

Security Management System User Guide
Oracle Banking Liquidity Management
Release 14.3.0.0.0

Part No. F18156-01

May 2019

Security Management System User Guide
May 2019
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

www.oracle.com/financialservices/

Copyright © 2018, 2019, 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.

Table of Contents

1. Welcome to Security Management System	1-1
1.1 Role	1-1
1.1.1 <i>Role Summary</i>	1-1
1.1.2 <i>Role Maintenance</i>	1-2
1.2 User	1-2
1.2.1 <i>User Summary</i>	1-3
1.2.2 <i>User Maintenance</i>	1-3
1.3 Functional Activity	1-5
2. Reference and Feedback	2-1
2.1 References	2-1
2.2 Documentation Accessibility	2-1
2.3 Feedback and Support	2-1

1. Welcome to Security Management System

Welcome to the Security Management System (SMS) User Guide. It 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 chapter contains the following sections:

- [Section 1.1, "Role"](#)
- [Section 1.2, "User"](#)
- [Section 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.

1.1.1 Role Summary

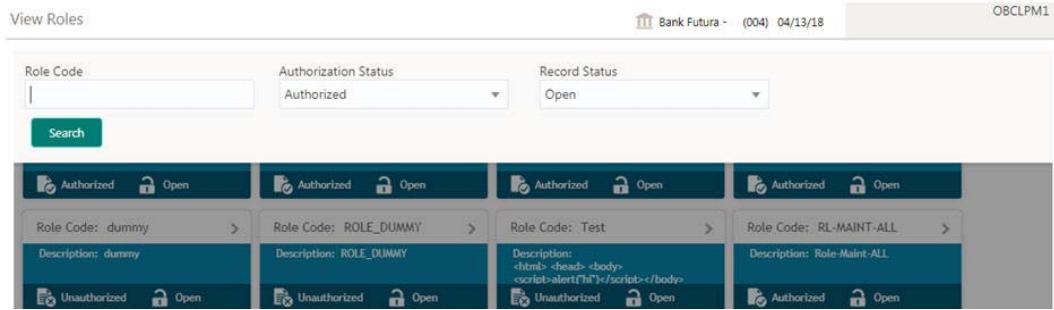
The summary screen provides a list of configured roles. You can configure a role using the Role Maintenance.

How to reach here:

Security Management > View Roles

Role Code: RL_CFPML_CREDITAPP Description: Credit Approver Authorized Open	Role Code: RL_CFPML_CREDITREVIEW Description: Credit Reviewer Authorized Open	Role Code: RL_CFPML_RISKAPP Description: Risk Approver Authorized Open	Role Code: RL_GTEADV_REJECT Description: Role-GTEADV_REJECT Authorized Open
Role Code: ROLE_DUMMY Description: dummy Unauthorized Open	Role Code: Test Description: <html><head><body><script>alert('hi')</script></body></html> Unauthorized Open	Role Code: RL_MAINT_ALL Description: Role-Maint-ALL Authorized Open	Role Code: RL_MAINT_ALL Description: Role-Maint-ALL Authorized Open
Role Code: LOAN_MAKER Description: Actions - View and Create Authorized Open	Role Code: RL_MAINT_AUTH Description: Role-Maint-AUTH Authorized Open	Role Code: TFPML_WFRL_IMPLCISS_SPECIALIST Description: Import I C Insurance Specialist Authorized Open	Role Code: TFPML_WFRL_IMPLCISS_PRO_USER Description: Import I C Insurance Process User Authorized Open
Role Code: TFPML_WFRL_IMPLCISS_MGR_L1 Description: Import I C Insurance Manager 1 Authorized Open	Role Code: TFPML_WFRL_IMPLCISS_MGR_L2 Description: Import I C Insurance Manager 2 Authorized Open	Role Code: TFPML_WFRL_IMPLCISS_MGR_L3 Description: Import I C Insurance Manager 2 Authorized Open	Role Code: RL_WF_ACQUIRE Description: Role-WF_ACQUIRE Authorized Open

Searching a Record



- Click **Search** to query the roles based on the search criteria.

1.1.2 Role Maintenance

The maintenance screen allows you to create roles and assign their activities.

How to reach here:

Security Management > Role Maintenance

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

How to create a role:

- In the **Role Maintenance** screen, click **New** to enable the fields.
- Provide the require details:
 - Role Code: Enter a code for the role.
 - Role Description: Enter additional information about the role.

Role Activity

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 Functional Activity.

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

1.2 User

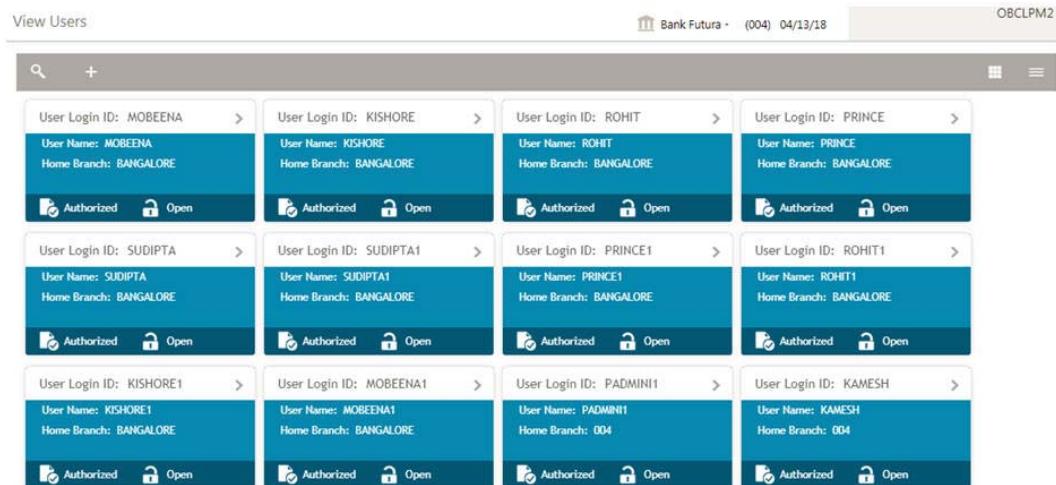
Controlled access to the system is a basic parameter that determines the robustness of the security in banking software. Only authorized users can access the system with the help of a unique User Login ID and password. The user profile of a user contains the details of the user in four sections - User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

1.2.1 User Summary

The summary screen provides a list of configured users. You can configure a user using the User Maintenance.

How to reach here:

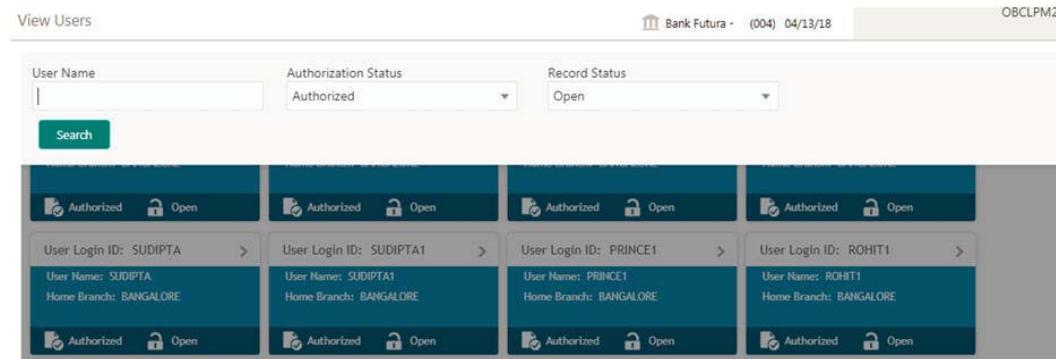
Security Management > View Users



The screenshot shows a grid of user records. Each record card contains the following information:

User Login ID	User Name	Home Branch	Authorization Status	Record Status
MOBEENA	MOBEENA	BANGALORE	Authorized	Open
KISHORE	KISHORE	BANGALORE	Authorized	Open
ROHIT	ROHIT	BANGALORE	Authorized	Open
PRINCE	PRINCE	BANGALORE	Authorized	Open
SUDIPTA	SUDIPTA	BANGALORE	Authorized	Open
SUDIPTA1	SUDIPTA1	BANGALORE	Authorized	Open
PRINCE1	PRINCE1	BANGALORE	Authorized	Open
ROHIT1	ROHIT1	BANGALORE	Authorized	Open
KISHORE1	KISHORE1	BANGALORE	Authorized	Open
MOBEENA1	MOBEENA1	BANGALORE	Authorized	Open
PADMINI1	PADMINI1	004	Authorized	Open
KAMESH	KAMESH	004	Authorized	Open

Searching a Record



The screenshot shows the 'View Users' screen with a search interface. The search fields are:

- User Name:
- Authorization Status:
- Record Status:

Below the search fields is a 'Search' button. The results grid is identical to the one in the previous screenshot, showing the same 12 user records.

- Click **Search** to query the users based on the search criteria.

1.2.2 User Maintenance

The maintenance screen allows you to create a user.

How to reach here:

Security Management > User Maintenance

The screenshot shows the Oracle User Maintenance screen. At the top, there is a toolbar with a 'New' button. Below the toolbar, the 'UserDetail' section is displayed. It includes fields for 'Username' (DBCLPM4), 'Login ID' (DBCLPM4), 'Home Branch' (004), and a 'Status' section with dropdowns for 'User Status' (Enable), 'Status Changed On' (04/11/18), 'Is Supervisor' (On), and 'Manager ID' (ADMINUSER1). The 'Other Details' section contains fields for 'Access to PII' (Off), 'Email ID' (loan.makar@oracle.com), 'Telephone Number' (12345678), 'Home Phone Number' (333 234567), 'Mobile Number' (+919879497892), 'Fax' (758457), 'Theme' (LOAN), and 'Locale' (IND). The 'User Role Branches' section shows a grid with 'Branch Code' (004) and 'Role Code' (LOAN_OPS). At the bottom of the screen, there is a toolbar with a 'Audit' button.

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 record.
Status	Displays the status of the record.

How to create a user:

1. In the **User Maintenance** screen, click **New** to enable the fields.

2. Provide the require details:

User Details

- **Username:** Enter a user name.
- **Login ID:** Enter a 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 **Search** to view and select the required home branch.

Status

- **User Status:** Select a user status from the dropdown list.
- **Status Changed On:** Select a status change date from the dropdown calendar.
- **Is Supervisor:** By default, this option is disabled. If enabled, indicates the user is a supervisor.
- **Manager ID:** Click **Search** to view and select the required manager ID.

- Start Date: Select a start date from which the user is valid from the drop down calendar.
- End Date: Select an end date for the user from the drop down calendar.

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.
- Email: Enter 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: Enter the user contact number.
- Home Phone: Enter the user's home contact number.
- Mobile Number: Enter the user's mobile number.
- Fax: Enter the fax details of the user.
- Theme: Enter the theme details.
- Locale: Enter the locale details.

User Role Branches

3. Click + to add a row and provide the required details in the column:

- Branch Code: Click **Search** to view and select the required branch code.
- Role Code: Click **Search** to view and select the required role code.

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

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.

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

Functional Activity	Description
SMS_FA_APPLICATION_VIEW	Functional activity for Viewing Application.
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
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
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.

2. Reference and Feedback

2.1 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

2.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

2.3 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.