Oracle® Banking Supply Chain Finance

Oracle Banking Security Management System User Guide

Release 14.7.0.0.0 , Part Number - F72110-01
November 2022

Oracle Banking Supply Chain Finance Oracle Banking Security Management System User Guide, Release 14.7.0.0.0 , Part Number - F72110-01

Contents

List of Figures

List of Tables

1 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:

- Role
- User
- Functional Activity

1.1 Role

This topic describes about the maintenance of role and the respective access rights.

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.

This section includes following subsections:

- View Role
- Create Role

1.1.1 View Role

This topic provides the systematic instructions to view the list of configured roles.

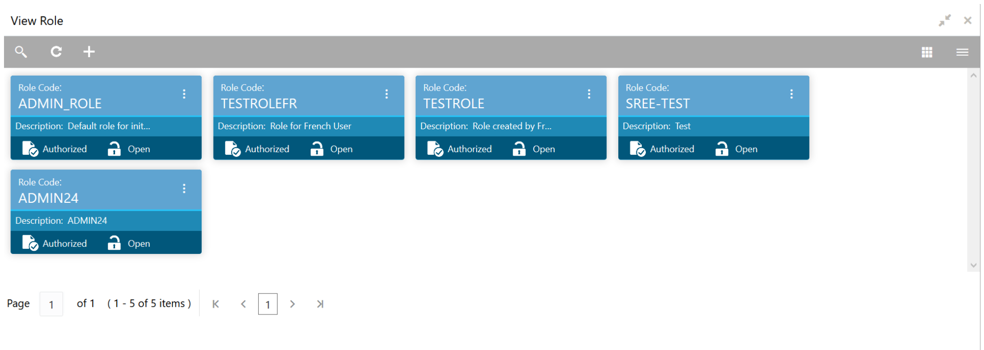
Specify **User ID** and **Password**, and login to the **Home** screen.

The user can configure the role using the #unique_14 screen.

1. On **Home** screen, click **Security Management**. Under **Security Management**, click **Role**.
2. Under **Role**, click **View Role**.

   The **View Role** screen displays.

Figure 1-1 View Role



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

Table 1-1 View Role - Field Description

Field	Description
Role Code	Displays the code of the role.
Description	Displays additional details about the role.
Authorization Status	Displays the authorization status of the configured role. The available options are: • **Authorized** • **Rejected** • **Unauthorized**
Record Status	Displays the record status of the configured role. The available options are: • **Open** • **Closed**
Modification Number	Displays the number of modifications performed on the record.

1.1.2 Create Role

This topic provides the systematic instructions to create role.

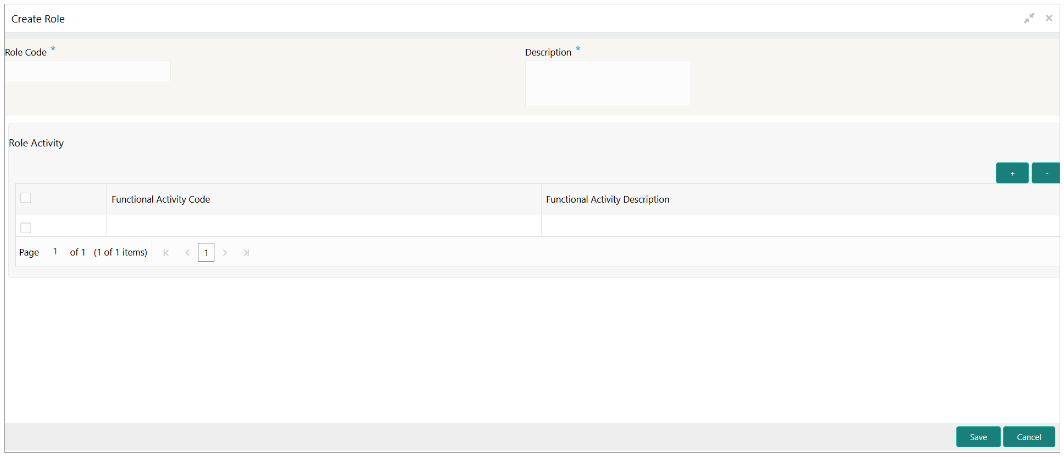
Specify **User ID** and **Password**, and login to the **Home** screen.

The **Create Role** screen allows the user to create roles and assign their activities.

1. On **Home** screen, click **Security Management**. Under **Security Management**, click **Role**.
2. Under **Role**, click **Create Role**.

   The **Create Role** screen displays.

Figure 1-2   Create Role



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

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

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

Table 1-2   Create Role - Field Description

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

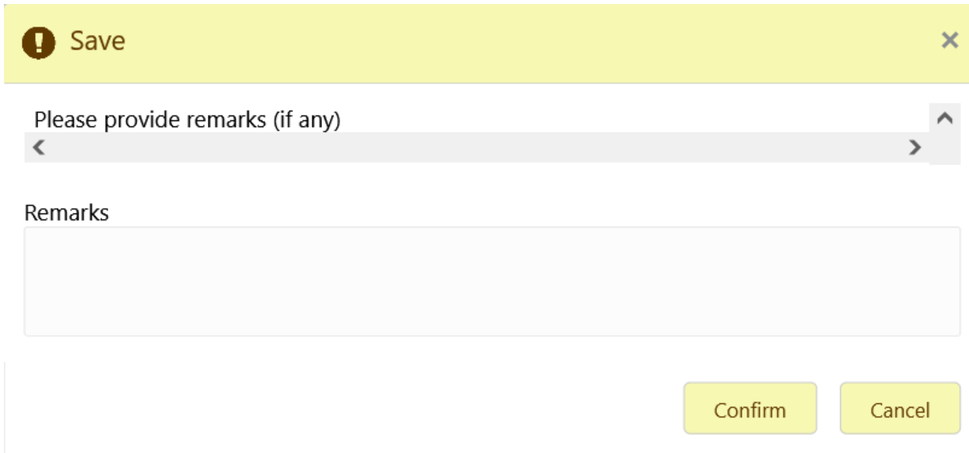
4. Click **+** to add a functional activity code and select the required functional activities to which the role profile must have access.

   For more information on functional activity, refer to the Functional Activity (page 1-9).

5. Click **Save**. You can view the configured roles in View Role (page 1-1).

   The **Save - Confirmation Message** popup screen displays.

Figure 1-3 Save - Confirmation Message



6. Click **Confirm** to save the details.

1.2 User

This topic describes about the maintenance of the user and their access.

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.

1.2.1 View User

This topic provides the systematic instructions to view the list of configured users.

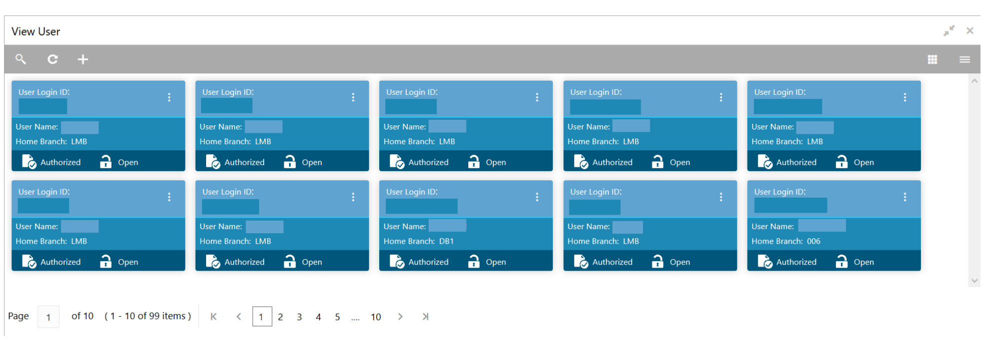
Specify **User ID** and **Password**, and login **Home** screen.

The user can configure the user using the #unique_19 screen.

1. On **Home** screen, click **Security Management**. Under **Security Management**, click **User**.
2. Under **User**, click **View User**.

   The **View User** screen displays.

Figure 1-4 View User



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

Table 1-3 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	Displays the authorization status of the configured user. The available options are: • **Authorized** • **Rejected** • **Unauthorized**
Record Status	Displays the record status of the configured user. The available options are: • **Open** • **Closed**
Modification Number	Displays the number of modifications performed on the record.

1.2.2 Create User

This topic provides the systematic instructions to create the user and assign their activities.

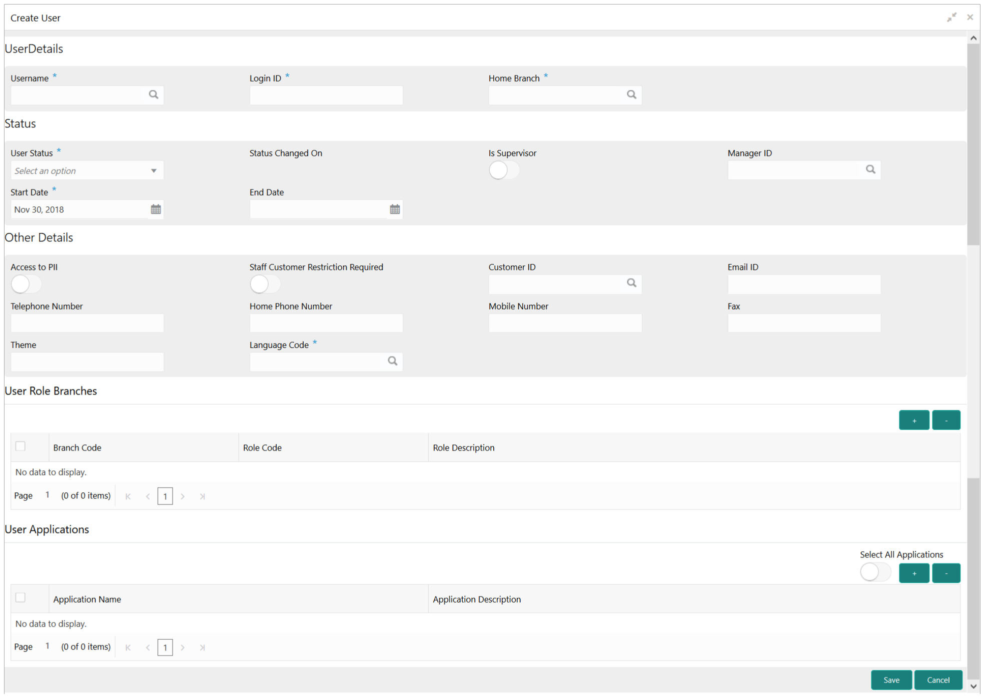
Specify **User ID** and **Password**, and login **Home** screen.

The **Create User** screen allows the user to create the user and assign their activities.

1. On **Home** screen, click **Security Management**. Under **Security Management**, click **User**.
2. Under **User**, click **Create User**.

   The **Create User** screen displays.

Figure 1-5 Create User



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

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

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

Table 1-4 Create User - Field Description

Field	Description
User Details	Specify the 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 must be six and the maximum number can be 12 characters.
Home Branch	Click the **Search** icon and select required home branch.
Status	Specify the status.
User Status	Select the user status from the drop-down list.
Status Changed On	Displays the latest status change date.
Is Supervisor	Select the toggle to indicate whether the user is a supervisor or not. By default, this option is disabled.
Manager ID	Click the **Search** icon and select the required manager ID.
Start Date	Select the start date from when the user is valid.

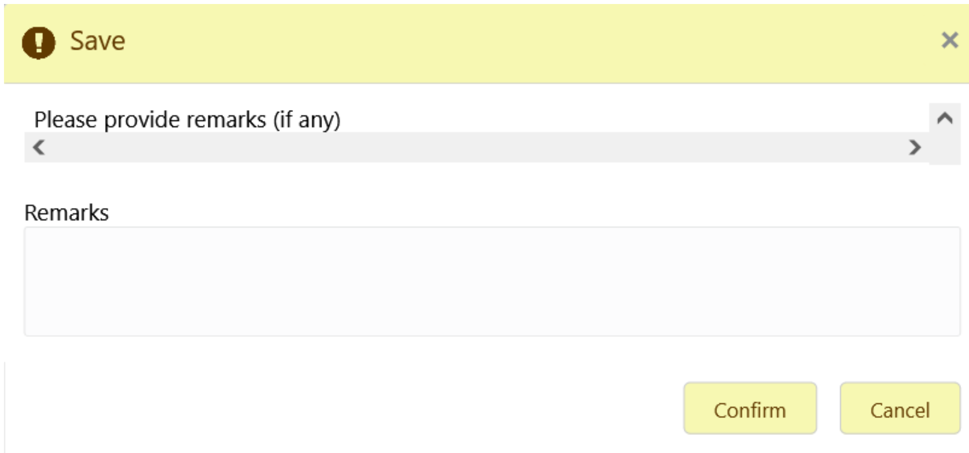
Table 1-4 (Cont.) Create User - Field Description

Field	Description
End Date	Select the end date till when the user is valid.
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	Click the **Search** icon 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 home contact number.
Mobile Number	Specify the user mobile number.
Fax	Specify the fax details of the user.
Language Code	Click the **Search** icon and select the required language code.
User Role Branches	Specify the user role branches details.
Branch Code	Click the **Search** icon and select the required branch code.
Role Code	Click the **Search** icon and select the required role code.
Role Description	Displays the description about the role, based on the selected role code.
User Applications	Specify the user application details.
Application Name	Click the **Search** icon and select the required application.
Application Description	Displays the description 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 **Save**.

   The **Save - Confirmation Message** popup screen displays.

Figure 1-6   Save - Confirmation Message



6. Click **Confirm** to save the details.

   The user can view the configured users in the View User (page 1-4).

> **Note:**
>
> User modification is not allowed while the user is logged in. However, the administrator can clear off the user and perform modifications. For more information, refer to the Clear User (page 1-8) topic.

1.2.3 Clear User

This topic provides the systematic instructions to clear the user.

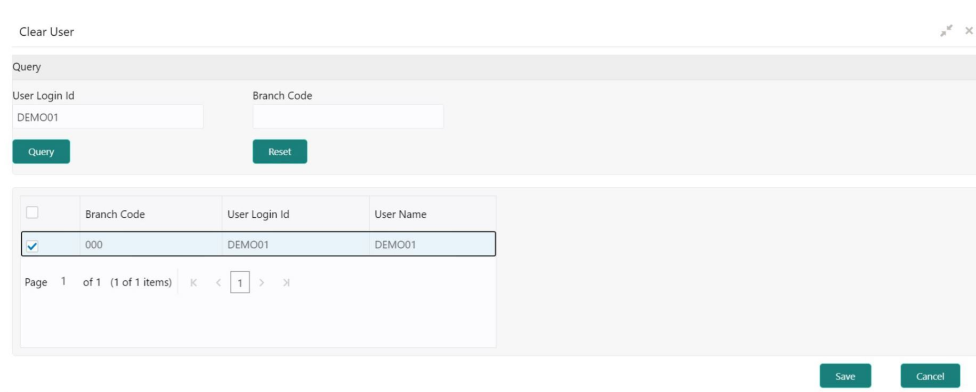
Specify **User ID** and **Password**, and login **Home** screen.

The **Clear User** screen allows the user to clear off the current users.

1. On **Home** screen, click **Security Management**. Under **Security Management**, click **User**.
2. Under **User**, click **Clear User**.

   The **Clear User** screen displays.

Figure 1-7   Clear User



The user can search for the user based on the **User Login ID** and **Branch Code** parameters.

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

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

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

Table 1-5 Clear User - Field Description

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

4. Click **Query**, once the parameters are specified.

   The system displays the following details of the users who have logged into the system.

   - Branch Code
   - User Login ID
   - User Name

5. Click **Reset** to reset the query parameters.
6. Select the check box against the relevant user record and click **Save** to force log out of the selected user.

1.3 Functional Activity

This topic describes about the functional activity for Security Management System services.

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 must be mapped to a Role for Menu, Dashboard, User maintenance, and Role maintenance related access. It is as follows:

Table 1-6 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.

Table 1-6 (Cont.) Functional Activity

Functional Activity	Description
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.
SMS_FA_USER_GET_HIERARCHY	Functional activity for getting the user hierarchy.
SMS_FA_USER_GET_PEER_REPORTEES	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_USR_FUN_ACT	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_FUNC_ACTIVITIES	Functional activity for getting all the functional activities.
SMS_FA_USER_GET_REPORTEES	Functional activity for getting the reportees.
SMS_FA_GET_ALL_FUNC_ACTIVITIES_SUB	Functional activity for getting all the functional activities for subordinates.
SMS_FA_USER_GET_FILTERED_USERS	Functional activity for getting all filtered users.
SMS_FA_USER_MAINT_BATCH	Functional activity for maintaining the user batch.
SMS_FA_USER_CUST_ACCESS_GROUP	Functional activity for maintaining the user customer access group.

2 Error Codes and Messages

This topic contains the error codes and messages.

Table 2-1 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 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 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 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 unauthorised 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.

Table 2-1 (Cont.) Error Codes and Messages

Error Code	Messages
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.
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.

3 Reference and Feedback

References

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

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

Documentation 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.

Feedback and Support

Oracle welcomes customers' comments and suggestions on the quality and usefulness of the document. Your feedback is important to us. If you have a query that is not covered in this user guide or if you still need assistance, please contact documentation team.

Glossary

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 adhoc, 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.

Index