

Oracle Banking Security Management System User Guide

Oracle Banking Branch

Release 14.5.0.9.0

Part Number F85404-01

August 2023

Oracle Banking Security Management System User Guide

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

<https://www.oracle.com/industries/financial-services/>

Copyright © 2018, 2023, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

ORACLE®

Contents

1 Preface	1
1.1 Purpose	1
1.2 Audience	1
1.3 Document Accessibility	1
1.4 Screenshot Disclaimer	1
1.5 Acronyms and Abbreviations	1
1.6 List of Topics	1
1.7 Basic Actions	2
1.8 Symbols and Icons	2
1.9 Related Resources	4
2 Welcome to Security Management	5
2.1 Role	6
2.1.1 View Role	6
2.1.2 Create Role	7
2.2 User	9
2.2.1 View User	9
2.2.2 Create User	11
2.2.3 Clear User	14
2.3 Functional Activity	16
3 Error Codes and Messages	19
4 Definitions	22
5 Index	23

1. Preface

1.1 Purpose

This user guide provides an overview to the module and takes you through the various steps involved setting up and using the security features that Oracle offers.

1.2 Audience

This document is intended for Oracle Implementers, SMS Administrator for the Bank, SMS Administrator for the Branch, and an Oracle user.

1.3 Document Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/us/corporate/accessibility/index.html>.

1.4 Screenshot Disclaimer

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

1.5 Acronyms and Abbreviations

The following are the acronyms and abbreviations used in the guide:

Table 1.1: Acronyms and Abbreviations

Abbreviations	Description
SMS	Security Management System
PII	Personally Identifiable Information

1.6 List of Topics

This guide is organized into the following topics:

Table 1.2: List of Topics

Topics	Description
Welcome to Security Management	Provides an overview to the module and takes you through the various steps involved in setting up and using the security features.
Error Codes and Messages	Provides the list of error codes and its descriptions.

1.7 Basic Actions

Most of the screens contain buttons to perform all or few of the basic actions. The actions which are called here are generic, it varies based on the usage and the applicability. The table below gives a snapshot of them:

Table 1.3: Basic Actions

Action	Description
Back	Navigate to the previous tab.
Submit	Click to complete the transaction after you specify all the input parameters for a particular transaction.
Cancel	Click to cancel the transaction input midway without saving any data.
Clear	Click to clear the transaction input data. The system displays a pop-up screen with confirmation to clear data. You can click OK to confirm or click x icon to retain the data.
Query	On completion of input of necessary parameters, click this button to fetch and display the details.
Save	Click to save the details specified in the screen.
Exit	Click to close the screen and go to Home screen.
OK	Click to confirm the details in the pop-up screen.

1.8 Symbols and Icons

The following symbols and icons are used in the guide:

Table 1.4: Symbols and Icons

Symbols and Icons	Description
	Add a record
	Authorized or Open
	Authorized Status
	Close
	Closed Status
	Date and Time
	Grid View
	List View
	Maximize
	Minimize
	Navigate to first record
	Navigate to last record
	Navigate to next record

Symbols and Icons	Description
	Navigate to previous record
	Notes
	Open List
	Open Status
	Refresh
	Search
	Unauthorized Status
	Tips
	Users
	Warning

1.9 Related Resources

For more information on any related features, you can refer to the following documents:

- Oracle Banking Getting Started User Guide
- Oracle Banking Common Core User Guide

2. Welcome to Security Management

This user guide provides an overview to the module and takes you through the various steps involved setting up and using the security features that Oracle offers.

This document is intended for Oracle Implementers, SMS Administrator for the Bank, SMS Administrator for the Branch, and an Oracle user.

This section includes following topics:

- [2.1 Role](#)
- [2.2 User](#)
- [2.3 Functional Activity](#)

2.1 Role

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

Prerequisite

Specify **User Id** and **Password**, and login to **Home screen**.

This section includes following subsections:

- [2.1.1 View Role](#)
- [2.1.2 Create Role](#)

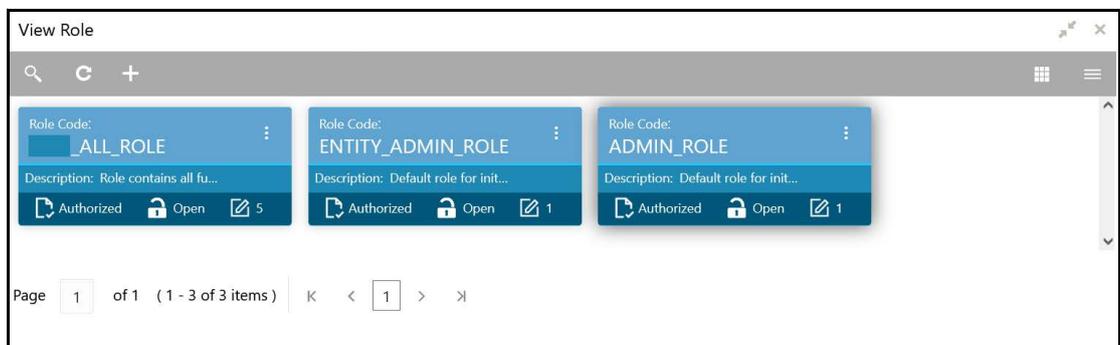
2.1.1 View Role

The summary screen provides a list of configured roles. You can configure a role using the [2.1.2 Create Role](#). To process this screen, perform the following steps:

- 1) From **Home screen**, click **Security Management**. Under **Security Management**, click **Role**.
- 2) Under **Role**, click **View Role**.

STEP RESULT: The **View Role** screen is displayed.

Figure 2.1: Role Summary



For more information on menus, refer to [Table 2.1: Role Summary - Field Description](#).

Table 2.1: Role Summary - Field Description

Field	Description
Role Code	Displays the code of the role.
Description	Displays additional details about the role.

Field	Description
Authorization Status	<p>Displays the authorization status of the record.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Authorized • Rejected • Unauthorized
Record Status	<p>Displays the status of the record.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Open • Closed
Modification Number	<p>Displays the number of modification performed on the record.</p>

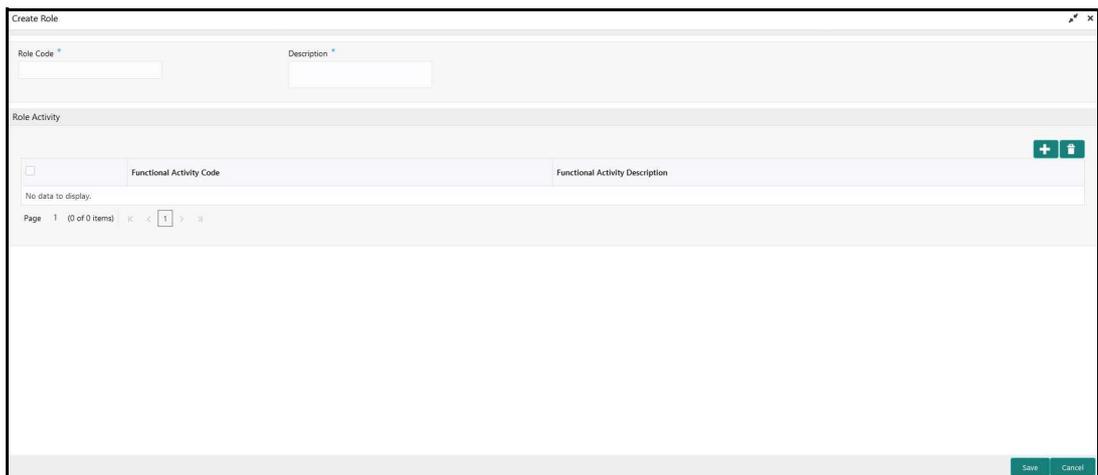
2.1.2 Create Role

The maintenance screen allows you to create roles and assign their activities. To process this screen, perform the following steps:

- 1) From **Home screen**, click **Security Management**. Under **Security Management**, click **Role**.
- 2) Under **Role**, click **Create Role**.

STEP RESULT: The **Create Role** screen is displayed.

Figure 2.2: Create Role



- 3) Provide the details in the relevant data fields. Mandatory data fields are indicated accordingly. For more information on menus, refer to [Table 2.2: Create Role - Field Description](#).

Table 2.2: Create Role - Field Description

Field	Description
Role Code	Specify the code of the role.
Role Description	Specify the additional details about the role.
Role Activity	Specify the role activity details.

- 4) Click + to add a functional activity code and select the required functional activities to which the role profile must have access. For more information on functional activity, see [2.3 Functional Activity](#).
- 5) Click **Save**. You can view the configured roles in the [2.1.1 View Role](#).

2.2 User

Controlled access to the system is a basic parameter that determines the robustness of the security in banking software. Only authorized users can access the system with the help of a unique User Login ID and password. The user profile of a user contains the details of the user in four sections - User details, Status, Other details and User role branches.

Prerequisites

Specify **User Id** and **Password**, and login to **Home screen**.

This section includes following subsections:

- [2.2.1 View User](#)
- [2.2.2 Create User](#)
- [2.2.3 Clear User](#)

2.2.1 View User

The summary screen provides a list of configured roles. You can configure a role using the [2.2.2 Create User](#). To process this screen, perform the following steps:

- 1) From **Home screen**, click **Security Management**. Under **Security Management**, click **User**.
- 2) Under **User**, click **View User**.

STEP RESULT: The **View User** screen is displayed.

Figure 2.3: View User



For more information on menus, refer to [Table 2.3: View User - Field Description](#).

Table 2.3: View User - Field Description

Field	Description
User Login ID	Displays the user login ID details.
User Name	Displays the user who has created the record.
Home Branch	Displays the details of the home branch associated with the user.
Authorization Status	<p>Displays the authorization status of the record.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Authorized • Rejected • Unauthorized
Record Status	<p>Displays the status of the record.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Open • Closed
Modification Number	Displays the number of modification performed on the record.

2.2.2 Create User

The maintenance screen allows you to create users and assign their activities based on their entity login. To process this screen, perform the following steps:

- 1) From **Home screen**, click **Security Management**. Under **Security Management**, click **User**.
- 2) Under **User**, click **Create User**.

STEP RESULT: The **Create User** screen is displayed.

Figure 2.4: Create User - Single Entity

The screenshot shows the 'Create User' form with the following sections and fields:

- User Details:** Login ID, Username, Home Branch.
- Status:** User Status (dropdown), Status Changed On, Is Supervisor (radio), Manager ID, Start Date, End Date, System User (radio).
- Other Details:** Access to PII (radio), Staff Customer Restriction Required (radio), Customer ID, Email ID, Telephone Number, Home Phone Number, Mobile Number, Fax, Language Code.
- User Role Branches:** Table with columns: Branch Code, Role Code, Role Description. (No data to display)
- User Applications:** Table with columns: Application Name, Application Description. (No data to display)
- Customer Access Groups:** Table with columns: Customer Access Group, Customer Access Description. (No data to display)

Buttons for '+', '-', and 'Select All Applications' are present in the table sections. 'Save' and 'Cancel' buttons are at the bottom right.

Figure 2.5: Create User - Multi Entity

- 3) Provide the details in the relevant data fields. Mandatory data fields are indicated accordingly. For more information on fields, refer to [Table 2.4: Create User - Field Description](#).

Table 2.4: Create User - Field Description

Field	Description
User Details	Specify the user details.
Username	Specify the user name.
Login ID	<p>Single Entity - Specify login ID with which a user logs into the system. This login ID is unique across all branches. The minimum length of login ID must be six and the maximum number can be 12 characters.</p> <p>Multi Entity - Search and select the required login ID from the LOV.</p>
Home Branch	Search and select required home branch.

Field	Description
Status	Specify the status.
User Status	Select the user status from the drop-down list.
Status Changed On	Displays a status changed.
Is Supervisor	By default, this option is disabled. If selected, indicates the user is a supervisor.
Manager ID	Search and select the required manager ID.
Start Date	Select the start date from which the user is valid from the calendar.
End Date	Select the end date for the user from the calendar.
System User	By default, this option is disabled. If enabled, indicates the system user. This system user will never be disabled or closed. Example: Mainly enabled for users to provide service API access.
Other Details	Specify the other details.
Access to PII	By default, this option is disabled. If enabled, it provides the user access to personally identifiable information of the entity that they are accessing.
Staff Customer Restriction Required	By default, this option is disabled. If enabled, it provides the staff customer restriction.
Customer ID	Search and select required customer ID.
Email ID	Specify the user Email ID at the time of the creation. All system generated password is communicated to the user through this mail ID.
Telephone Number	Specify the user contact number.
Home Phone Number	Specify the user's home contact number.
Mobile Number	Specify the user's mobile number.
Fax	Specify the fax details of the user.
Language Code	Search and select the required language code.
User Role Branches	Specify the user role branches details.

Field	Description
Branch Code	Search and select the required branch code.
Role Code	Search and select the required role code.
Role Description	Displays additional information about the role, based on the selected role code.
User Applications	Specify the user application details.
Application Name	Search and select the required application.
Application Description	Displays additional information about the application based on the selected application.
Customer Access Groups	Specify the customer access group details.
Customer Access Group	Search and select the required customer access group from the list.
Customer Access Description	Displays the additional information about the customer access based on the selected group.

- 4) Click + to add a row and provide the required details in the columns.
- 5) Click **Select All Applications** button to select all the applications for which the user needs the access.
- 6) Click **Save**. You can view the configured users in the [2.2.1 View User](#).

Note:

User modification will not be allowed while the user is logged in. However, the administrator can clear off the user and perform modifications. For more information, refer to section [2.2.3 Clear User](#).

2.2.3 Clear User

The **Clear User** screen allows you to clear off the current users. To process this screen, perform the following steps:

- 1) From **Home screen**, click **Security Management**. Under **Security Management**, click **User**.
- 2) Under **User**, click **Clear User**.

STEP RESULT: The **Clear User** screen is displayed.

Figure 2.6: Clear User

The screenshot shows a web application window titled "Clear User". It contains a "Query" section with two input fields: "User Login Id" (containing "DEMO01") and "Branch Code" (empty). Below these fields are "Query" and "Reset" buttons. The main area displays a table with the following data:

<input type="checkbox"/>	Branch Code	User Login Id	User Name
<input checked="" type="checkbox"/>	000	DEMO01	DEMO01

Below the table, it shows "Page 1 of 1 (1 of 1 items)" with navigation arrows. At the bottom right, there are "Save" and "Cancel" buttons.

- 3) You can search for the user based on the **User Login ID** and **Branch Code** parameters. Provide the details in the relevant data fields. Mandatory data fields are indicated accordingly. For more information on fields, refer to [Table 2.5: Clear User](#).

Table 2.5: Clear User

Field	Description
User Login ID	Enter the user login ID.
Branch Code	Enter the branch code.

- 4) Click **Query**, once you have specified the parameters. System displays the following details of the users who have logged into the system.
- Branch Code
 - User Login ID
 - User Name
- Click **Reset**, if you need to reset the query parameters.
- 5) To force log out of a user, check the box against the relevant user record and click **Save**.

2.3 Functional Activity

SMS manages the user access by associating various functional activities to a role. Based on the business use cases, the granular level activities / operations are defined at Functional activity.

SMS related functional activities which must be mapped to a Role for Menu, Dashboard, User maintenance, and Role maintenance related access are as follows:

Table 2.6: Functional Activity

Functional Activity	Description
SMS_FA_LOAN_DASHBOARD_PREFERENCE	Functional activity for reading User Dashboard preference.
SMS_FA_LOAN_DASHBOARD_PREFERENCE_PUT	Functional activity for updating User Dashboard preference.
SMS_FA_LOAN_DASHBOARD_VIEW	Functional activity for reading User Dashboard tiles.
SMS_FA_MENU_DASHBOARD_VIEW	Functional activity for constructing menu.
SMS_FA_ROLE_AMEND	Functional activity for modifying a role record.
SMS_FA_ROLE_AUTHORIZE	Functional activity for authorizing a role record including Authority query and View changes.
SMS_FA_ROLE_CLOSE	Functional activity for closing a role record.
SMS_FA_ROLE_REOPEN	Functional activity for reopening a role record.
SMS_FA_ROLE_VIEW	Functional activity for viewing a role record including role LOV validation.
SMS_FA_ROLE_DELETE	Functional activity for deleting a role record.
SMS_FA_ROLE_NEW	Functional activity for creating a role record.
SMS_FA_USER_AMEND	Functional activity for modifying a user record.
SMS_FA_USER_AUTHORIZE	Functional activity for authorizing a user record including Authority query and View changes.
SMS_FA_USER_CLOSE	Functional activity for closing a user record.
SMS_FA_USER_DELETE	Functional activity for deleting a user record.
SMS_FA_USER_NEW	Functional activity for creating a user record.

Functional Activity	Description
SMS_FA_USER_REOPEN	Functional activity for reopening a user record.
SMS_FA_USER_VIEW	Functional activity for viewing a user record including user LOV validation.
SMS_FA_USER_GET_HIERARCHY	Functional activity for getting the user hierarchy.
SMS_FA_USER_GET_PEER_REPORTTEES	Functional activity for getting the peer reportees.
SMS_FA_USER_GET_LOGIN_STATUS	Functional activity for getting the login status.
SMS_FA_USER_AUDIT_TRAIL_GET	Functional activity for getting the audit trail.
SMS_FA_USER_GET_USER_FUNCTIONAL_ACTIVITIES	Functional activity for getting the user functional activities.
SMS_FA_USER_LOGIN	Functional activity for logging in the user.
SMS_FA_USER_CLEAR	Functional Activity for Clear User.
SMS_FA_USER_VIEW_NEW	Functional activity to validate existing User.
SMS_FA_USER_SERVICE_AMEND	Functional Activity for user amendment using service API.
SMS_FA_USER_SERVICE_NEW	Activity for user creation using service API.
SMS_FA_GET_ALL_FUNCTIONAL_ACTIVITIES	Functional activity for getting all the functional activities.
SMS_FA_USER_GET_REPORTTEES	Functional activity for getting the reportees.
SMS_FA_GET_ALL_FUNCTIONAL_ACTIVITIES_SUB	Functional activity for getting all the functional activities for subordinates.
SMS_FA_USER_GET_FILTERED_USERS	Functional activity for getting users filtered using and branch code and role code.

Functional Activity	Description
SMS_FA_USER_MAINT_BATCH	Functional activity for maintaining the user batch.
SMS_FA_USER_CUST_ACCESS_GROUP	Functional activity for getting the user customer access group.

3. Error Codes and Messages

This section contains error codes and messages.

Table 3.1: Error Codes and Messages

Error Code	Messages
GCS-AUTH-01	Record Successfully Authorized
GCS-AUTH-02	Valid modifications for approval were not sent. Failed to match
GCS-AUTH-03	Maker cannot authorize
GCS-AUTH-04	No Valid unauthroized modifications found for approval.
GCS-CLOS-002	Record Successfully Closed
GCS-CLOS-01	Record Already Closed
GCS-CLOS-02	Record Successfully Closed
GCS-CLOS-03	Unauthorized record cannot be closed, it can be deleted before first authorization
GCS-COM-001	Record does not exist
GCS-COM-002	Invalid version sent, operation can be performed only on latest version
GCS-COM-003	Please Send Proper ModNo
GCS-COM-004	Please send makerId in the request
GCS-COM-005	Request is Null. Please Resend with Proper Values
GCS-COM-006	Unable to parse JSON
GCS-COM-007	Request Successfully Processed
GCS-COM-008	Modifications should be consecutive.
GCS-COM-009	Resource ID cannot be blank or "null".
GCS-COM-010	Successfully cancelled \$1.
GCS-COM-011	\$1 failed to update.
GCS-DEL-001	Record deleted successfully
GCS-DEL-002	Record(s) deleted successfully
GCS-DEL-003	Modifications didnt match valid unauthorized modifications that can be deleted for this record

Error Code	Messages
GCS-DEL-004	Send all unauthorized modifications to be deleted for record that is not authorized even once.
GCS-DEL-005	Only Maker of first version of record can delete modifications of record that is not once authorized.
GCS-DEL-006	No valid unauthroized modifications found for deleting
GCS-DEL-007	Failed to delete. Only maker of the modification(s) can delete.
GCS-MOD-001	Closed Record cannot be modified
GCS-MOD-002	Record Successfully Modified
GCS-MOD-003	Record marked for close, cannot modify.
GCS-MOD-004	Only maker of the record can modify before once auth
GCS-MOD-005	Not amendable field, cannot modify
GCS-MOD-006	Natural Key cannot be modified
GCS-MOD-007	Only the maker can modify the pending records.
GCS-REOP-003	Successfully Reopened
GCS-REOP-01	Unauthorized Record cannot be Reopened
GCS-REOP-02	Failed to Reopen the Record, cannot reopen Open records
GCS-REOP-03	Successfully Reopened
GCS-REOP-04	Unauthorized record cannot be reopened, record should be closed and authorized
GCS-SAV-001	Record already exists
GCS-SAV-002	Record Saved Successfully.
GCS-SAV-003	The record is saved and validated successfully.
GCS-VAL-001	The record is successfully validated.
GCS-REJ-001	A rejected record cannot be closed. Please delete this modification.
GCS-REJ-002	A rejected record cannot be reopened. Please delete this modification.
GCS-REJ-003	Invalid modifications sent for reject. Highest modification must also be included.
GCS-REJ-004	Record Rejected successfully
GCS-REJ-005	Maker cannot reject the record.

Error Code	Messages
GCS-REJ-006	Checker remarks are mandatory while rejecting.
GCS-REJ-007	No valid modifications found for reject.
GCS-REJ-008	Invalid modifications sent for reject. Consecutive modifications must be included.
SMS-COM-001	End Date cannot be less than Start Date
SMS-COM-002	Start Date Cannot be less than Application Date and Application date is \$1
SMS-COM-003	Cannot create/modify own User record
SMS-COM-004	Cannot authorize own User record
SMS-COM-005	Start date cannot be modified
SMS-COM-006	User is already logged in. Modification not allowed.
SMS-COM-007	User is unauthorized.
SMS-COM-008	Invalid RoleCode.
SMS-COM-009	Invalid Role Description.
SMS-COM-010	Invalid User LoginId.
SMS-COM-011	Invalid User Name.
SMS-COM-012	Invalid Home Branch.
SMS-COM-100	\$1 is a Duplicate Application Number in Users Applications.
SMS-LOV-001	Invalid Home Branch
SMS-LOV-003	User Login ID should not contain Special Characters or Spaces
SMS-LOV-004	Invalid Manager Id
SMS-LOV-005	Not a Valid Email Id format
SMS-URB-001	Duplicate records present under User Role Branches for Branch code \$1 and Role code \$2
SMS-ROLE-001	\$1 is a Duplicate Functional Activity Code in Role Activity
ST-SAVE-027	Request Successfully Processed

4. Definitions

This section provides a glossary of all terms and abbreviations used in the user manual.

Accounts

Continuing financial relationship between a bank and a customer, in which deposits and debts are held and processed within a framework of established rules and procedures.

Reports

A page containing information organized in a narrative, graphic, or tabular format, prepared on ad-hoc, periodic, recurring, regular, or as required basis. Reports may refer to specific periods, events, occurrences, or subjects.

Pareto Chart

It is a type of chart that consists of both bars and a line graph, where individual values are represented in descending order by bars, and the cumulative total is represented by the line.

Sunburst Chart

It is a type of chart that is ideal for displaying hierarchical data. Each level of the hierarchy is represented by one ring or circle with the innermost circle as the top of the hierarchy. A sunburst chart without any hierarchical data (one level of categories), looks similar to a doughnut chart.

Virtual Account

Virtual accounts are provided to a corporate by its banking partner. Each account is a subsidiary or sub-account of the client's own physical account with the bank; they cannot exist outside of the immediate relationship, hence they are virtual.

Virtual Identifier

Virtual identifier serves to segregate any funds from any other funds in the same main account and yet is inextricably linked to the virtual account.

5. Index

C

Clear User	10
Create Role	3
Create User	7

F

Functional Activity	11
---------------------------	----

R

Role	2
------------	---

U

User	5
------------	---

V

View Role	2
View User	5