Oracle® Banking Microservices Architecture

Oracle Banking Security Management System User Guide

Release 14.6.0.0.0
F59278-01
May 2022

Oracle Banking Microservices Architecture Oracle Banking Security Management System User Guide, Release 14.6.0.0.0

F59278-01

Copyright © 2018, 2022, Oracle and/or its affiliates.

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.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. 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 fail-safe, 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.

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Purpose iv
Audience iv
Acronyms and Abbreviations iv
List of Topics iv
Related Documents iv

1 Role

1.1 Create Role 1-1
1.2 View Role 1-2

2 User

2.1 Create User 2-1
2.2 View User 2-4
2.3 Clear User 2-5

A Error Codes and Messages

B Functional Activity

Index

Preface

Purpose

This guide provides an overview to the module and takes through the various steps involved 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.

Acronyms and Abbreviations

The list of the acronyms and abbreviations that are used in this guide are as follows:

Table 1 Acronyms and Abbreviations

Abbreviation	Description
SMS	Security Management System

List of Topics

This guide is organized as follows:

Table 2 List of Topics

Topics	Description
Role	This topic provides the information about creating and viewing the configured roles.
User	This topic provides the information about creating and viewing the configured users.
Error Codes and Messages	This topic provides the information about error codes and messages.
Functional Activity	This topic provides the information about functional activity.

Related Documents

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

- Oracle Banking Getting Started User Guide

- Oracle Banking Common Core User Guide

1 Role

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

The users who works in the same department at the same level of hierarchy need to have similar user profiles. In such cases, the user 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 giving the user access rights to all the functional activities in the Role Profile.

The roles defined is effective only after the dual authorization.

1.1 Create Role

This topic provides the systematic instructions to create role.

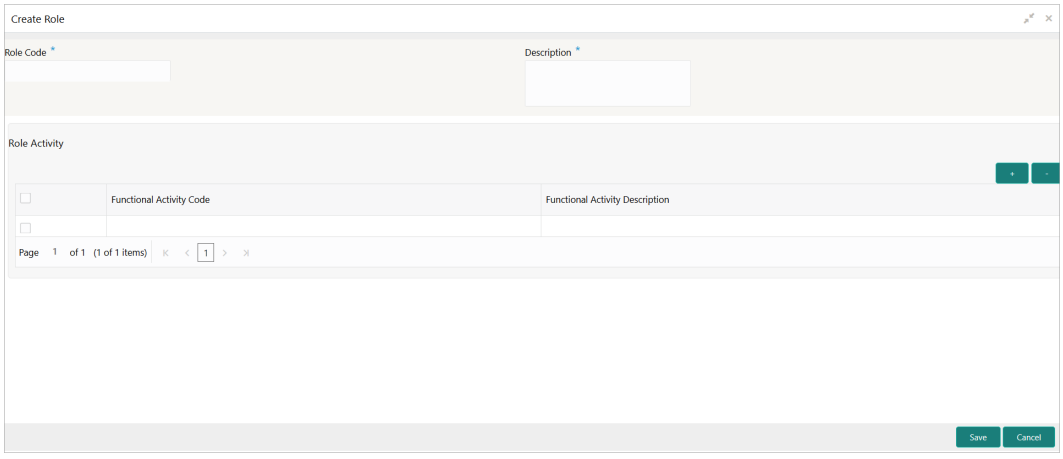
Specify **User ID** and **Password**, and login **Home** screen.

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 1-1 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 1-1 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.
Functional Activity Code	Click the **Search** icon and select the function activity code from the list.
Functional Activity Description	Specify the description about the selected function activity code.

4. Click **+** button 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.

5. Click **Save** to save the details.

   The user can view the configured roles in the View Role.

1.2 View Role

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

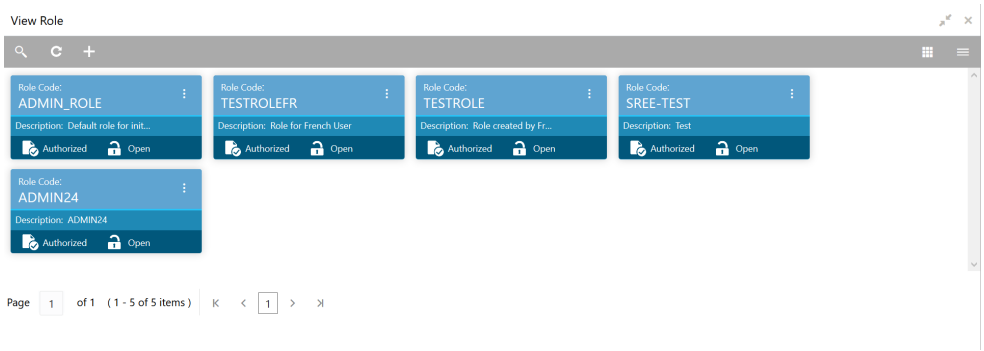
Specify **User ID** and **Password**, and login **Home** screen.

The user can configure the role using the Create Role 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 1-2 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.
Authorization Status	Displays the authorization status of the configured role. The available options are: • Authorized • Unauthorized
Record Status	Displays the record status of the configured role. The available options are: • Open • Close

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.

2.1 Create User

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

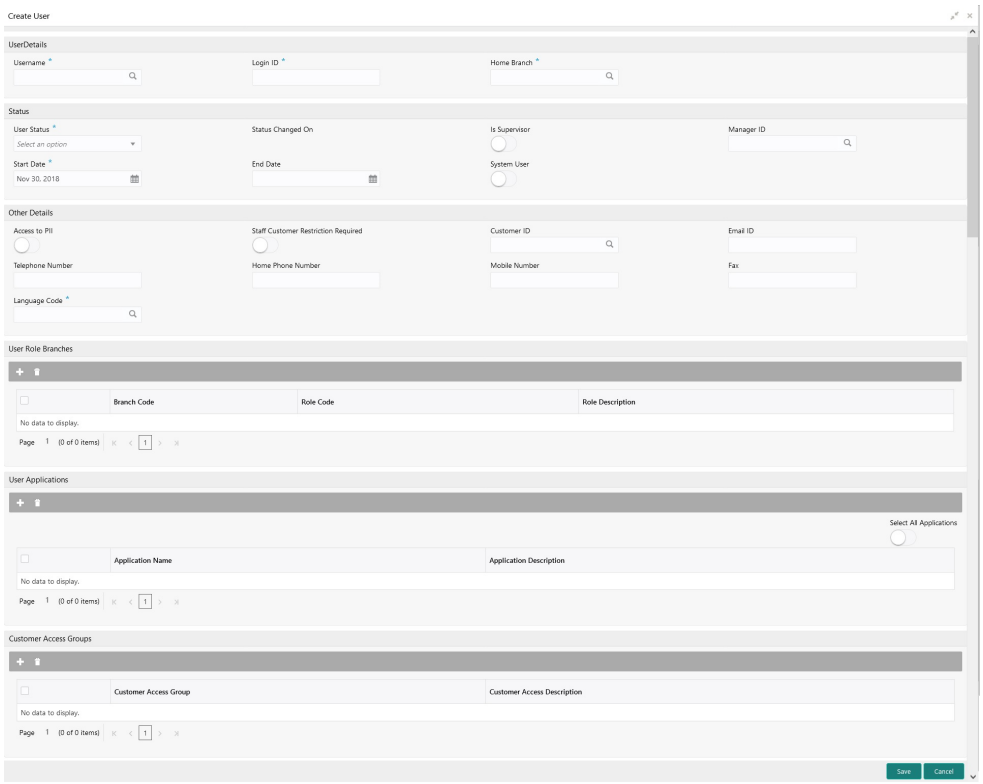
Specify **User ID** and **Password**, and login **Home** screen.

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 2-1 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 2-1 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.

Table 2-1 (Cont.) Create User - Field Description

Field	Description
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.
End Date	Select the end date till when the user is valid.
Other Details	Specify the other details.
Access to PII	Select the toggle to enable the user to access the Personal Identifiable Information of the entity. By default, this option is disabled.
Staff Customer Restriction Required	Select the toggle to enable the staff customer restriction. By default, this option is disabled.
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** to save the details.

   The user can view the configured users in the View User.

> **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 topic.

2.2 View User

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

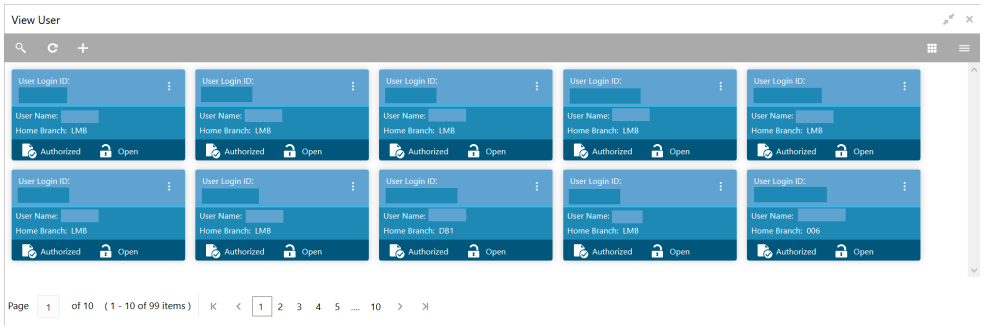
Specify **User ID** and **Password**, and login **Home** screen.

The user can configure the user using the Create User 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 2-2 View User



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

Table 2-2 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 • Unauthorized
Record Status	Displays the record status of the configured user. The available options are: • Open • Close

2.3 Clear User

This topic provides the systematic instructions to clear the user.

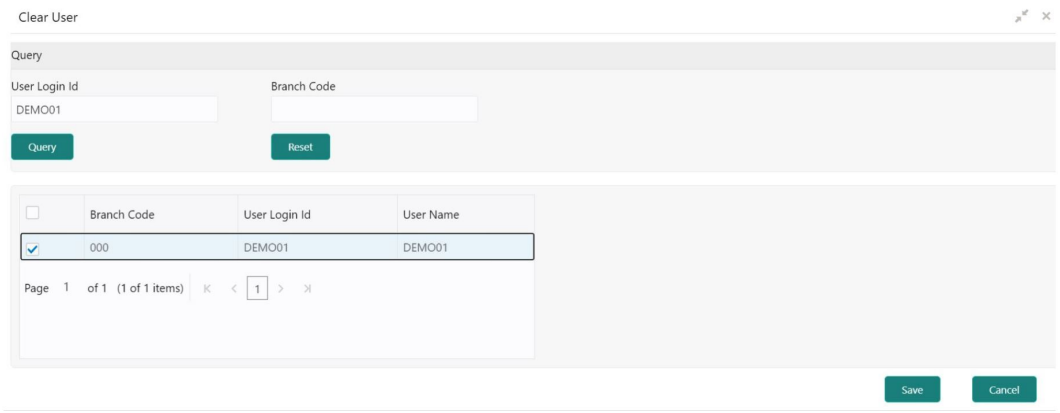
Specify **User ID** and **Password**, and login **Home** screen.

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 2-3 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 2-3 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.

A

Error Codes and Messages

This topic contains the error codes and messages.

Table A-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 A-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.
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-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.

B

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 B-1 Functional Activity

Functional Activity	Description
SMS_FA_LOAN_DASHBO ARD_PREFERENCE	Functional activity for reading User Dashboard preference.
SMS_FA_LOAN_DASHBO ARD_PREFERENCE_PUT	Functional activity for updating User Dashboard preference.
SMS_FA_LOAN_DASHBO ARD_VIEW	Functional activity for reading User Dashboard tiles.
SMS_FA_MENU_DASHBO ARD_VIEW	Functional activity for constructing menu.
SMS_FA_ROLE_AMEND	Functional activity for modifying a role record.
SMS_FA_ROLE_AUTHORI ZE	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_AUTHORI ZE	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.

Index

C

Clear User, *2-5*
Create Role, *1-1*
Create User, *2-1*

R

Role, *1-1*

U

User, *2-1*

V

View Role, *1-2*
View User, *2-4*