Oracle® Banking Accounts Cloud Service

Security Management System User Guide

Release 14.6.0.0.0

F73990-01

December 2022

ORACLE

Oracle Banking Accounts Cloud Service Security Management System User Guide, Release 14.6.0.0.0

F73990-01

Contents

Preface

Introduction

This **Security Management System (SMS)** guide provides an overview and takes you through the various steps involved in setting up and using the security features that Oracle offers.

Audience

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

List of Topics

This guide is organized as follows:

Table List of Topics

Topics	Description
Role	This topic provides the information about creating, defining and linking a Role Profile that includes access rights to the functional activities that are common to a group of users.
User	This topic provides the information about creating users, viewing users and clearing users.
Functional Activity Codes	This topic provides the information about the functionality that can be defined at the granular level activities/operations for different business use cases.
Error Codes and Messages	This topic provides the information about error codes and messages.
Glossary	This topic provides the information about the glossary of all terms and abbreviations used in the user guide.

Symbols and Icons

The following buttons are used in the screens:

Table Symbols and Icons - Common

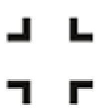
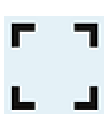
Symbol/Icon	Function
	Minimize
	Maximize

Table (Cont.) Symbols and Icons - Common

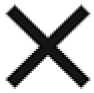
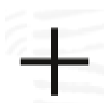
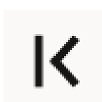
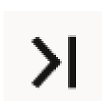
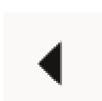
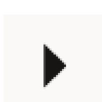
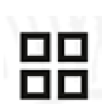
Symbol/Icon	Function
	Close
	Perform Search
	Open a list
	Add a new record
	Navigate to the first record
	Navigate to the last record
	Navigate to the previous record
	Navigate to the next record
	Grid view

Table (Cont.) Symbols and Icons - Common

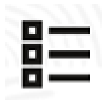
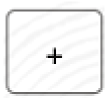
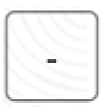
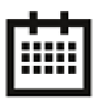
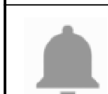
Symbol/Icon	Function
	List view
	Refresh
	Click this icon to add a new row.
	Click this icon to delete a row, which is already added.
	Calendar
	Alerts

Table Symbols and Icons – Audit Details

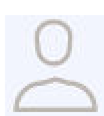
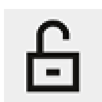
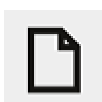
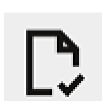
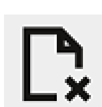
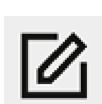
Symbol/Icon	Function
	A user
	Date and time

Table (Cont.) Symbols and Icons – Audit Details

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

Table Symbols and Icons - Widget

Symbol/Icon	Function
	Open status
	Unauthorized status
	Closed status
	Authorized status
	Rejected status
	Modification Number

Related Documents

The related documents are as follows:

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

Screenshot Disclaimer

Sample information used in the interface or documents are dummy, it does not exist in real world, and it is for reference purpose only.

1 Role Profile

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.

It is most 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. The roles defined is effective only after the *dual* authorization.

This topic contains the following subtopics:

- Create Role
  This topic describes the systematic instructions to create a role profile.
- View Role
  This topic describes the systematic instructions to view role profiles.

1.1 Create Role

This topic describes the systematic instructions to create a role profile.

This screen allows the user to create roles and assign their activities.

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

1. From **Home screen**, under **Menu**, click **Security Management**.

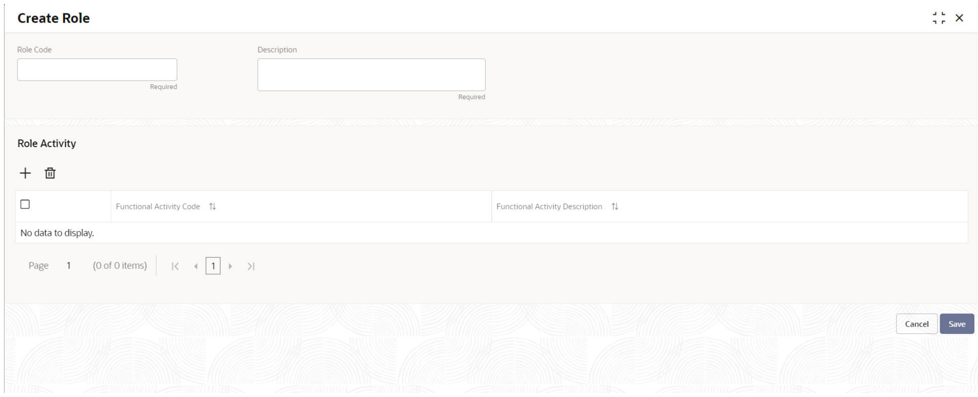
   The **Security Management** pane displays.
2. Under **Security Management**, click **Role**.

   The **Role** pane displays.
3. Under **Role**, click **Create Role**.

   The **Create Role** screen displays.
4. Alternatively, you can search via **Menu Item Search** field from **Home screen**. Enter **Role** and select **Security Management-->Role-->Create Role**.

   The **Create Role** screen displays.

Figure 1-1 Create Role



5. Specify the fields on **Create Role** screen.

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

Table 1-1 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.

6. Click **+** to add a **functional activity code** and select the required functional activities to which the role profile must have access to. For more information about functional activity, refer Functional Activity.
7. Click **Save**. You can view the configured roles in **View Role**.
8. Or, click **Cancel** to exit the screen.

1.2 View Role

This topic describes the systematic instructions to view role profiles.

The **View** screen allows you to view the list of configured roles.

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

1. From **Home screen**, under **Menu**, click **Security Management**.

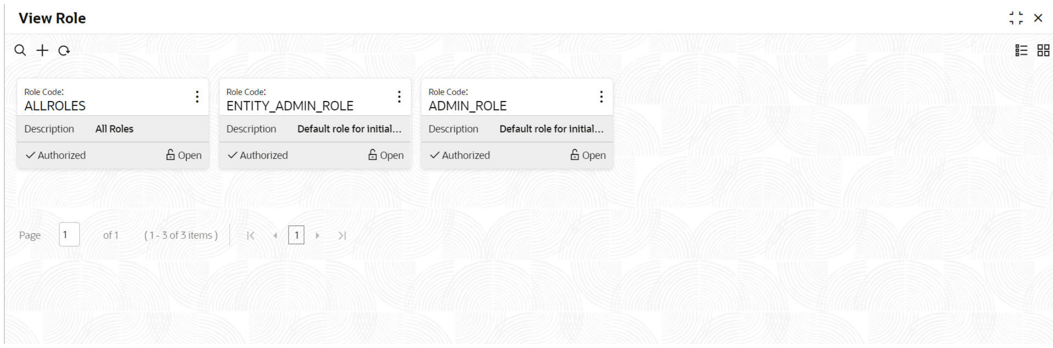
   The **Security Management** pane displays.
2. Under **Security Management**, click **Role**.

   The **Role** pane displays.
3. Under **Role**, click **View Role**.

   The **View Role** screen displays.
4. Alternatively, you can search via **Menu Item Search** field from **Home screen**. Enter **Role** and select **Security Management-->Role-->View Role**.

   The **View Role** screen displays.

Figure 1-2 View Role



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

Table 1-2 View Role - Field Description

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

Click the menu icon on the tile to perform the following actions.

- **Unlock** the maintenance parameter to make amendments.
- **Close** the parameter maintenance.
- **View** the details of that parameter maintenance.
- **Copy** the parameter maintenance.
- **Authorize** the parameter maintenance depending on user rights.
- **Search** for a particular parameter by clicking the search icon at the left corner of the section.
- Change views by selecting the option from the right corner of the section. The two view options available are **tile** view and **list** view.
- Click **Audit** to view the Maker, Checker, Status and Modification No.

2
User Role

Controlled access to the system is a basic feature that determines the robustness of security in any banking software. Only authorized users can access the system with the help of unique login credentials.

The user profile of a user contains details of the user in four sections - User details, Status, Other details and User role branches.

This topic contains the following subtopics:

- Create User
  This topic describes the systematic instructions to create a user.
- Clear User
  This topic describes the systematic instructions to clear a user profile.
- View User
  This topic describes the systematic instructions to view user profiles.

2.1 Create User

This topic describes the systematic instructions to create a user.

This screen allows you to create users and assign their activities.

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

1. From **Home screen**, under **Menu**, click **Security Management**.

   The **Security Management** pane displays.
2. Under **Security Management**, click **User**.

   The **User** pane displays.
3. Under **User**, click **Create User**.

   The **Create User** screen displays.
4. Alternatively, you can search via **Menu Item Search** field from **Home screen**. Enter **User** and select **Security Management-->User-->Create User**.

   The **Create User** screen displays. For clarity, the same **Create User** screen is split and displayed using three images below.

Figure 2-1 Create User1

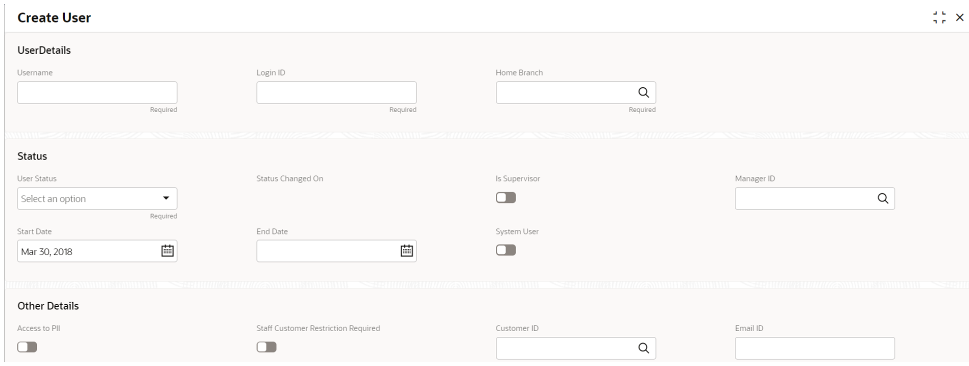


Figure 2-2 Create User2

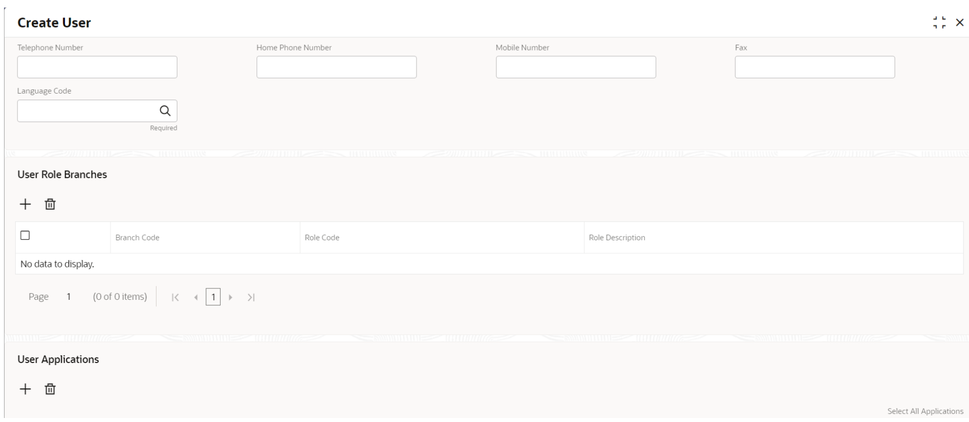
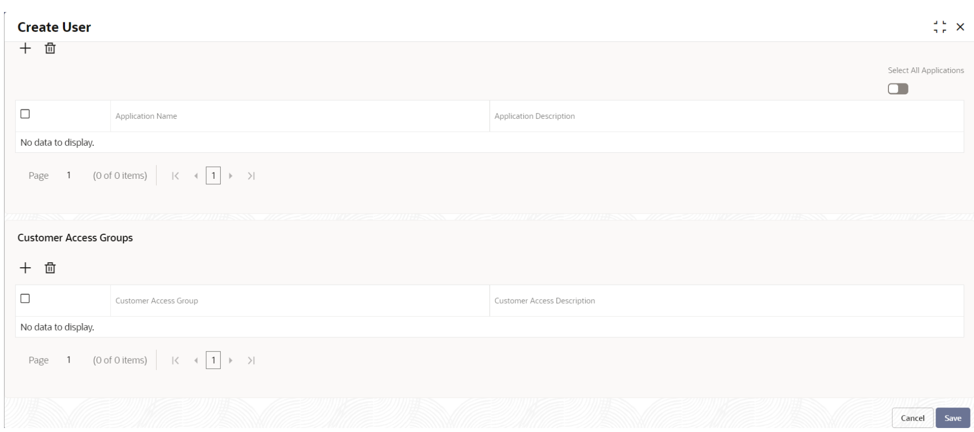


Figure 2-3 Create User3



5. Specify the fields on **Create User** screen.

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

Table 2-1 Create User - Field Description

Field	Description
User Details	
Username	Specify the user name.
Login ID	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 is 6 (six) characters and the maximum length is 12 characters.
Home Branch	Search and select required home branch.
Status	
User Status	Select the user status from the drop-down list.
Status Changed On	Select a status change date from the calendar.
Is Supervisor	By default, this option is disabled. If selected, it indicates that 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	Select to specify if the user is a system user.
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	
Branch Code	Search and select the required branch code.
Role Code	Search and select the required role code.
Role Description	This field displays additional information about the role, based on the selected role code.
User Applications	
Application Name	Search and select the required application.
Application Description	Displays additional information about the application based on the selected application.
Customer Access Groups	
Customer Access Group	Search and select the required customer access group.
Customer Access Description	Displays additional information about the customer access.

6. Click **+** to add a row and provide the required details in the columns.

7. Click **Save**. You can view the configured roles in **View User**.
8. Or, click **Cancel** to exit the screen.

> **Note:**
>
> User modification will not be allowed while the user is logged in. However, the administrator can clear off the user and perform modifications.

2.2 Clear User

This topic describes the systematic instructions to clear a user profile.

This screen allows you to clear off current users.

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

1. From **Home screen**, under **Menu**, click **Security Management**.

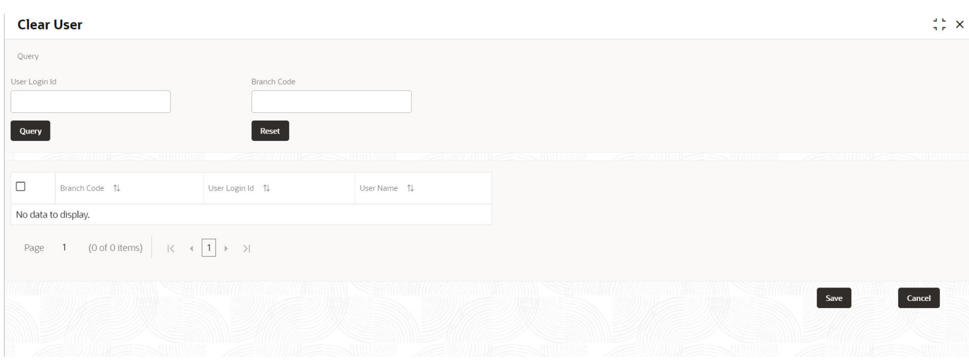
   The **Security Management** pane displays.
2. Under **Security Management**, click **User**.

   The **User** pane displays.
3. Under **User**, click **Clear User**.

   The **Clear User** screen displays.
4. Alternatively, you can search via **Menu Item Search** field from **Home screen**. Enter **User** and select **Security Management-->User-->Clear User**.

   The **Clear User** screen displays.

Figure 2-4 Clear User



5. Specify the fields on **Clear User** screen.

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

Table 2-2 Clear User - Field Description

Field	Description
User Login ID	Specify the user login ID.

Table 2-2 (Cont.) Clear User - Field Description

Field	Description
Branch Code	Specify the branch code.

6. Click **Query** after specifying the parameters. The system displays the following details of the users who have logged into the system.
   - **Branch Code**
   - **User Login ID**
   - **User Name**
7. Click **Reset** to reset the query parameters.
8. To force log out a user, select the box against the relevant user record and click **Save**.
9. Or, click **Cancel** to exit the screen.

2.3 View User

This topic describes the systematic instructions to view user profiles.

The **View** screen allows you to view the list of configured users.

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

1. From **Home screen**, under **Menu**, click **Security Management**.

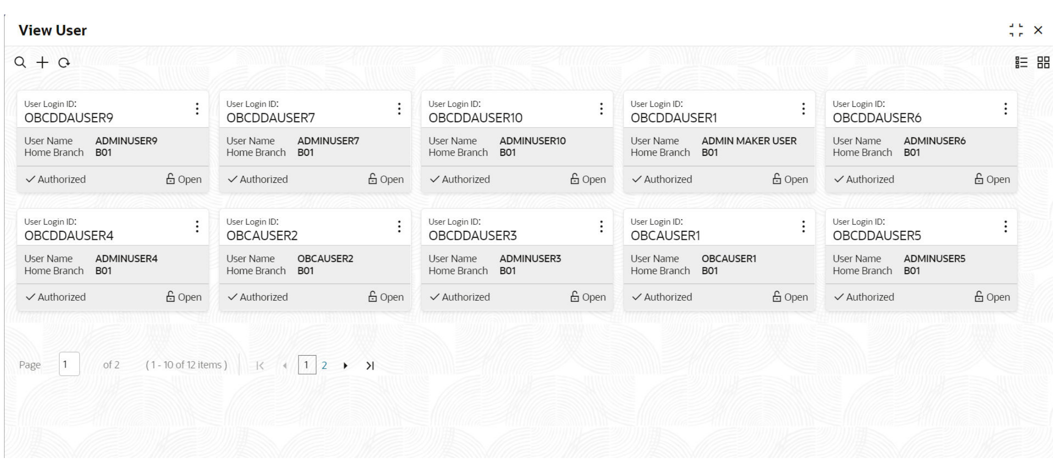
   The **Security Management** pane displays.
2. Under **Security Management**, click **User**.

   The **User** pane displays.
3. Under **User**, click **View User**.

   The **View User** screen displays.
4. Alternatively, you can search via **Menu Item Search** field from **Home screen**. Enter **User** and select **Security Management-->User-->View User**.

   The **View User** screen displays.

Figure 2-5 View User



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

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.
Status	Displays the status of the record.

Click the menu icon on the tile to perform the following actions.

- **Unlock** the maintenance parameter to make amendments.
- **Close** the parameter maintenance.
- **View** the details of that parameter maintenance.
- **Copy** the parameter maintenance.
- **Authorize** the parameter maintenance depending on user rights.
- **Search** for a particular parameter by clicking the search icon at the left corner of the section.
- Change views by selecting the option from the right corner of the section. The two view options available are **tile** view and **list** view.
- Click **Audit** to view the Maker, Checker, Status and Modification No.

A
Functional Activity Codes

This topic contains **Functional Activity Codes**.
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 A-1 Functional Activity Codes

Functional Activity Code	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.
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.

B

Error Codes and Messages

This topic contains **Error Codes and Messages**.

Table B-1 Error Codes and Messages

Error Code	Message
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 unauthorized 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 canceled $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 didn’t match valid unauthorized modifications that can be deleted for this record
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 unauthorized 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 authorized
GCS-MOD-005	Not amendable field, cannot modify
GCS-MOD-006	Natural Key cannot be modified

Table B-1 (Cont.) Error Codes and Messages

Error Code	Message
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.
SMS-COM-001	End Date cannot be less than Start Date
SMS-COM-002	StartDate 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-LOV-001	Invalid Home Branch
SMS-LOV-003	User LoginID should not contain Special Characters or Spaces
SMS-LOV-004	Invalid Manager ID
SMS-URB-001	Duplicate records present under User Role Branches for Branch code $1 and Role code $2
ST-SAVE-027	Request Successfully Processed

Glossary

Index