save all entered details.
4. Click **Exit** to end the transaction.

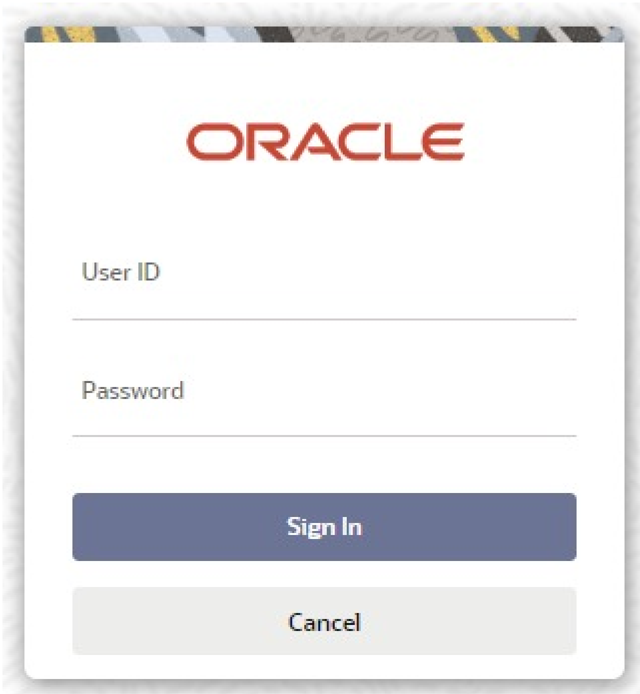
1.39 Single Sign On Enabled Environment

This topic describes an overview of the Single Sign On enabled environment.

If the user has opted for the **SSO Enabled** option at the bank level, the user can log in from an LDAP (Oracle Internet Directory) external system into Oracle FLEXCUBE Universal Banking through the screen shown below.

Figure 1-44 Single Sign On Login Page

Figure 1-45 Oracle FLEXCUBE Universal Banking Login Page



After authentication and authorization of the user is carried out by the LDAP (Oracle Internet Directory) successfully, a request is forwarded to gain access to Oracle FLEXCUBE Universal Banking. On clicking **Submit**, the user can directly get into Oracle FLEXCUBE Universal Banking without specifying the Oracle FLEXCUBE Universal Banking user ID and password.

1.40 Maintain Entities

This topic explains systematic instructions to maintain entities.

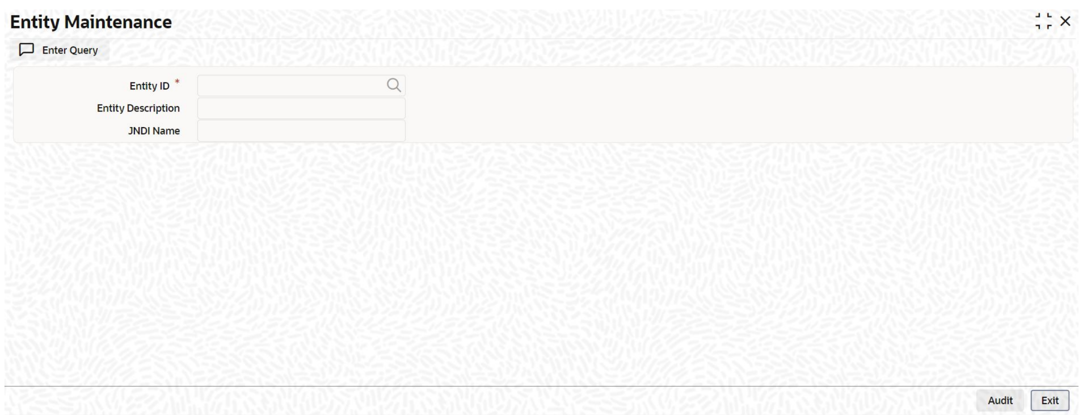
The **Entity Maintenance** screen is used for maintaining or modifying the entities and Java Naming and Directory Interface (JNDI).

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDENTDT** in the text box, and click **Next**.

   The **Entity Maintenance** screen displays.

   Figure 1-46 Entity Maintenance



2. On the **Entity Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-57 Entity Maintenance - Field Description

Field	Description
Entity ID	Click **Search** and specify the **Entity ID**.
Entity Description	The system displays the description of the entity.
JNDI Name	Specify the **JNDI Name**.

3. Click **Exit** to end the transaction.

2 Associated Functions

The topic contains the following subtopics:

- #unique_110
- #unique_111
- #unique_112
- #unique_113
- #unique_114
- #unique_115
- #unique_116
- #unique_117
- #unique_118

- Maintain Clear User Screen
  This topic explains systematic instructions to maintain the **Clear User** screen.
- Change the System Time Level
  This topic explains systematic instructions to change the system time level.
- Define Language Codes
  This topic explains systematic instructions to define language codes.
- Change Branch of Operation
  This topic describes the process of changing the branch of operation for a specific user.
- Change User Password
  This topic explains systematic instructions to change the user password.
- Maintain SSO Parameters
  This topic explains systematic instructions to maintain SSO parameters.
- Process Transaction Status Control Maintenance
  This topic explains systematic instructions to process transaction status control maintenance.
- Configure Customized Hot Keys
  This topic explains systematic instructions to configure customized hot keys.
- Process User Activities
  This topic explains systematic instructions to process user activities.

2.1 Maintain Clear User Screen

This topic explains systematic instructions to maintain the **Clear User** screen.

When a user logs into the system, the system maintains a record of the user with the date and time of login. After logging out, this record gets deleted. When a user who is logged into the system is forced out, the ID of the user 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** screen.

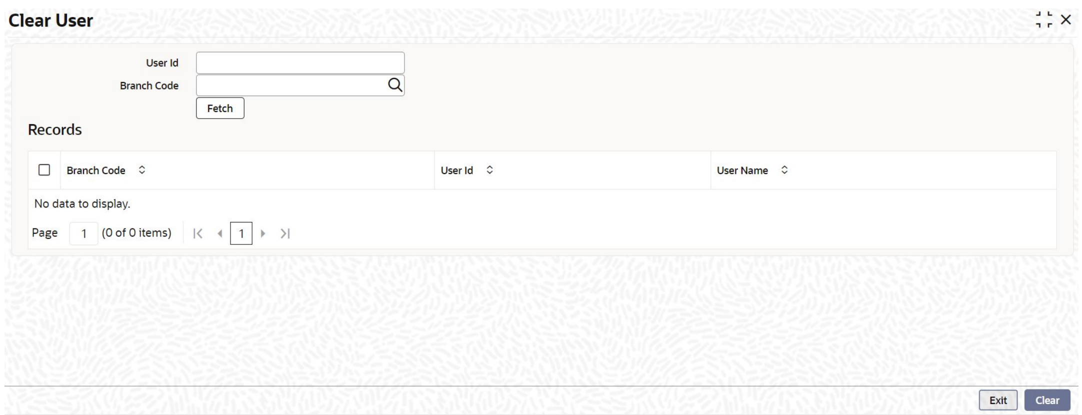
Note:

The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **CLRU** in the text box, and click **Next**.

   The **Clear User** screen displays.

Figure 2-1 Clear User



2. On **Clear User** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 2-1 Clear User - Field Description

Field	Description
User ID	Specify the **User ID**.
Branch Code	Click **Search** and specify the branch code from the list of values.

3. Click **Fetch**.

   The system lists the following details of the users who have logged into the application:

   - **Branch Code**
   - **User ID**
   - **User Name**
4. Check the box against the relevant user record and click **Clear** to force log out a user.

   The system displays a message to confirm the clear operation.
5. Check the box against the header row which selects all the users on the page and click **Clear** to force log out all the users.

   The selected users are logged off from the application.
6. Click **Exit** to end the transaction.

2.2 Change the System Time Level

This topic explains systematic instructions to change the system time level.

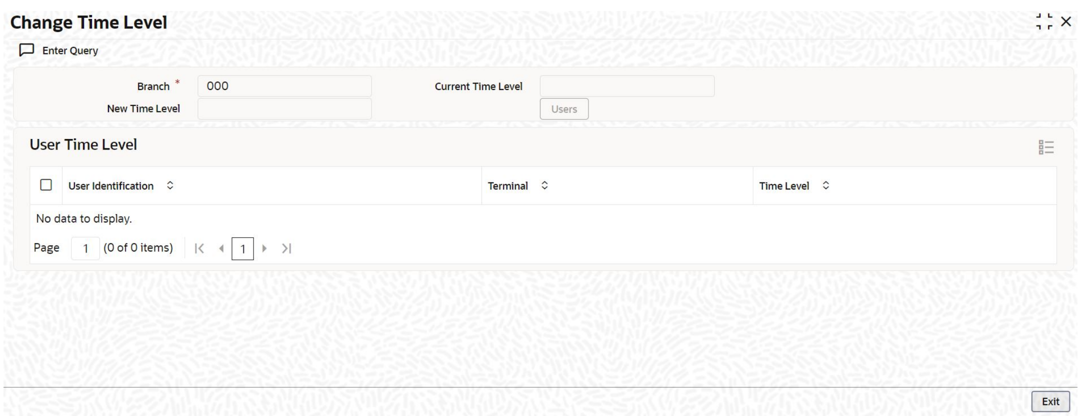
The time level is allotted at two levels that are at the system (branch) level and the user level. For a user to be able to log in, the time level for the user profile should be greater than or equal to that of the system. The time level can be between zero to nine. Through the **Change Time Level** screen, the user can change the time level of the branch.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDCHNTL** in the text box, and click **Next**.

   The **Change Time Level** screen displays.

   Figure 2-2 Change Time Level

2. On the **Change Time Level** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 2-2 Change Time Level - Field Description

Field	Description
Branch	Specify the **Branch**.
New Time Level	Specify the **New Time Level**.
Current Time Level	Specify the **Current Time Level**.
Users	Click **Users** to view the details of users who are currently logged in.

3. On the **Change Time Level** screen, click **Users**.

   The system displays a list of all users who are currently logged in and their respective time levels.

   - **User Identification**
   - **Terminal**

- **Time Level**

  When the **Time Level** of the branch is changed, the system validates and displays a message if the **Time Level** of any of the users is lesser than that of the newly changed value. These users can continue to log in and work on the system till they log off. When users try to log in back, the system validates and only allows such user accesses whose time levels are greater than that of the system.

4. Click **Exit** to end the transaction.

2.3 Define Language Codes

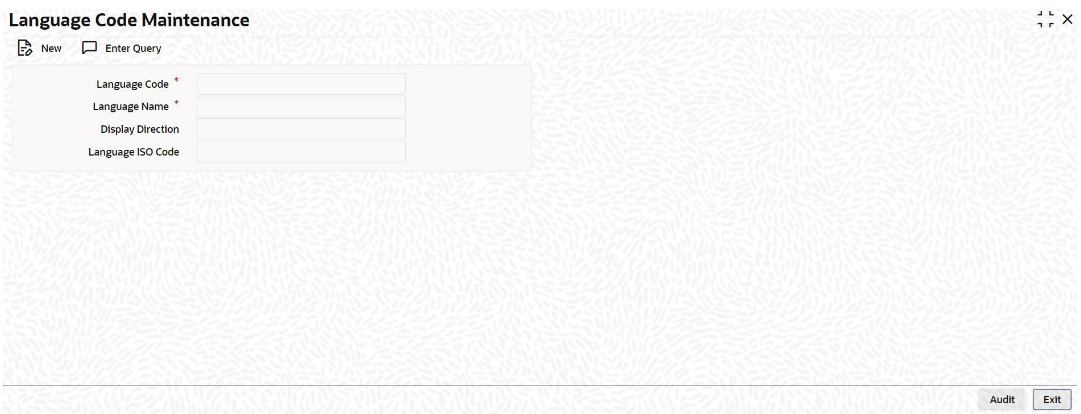
This topic explains systematic instructions to define language codes.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDLNGCE** in the text box, and click **Next**.

   The **Language Code Maintenance** screen displays.

Figure 2-3 Language Code Maintenance



2. On the **Language Code Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 2-3 Language Code Maintenance - Field Description

Field	Description
Language Code	Every language that is supported by the system is identified by a **Language Code**. In Oracle FLEXCUBE Universal Banking, this code is a three-character alphanumeric code. Specify the language code. For example, ENG for the English language
Language Name	Specify the language name for the specified **Language Code**.
Display Direction	Specify the direction in which the language is to be displayed.
Language ISO Code	Specify the language ISO code.

3. Click **Exit** to end the transaction.

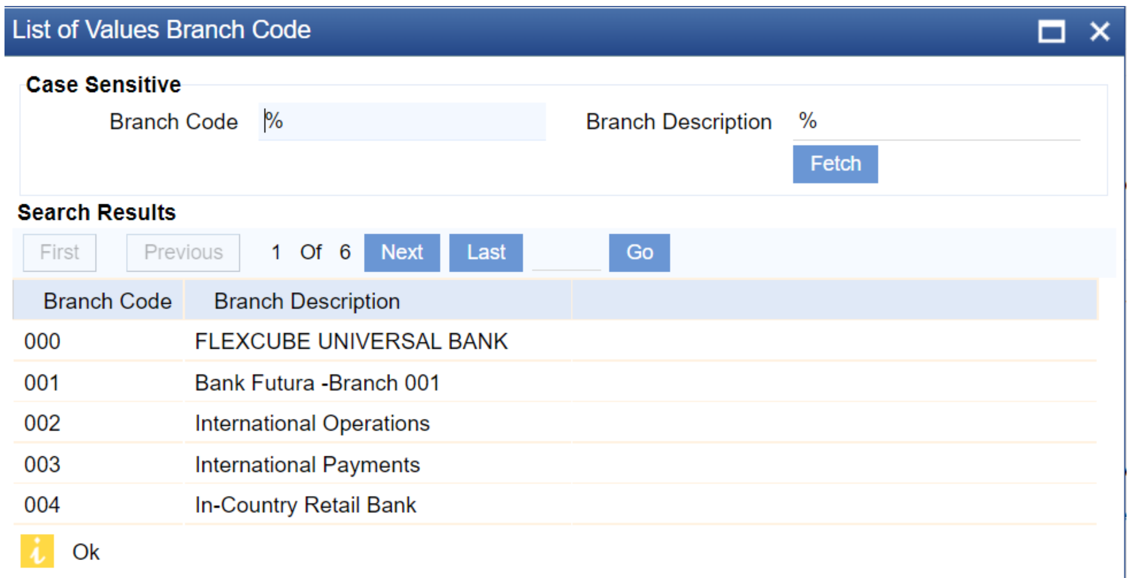
2.4 Change Branch of Operation

This topic describes the process of changing the branch of operation for a specific user.

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

For example, the screen shown below shows the list of branches:

Figure 2-4 List of Values Branch Code



2.5 Change User Password

This topic explains systematic instructions to change the user password.

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

1. On **Homescreen**, navigate to the **User** and click **Change Password**.

   The **Change Password** screen displays.

Figure 2-5 Change Password

2. On **Change Password** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 2-4 Change Password - Field Description

Field	Description
Enter Old Password	Specify the old password which has to be changed.
Enter New Password	Type the new password.
Confirm New Password	Type the new password again, the same as entered in the **Enter new password** field.

3. Click **Save** to save the new password.
4. Click **Cancel** to end the transaction.

2.6 Maintain SSO Parameters

This topic explains systematic instructions to maintain SSO parameters.

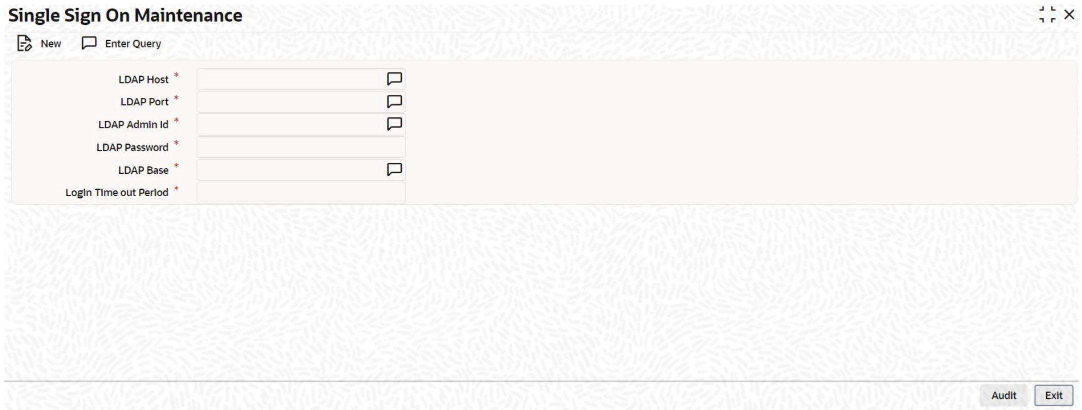
LDAP is an external directory system that stores the details regarding user ids and passwords. Once SSO has been enabled for the bank, the SSO parameters need to be maintained. This can be done using the **Single Sign On Maintenance** screen.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDSOPRM** in the text box, and click **Next**.

   The **Single Sign On Maintenance** screen displays.

Figure 2-6 Single Sign On Maintenance



2. On the **Single Sign On Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 2-5 Single Sign On Maintenance - Field Description

Field	Description
LDAP Host	Type the machine or server name where LDAP (Oracle Internet Directory) is installed.
LDAP Port	Specify the network port number where the LDAP (Oracle Internet Directory) listens to the server.
LDAP Admin id	Specify the admin user ID of the LDAP (Oracle Internet Directory).
LDAP Password	Specify the password for the LDAP admin user which is provided during installation.
LDAP Base	Specify the directory information tree (DIT) structure under which the data is to be stored, which is provided during installation. This is used while validating the user present in the LDAP (Oracle Internet Directory).
Login Time Out Period	Specify the allowable idle time (in seconds) that a user can spend without performing any activity, after logging in to the system.

3. Click **Exit** to end the transaction.

2.7 Process Transaction Status Control Maintenance

This topic explains systematic instructions to process transaction status control maintenance.

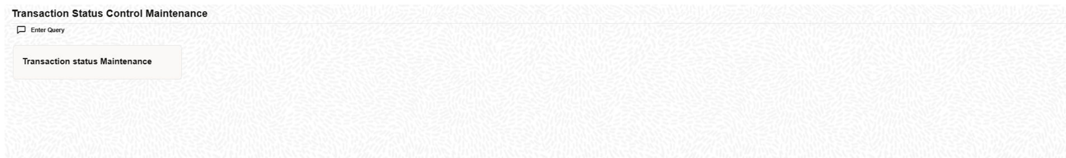
The **Transaction Status Control Maintenance** screen allows the user to define the various actions depending on the status of the contract.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDTXNST** in the text box, and click **Next**.

   The **Transaction Status Control Maintenance** screen displays.

Figure 2-7 Transaction Status Control Maintenance



2. On the **Transaction Status Control Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 2-6 Transaction Status Control Maintenance - Field Description

Field	Description
Authorization	For each transaction status, the record status **A (Authorized)** or **U (Unauthorized)**, could also affect the actions.
Actions	Check the box against a transaction record to select the actions allowed for that transaction. The following are the actions that are allowed on a record: • **New** • **Copy** • **Delete** • **Closed** • **Unlock** • **Reopen** • **Print** • **Authorize** • **Reverse** • **Rollover** • **Confirm** • **Liquidate** • **Hold** • **Template** • **View** • **Generate**
Transaction Status Maintenance	Some of the statuses that a contract could have are as follows: • **Y-Irrevocable** • **A-Authorized** • **U-Unauthorized** • **V-Reversed** • **L-Liquidated** • **S-Closed** • **H-Hold** • **K-Cancelled** • **N-NON-CUMULATIVE** • **T-TIME** • **O-OUR**

3. Click **Exit** to end the transaction.

2.8 Configure Customized Hot Keys

This topic explains systematic instructions to configure customized hot keys.

Oracle FLEXCUBE Universal Banking allows configuring Hotkeys or Shortcut keys for function ids, using which the function id screens can be launched without typing the function IDs. For this, map each function id to a hotkey using the **Hot Keys Maintenance** screen.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMDHOTKY** in the text box, and click **Next**.

   The **Hot Keys Maintenance** screen displays.

   Figure 2-8 Hot Key Maintenance

2. On the **Hot Key Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 2-7 Hot Key Maintenance - Field Description

Field	Description
User ID	The system displays the ID of the user who has logged in.
Ctrl+1, **Ctrl+2**, **Ctrl+3**, **Ctrl+4**, **Ctrl+5**, **Ctrl+6**, **Ctrl+7**, **Ctrl+8**, and **Ctrl+9**	The user can map a function ID against each hotkey. Select the function ID to be mapped against the hotkey from the adjoining list of values.

3. Click **Exit** to end the transaction.

2.9 Process User Activities

This topic explains systematic instructions to process user activities.

Through the **User Activity** screen, view a log of activities of Oracle FLEXCUBE Universal Banking users. The user activities can be viewed only through the Oracle FLEXCUBE

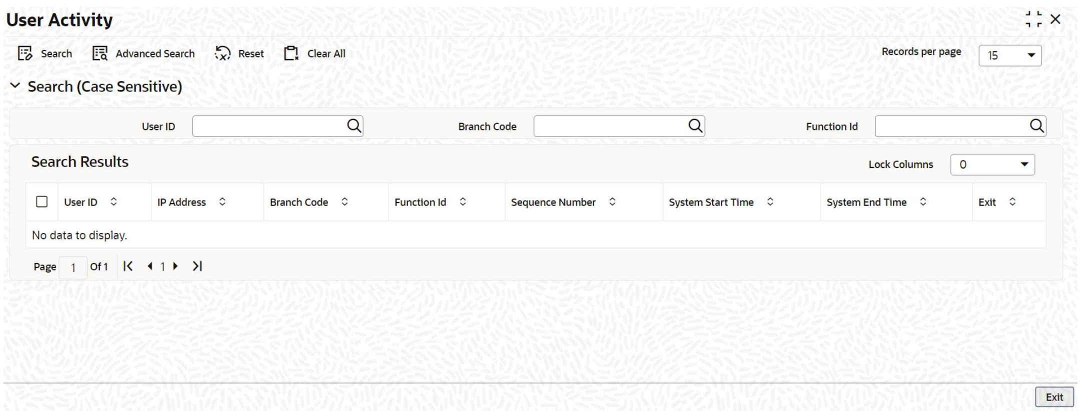
Universal Banking host system. This screen is not available for viewing in the branch installations.

> **Note:**
>
> The fields which are marked in asterisk are mandatory.

1. On **Homescreen**, type **SMSUSRAC** in the text box, and click **Next**.

   The **User Activity** screen displays.

   Figure 2-9 User Activity

2. On the **User Activity** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 2-8 User Activity - Field Description

Field	Description
User ID	Click **Search** and specify the **User ID** from the list of values.
Branch Code	Click **Search** and specify the **Branch Code** from the list of values.
Function ID	Click **Search** and specify the **Function ID** from the list of values.

3. Click **Search** after specifying the search parameters.

   The system identifies all records satisfying the specified criteria and displays the following details for each one of them:

   - **User ID**
   - **IP Address**
   - **Branch Code**
   - **Function ID**
   - **Sequence Number**
   - **System Start Time**
   - **System End Time**
   - **Exit**

4. Click **Exit** to end the transaction.

3

Error Codes and Messages

This topic contains error codes and messages.

Table 3-1 Error Codes

Error Code	Message
SM-00001	Unauthorized installation. Contact Oracle Financial Services representative
SM-00002	Licensed number of users exceeded. Try again after a while
SM-00003	Guest ids can sign on only via change branch function
SM-00004	Invalid login
SM-00005	User already logged in
SM-00006	User status is disabled. Please contact your system administrator.
SM-00007	User status on hold. Contact your system administrator
SM-00008	Your time level does not permit you to log in. Contact your branch system administrator
SM-00009	Please change password now!
SM-00010	Password file missing or corrupt
SM-00011	Contact your system administrator. Oracle built in problem
SM-00012	SMTBS_passwords table missing or entries not found
SM-00014	Password due to expire on $1
SM-00015	User profile expired. Contact branch system administrator
SM-00016	Your time level does not permit you to launch this function
SM-00030	This function is currently not available for execution
SM-00031	This form $1 is not available. Contact your branch system administrator
SM-00032	The time level in the branch has changed. Your time level does not permit you to execute any functions
SM-00033	The number of users currently executing functions in this module has exceeded the license limit.
SM-00034	This function is not available for customer access
SM-00035	This function is not available for staff access
SM-00036	Function ID is not correct. Enter function ID again
SM-00037	Main menu and sub menu descriptions cannot be same
SM-00040	Wrong password. Enter password again
SM-00041	The new and confirmed passwords do not match. Enter passwords again
SM-00042	The password entered is restricted. Try another password
SM-00043	The password entered has already been used. Try another password
SM-00044	Length of password is less than $1 characters
SM-00045	Length of password is more than $1 characters
SM-00046	The password string contains special characters that are not allowed. Retype password
SM-00050	Control clerks passwords do not match. Retype passwords again

Table 3-1 (Cont.) Error Codes

Error Code	Message
SM-00060	There are users currently logged in with a lesser time level. Do you want to change?
SM-00070	You are currently executing some functions. Exit from those functions and try again
SM-00080	User ID already exists.
SM-00081	Negative amount not allowed
SM-00082	Start cannot be before today
SM-00083	End date cannot be before start date
SM-00084	Start date cannot be null
SM-00085	User profile saved
SM-00086	Could not save user profile
SM-00087	User profile deleted
SM-00088	Could not delete user profile
SM-00089	Mandatory or not null fields are missing
SM-00090	Role ID already exists
SM-00091	Users attached to the role. Cannot delete
SM-00092	Role deleted
SM-00093	Invalid role ID
SM-00094	Currency code not defined
SM-00095	Branch code not defined
SM-00096	Customer no not defined
SM-00097	Customer category not defined
SM-00098	Role profile saved
SM-00100	Cannot delete the role. There are users attached to this role.
SM-00101	Cannot delete function. There are users attached to this function.
SM-00102	Cannot modify function. There are users attached to this function.
SM-00103	Do you want to delete the user?
SM-00104	Do you want to delete the role?
SM-00105	Cannot delete role. Users attached to role.
SM-00110	Site code length cannot be less than 4 characters
SM-00111	Cumulative invalid logins - number should be greater than 5 and less than 100
SM-00112	Successive invalid logins - number should be greater than 2 and less than 6
SM-00113	Password prevent reuse value should be between 1 and 5
SM-00114	Minimum password length should be between 6 and 10
SM-00115	Maximum password length should be between 9 and 12
SM-00116	Graph not found. Contact your branch administrator
SM-00117	Password change after message - no of days should be greater than 15 and less than 180
SM-00118	Archival period should be greater than 0
SM-00119	Enter the role description
SM-00120	Cannot delete/modify role of other branch
SM-00121	Idle time before sign off should be between 30 and 600

Table 3-1 (Cont.) Error Codes

Error Code	Message
SM-00122	Password expiry message - between 0 and 5
SM-00123	Enter a valid module ID
SM-00125	Min password length should be less than Max password length
SM-00126	Override idle time should be greater than 10
SM-00130	User access to $1 $2 denied
SM-00131	Duplicate values encountered
SM-00140	Guest ID not defined in branch $1
SM-00150	Maximum value encountered
SM-00160	Users attached to the language code. Cannot delete
SM-00161	Language code already exists. Try another one
SM-00170	Reserved word cannot be used
SM-00500	Mandatory values missing or null
SM-00501	Activation key contains irrelevant characters. Wrong activation key
SM-00502	Installation with this key already done. Cannot duplicate
SM-00503	Installation not done. Contact BSA or Oracle Financial Services representative
SM-00510	No branches defined for user
SM-00520	Could not delete function. Role attached
SM-00530	Could not delete function. Users attached
SM-00171	Max password Length cannot be null
SM-00172	Min password Length cannot be null
SM-00173	Min password alphabets length cannot be greater than Max password alphabets length
SM-00174	Min password alphabets length cannot be greater than Max password length
SM-00175	Min password alphabets length + Max password numeric length cannot be greater than Max password Length
SM-00176	Min password alphabets length + Min password numeric length cannot be greater than Min password Length
SM-00177	Min password numeric length cannot be greater than Max password numeric length
SM-00178	Min password numeric length cannot be greater than Max password length
SM-00179	Min password numeric length + Max password alphabets length cannot be greater than Max password Length
SM-00180	Max password alphabets length cannot be lesser than Min password alphabets length
SM-00181	Max password alphabets length cannot be greater than Max password length
SM-00183	Max password numeric length cannot be greater than Max password length
SM-00184	Max password numeric length cannot be lesser than Min password numeric length
SM-00185	Password cannot contain more than $1 consecutive characters
SM-00186	Password should contain atleast $1 Numeric characters
SM-00187	Password should contain atleast $1 Alphabetic characters

Table 3-1 (Cont.) Error Codes

Error Code	Message
SM-00188	Min password alphabetic length cannot be lesser than Min password length
SM-00189	Min password numeric length cannot be Greater than Min password length
SM-00200	Maximum No of Consecutive Characters should be Greater than 0
SM-00201	The transaction amount exceeds the maximum input amount for the user
SM-00202	The User is UnAuthorized
SM-00203	The Last Login date was - $1
SM-00204	Failed to validate transaction limits for the User
SM-00205	Limits Id already exists
SM-00206	Dormancy Days Should be Greater than 0
SM-00207	Warning Screen Text cannot be Null
SM-00208	Role Limits attached to the User are Unauthorized
SM-00209	Restriction type cannot be null
SM-00251	Value for legal notice is needed.
SM-00252	Value for legal notice is not needed.
SM-00300	Values for user limits are not applicable for the chosen transaction limit
SM-00301	Values for role limits are not applicable for the chosen transaction limit
SM-00500	Mandatory values missing or null
SM-00501	Activation key contains irrelevant characters. Wrong activation key
SM-00502	Installation with this key already done. Cannot duplicate
SM-00503	Installation not done. Contact BSA or i-flex representative
SM-00510	No branches defined for user
SM-00520	Could not delete function. Role attached
SM-00530	Could not delete function. Users attached
SM-00540	Could not delete function
SM-00550	Function successfully saved
SM-00560	Function not implemented
SM-00610	No functions defined for the user
SM-00612	You are not logged on
SM-00900	Process completed
SM-00901	Please select user ids to Enable
SM-00998	Password should be alphanumeric
SM-00999	First and last letter cannot be numeric
SM-01000	Invalid password. Bad sign on
SM-01001	Invalid name. Bad sign on
SM-01002	Successive invalid logins. Forced disable
SM-01003	Cumulative invalid logins. Forced disable
SM-01004	Password expired. Password changed
SM-01005	User initiated password change.
SM-01006	Forced password change
SM-01007	Status enabled
SM-01008	Status put on hold

Table 3-1 (Cont.) Error Codes

Error Code	Message
SM-01009	No of licensed users for modules exceeded
SM-01010	No of licensed users for bank exceeded
SM-01011	Wrong activation key entered
SM-01012	Duplicate terminal ID encountered.
SM-01013	SMS user profile cleared
SM-01014	Restricted access program invoked by control clerks
SM-01015	User profile definition form invoked
SM-01016	Role profile definition form invoked
SM-01017	SMS bank parameters definition form invoked
SM-01018	Wrong control clerk password entered
SM-01019	Function id is not available for current module
SM-01099	Your Current amount decimal separator is not $1'. Please ask IT to change machine oracle settings.'
SM-01100	Entries in SMS bank parameters missing
SM-01101	Could not get today s date for the head office
SM-01102	Bank code not maintained in branch table
SM-01103	Local currency not maintained in bank table
SM-01104	User already signed on
SM-01105	User $1 in branch $2 changed branch to branch $3 as user $4
SM-01205	Both Passwords expired. Change Password Now
SM-01206	Password1 expired. Change Password Now
SM-01207	Password2 expired. Change Password Now
SM-0200	Cannot restrict current password
SM-02000	Internal error: exception raised in $1
SM-02001	Enter from date
SM-02002	Enter to date
SM-02003	From date cannot be later than to date
SM-02004	Enter from time
SM-02005	Enter to time
SM-02006	From time cannot be later than to time
SM-02007	Select all users to use purge option
SM-02008	Role ID should be entered
SM-02009	User ID should be entered
SM-05000	Installation successful
SM-06001	User does not exist
SM-06500	Document Long Description is Mandatory
SM-0999	You do not have access to this function
SM-09999	Internal error: unhandled exception raised
SM-10000	Do you want to reset cumulative invalid logins to 0?
SM-10001	Head office branch code is not valid
SM-10002	Language code must be 3 characters
SM-10003	Branch is closed
SM-10004	Number of invalid logins since last logout = $1

Table 3-1 (Cont.) Error Codes

Error Code	Message
SM-10005	This Function has been linked to a role
SM-3001	User does not have rights
SM-3002	Incorrect User ID or password
SM-555555	Sign off allowed only from home branch
SM-555556	Logout allowed only from home branch
SM-555557	Triggers in the database are disabled. Please contact System Administrator.
SM-66666	Amount exceeds users authorization limit
SM-66666	Amount exceeds users authorization limit
SM-700007	Terminal ID should be Four Characters in Length
SM-7001	Invalid User Id or Password
SM-7002	User does not have rights
SM-7003	Invalid Login
SM-7004	User already logged in
SM-7005	User Status is Disabled
SM-7006	User Status on Hold
SM-7007	Your Time level does not permit you to Login
SM-7008	Please change Password now!
SM-7010	Password file missing or corrupt
SM-7011	Oracle built in problem
SM-7012	Password due to expire on $1
SM-7013	User Profile expired
SM-7014	Wrong Password
SM-7015	Enter Password again
SM-7016	The New and Confirmed Passwords do not match
SM-7017	Enter Passwords again
SM-7018	The Password entered is Restricted. Try another Password
SM-7019	The Password entered has already been used. Try another Password
SM-7020	Length of Password is less than $1 characters
SM-7021	Length of Password is more than $1 characters
SM-7022	The Password string contains special characters that are not allowed. Retype Password
SM-7023	Password cannot contain more than $1 consecutive identical characters
SM-7024	You cannot change Password today
SM-7025	The password should be mix of alphabetic and numeric characters
SM-7026	Control Clerks Passwords do not match. Retype Passwords again
SM-7027	There are Users currently logged in with a lesser time level. Do you want to change?
SM-7028	User Id already exists.
SM-7029	Cumulative Invalid Logins - Number should be greater than 5 and less than 100
SM-7031	Password prevent reuse value should be between 1 and 5 Minimum
SM-7032	Password length should be between 6 and 10
SM-7033	Maximum Password Length should be between 9 and 12

Table 3-1 (Cont.) Error Codes

Error Code	Message
SM-7034	Password expiry message - between 0 and 5
SM-7035	Password change after message - no of days should be greater than 15 and less than 180
SM-7036	User Access to $1 $2 denied
SM-7037	Consecutive Password Characters should be greater than 1
SM-7038	The User is un-authorized
SM-7039	The Last Login date was - $1
SM-7040	Password Changed Successfully
SM-7041	Invalid Password. Bad Sign On
SM-7042	Invalid Name. Bad Sign On
SM-7043	Successive Invalid Logins
SM-7044	Forced Disable Cumulative Invalid Logins
SM-7045	Forced Disable Password expired.
SM-7046	Password changed
SM-7047	User initiated Password change
SM-7048	Forced password change
SM-7049	Status Enabled
SM-7050	Status put on
SM-7051	Hold User already Signed on
SM-7052	Do you want to reset Cumulative Invalid Logins to 0 ?
SM-7053	Number of Invalid Logins Since Last Logout = $1
SM-7054	User Password Changed Successfully
SM-7055	Change password now!!
SM-7056	Terminal Id not set
SM-7057	Message Digest not matched
SM-7058	User Not Logged In. Please login again
SM-7059	Fast Path Cannot Contain Special Characters
SM-7060	Currency sold and Currency bought cannot be same.
SM-7070	Branch date is ahead of host date, cannot proceed
SM-77777	User does not have rights to authorize the override
SM-AUTH01	The transaction amount exceeds the maximum authorization amount for the User
SM-BRN01	Not a Valid user for Branch
SM-BRN02	Password for Branch User cannot be null
SM-BVALUE1	$1 Back value days cannot be null
SM-C0050	Invalid Branch Code
SM-C0051	Function ID Already attached
SM-C0052	Branch or Function id should not be null
SM-CHBRLO	Change Branch to Home Branch In-Order to Logoff.
SM-CHBRSO	Change Branch to Home Branch In-Order to Signoff.
SM-CLBRN01	Branch User Profile Updated at Host
SM-CLS001	Users attached to Role. Close?
SM-CV001	Sequence no cannot be null

Table 3-1 (Cont.) Error Codes

Error Code	Message
SM-CV002	Sequence no is a numeric field
SM-CV003	Group ID cannot be null
SM-CV004	Module code cannot be null
SM-CV005	Source code cannot be null
SM-CV006	Template ID cannot be null
SM-CV007	Duplicate broker ID
SM-CV008	Liquidation code cannot be null
SM-CV009	Duplicate details in record not allowed
SM-CV010	Basis amount to cannot be null
SM-CV011	Floor basis amount has to be less than basis amount to
SM-CV012	Rate cannot be null for percentage type
SM-CV013	Min amount cannot be more than floor charge for percentage type
SM-CV014	Max amount cannot be less than floor charge for percentage type
SM-CV015	Flat amount cannot be null for flat amount type
SM-CV016	Invalid rate, rate is too high
SM-CV017	Floor basis amount cannot be null
SM-CV018	Floor charge cannot be null
SM-CV019	Basis amount to cannot be less than basis amount from
SM-CV020	Duplicate rule code
SM-CV021	Minimum amount must be less than maximum amount
SM-CV022	Maximum amount must be more than minimum amount
SM-CV023	Rule cannot be null
SM-CV024	Group already exists
SM-CV025	The record is already closed
SM-CV026	Intermediate table has to be entered
SM-CV027	Upload table has to be entered
SM-CV028	Cube table has to be entered
SM-CV029	Source field cannot be null
SM-CV030	Destination field cannot be null
SM-CV031	Destination field already maintained
SM-CV032	Group ID already maintained
SM-CV033	Template ID already maintained for this group
SM-CV034	Sequence no already maintained for this group
SM-CV035	Invalid column name
SM-DATE1	Failed to convert date format
SM-DEMO01	Oracle FLEXCUBE not properly installed, exiting!
SM-DEMO02	Demo version will expire after $1 day(s)
SM-DEMO03	Welcome to Oracle FLEXCUBE
SM-DEMO04	Only one user is allowed to login in demo version of Oracle FLEXCUBE, exiting!
SM-DEMO05	Insufficient parameters to launch Oracle FLEXCUBE, exiting!
SM-DEMO06	Oracle FLEXCUBE demo version does not allow this function
SM-DEMO07	Demo version expired, please contact i-flex!!!

Table 3-1 (Cont.) Error Codes

Error Code	Message
SM-DEMO08	Demo version allows only $1 contracts.
SM-DEMO09	Demo version expires today
SM-DTCH01	Users are running functions.
SM-DTCH02	AEOD dates not maintained
SM-DTCH03	Wrong branch status to run this form
SM-EFIN01	Users in transactions input
SM-EXTUS	Oracle FLEXCUBE has been launched from another application. Sign oP disallowed. Please exit
SM-FND01	Menu items not populated
SM-PRD02	Deletion not allowed as periods beyond $1 exist for the financial cycle
SM-PRD03	The period end date has to be the last day of a month
SM-PWC01	Password same as previously used password
SM-QRY-01	The form is in the enter-query mode. Please click on the exit toolbar button or exit menu item to get to the normal mode.
SM-QRY01	The form is in the enter-query mode. Please click on the exit toolbar button or exit menu item to get to the normal mode.