Oracle Banking Security Management System User Guide

Oracle Banking Origination

Release 14.5.4.0.0

Part Number F54319-01

February 2022

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/

Contents

1 **Welcome to Security Management** ... 1

1.1 Role ... 2

1.1.1 View Role ... 2

1.1.2 Create Role ... 3

1.2 User ... 4

1.2.1 View User ... 4

1.2.2 Create User ... 5

1.2.3 Clear User ... 8

1.3 Functional Activity ... 9

2 **Error Codes and Messages** ... 11

3 **Glossary** ... 14

4 **Index** ... 15

5 **Reference and Feedback** ... 16

5.1 References ... 16

5.2 Documentation Accessibility ... 16

5.3 Feedback and Support ... 16

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:

- 1.1 Role
- 1.2 User
- 1.3 Functional Activity

1.1 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:

- 1.1.1 View Role
- 1.1.2 Create Role

1.1.1 View Role

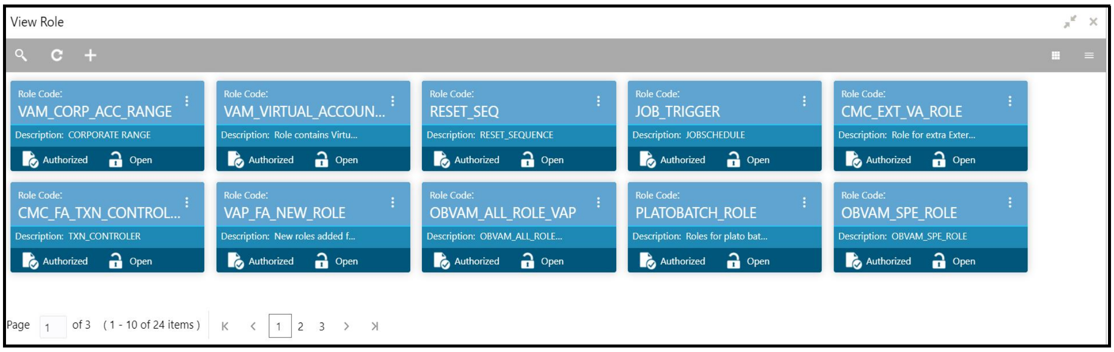
The summary screen provides a list of configured roles. You can configure a role using the 1.1.2 Create Role. To process this screen, perform the following steps:

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 1.1: Role Summary



For more information on menus, refer to Table 1.1: Role Summary - Field Description.

Table 1.1: Role Summary - 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.

1.1.2 Create Role

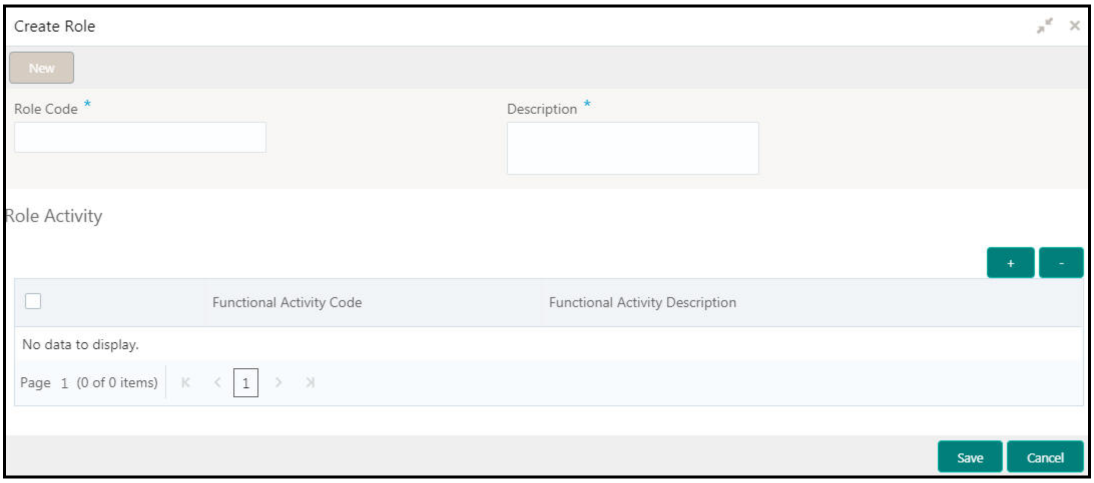
The maintenance screen allows you to create roles and assign their activities. To process this screen, perform the following steps:

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 1.2: 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 1.2: Create Role - Field Description.

Table 1.2: 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 1.3 Functional Activity.

5) Click **Save**. You can view the configured roles in the 1.1.1 View Role.

1.2 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:

- 1.2.1 View User
- 1.2.2 Create User
- 1.2.3 Clear User

1.2.1 View User

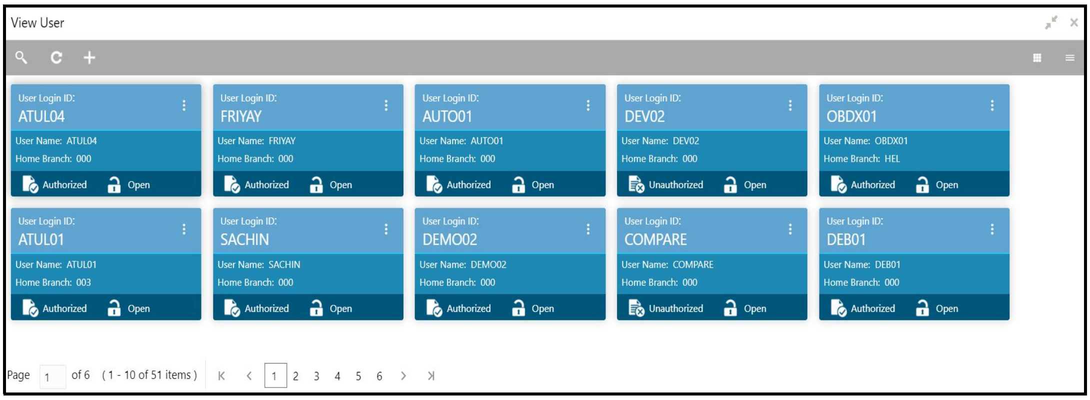
The summary screen provides a list of configured roles. You can configure a role using the 1.2.2 Create User. To process this screen, perform the following steps:

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 1.3: View User



For more information on menus, refer to Table 1.3: View User - Field Description.

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.
Status	Displays the status of the record.

1.2.2 Create User

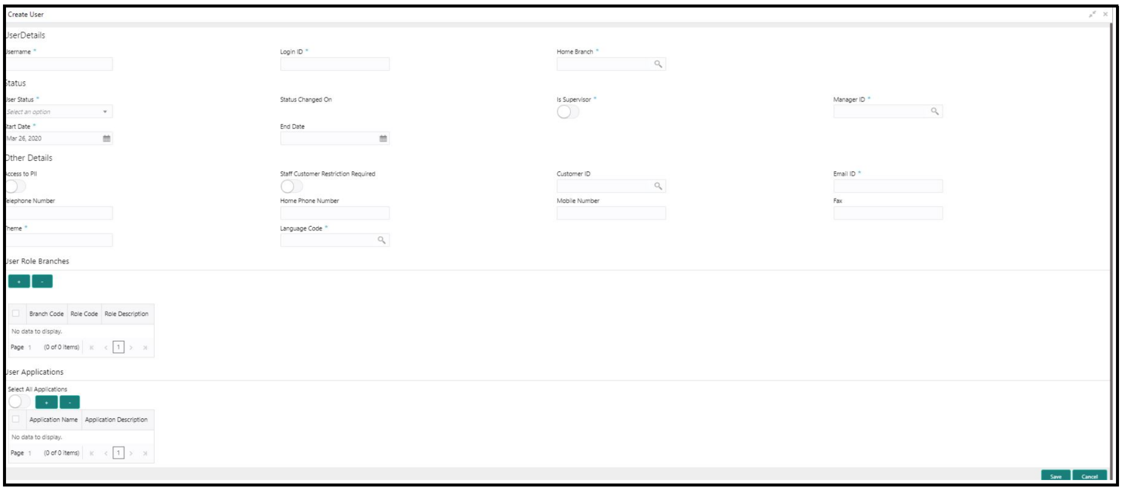
The maintenance screen allows you to create users and assign their activities. To process this screen, perform the following steps:

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 1.4: Create User



3) Provide the details in the relevant data fields. Mandatory data fields are indicated accordingly. For more information on fields, refer to Table 1.4: Create User - Field Description.

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	Search and select required home branch.
Status	Specify the 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, 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.
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.

Field	Description
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.
Theme	Specify the theme details.
Language Code	Search and select the required language code.
User Role Branches	Specify the user role branches details.
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.

4) Click + to add a row and provide the required details in the columns.

5) Click **Save**. You can view the configured users in the 1.2.1 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 1.2.3 Clear User.

1.2.3 Clear User

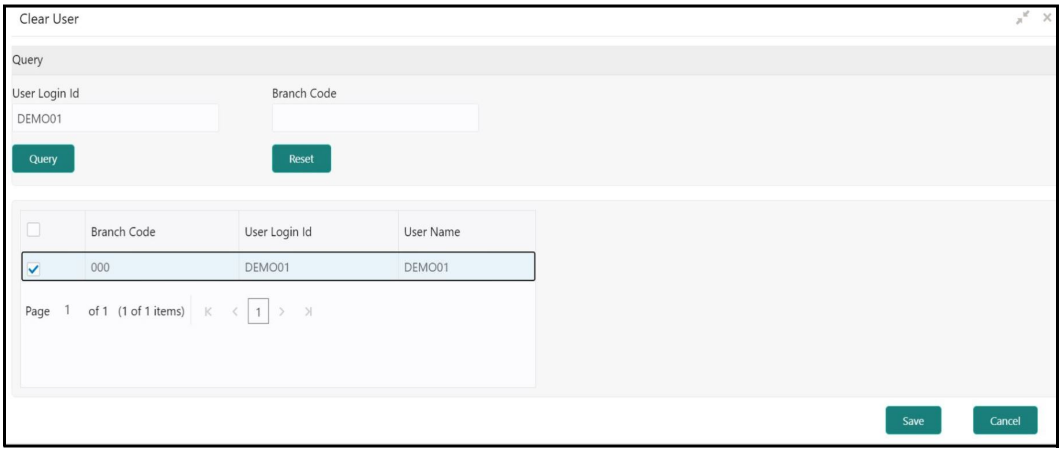
The **Clear User** screen allows you to clear off the current users. To process this screen, perform the following steps:

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 1.5: Clear User



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 1.5: Clear User.

Table 1.5: 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**.

1.3 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 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.
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.

2. Error Codes and Messages

This section contains 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 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.
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

Error Code	Messages
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-URB-001	Duplicate records present under User Role Branches for Branch code $1 and Role code $2
ST-SAVE-027	Request Successfully Processed

3. Glossary

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.

4. Index

C

Clear User 8
Create Role 3
Create User 5

F

Functional Activity 9

R

Role 2

U

User 4

V

View Role 2
View User 4

5. Reference and Feedback

This chapter includes following sections:

- 5.1 References
- 5.2 Documentation Accessibility
- 5.3 Feedback and Support

5.1 References

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

5.2 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.

5.3 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.