Oracle® Banking Microservices Architecture

Oracle Banking Security Management System Service User Guide

Innovation Release 14.8.1.0.0
G43756-01
October 2025

Oracle Banking Microservices Architecture Oracle Banking Security Management System Service User Guide, Innovation Release 14.8.1.0.0

G43756-01

Contents

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.

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.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to make sure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which user supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that user enter.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

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
FA	Functional Activity
PII	Personally Identifiable Information

Table 1 (Cont.) Acronyms and Abbreviations

Abbreviation	Description
HNI	High Net-Worth Individuals

Basic Actions

Table 2 List of Basic Actions

Action	Description
Approve	Used to approve the initiated record. The **Approve** button displays on the widget after the user clicks **Authorize**.
Audit	Used to view the maker details, checker details, and the record's status.
Authorize	Used to authorize the created or amended record. A maker of the record cannot authorize a record. Only a checker with authorization permissions can.
Close	Used to close a record. This action is available for a record in the Open state.
Confirm	Used to confirm the performed action.
Cancel	Used to cancel the performed action.
Compare	Used to view a comparison of the older field values of a record and the current values. The **Compare** button displays on the widget after the user clicks **Authorize**.
Collapse All	Used to hide all the details in the section. The **Collapse All** button displays after the user clicks **Compare**.
Expand All	Used to expand and view all the details in the section. The **Expand All** button displays after the user clicks **Compare**.
New	Used to add a new record. When the user clicks **Add**, the system displays a **Create Record** screen.
OK	Used to confirm the details in the screen.
Save	Used to save the details entered or modified on the screen.
View	Used to view the record details in a particular modification stage. The **View** button displays on the widget after the user clicks **Authorize**.
View Difference Only	Used to view a comparison through the field element values of old record and the current record, which has undergone changes. The **View Difference Only** button displays after the user clicks **Compare**.
Unlock	Used to unlock and update the details of an existing record. The system displays the record in editable mode.

Symbols and Icons

The following symbols and icons are used in the screens.

Table 3 Symbols and Icons - Common

Symbol/Icon	Function
	Minimize
	Maximize
	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

Table 3 (Cont.) Symbols and Icons - Common

Symbol/Icon	Function
	Navigate to the next record
	Grid view
	List view
	Refresh
	Click this icon to add a new row.
	Click this icon to delete an existing row.
	Click to view the created record.
	Click to modify the fields.
	Click to unlock, delete, authorize or view the created record.

Table 4 Symbols and Icons - Audit Details

Symbol/Icon	Function
	A user
	Date and time
	Unauthorized or Closed status
	Authorized or Open status

Table 5 Symbols and Icons - Widget

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

1 Role

A role refers to a set of permissions, access rights, and functions.

Roles are assigned based on the functions and responsibility of a persona in the bank. For example, users working in the same department and at the same hierarchy level usually have similar roles. In such cases, you can define a role that provides access to all the standard activities of the group of users.

Distinct features of roles are:

- Roles defines what actions and data a user can access in the banking system. For example, viewing customer information, performing transactions, managing accounts, accessing reports, and other functions.
- Each role provides specific permissions or privileges that determine the actions a user can perform. For example, a teller role may have permissions to process transactions. A manager role may have additional permissions to approve transactions and generate reports.
- Roles ensure data security and prevent unauthorized access. By assigning roles with appropriate permissions, banks can ensure that users have access only to the resources necessary for their roles.
- Roles simplify user management by grouping users based on their responsibilities and access needs. Having defined roles makes it easier to onboard new users, update user permissions, and deactivate user access when users change roles or leave the organization.

This topic contains the following subtopics:

- Create Role
  Role creation is the process by which administrators create a role by associating functional activities that identify with the role code and description. This topic provides systematic instructions to create roles and assign their activities.
- View Role
  The View Role page displays the list of roles. Each role record allows you to view, amend, copy, authorize, and delete the role. This topic provides the systematic instructions to view the list of configured roles and perform specific actions on a role record.
- Bulk Upload - Roles
  This topics describes the information to create the sms roles in bulk.

1.1 Create Role

Role creation is the process by which administrators create a role by associating functional activities that identify with the role code and description. This topic provides systematic instructions to create roles and assign their activities.

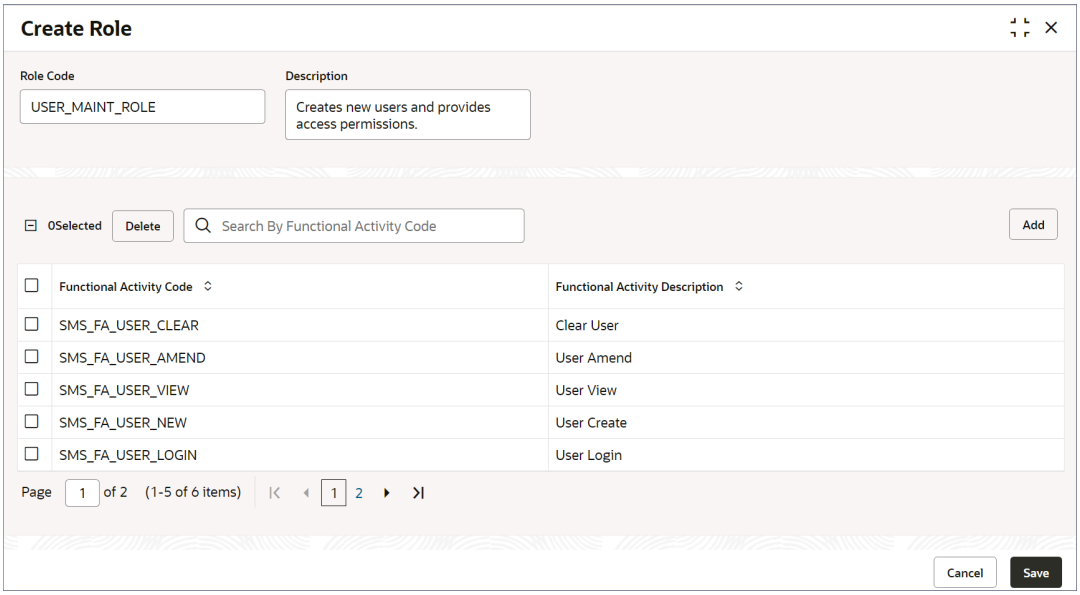
Roles help manage functional responsibility, security, and access control by grouping related permissions and privileges.

1. Click **Security Management**, and 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 marked as **Required** 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 a unique identifier or code assigned to a specific role within the system. The field is mandatory and takes alphanumeric characters and the underscore character . Security administrators create roles that determine the permissions the system grants to the users assigned a role. Administrators use Roles to sort employees or contractors into groups such as Bank Tellers, Loan Officers, underwriters, and Relationship Managers. Based on the functional responsibilities expected of a role, corresponding functional activities (FAs) defined in the system map to the role. For instance, administrators can create a role code BANK_TELLER specifically for individuals who need permission to handle customers' cash and instruments and perform operations like cash deposits and withdrawals. This role would have the relevant functional activity codes mapped to the role.

Table 1-1 (Cont.) Create Role - Field Description

Field	Description
Description	Specify a description of the role. Provide additional details about the role that cover the functions and responsibilities associated with the role. The length of the description is 255 characters.

4. Specify the functional activity codes that map to the functions of the role.
   a. Click **Add** to add a functional activity code

      The **Functional Activity Code** dialog displays.

> **Note**
>
> When a user modifies their role, any functional activity codes already assigned will not appear in the list of available functional activity codes.

Figure 1-2 Function Activity Code

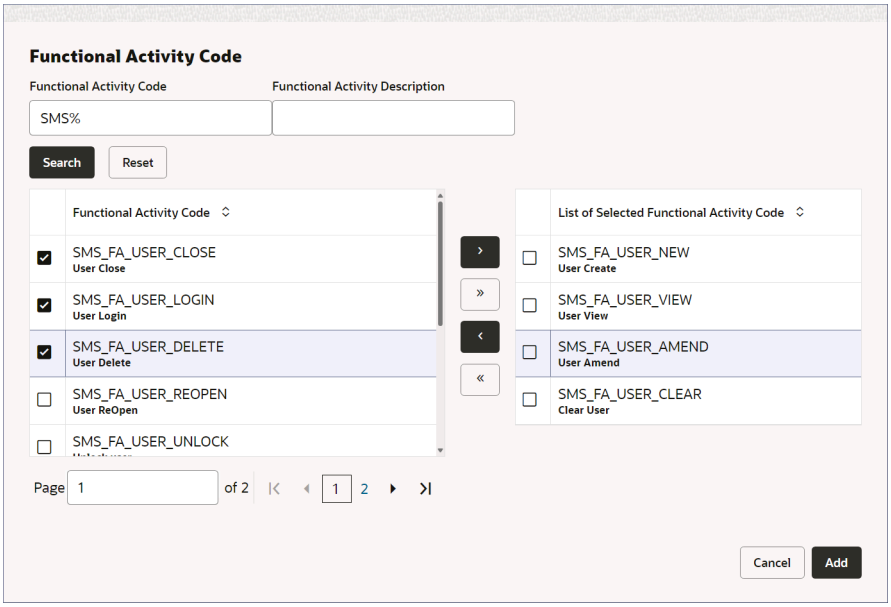


Table 1-2 Add Functional Activity - Field Description

Field	Description
Functional Activity Code	Specify and search for the required functional activity code. Functional Activity Codes indicate the functions in the system that are associated with the role based on the nature, purpose, and characteristics of the role. A Functional Activity Code is an entitlement that allows the user to access a unique system function. Functional activity codes are factory shipped and are available as a list of values for use by system and security administrators. For example, the functional activity code **SMS_FA_USER_NEW** is internally mapped to a code that governs the user creation action. Even if a user has access to the user interface to create users, without access permission to this functional activity code, they cannot create a new user.
Functional Activity Description	Specify a description of the functional activity codes to search.

> **Note**
>
> You can search using either Functional Activity Code, or Functional Activity Description, or both.

b. Scroll the list or search for the required functional activity codes.

> **Note**
>
> Use the **Reset** button to clear the current search terms and provide new ones.

For more information on the required functional activity codes, refer to the product specific user manual for the respective functional activity codes. For SMS related functional activity codes, see Functional Activity Codes.

c. Click to select the required codes in the **Functional Activity Code** column on the left.

d. Click › to add the selected codes to the **List of Selected Functional Activity Code** column on the right.

> **Note**
>
> You can select up to fifty functional activity codes at a time. Use the **>>** button to select all the functional activity codes listed in the left column, up to fifty at a time.

e. Click **Add**.

The **Create Role** page displays the selected functional activity codes.

5. (Optional Step)Verify and complete the set of functional activity codes required for the role.

Add more FA codes required or delete unnecessary FA codes from the list.

> **Note**
>
> Usually, this step is necessary when you amend a Role.

a. Search for the required FA codes or scroll through the list of FA codes.

> **Note**
>
> The search field is case sensitive and filters the FA codes as you type.

b. Clear the search field to get back the full list of FA codes.

c. To add more FA codes, return to **Step 4**.

d. To delete FA codes, proceed to Step 6..

6. Delete the functional activity codes that are not required for the role.

   a. Select the functional activity code(s) you want to delete.

      The number of codes selected display beside the **Delete** button.

   b. Click **Delete**.

7. Click **Save**.

   The **Save** dialog displays.

8. Provide appropriate maker remarks about the role.

9. Click **Confirm**.

   The new role is created.

> **Note**
>
> At this point, the status of the Role is *Unauthorized*. After approval, the status changes to *Authorized*, and the Role is available for use by another process.

10. Approve the Role.

    To approve or reject the Role, see View Role.

> **Note**
>
> As a maker of the Role, you cannot approve it. It has to be approved by another user with appropriate permissions.

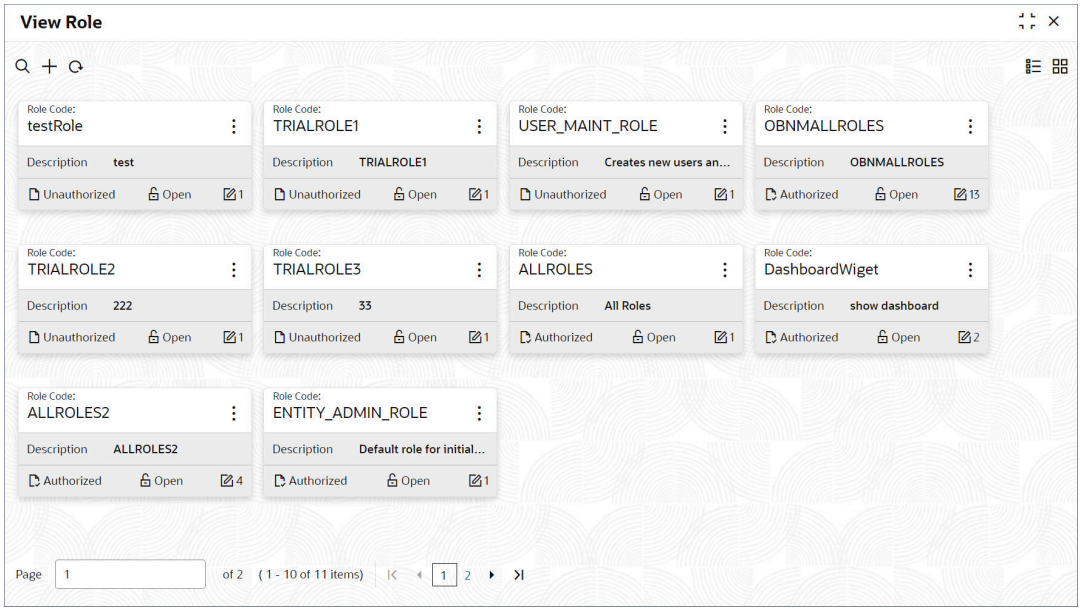
1.2 View Role

The View Role page displays the list of roles. Each role record allows you to view, amend, copy, authorize, and delete the role. This topic provides the systematic instructions to view the list of configured roles and perform specific actions on a role record.

1. Click **Security Management**, and under **Security Management**, click **Role**.
2. Under **Role**, click **Create Role**.

The **View Role** page displays the existing Roles in the Tile view.

Figure 1-3 View Role



Tip

Click ⊞ or ☰ to switch between the **Tile** view and the **List** view.

Note

The fields marked as **Required** are mandatory.

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

Table 1-3 View Role Tile - Field Description

Field	Description
Role Code	Displays the Role code.
Description	Displays additional details about the Role.
Authorization Status	Displays the authorization status of the record. The available options are: • **Authorized** • **Rejected** • **Unauthorized**
Record Status	Displays the status of the record. The available options are: • **Open** • **Closed**

The following table describes the action items in the More Options (⋮) menu on a record and the action items on the page.

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

Table 1-4 Action Items Description

Action Item	Description
Unlock	Unlock a record and make amendments.
Close	Close a record to make it inactive. The record ceases to be available in the system. **Note** A closed record can be reopened to make it active.
View	View the details of a record.
Delete	Delete a record. **Note** Once deleted, the component can no longer be used to define an entity. But entities already defined using the component can continue to use it.
Reopen	Reopen a closed record.
Authorize	Authorize a record to make it active and available to define entities. **Note** Creator of a record cannot authorize the component. Another user with authorize permissions can.
Audit	Select to view the **Maker**, **Checker**, **Status**, and **Modification Number** of a record.
Errors and Overrides	Select to view all existing errors or warnings on the page.

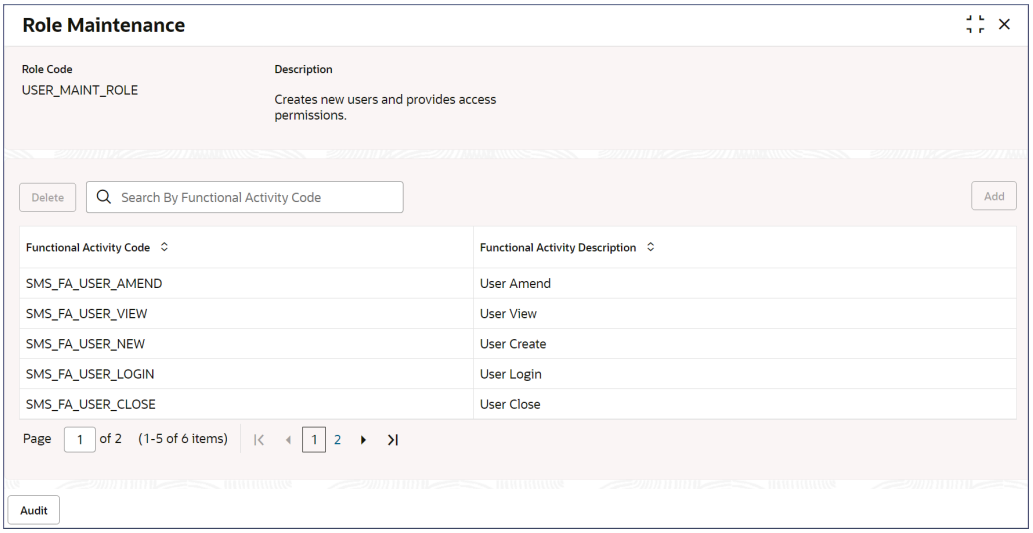
Note

The actions you can perform depend on your role and the record status.

3. View the details of a Role.
   a. Click ⋮ and select **View**.

      The **Role Maintenance** page displays Role details.

Figure 1-4 View Role



> **Note**
>
> To know more about the fields, see Create Role.

b. Click **Audit**.

   The Maker, Checker, Status, and Modification No of the record displays.

4. Unlock and update Role details.

   a. Click ⋮ and select **Unlock**.

      The **Role Maintenance** page displays.

   b. Update the Role details as necessary.

> **Note**
>
> To know more about updating Role details, see Create Role.

5. Approve or Reject an unauthorized Role.

   a. From the Search Filter, search for the required record that is in an **Unauthorized** and **Open** state.

   b. Click ⋮ and select **Authorize**.

      The **View** page displays.

Figure 1-5 Approve the Record

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

Table 1-5 Authorize View

Field Name	Description
Mod Number<N>	Indicates the number of times the record was modified. Where **N** represents the number of modifications. **Note** For a newly created record the modification number is **1**.
Done By	Name of the user who performed the latest modification.
Done On	Date on which the record was modified.
Record Status	The status of the record. **Note** To authorize a record, its status should be **Open**.
Once Auth	Specifies if the record was authorized at least once. **Note** For a newly created record, the value is **No**.
Compare (Button)	Click to compare the modified record with the previous version of the record.

Table 1-5 (Cont.) Authorize View

Field Name	Description
View (Button)	Click to display the record details.

c. Click the check box besides **Mod Number<N>** to select the modified record.

d. Click **Approve** or **Reject**.

The **Confirm** dialog displays.

e. Enter checker remarks and click **Confirm**.

A toast message confirms the successful approval or rejection of the record.

1.3 Bulk Upload - Roles

This topics describes the information to create the sms roles in bulk.

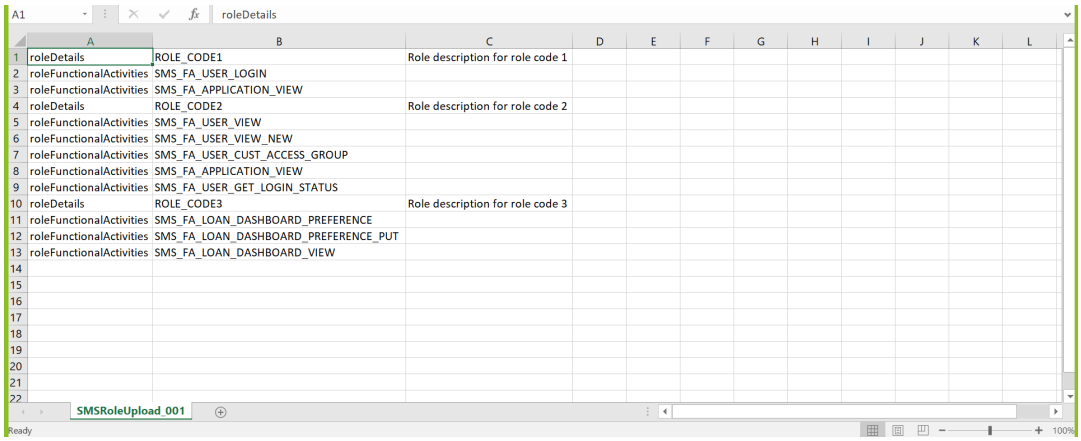
1. Users can create multiple roles by entering the required information in a csv file and uploading it.

> **Note**
>
> **File Type Supported**: CSV

> **Note**
>
> **File Naming Convention** - SMSRoleUpload_<UniqueName>.csv

> **Note**
>
> The fields marked as **Asterisk (*)** are mandatory.

Figure 1-6 Bulk Upload - Roles - Sample



	A	B	C
1	roleDetails	ROLE_CODE1	Role description for role code 1
2	roleFunctionalActivities	SMS_FA_USER_LOGIN	
3	roleFunctionalActivities	SMS_FA_APPLICATION_VIEW	
4	roleDetails	ROLE_CODE2	Role description for role code 2
5	roleFunctionalActivities	SMS_FA_USER_VIEW	
6	roleFunctionalActivities	SMS_FA_USER_VIEW_NEW	
7	roleFunctionalActivities	SMS_FA_USER_CUST_ACCESS_GROUP	
8	roleFunctionalActivities	SMS_FA_APPLICATION_VIEW	
9	roleFunctionalActivities	SMS_FA_USER_GET_LOGIN_STATUS	
10	roleDetails	ROLE_CODE3	Role description for role code 3
11	roleFunctionalActivities	SMS_FA_LOAN_DASHBOARD_PREFERENCE	
12	roleFunctionalActivities	SMS_FA_LOAN_DASHBOARD_PREFERENCE_PUT	
13	roleFunctionalActivities	SMS_FA_LOAN_DASHBOARD_VIEW	

Table 1-6 Bulk Upload - Roles

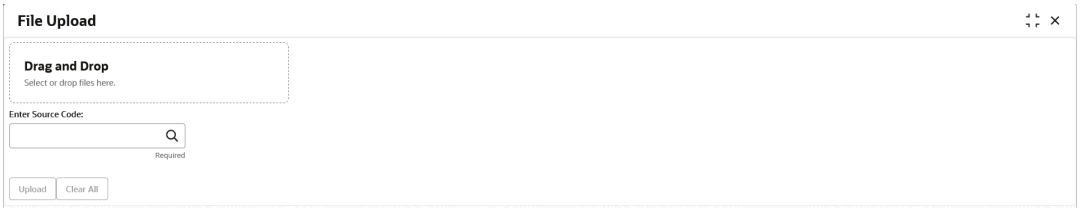
Sequence	Attribute Name	Type	Size	Description
1	Discriminator	String	1	Denotes master record type. Default value is always “RoleDetails”. For example, refer A1 column.
2	Role Code*	String	100	Denotes the unique code for the role. For example, refer B1 column.
3	Description*	String	300	Indicates the description about the role. For example, refer C1 column.
4	Functional Activity Code	String	-	Denotes the necessary activities codes assigned to the role. For example, refer B2 column.

Follow the below steps to upload the file:

2. On **Home** screen, click **File Management**, under **File Management**, click **File Upload**.

   The **File Upload** screen displays.

Figure 1-7



3. Drag and drop or select a role bulk upload csv file.
4. Click **Search** icon and select the source code **SMS_UPLOAD** from the LOV.
5. Click the **Upload** to upload the selected file.

   For more information on **File Upload** screen, refer **File Upload** in the *Oracle Banking Microservices Platform Foundation User Guide*.

   Records created by bulk upload will be in an unauthorized status; users must manually authorize all the records through application.

> **Note**
>
> To authorize all uploaded records automatically, create an **Upload Source** named **SMS_UPLOAD**, enable the **System Authorization Required** toggle, and **authorize** the source.

2
User

Users with access to the banking system perform various tasks, access specific functions, and manage banking operations based on their assigned roles and permissions. This topic describes the maintenance of the user and their access.

Controlled access to the system determines the robustness of security in banking software. Only authorized users can access the system with the help of a unique Login ID and password.

A user profile contains the following details:

- Login Details
- Status Details
- Personal Details
- Role and Branch Details
- User Access to Applications
- Customer Access Groups

This topic contains the following subtopics:

- Create User
  User creation is a process by which administrators add or delete authorized system users. The **Create User** screen allows the administrator to create the user and assign their activities. This topic provides systematic instructions to create a new user.
- View User
  View user displays the list of users in the system. Each user record allows you to view, amend, copy, authorize, and delete the user. This topic provides the systematic instructions to view the list of users and perform specific actions on a user record.
- Bulk Upload - Users
  This topics describes the information to create the sms users in bulk.

2.1 Create User

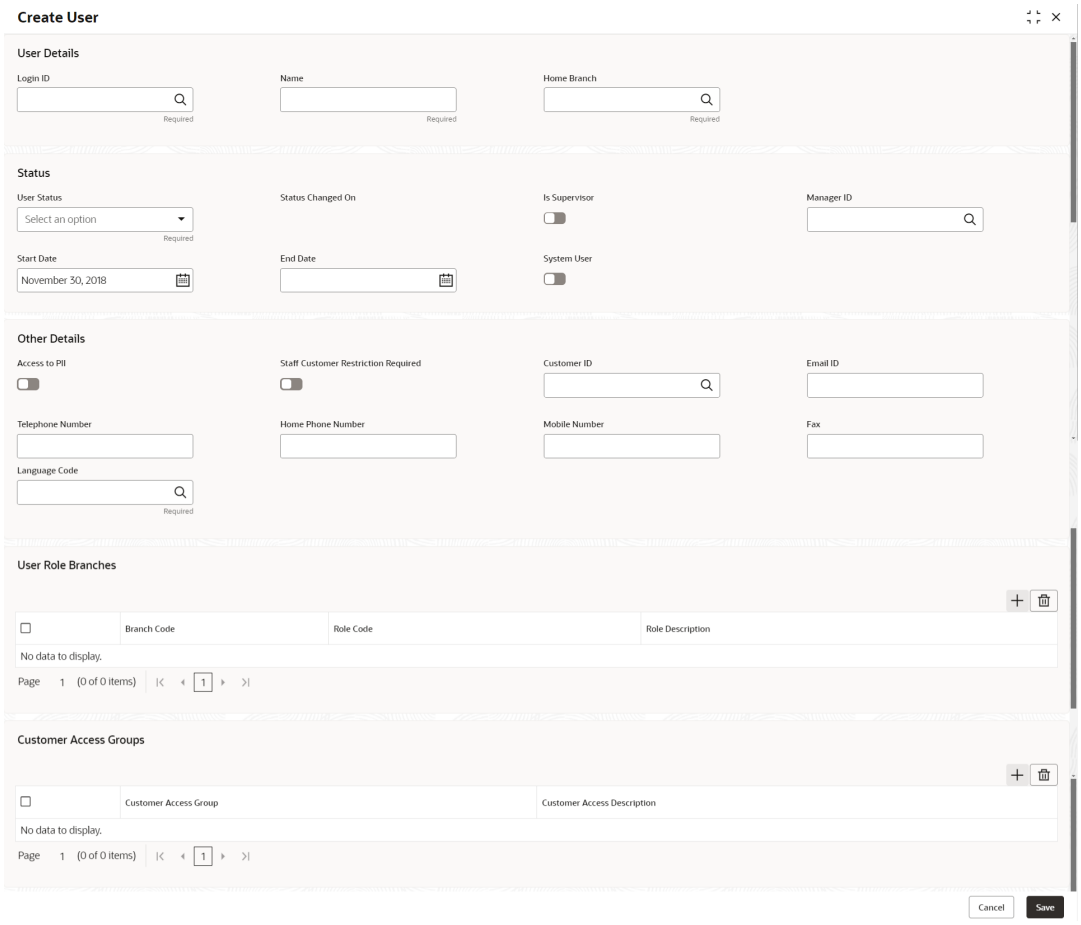
User creation is a process by which administrators add or delete authorized system users. The **Create User** screen allows the administrator to create the user and assign their activities. This topic provides systematic instructions to create a new user.

Administrators can add or delete user groups and edit user profiles. Along with user profiles, administrators can provide various accesses and permissions. For example, access to specific applications, access to Personally Identifiable Information (PII), prevent staff members from viewing each others data, permissions to view data of specific Customer Access Groups like High Net-Worth Individuals (HNIs), and view other sensitive information.

1. Click **Security Management**, and under **Security Management**, click **User**.
2. Under **User**, click **Create User**.

   The **Create User** page displays.

Figure 2-1 Create User



3. Specify the fields in the **User Details** section.

> **Note**
>
> The fields marked as **Required** are mandatory.

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

Table 2-1 User Details - Field Description

Field	Description
Login ID	Specify the unique identification for a user who can use the ID to log in and access the application. The Login ID is unique across all branches. Login ID can have a maximum length of 320 characters. It can contain alphanumeric characters with only capital letters, the Hyphen, @, dot, and Underscore characters. The login ID applies across the domain as a checker or maker ID. For example, JOE_SMITH. **Note** You can configure the minimum length of the Login ID in the Common Core.
Name	Specify the name of the user. The user name can contain less than or equal to 100 characters. For example, Joe Smith. **Note** Username can be specified in any language.
Home Branch	Select the user's home branch from the list of values. The home branch is the default branch of the user when he logs into the system. **Note** The branch configurations are defined in the common core. For more information, see **External Branch Parameters** in the *Common Core User Guide*.

4. Specify the fields in the **Status** section described in the following table.

Note

The fields marked as **Required** are mandatory.

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

Table 2-2 Status - Field Description

Field	Description
User Status	Select the state of the user account from the list of values. • **Enable** - Select this state for active users. • **Disable** - Select this state for inactive users. Inactive users cannot log in to the system.

Table 2-2 (Cont.) Status - Field Description

Field	Description
Status Changed On	Displays the date when the new user is created. Displays the date when any changes to the user's status is made by the user maintenance batch. The user maintenance batch disables the user when the user validity expires. The field is auto-populated by the system.
Is Supervisor	Turn this option **On** to specify the user as a manager. By default, this option is disabled.
Manager ID	Specify the User ID of the user's manager.
Start Date	Specify the start date when the user is enabled. Before this date, the user is inactive and cannot log in to the system.
End Date	Specify the end date when the user validity expires. The user cannot log in to the system after the end date.
System User	Turn this option **On** to specify that the user is internal. Internal users can be configured to run batch processes.

5. Specify the fields in the **Other Details** section described in the following table.

> **Note**
>
> The fields marked as **Required** are mandatory.

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

Table 2-3 Other Details - Field Description

Field	Description
Access to PII	Turn this option **On** to allow the user to access the Personal Identifiable Information of entities in the banking system. By default, this option is disabled and all personal customer information is masked. For example, if a user has the PII flag enabled, then the user can view the personal information of the customer in the party system.
Staff Customer Restriction Required	Turn this option **On** to indicate that this user is restricted from accessing records of other staff customer data. Users with restricted access cannot view or modify the account details of other staff members and cannot perform transactions on their accounts. By default, this option is disabled. **Note** If staff customer restrictions are enabled in the respective domains or modules like Accounts, Loans, Deposits, and others then these users are restricted from accessing other staff customer records.

Table 2-3 (Cont.) Other Details - Field Description

Field	Description
Customer ID	Specify the Customer ID of the user from the list of values. This is required if the **Staff Customer Restriction Required** flag is enabled. **Note** External Customers are configured in the Common Core. For more information, see **External Customer** in **Common Core User Guide**.
Email ID	Specify the Email ID of the user. For example, **joe.good@xyz.com**.
Telephone Number	Specify the user's telephone contact number. Prefix the country code to the telephone number. For example, **+15555555555**.
Home Phone Number	Specify the user's home contact number. Prefix the country code to the telephone number. For example, **+15555555555**.
Mobile Number	Specify the user's mobile number. Prefix the country code to the mobile number. For example, **+14545454545**.
Fax	Specify the user's fax number. Prefix the country code to the Fax number. For example, **+12342342322**.
Language Code	Specify the language code of the user's preferred language from the list of values. The user interface of the application is presented in the preferred language. **Note** Language codes are defined in the common core configuration. For more information, see **Language Code** in the *Common Core User Guide*.

6. Specify the user's role-branch combination in the **User Role Branches** section.

   Access to the user is allocated based on the role of the user in a branch. For example, a user can be assigned the BANK_TELLER role in the branch B01 and the ACCOUNT_OFFICER role in the branch B02.

   a. Click **+** in the **User Role Branches** section.

      A new blank row displays.

   b. Specify the column values described in the following table.

      Note

      The fields marked as **Required** are mandatory.

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

Table 2-4 User Role Branches - Column Description

Field	Description
Branch Code	Specify the branch code to allocate access permissions for the user from the list of values. **Note** Branch configurations are performed in the common core. For more information, see **External Branch Parameters** in the *Common Core User Guide*.
Role Code	Select the role code to allocate access permissions for this user from the list of values. The Role screen specifies the role code that maps functional activity codes to access permissions during role creation. **Note** For more information on roles, see Role.
Role Description	Displays the description about the role, based on the selected role code.

7. Specify the customer segments or groups the user can interact with the **Customer Access Groups** section.
   a. Click **+** in the **Customer Access Groups** section.

      A new blank row displays.
   b. Specify the column values described in the following table.

      Note

      The fields marked as **Required** are mandatory.

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

Table 2-5 Customer Access Groups - Column Description

Field	Description
Customer Access Group	Specify the customer access groups from the list of values the user can access subject to such restrictions at the product processor level. Customer Access Groups are organized based on criteria such as customer segments, account types, product holdings, geographical regions, and additional factors that define customer relationships and profiles. For example, high net-worth individuals. **Note** The actual access to the Customer Access Groups is based on the access restrictions implemented by the respective domains like Accounts, Deposits and others. This field can be used by the domains as an indicator to provide or deny access to the specified customer access groups. **Note** Customer Access Groups are configured in the Common Core. For more information, see **Customer Access Group** in the *Common Core User Guide*.
Customer Access Description	Displays additional information of the selected customer access group.

c. Repeat the above steps to add more Customer Access Groups.

8. Click **Save**.

   The **Save** dialog displays.

9. Provide appropriate maker remarks about the user.

10. Click **Confirm**.

    The new User is created.

> **Note**
>
> At this point, the status of the User is *Unauthorized*. After approval, the status changes to *Authorized*, and the User is available in the system.

11. Approve the User.

    To approve or reject the User, see View Role.

> **Note**
>
> As a maker of the Role, you cannot approve it. It has to be approved by another user with appropriate permissions.

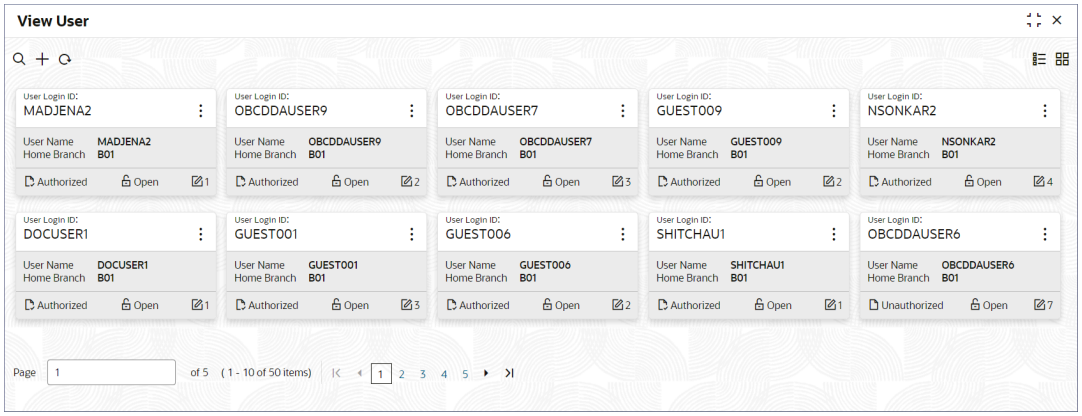
2.2 View User

View user displays the list of users in the system. Each user record allows you to view, amend, copy, authorize, and delete the user. This topic provides the systematic instructions to view the list of users and perform specific actions on a user record.

1. Click **Security Management**, and under **Security Management**, click **User**.
2. Under **User**, click **View User**.

   The **View User** page displays the existing Users in the Tile view.

Figure 2-2 View User



> **Tip**
>
> Click ⊞ or ☰ to switch between the **Tile** view and the **List** view.

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

Table 2-6 View Role Tile - 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 record. The available options are: • **Authorized** • **Rejected** • **Unauthorized**
Record Status	Displays the status of the record. The available options are: • **Open** • **Closed**

The following table describes the action items in the More Options (⋮) menu on the record and the action items on the page.

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

Table 2-7 Action Items Description

Action Item	Description
Unlock	Unlock a record and make amendments.
Close	Close a record to make it inactive. The record ceases to be available in the system. **Note** A closed record can be reopened to make it active.
View	View the details of a record.
Delete	Delete a record. **Note** Once deleted, the component can no longer be used to define an entity. But entities already defined using the component can continue to use it.
Reopen	Reopen a closed record.
Authorize	Authorize a record to make it active and available to define entities. **Note** Creator of a record cannot authorize the component. Another user with authorize permissions can.
Audit	Select to view the **Maker**, **Checker**, **Status**, and **Modification Number** of a record.
Errors and Overrides	Select to view all existing errors or warnings on the page.

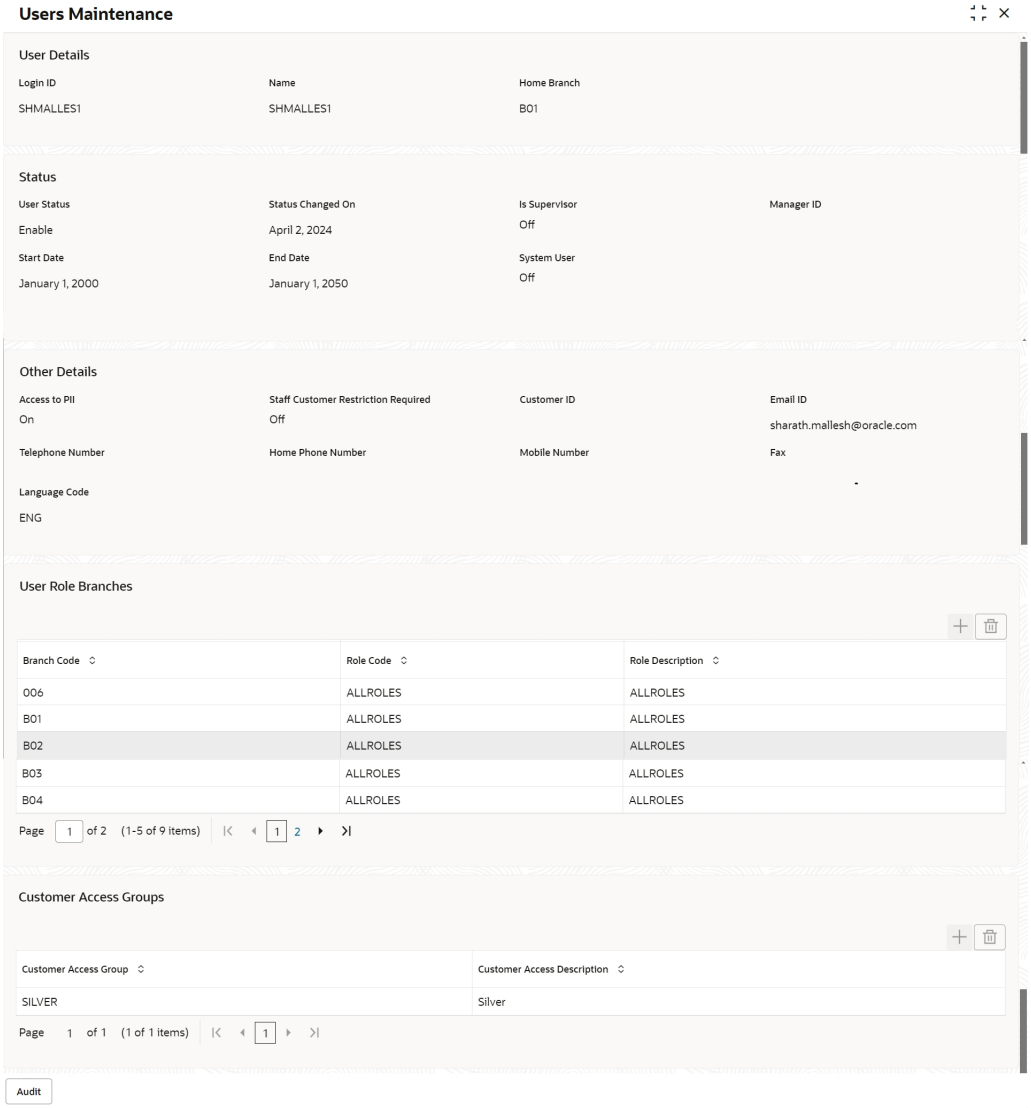
Note

The actions you can perform depend on your role and the record status.

3. View the details of a User.
   a. Click ⋮ and select **View**.

      The **Users Maintenance** page displays Role details.

Figure 2-3 View User



> **Note**
>
> To know more about the fields, see Create User.

b. Click **Audit**.

   The Maker, Checker, Status, and Modification No of the record displays.

4. Unlock and update the User details.

   a. Click ⋮ and select **Unlock**.

      The **Users Maintenance** page displays.

   b. Update the User details as necessary.

> **Note**
>
> To know more about updating Role details, see Create User.

5. Approve or Reject an unauthorized User.
   a. From the Search Filter, search for the required record that is in an **Unauthorized** and **Open** state.
   b. Click ⋮ and select **Authorize**.

      The **View** page displays.

Figure 2-4 Approve the Record

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

Table 2-8 Authorize View

Field Name	Description
Mod Number<N>	Indicates the number of times the record was modified. Where **N** represents the number of modifications. **Note** For a newly created record the modification number is **1**.
Done By	Name of the user who performed the latest modification.
Done On	Date on which the record was modified.

Table 2-8 (Cont.) Authorize View

Field Name	Description
Record Status	The status of the record. **Note** To authorize a record, its status should be **Open**.
Once Auth	Specifies if the record was authorized at least once. **Note** For a newly created record, the value is **No**.
Compare (Button)	Click to compare the modified record with the previous version of the record.
View (Button)	Click to display the record details.

c. Click the check box besides **Mod Number<N>** to select the modified record.

d. Click **Approve** or **Reject**.

The **Confirm** dialog displays.

e. Enter any remarks and click **Confirm**.

A toast message confirms the successful approval or rejection of the record.

2.3 Bulk Upload - Users

This topics describes the information to create the sms users in bulk.

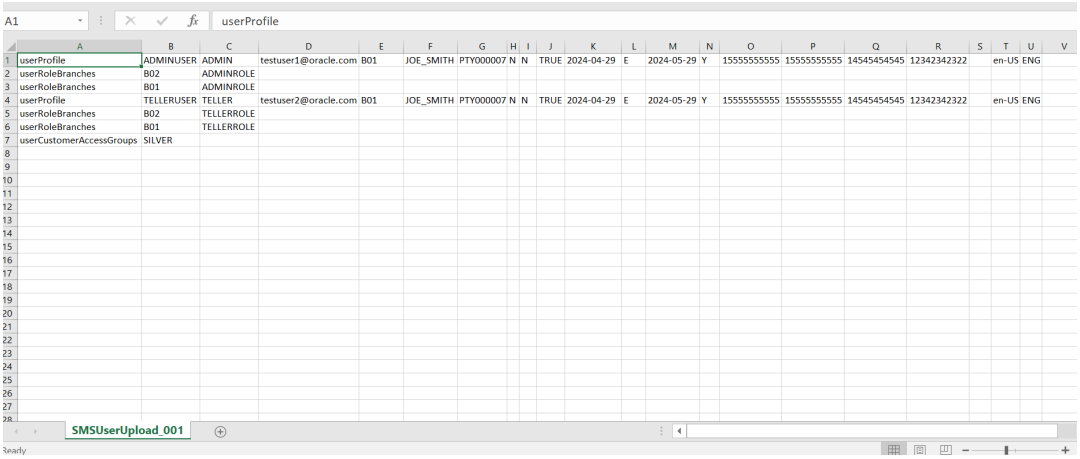
1. Users can create multiple user by entering the required information in a csv file and uploading it.

> **Note**
>
> **File Type Supported**: CSV

> **Note**
>
> **File Naming Convention** - SMSUserUpload_<UniqueName>.csv

> **Note**
>
> The fields marked as **Asterisk (*)** are mandatory.

Figure 2-5 Bulk Upload - Users - Sample



1	userProfile	ADMINUSER	ADMIN	testuser1@oracle.com	B01	JOE_SMITH	PTY000007	N	N	TRUE	2024-04-29	E	2024-05-29	Y	15555555555	15555555555	14545454545	12342342322		en-US	ENG			
2	userRoleBranches	B02	ADMINROLE																					
3	userRoleBranches	B01	ADMINROLE																					
4	userProfile	TELLERUSER	TELLER	testuser2@oracle.com	B01	JOE_SMITH	PTY000007	N	N	TRUE	2024-04-29	E	2024-05-29	Y	15555555555	15555555555	14545454545	12342342322		en-US	ENG			
5	userRoleBranches	B02	TELLERROLE																					
6	userRoleBranches	B01	TELLERROLE																					
7	userCustomerAccessGroups	SILVER																						

Table 2-9 Bulk Upload - Users - Records

Sequence	Attribute Name	Type	Size	Description
1	Discriminator	String	1	Denotes master record type. Default value is always “UserProfile”. For example, refer A1 column.
2	Login ID*	String	320	Denotes login ID with which a user logs into the system. For example, refer B1 column.
3	Name*	String	100	Name of the user. For example, refer C1 column.
4	Email*	String	320	Email of the user. For example, refer D1 column.
5	Home Branch*	String	6	Indicates the home branch. For example, refer E1 column.
6	Manager ID	String	320	Denotes the manager. For example, refer F1 column.
7	Customer Number*	String	20	Number for the customer. For example, refer G1 column.
8	System User	String	1	Indicates the toggle to enable this feature. For example, refer H1 column.
9	Is Supervisor	String	1	Indicates the toggle to indicate whether the user is a supervisor or not. For example, refer I1 column.
10	PII	String	1	Indicates the toggle to enable the user to access the Personal Identifiable Information of the entity. For example, refer J1 column.
11	Start Date	Date	-	Indicates the start date. The format will be in yyyy-mm-dd. For example, refer K1 column.
12	User Status*	String	1	Indicates the user status. For example, refer L1 column.

Table 2-9 (Cont.) Bulk Upload - Users - Records

Sequence	Attribute Name	Type	Size	Description
13	End Date	Date	-	Indicates the end date. The format will be in yyyy-mm-dd. For example, refer M1 column.
14	Staff Acc Restriction	String	1	Indicates the toggle to enable the staff customer restriction. For example, refer N1 column.
15	Telephone Number	String	50	Denotes the user contact number. For example, refer O1 column.
16	Home Number	String	50	Denotes the user home contact number. For example, refer P1 column.
17	Mobile Number	String	50	Denotes the user mobile number. For example, refer Q1 column.
18	Fax	String	50	Denotes the fax details of the user. For example, refer R1 column.
19	Theme	String	100	Denotes the theme for the user. For example, refer S1 column.
20	Locale	String	10	Indicates locality of the user. For example, refer T1 column.
21	Language Code*	String	3	Denotes the language code. For example, refer U1 column.

Table 2-10 Bulk Upload - Users - Child Records 1

Sequence	Attribute Name	Type	Size	Description
1	Discriminator	String	1	Denotes child record type. Default value is always “UserProfile”. For example, refer A2 column.
2	Branch Code*	String	6	Denotes the branch code. For example, refer B2 column.
3	Role Code*	String	100	Denotes the role code. For example, refer C2 column.

Table 2-11 Bulk Upload - Users - Child Records 2

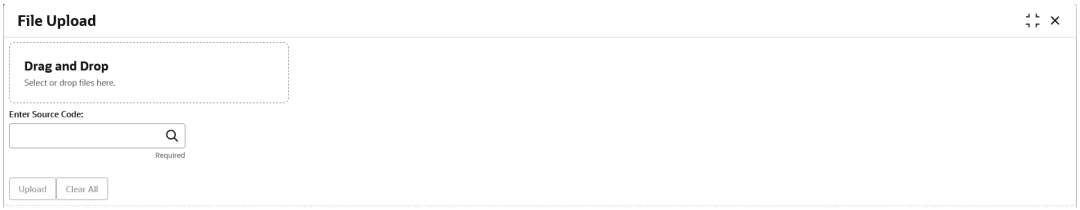
Sequence	Attribute Name	Type	Size	Description
1	Discriminator	String	1	Denotes child record type. Default value is always “UserProfile”. For example, refer A7 column.
2	Customer Access Groups*	String	100	Denotes the customer access group details. For example, refer B7 column.

Follow the below steps to upload the file:

2. On **Homescreen**, click **File Management**, under **File Management**, click **File Upload**

   The **File Upload** screen displays.

Figure 2-6



3. Drag and drop or select a user bulk upload csv file.
4. Click **Search** icon and select the source code **SMS_UPLOAD** from the LOV.
5. Click the **Upload** to upload the selected file.

   For more information on **File Upload** screen, refer **File Upload** in the *Oracle Banking Microservices Platform Foundation User Guide*.

   Records created by bulk upload will be in an unauthorized status; users must manually authorize all the records through application.

> **Note**
>
> To authorize all uploaded records automatically, create an **Upload Source** named **SMS_UPLOAD**, enable the **System Authorization Required** toggle, and **authorize** the source.

3
Group Role Mapping

Groups are responsible for authorization in OCI. With Group Role Mapping, user can map IAM groups with existing SMS Roles and Branch, so it can authorize user in SMS.

This topic contains the following subtopics:

- Create Group Role Mapping
  This topic provides the systematic instructions to create the group role mapping and perform specific actions on a record.
- View Group Role Mapping
  View Group Role Mapping displays the list of group role mapped in the system. Each record allows you to view, amend, copy, authorize, and delete the group role mapped. This topic provides the systematic instructions to view the list of group role mapped and perform specific actions on a record.

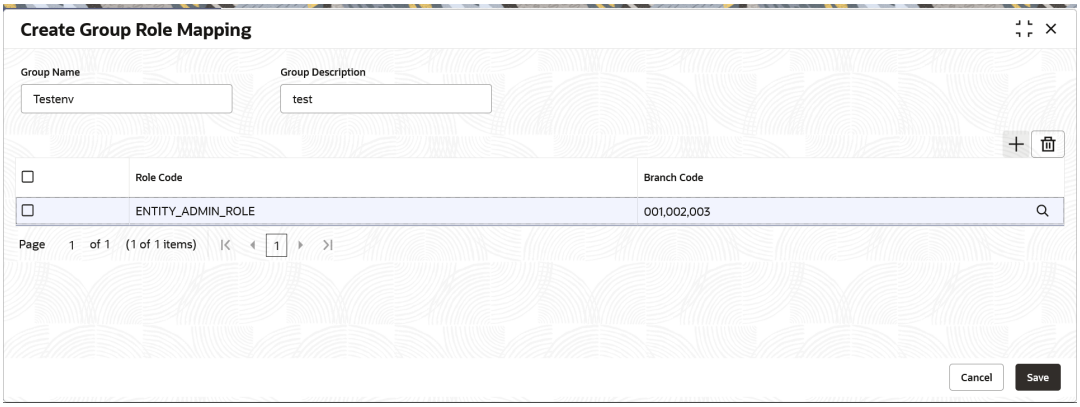
3.1 Create Group Role Mapping

This topic provides the systematic instructions to create the group role mapping and perform specific actions on a record.

1. Click **Security Management**, and under **Security Management**, click **Group Role Mapping**.
2. Under **Group Role Mapping**, click **Create Group Role Mapping**.

   The **Create Group Role Mapping** screen is displayed.

Figure 3-1 Create Group Role Mapping



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

> **Note**
>
> The fields marked as **Required** are mandatory.

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

Table 3-1 Create Group Role Mapping - Field Description

Field	Description
Group Name	Specify the name of the group. The field is mandatory and takes alphanumeric characters and the underscore character.
Group Description	Specify the description for the group.
Role Code	Select the role code that group should be associated with.
Branch Code	Select the branch code(s) that group should be associated with.

a. Click **+** to add Branch Code, and Role Code for Group Role Mapping.

   A new blank row displays.

b. Click the search icon under **Role Code** column.

   The **Role Code** popup is displayed.
   Click **Fetch** and select the desired role code that group should be associated with.

c. Click the search icon under **Branch Code** column.

   The **Branch Selection** popup screen.
   Click **Search** and select the desired branch code(s).

   Click **>** to select the branch code(s) from the list that group should be associated with.

   Click **Add** to add the selected branch code(s).

4. Click **Save**.

   The **Save** dialog displays.

5. Provide appropriate maker remark.

6. Click **Confirm**.

   The new group role mapping is created.

3.2 View Group Role Mapping

View Group Role Mapping displays the list of group role mapped in the system. Each record allows you to view, amend, copy, authorize, and delete the group role mapped. This topic provides the systematic instructions to view the list of group role mapped and perform specific actions on a record.

1. Click **Security Management**, and under **Security Management**, click **Group Role Mapping**.

2. Under **Group Role Mapping**, click **View Group Role Mapping**.

   The **View Group Role Mapping** screen displays the existing Group Role Mapped in the Tile view.

Figure 3-2 View Group Role Mapping

> **Tip**
>
> Click ⊞ or ☰ to switch between the **Tile** view and the **List** view.

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

Table 3-2 View Group Role Mapping - Field Description

Field	Description
Group Name	Displays the name of the group role mapping record.
Group Description	Displays the description for the group role mapping record.
Authorization Status	Displays the authorization status of the record. The available options are: • **Authorized** • **Rejected** • **Unauthorized**
Record Status	Displays the status of the record. The available options are: • **Open** • **Closed**

The following table describes the action items in the More Options (⋮) menu on the record and the action items on the page.

Table 3-3 Action Items Description

Action Item	Description
Unlock	Unlock a record and make amendments.
Close	Close a record to make it inactive. The record ceases to be available in the system. **Note** : A closed record can be reopened to make it active.
View	View the details of a record.

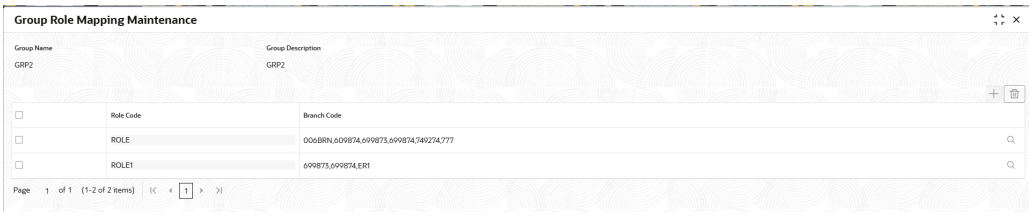
Table 3-3 (Cont.) Action Items Description

Action Item	Description
Delete	Delete a record. **Note**: Once deleted, the component can no longer be used to define an entity. But entities already defined using the component can continue to use it.
Reopen	Reopen a closed record.
Authorize	Authorize a record to make it active and available to define entities. **Note**: Creator of a record cannot authorize the component. Another user with authorize permissions can.
Audit	Select to view the **Maker**, **Checker**, **Status**, and **Modification Number** of a record.
Errors and Overrides	Select to view all existing errors or warnings on the page.

3. View the details of a Group Role Mapping.
   a. Click ⋮ and select **View**.

      The **View Group Role Mapping** screen is displayed with **Audit** details.

Figure 3-3 View Group Role Mapping - Details



> **Note**
>
> To know more about the fields, see Create Group Role Mapping.

   b. Click **Audit**.

      The Maker, Checker, Status, and Modification No of the record displays.

4. Unlock and update the Group Role Mapping details.
   a. Click ⋮ and select **Unlock**.

      The **Group Role Mapping** screen is displayed.

   b. Update the Group Role Mapping details as necessary.

5. Approve or Reject an unauthorized Group Role Mapping.
   a. From the Search Filter, search for the required record that is in an **Unauthorized** and **Open** state.

   b. Click ⋮ and select **Authorize**.

      The **View** screen is displayed.

Figure 3-4 Approve the Record

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

Table 3-4 Authorize View

Field Name	Description
Mod Number<N>	Indicates the number of times the record was modified. Where **N** represents the number of modifications. **Note**: For a newly created record the modification number is **1** .
Done By	Name of the user who performed the latest modification.
Done On	Date on which the record was modified.
Record Status	The status of the record. **Note** To authorize a record, its status should be **Open**.
Once Auth	Specifies if the record was authorized at least once. **Note** For a newly created record, the value is **No**.
Compare (Button)	Click to compare the modified record with the previous version of the record.
View (Button)	Click to display the record details.

c. Click the check box besides **Mod Number<N>** to select the modified record.

d. Click **Approve** or **Reject**.

The **Confirm** dialog displays.

e. Enter any remarks and click **Confirm**.

A toast message confirms the successful approval or rejection of the record.

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.
GCS-MOD-007	Only the maker can modify the pending records.

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

Error Code	Messages
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-008	Invalid RoleCode.
SMS-COM-009	Invalid Role Description.
SMS-COM-010	Only alphanumeric characters, hyphens, underscores, dots and @ are allowed in User Login Id.
SMS-COM-011	User Name should be less than or equal to 100 characters.
SMS-COM-012	Invalid Home Branch.
SMS-COM-017	Start date cannot be less than application date or more than previous start date.
SMS-LOV-001	Invalid Home Branch.
SMS-LOV-004	Invalid Manager Id.
SMS-LOV-005	Not a Valid Email Id format.
SMS-LOV-006	Invalid Branch Code.
SMS-LOV-008	Invalid Role Code.
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 Codes

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 Codes

Screen/API Names	Functional Activity Codes	Action	Description
Role	SMS_FA_ROLE_AMEND	UNLOCK	Functional activity for modifying a role record.
Role	SMS_FA_ROLE_AUTHORIZE	AUTHORIZE	Functional activity for authorizing a role record including Authority query and View changes.
Role	SMS_FA_ROLE_CLOSE	CLOSE	Functional activity for closing a role record.
Role	SMS_FA_ROLE_REOPEN	REOPEN	Functional activity for reopening a role record.
Role	SMS_FA_ROLE_VIEW	VIEW	Functional activity for viewing a role record including role LOV validation.
Role	SMS_FA_ROLE_DELETE	DELETE	Functional activity for deleting a role record.
Role	SMS_FA_ROLE_NEW	NEW	Functional activity for creating a role record.
Role	SMS_FA_GET_ALL_FUNC_ACTIVITIES	VIEW	Functional activity for getting all the functional activities.
User	SMS_FA_USER_AMEND	UNLOCK	Functional activity for modifying a user record.
User	SMS_FA_USER_AUTHORIZE	AUTHORIZE	Functional activity for authorizing a user record including Authority query and View changes.
User	SMS_FA_USER_CLOSE	CLOSE	Functional activity for closing a user record.
User	SMS_FA_USER_DELETE	DELETE	Functional activity for deleting a user record.
User	SMS_FA_USER_NEW	NEW	Functional activity for creating a user record.
User	SMS_FA_USER_REOPEN	REOPEN	Functional activity for reopening a user record.

Table B-1 (Cont.) Functional Activity Codes

Screen/API Names	Functional Activity Codes	Action	Description
User	SMS_FA_USER_VIEW	VIEW	Functional activity for viewing a user record including user LOV validation.
User	SMS_FA_USER_VIEW_NEW	VIEW	Functional activity to validate existing User.
User	SMS_FA_USER_CUST_ACCESS_GROUP	VIEW	Functional activity for maintaining the user customer access group.
User	SMS_FA_APPLICATION_VIEW	VIEW	Functional activity for viewing all the applications.
Clear User	SMS_FA_USER_GET_LOGIN_STATUS	VIEW	Functional activity for getting the login status.
Clear User	SMS_FA_USER_CLEAR	UPDATE	Functional Activity for Clear User.
sms-core-services	SMS_FA_LOAN_DASHBOARD_PREFERENCE	VIEW	Functional activity for reading User Dashboard preference.
sms-core-services	SMS_FA_LOAN_DASHBOARD_PREFERENCE_PUT	UPDATE	Functional activity for updating User Dashboard preference.
sms-core-services	SMS_FA_LOAN_DASHBOARD_VIEW	VIEW	Functional activity for reading User Dashboard tiles.
sms-core-services	SMS_FA_MENU_DASHBOARD_VIEW	VIEW	Functional activity for constructing menu.
sms-core-services	SMS_FA_USER_GET_HIERARCHY	VIEW	Functional activity for getting the user hierarchy.
sms-core-services	SMS_FA_USER_GET_PEER_REPORTEES	VIEW	Functional activity for getting the peer reporters.
sms-core-services	SMS_FA_USER_AUDIT_TRAIL_GET	VIEW	Functional activity for getting the audit trail.
sms-core-services	SMS_FA_USER_GET_USR_FUN_ACT	VIEW	Functional activity for getting the user functional activities.
sms-core-services	SMS_FA_USER_SERVICE_AMEND	UNLOCK	Functional Activity for user amendment using service API.
sms-core-services	SMS_FA_USER_SERVICE_NEW	NEW	Activity for user creation using service API.
sms-core-services	SMS_FA_USER_GET_REPORTEES	VIEW	Functional activity for getting the reportees.
sms-core-services	SMS_FA_GET_ALL_FUNC_ACTIVITIES_SUB	VIEW	Functional activity for getting all the functional activities for subordinates.
sms-core-services	SMS_FA_USER_GET_FILTERED_USERS	VIEW	Functional activity for getting all filtered users.
sms-core-services	SMS_FA_USER_MAINT_BATCH	BATCH	Functional activity for maintaining the user batch.
sms-core-services	PLATO_FA_BATCH_SMS_FUNC	BATCH	Functional activity required to execute the batch processes through SMS.
Login	SMS_FA_USER_LOGIN	LOGIN	Functional activity for logging in the user.

Index