

# Oracle® Banking Microservices Architecture

## Oracle Banking Cloud Services SCIM Setup



Release 14.7.4.0.0

G10565-01

June 2024

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2024, 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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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, MySQL, and NetSuite 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

## 1 User Replication from OCI IAM to SMS Module

### Index

---

# Preface

- [Purpose](#)
- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Conventions](#)
- [Acronyms and Abbreviations](#)

## Purpose

The purpose of this guide is to explain how to set up OCI IAM to OBCS connectivity for user provisioning using OBCS SCIM APIs.

## Audience

This guide is intended for users utilizing Oracle Banking Cloud Services who are responsible for managing the services or wish to develop Oracle Banking Cloud Services.

## 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 customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## 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.

## Conventions

The following text conventions are used in this document:

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

## Acronyms and Abbreviations

**Table** Acronyms and Abbreviations

Abbreviation	Description
IAM	Identity and Access Management
OBCS	Oracle Banking Cloud Services
OCI	Oracle Cloud Infrastructure
SCIM	System for Cross-domain Identity Management
SMS	Security Management System

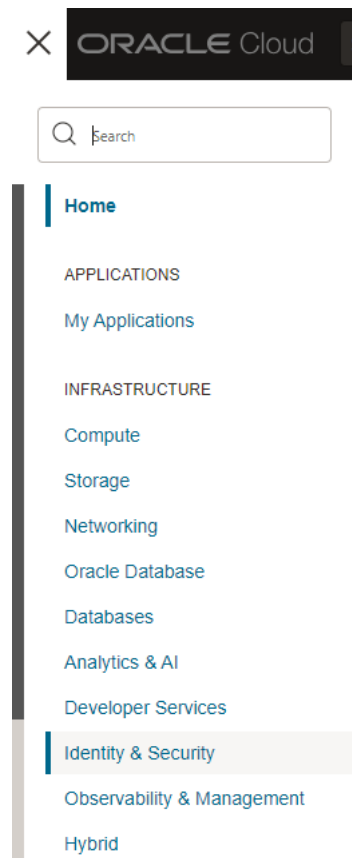
# 1

## User Replication from OCI IAM to SMS Module

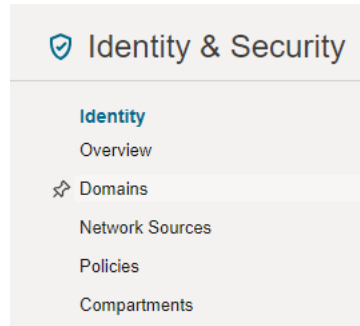
This topic provides the instruction to setup OCI IAM to OBCS connectivity for user provisioning using OBCS SCIM APIs.

1. Log in to your **OCI IAM** tenancy, and select **Identity and Security** from the **Home** menu.

**Figure 1-1 Identity and Security**

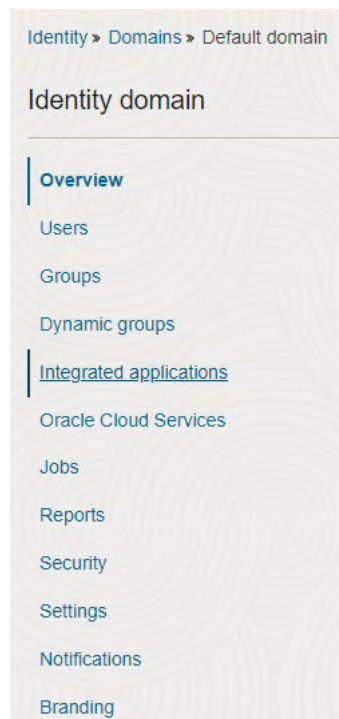


2. From **Identity and Security**, click **Domains**.

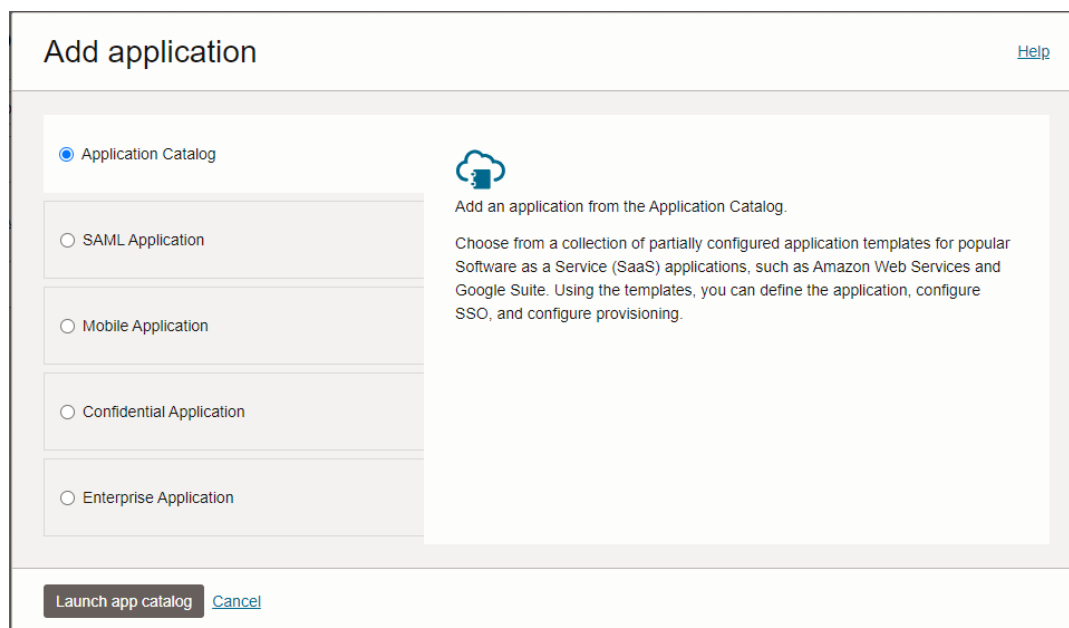
**Figure 1-2 Domains**

3. Click on your Domain name.

The screen below is an illustration using the name **Default Domain** as an example..

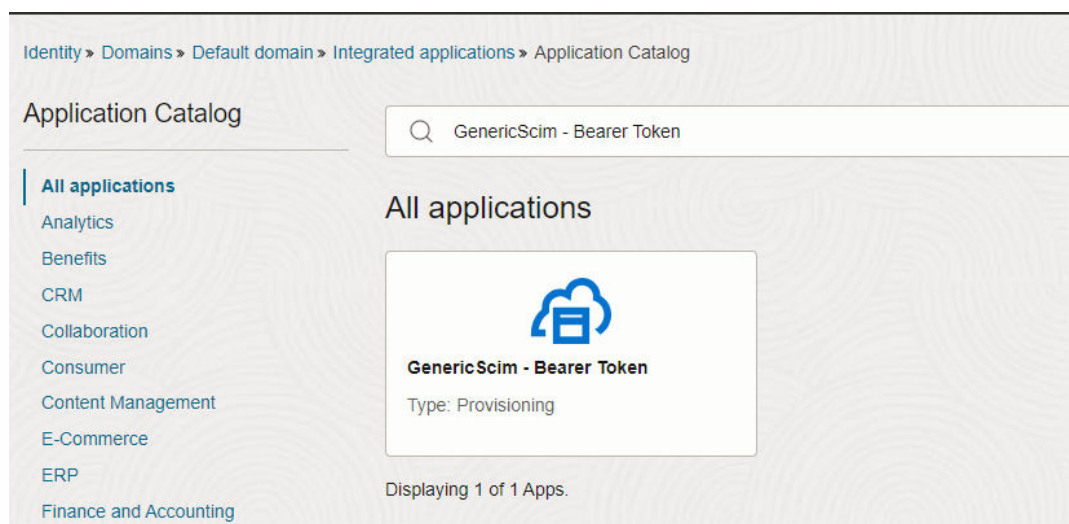
**Figure 1-3 Default Domain**

4. To add an application, click on **Add Application**, then select **Application Catalog**, and click on **Launch app catalog**.

**Figure 1-4 Add Application**

5. In the **Application Catalog** screen, search the application named **GenericScim – Bearer Token** using the search box.

The **GenericScim – Bearer Token** is displayed in the **Application Catalog** screen.

**Figure 1-5 Application Catalog**

6. In the **Add GenericScim - Bearer Token** screen, enter the **Name** and **Description** in the appropriate fields in the **Add Application Details** section, and then click **Next** to proceed.

**Figure 1-6 Add Application Details**




## Add GenericScim - Bearer Token

1 Add application details  
2 Configure provisioning

Name  
GenericScim - Bearer Token

Description *Optional*  
GenericScim - Bearer Token

Application icon ⓘ




**Display settings**

User can request access  
Select if you want to allow users to request access to the application from the Catalog.

**Authentication and authorization**

Define a more detailed authentication and authorization configuration.

Enforce grants as authorization  
Select if you want to allow access to this app only if the user has been granted this app.

 [Show advanced options](#)

**Next** [Cancel](#)

7. In the **Configure Provisioning** section of the **Add GenericScim - Bearer Token** screen, toggle on **Enable Provisioning** and then click **Finish**.

**Figure 1-7 Enable Provisioning**

Add GenericScim - Bearer Token

1 Add application details

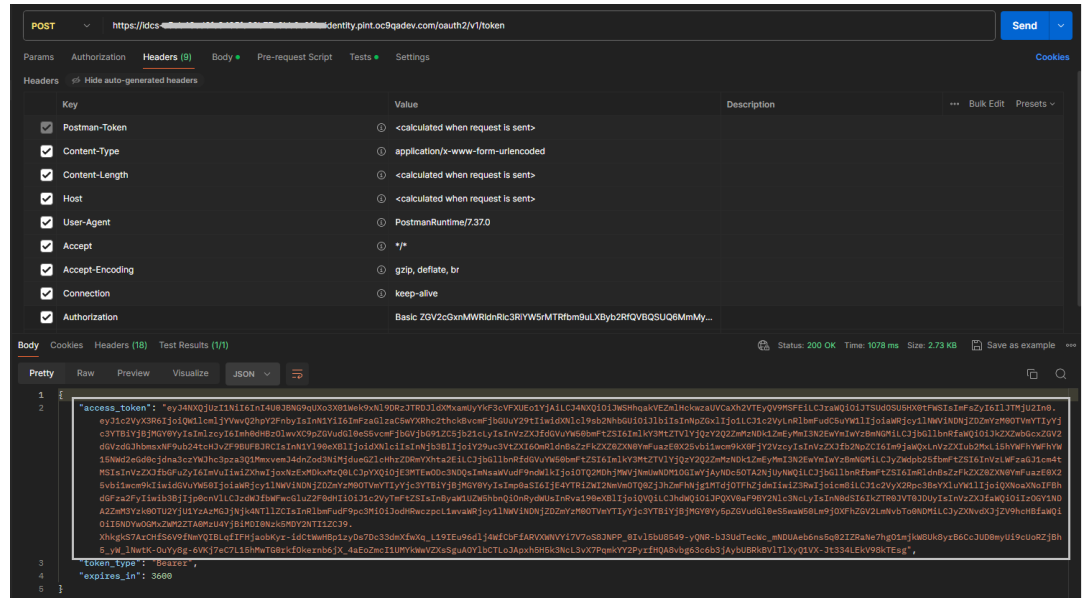
2 **Configure provisioning**

Enable provisioning

Previous Finish Cancel

8. To generate the access token, follow the steps outlined in the *Getting Started with Oracle Banking Cloud Services* guide for invoking Service APIs. Once generated, capture the access token.

Figure 1-8 Token Generation

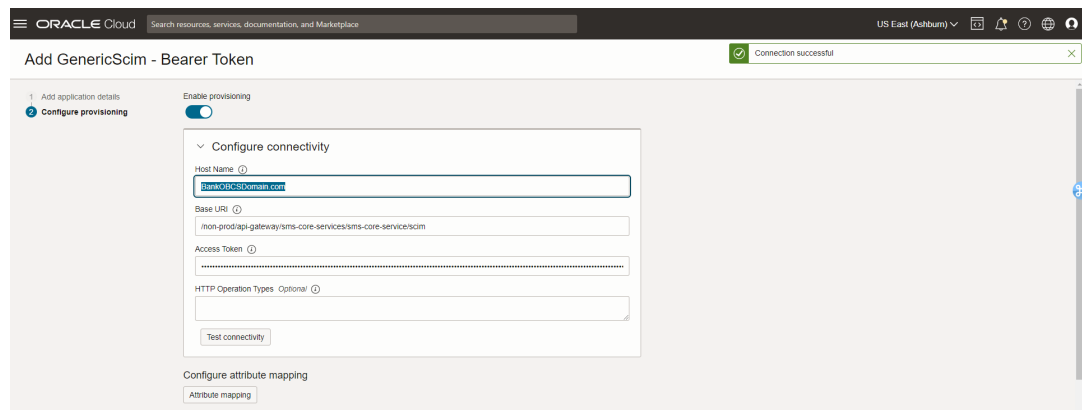


9. Enter the access token you have captured in the **Access Token** field, and provide the other details as indicated in the below screen. The Base URI should begin with either `/prod`, `/non-prod`, `/pre-prod`, and so on, depending on the environment you have selected for replication.

### Note:

Click on **Test Connectivity** to see a message that reads **Connection successful** displayed on the top right of your screen.

Figure 1-9 Configure Connectivity



**Figure 1-10 Test Connectivity**

The screenshot shows the 'Add GenericScim - Bearer Token' configuration page. The page is divided into two main sections: 'Configure connectivity' and 'Configure attribute mapping'. The 'Configure connectivity' section includes fields for 'Host Name' (BankOBCSDomain.com), 'Base URI' (/non-prod/api-gateway/sms-core-services/sms-core-service/scim), 'Access Token' (a masked field), and 'HTTP Operation Types' (Optional). A 'Test connectivity' button is located below these fields. The 'Configure attribute mapping' section has an 'Attribute mapping' button. Below this is a 'Select provisioning operations' section with two options: 'Authoritative sync' (unchecked) and 'Create an account' (checked). At the bottom of the page are 'Previous', 'Finish', and 'Cancel' buttons.

1 Add application details  
2 **Configure provisioning**

Enable provisioning

Configure connectivity

Host Name ⓘ  
BankOBCSDomain.com

Base URI ⓘ  
/non-prod/api-gateway/sms-core-services/sms-core-service/scim

Access Token ⓘ  
.....

HTTP Operation Types *Optional* ⓘ

Test connectivity

Configure attribute mapping  
Attribute mapping

Select provisioning operations

Authoritative sync  
Enable authoritative sync to automatically create and manage users based on the data from the authoritative application. When this option is enabled, user accounts in GenericScim - Bearer Token can't be managed from an identity domain.

Create an account  
Create an account in GenericScim - Bearer Token when the app is granted to the user in this identity domain, either directly or via a group membership.

Previous Finish Cancel

10. Click on **Attribute Mapping** to ensure that the mapping matches the one shown in the below screen. Make any necessary changes to the mapping if needed and then click **Save Changes** to proceed.

**Figure 1-11 Attribute Mapping**

Attribute mapping [Help](#)

You can map identity domain attributes to attributes in your application account. In most cases the default mapping is fine as is and should not be changed.

Identity domain to application  Application to identity domain

User	Maps to	SMS-SCIM account
<input type="text" value="\$ (user.phoneNumbers[type='mobile'], value)"/>	→	<input type="text" value="mobilePhoneNumber"/>
<input type="text" value="\$ (user.preferredLanguage)"/>	→	<input type="text" value="preferredLanguage"/>
<input type="text" value="\$ (user.phoneNumbers[type='home'], value)"/>	→	<input type="text" value="homePhoneNumber"/>
<input type="text" value="\$ (user.displayName)"/>	→	<input type="text" value="displayName"/>
<input type="text" value="\$ (user.phoneNumbers[type='work'], value)"/>	→	<input type="text" value="workPhoneNumber"/>
<input type="text" value="\$ (user.userName)"/>	→	<input type="text" value="name"/>
<input type="text" value="\$ (user.id)"/>	→	<input type="text" value="externalId"/>
<input type="text" value="\$ (user.active)"/>	→	<input type="text" value="active"/>
<input type="text" value="\$ (user.locale)"/>	→	<input type="text" value="locale"/>
<input type="text" value="\$ (user.um.ietf.params.scim.schemas.extension.enterprise)"/>	→	<input type="text" value="department"/>
<input type="text" value="\$ (user.emails[primary=true].value)"/>	→	<input type="text" value="primaryEmail"/>

[+ Add](#)

[Cancel](#)

- In the **Select Provisioning Operations** screen, set the provisioning operations as shown in the below screen.

**Figure 1-12 Select Provisioning Operations**

∨ Select provisioning operations

Authoritative sync  
Enable authoritative sync to automatically create and manage users based on the data from the authoritative application. When this option is enabled, user accounts in GenericScim - Bearer Token can't be managed from an identity domain.

Create an account  
Create an account in GenericScim - Bearer Token when the app is granted to the user in this identity domain, either directly or via a group membership.

Update the account  
Update the account in GenericScim - Bearer Token when the account is updated in this identity domain.

Deactivate the account  
Deactivate the account in GenericScim - Bearer Token when the account is deactivated in this identity domain.

Delete the account  
Delete account in GenericScim - Bearer Token when the account is deleted in this identity domain.

Push the identity domain user lifecycle events to GenericScim - Bearer Token

Push user updates  
Update the GenericScim - Bearer Token account when the user in this identity domain is updated.

Push user activation/deactivation status  
Deactivate or activate the account in the GenericScim - Bearer Token when the user in this identity domain is deactivated or activated.

- Switch to toggle on the **Enable Synchronization** option.

**Figure 1-13 Enable Synchronization**

Enable synchronization

Application refresh

Refresh reference application data, including entitlements and permissions. This refresh doesn't initiate a sync of application users.

Refresh application data

Configure synchronization

User identifier

External ID

Application identifier

externalId

When exact match is found

Link and confirm

Maximum number of creates *Optional*

Enter a number greater than or equal to 10 to limit the number of accounts that can be created.

Maximum number of deletes *Optional*

Enter a number greater than or equal to 10 to limit the number of accounts that can be deleted.

Synchronization schedule

Every hour

- Click on **Finish**.  
The application is created.
- Click on **Activate** in the **GenericScim - Bearer Token** screen.  
The application is activated.

Figure 1-14 Inactive Application

Identity > Domains > Default domain > Integrated applications > GenericScim - Bearer Token

## GenericScim - Bearer Token

Activate Edit application Add tags Delete

Application information Tags

**Application ID:** ...ef1031 [Show](#) [Copy](#)

**Description:** GenericScim - Bearer Token

**User can request access:** No

**Enforce grants as authorization:** Disabled

### Resources

- Provisioning
- Import
- Users
- Groups

### Provisioning

Edit provisioning Test connectivity Refresh application data

**Provisioning:** Enabled

**Synchronization:** Enabled

### Connectivity details

**Host Name:** BankOBSCSDomain.com

**Base URI:** /non-prod/api-gateway/sms-core-services/sms-core-service/scim

**Access Token:** \*\*\*\*\*

**HTTP Operation Types:**

Figure 1-15 Activated Application

Identity > Domains > Default domain > Integrated applications > GenericScim - Bearer Token

## GenericScim - Bearer Token

Deactivate Edit application Add tags Delete ⓘ

Application information Tags

**Application ID:** ...ef1031 [Show](#) [Copy](#)

**Description:** GenericScim - Bearer Token

**User can request access:** No

**Enforce grants as authorization:** Disabled

### Resources

**Provisioning**

Import

Users

Groups

### Provisioning

Edit provisioning Test connectivity Refresh application data

**Provisioning:** Enabled

**Synchronization:** Enabled

### Connectivity details

**Host Name:** BankOBCSDomain.com

**Base URI:** /non-prod/api-gateway/sms-core-services/sms-core-service/scim

**Access Token:** \*\*\*\*\*

**HTTP Operation Types:**

- Click on **Groups** under **Resources** section in the **GenericScim - Bearer Token** screen.

Figure 1-16 Assign Groups

Identity > Domains > Default domain > Integrated applications > GenericScim - Bearer Token > Groups

## GenericScim - Bearer Token

Deactivate Edit application Add tags Delete ⓘ

Application information Tags

**Application ID:** ...ef1031 [Show](#) [Copy](#) **Application icon:**

**Description:** GenericScim - Bearer Token

**User can request access:** No

**Enforce grants as authorization:** Disabled

### Resources

Provisioning

Import

Users

**Groups**

### Groups

Assign groups Revoke access

Search by name or de

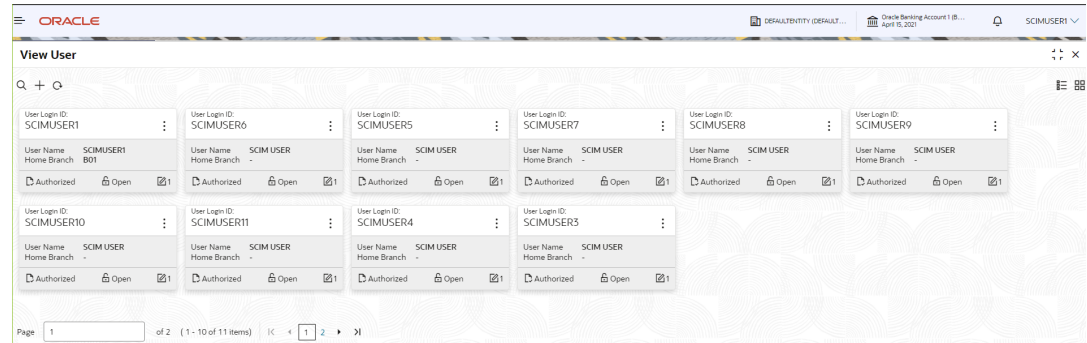
Name	Description
No items found	

0 selected No group to display < Page 1 >



16. Once you assign the User Groups that have been created, the users in those groups will get pushed to the OBCS SMS module.
17. User Creation on the OBCS end can be verified from the **View User** screen.

**Figure 1-17 View User**



18. Edit or Unlock the users that have been pushed from IAM, and specify the data into the highlighted fields.

**Figure 1-18 Users Maintenance**

The screenshot shows the 'Users Maintenance' form. The 'User Details' section contains fields for Login ID (SCIMUSER6), Name (SCIM USER), and Home Branch (a dropdown menu with a search icon and 'Required' label, highlighted with an orange box). The 'Status' section includes User Status (Enable), Status Changed On (April 15, 2021), Is Supervisor (checkbox), and Manager ID (searchable field). The 'Other Details' section includes Access to PII (checkbox), Staff Customer Restriction Required (checkbox), Customer ID (searchable field), Email ID (SCIMUSER@oracle.com), Telephone Number, Home Phone Number, Mobile Number, and Fax. The Language Code field (with a search icon and 'Required' label) is also highlighted with an orange box.

19. Add User Role Branches and User Applications.

**Figure 1-19 User Role Branches and Applications**

The screenshot displays two sections: 'User Role Branches' and 'User Applications'. The 'User Role Branches' section has a table with columns for Branch Code, Role Code, and Role Description. It shows 'No data to display' and a pagination indicator 'Page 1 (0 of 0 items)'. The 'User Applications' section has a table with columns for Application Name and Application Description. It also shows 'No data to display' and a pagination indicator 'Page 1 (0 of 0 items)'. There are '+', '-', and trash icons for both sections.

# Index

## U

---

User Replication from OCI IAM to SMS Module,  
[1-1](#)