

Oracle® Financial Services Lending and Leasing Cloud Service

Cloud Service User Provisioning



Oracle Financial Services Lending and Leasing Cloud Service,

Cloud Service User Provisioning

Copyright © 2025, 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.

Table of Contents

1. Preface.....	4
1.1. Introduction	4
1.2. Abbreviations and Acronyms.....	4
1.3. Audience	4
1.4. Pre-Requisites.....	4
1.5. Screenshot Disclaimer	4
2. Manage Users, Groups, Application Roles and Access	5
2.1. Create Groups.....	6
2.2. User Provisioning	9
2.3. Assign Users to Groups	10
3. OFSLL REST API Authentication.....	11
3.1. Setup the OAuth Clients in Identity Cloud Service & OFSLL.....	11
3.2. Access the OFSLL REST APIs with Access Token	14
4. Bulk Import User Accounts in Identity Cloud Service	15
5. References.....	15

1. Preface

1.1.Introduction

This document summarizes the OFSLL Cloud Service User and Access Management using Oracle Identity Cloud Service. Additionally, it explains the steps required to integrate the OFSLL Cloud Service with third-party Identity Provider systems, which act as a SAML 2.0 Identity Provider.

1.2.Abbreviations and Acronyms

Acronyms	Abbreviations
OFSLL	Oracle Financial Services Lending and Leasing
APIs	Application Programming Interface
DIS	Data Intelligence Services
ENV	Environment
SaaS	Software as a Service
SAML	Security Assertion Markup Language
REST	Representational State Transfer
OCI	Oracle Cloud Infrastructure

1.3.Audience

This document is intended for the following audiences:

- OFSLL Cloud Service customers who want to use OFSLL Cloud Service capabilities.
- Consultants and internal groups who want to demonstrate OFSLL Cloud Service capabilities.

1.4.Pre-Requisites

- Access to the Oracle Identity Cloud Service Administrative console of OFSLL Cloud Service.
- OFSLL Cloud Service application access end point details.
- Administering Oracle Identity Cloud Service - Understand Administrator Roles_
<https://docs.oracle.com/en/cloud/paas/identity-cloud/uaid/understand-administratorroles.html>

1.5.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.

2. Manage Users, Groups, Application Roles and Access

Identity domain administrators use Oracle Identity Cloud Service to manage users and set up user groups for OFSLL Cloud Service. Oracle Identity Cloud Service authenticates and authorizes users when they sign in to OFSLL Cloud Service applications.

OFSLL Cloud Service is integrated with Oracle Identity Cloud Service and initially offers a single user account (administrator). This default user can grant other users permissions for accessing OFSLL Cloud Service applications through several Oracle Identity Cloud Service application roles

Application Roles:

Below table summarizes the application roles that are used to access the OFSLL cloud service applications of an environment. As a best practice, you should create groups for OFSLL Cloud Service application roles and assign the appropriate user roles to those groups. Then you can add users to those groups to automatically assign them the appropriate user roles.

Application	Application Roles in Oracle Identity Cloud Service	Role Details
OFSLL - Prod Environment	OFSLL_USER_PRD	Allows users to access the OFSLL Application User Interface.
OFSLL - Non Prod Environment (Ex : Dev)	OFSLL_USER_DEV	Individual responsibilities of each User should be managed at the OFSLL Application level

Application	Groups in Oracle Identity Cloud Service	Group Details
DIS – Data Intelligence Services	<ENV>-DVContentAuthor	DVContentAuthor group to access Data Visualization
	<ENV>-DVConsumer	DVConsumer group to access Data Visualization
	<ENV>-BIContentAuthor	BIContentAuthor group to access Data Visualization
	<ENV>-BIConsumer	BIConsumer group to access Data Visualization
	<ENV>-BIAdministrator	BIAdministrator group to access Data Visualization

Note: Application roles pre-provisioned and mapped with groups for DIS Only [Step 1.3](#) (Assign Users to Groups), It is applicable for DIS.

2.1.Create Groups

You can create Groups only if you are granted access to the identity domain administrator or user administrator role in the **Administrators** Page of the Identity Cloud Service console.

Create the following Groups in Identity Cloud Service for each SaaS environment. Each SaaS environment requires.

Following four different groups to map them to the corresponding application roles. Below Group names are not fixed; you may name them uniquely based on your choice.

OFSLL SaaS Groups and Application Roles mapping:

SaaS Environment	Group Names	Application Roles
Ex - Production – OFSLL	PROD_USERS	OFSLL_USER_PRD

1. In the OCI Console (<https://cloud.oracle.com>), expand the Navigation Drawer, select Identity & Security, Navigate to the **Identity** screen, click **Domains**. Under **Domains**, click **Default domain**.
2. Under **Default domain**, click **Groups**. Under **Groups**, click **Create Groups**. The **Create Groups** screen displays.

Create group

Name
PROD_USERS

Description
OFSLL user group for Prod Environment

☐ User can request access

Users *Optional*
Select users to assign this group.

Search by user name, first name, last name, or email address

<input type="checkbox"/>	First name	Last name	Email
<input type="checkbox"/>	Test	Prod	Test@oracle.com

- Update the Name and Description, select the users as required (option at this moment).
- Click **Finish**.
- Repeat **Steps 1 to 3** for all the non-prod environments as required.

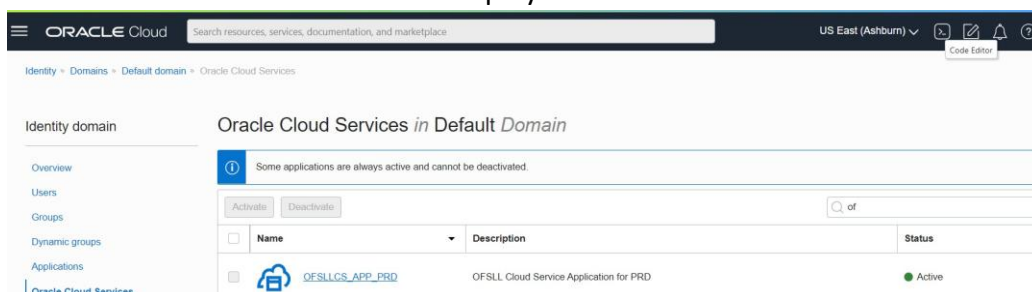
2.1.1. Assign Application Roles to Groups

After creating groups for your SaaS environments, assign the applicable user roles to those groups to give them access to the OFSLL Cloud Service applications. Refer to the below table for assigning Each group to the corresponding SaaS Application role for each SaaS environment.

Oracle Cloud Services	Application Roles	Group Names
Ex - Production – OFSLL	OFSLL_USER_PRD	PROD_USERS
Ex - Non Prod – Dev – OFSLL	OFSLLCS_APP_DEV	DEV_USERS

To assign app roles to groups:

- In the OCI Console (<https://cloud.oracle.com>), expand the Navigation Drawer, select Identity & Security, Navigate to the **Identity** screen, click **Domains**. Under **Domains**, click **Default domain**.
- Under **Default domain**, click **Oracle Cloud Services**.
- The **Oracle Cloud Services** screen displays.



4. Select the respective Oracle Cloud Service and select the Application roles.
The **Application Roles** screen displays.

The screenshot shows the Oracle Cloud console interface. At the top, there's a search bar and the Oracle Cloud logo. Below the logo, a large green circle with a white 'I' represents the application icon, labeled 'ACTIVE'. To the right of the icon, the application name 'OFSLLCS_APP_PRD' is displayed, along with 'Deactivate' and 'Edit application' buttons. Below this, the 'Application information' tab is active, showing details like Application ID, Description, Custom sign-in URL, Custom error URL, Display in My Apps, User can request access, and Enforce grants as authorization. To the right of this information, there are fields for Application icon, Application URL, Custom sign-out URL, and Custom social linking callback URL. Below the application information, there's a 'Resources' sidebar with links to OAuth configuration, Web tier policy, Application roles (selected), Users, and Groups. The main content area shows the 'Application roles' section with 'Import' and 'Export' buttons. Below these, a table lists application roles, with 'OFSLL_USER_PRD' selected. Below the table, there are links to manage assigned users, groups, and applications.

5. Click on Assigned groups and select **Manage**.
The **Manage** screen displays.

The screenshot shows the 'Manage group assignments' screen in the Oracle Cloud console. The left sidebar is the same as the previous screenshot. The main content area shows the 'Manage group assignments' section. It has a search bar and a table for 'Assigned groups (0)'. Below this, there's a link to 'Hide available groups'. Below that, there's a table for 'Available groups (2)'. The first group, 'PROD_USERS', is selected. Below the table, there's a '1 selected' indicator and a 'Showing 2 groups' message. At the bottom right, there's a 'Close' button.

6. Click on show available group, select the group which is already created in the previous **Step 1.1**.
7. Click **Assign** and **Close**.
The following screen displays.

The screenshot shows the Oracle Cloud console interface after assigning a group. The left sidebar is the same. The main content area shows the 'Application roles' section. The table now shows 'OFSLL_USER_PRD' with 'Assigned users: 1', 'Assigned groups: 1', and 'Assigned applications: -'. Below the table, there's a '0 Selected' indicator and a 'Showing 1 app role' message. At the bottom right, there's a 'Page 1' indicator.

2.2. User Provisioning

2.2.1. Create User Account in Identity Cloud Service

You can create user accounts only if you are granted access to the identity domain administrator or user administrator role in the Administrators page of the Identity Cloud Service console.

Create a new User Account in Identity Cloud Service by referencing the below URL.

Note: In OFSLL SaaS Username length cannot be greater than 30 characters.

<https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/addingusers.htm>

Additionally, create a User account (as explained in the below section) in the OFSLL Application in order to access the OFSLL application and authorize the users based on OFSLL user responsibilities.

2.2.2. Create User Account in OFSLL

1. Log in to the OFSLL Application with the Administrator user or any application user with SUPERUSER responsibility.
2. Navigate to the **Setup** screen, under **Setup**, click **Users**.
The **Users** screen displays.

The screenshot shows the 'Users' screen in the OFSLL application. It features a table of existing users and a 'User Definition' form for creating new users.

Organization	Division	User ID	ORG	Start Date	End Date	System Defined	Enabled	Batch
DEMOFSLAD	DMAC	US01	ORG	03/01/2001	03/31/2018	<input type="checkbox"/>	<input type="checkbox"/>	Y DEMO
DEMOFSLAD	DMAC	US01	ORG	01/01/1800	12/31/9999	<input type="checkbox"/>	<input type="checkbox"/>	Y DEMO
DEMOFSLAD	DMAC	US01	ORG	01/01/1800	12/31/9999	<input type="checkbox"/>	<input type="checkbox"/>	Y DEMO
DEMOFSLAD	DMAC	US01	ORG	01/01/1800	12/31/9999	<input type="checkbox"/>	<input type="checkbox"/>	Y DEMO
DEMOFSLAD	DMAC	US01	ORG	01/01/1800	12/31/9999	<input type="checkbox"/>	<input type="checkbox"/>	Y BATCH

User Definition Form:

- * User: [Text Field]
- * Organization: [Dropdown]
- * Division: [Dropdown]
- * Department: [Dropdown]
- * Start Dt: [Date Picker]
- * End Dt: [Date Picker]
- * System Defined: ☐ Yes ☒ No
- * Enabled: ☐
- * First Name: [Text Field]
- * Last Name: [Text Field]
- * Responsibility: [Dropdown]
- * Phone 1: [Text Field]
- * Phone 2: [Text Field]
- * Fax 1: [Text Field]
- * Fax 2: [Text Field]
- * Replacement User: [Text Field]
- * Type: [Text Field]
- * Reference #: [Text Field]
- * Email: [Text Field]
- * Default Language: [Text Field]
- * Time Zone: [Text Field]
- * Time Zone Level: [Text Field]

Buttons: Save and Add, Save and Stay, Save and Return, Return

3. Click **Add** in the **User Definition** screen, on the top right-hand corner, to add the users.
4. Provide the required details and click **Save and Return**. This completes the provisioning of the user within the OFSLL application.

Note: User field value in OFSLL should match the **Username** value in Identity Cloud Service.

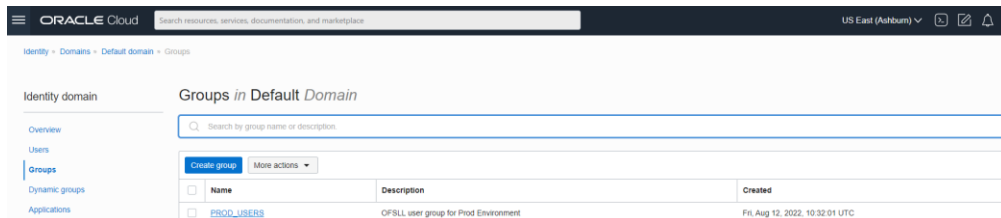
2.3.Assign Users to Groups

After the above-created groups are assigned to the corresponding cloud service application roles, user can assign the **Users to Groups** for the end user's system access.

To assign the Groups to User Account:

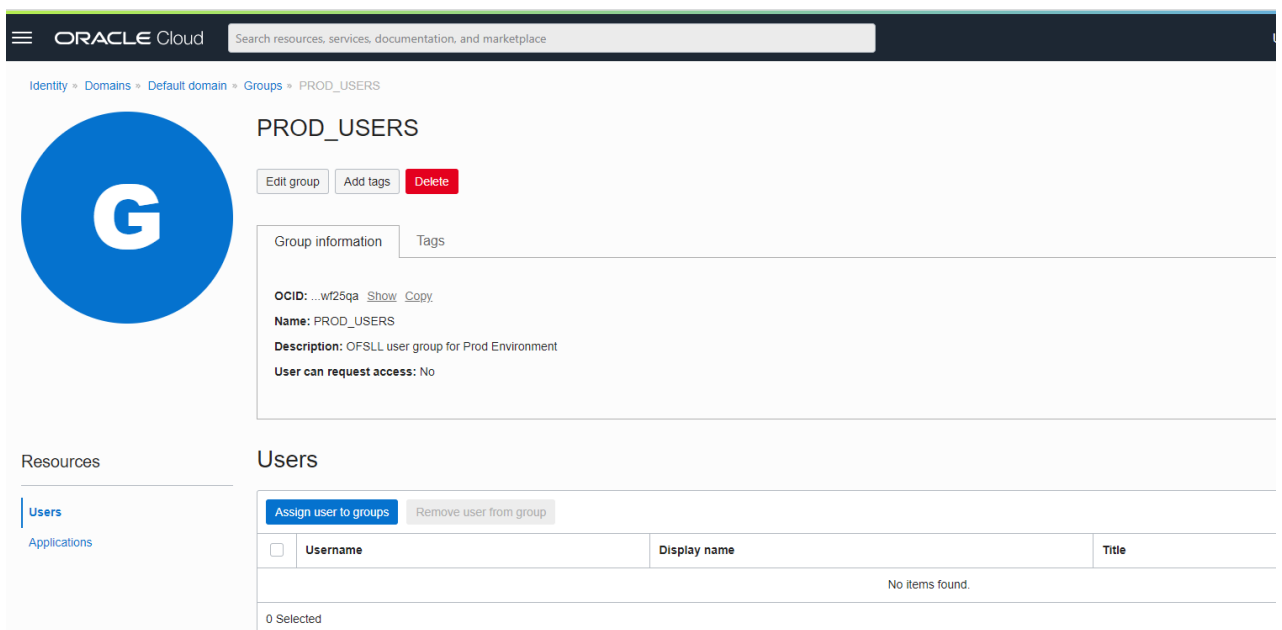
1. In the OCI Console (<https://cloud.oracle.com>), expand the Navigation Drawer, select Identity & Security, Navigate to the Identity domain, click **Identity**. Under **Identity**, click **Domains**.
2. Under **Domains**, click **Default domain**. Under **Default domain**, click **Groups**.

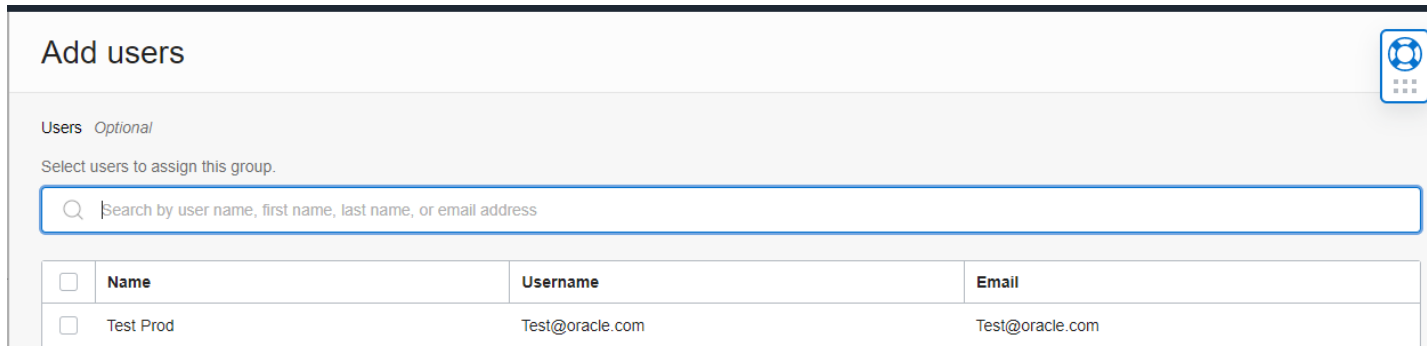
The **Groups** screen displays.



3. Select the group which created in the earlier **Step 1.1**.
4. Select **Assign users to group** and select the available user from the submenu.

The **Assign users to group** screen displays.





Add users

Users *Optional*

Select users to assign this group.

Search by user name, first name, last name, or email address

<input type="checkbox"/>	Name	Username	Email
<input type="checkbox"/>	Test Prod	Test@oracle.com	Test@oracle.com

3. OFSLL REST API Authentication

To make REST API calls to OFSLL, you need an OAuth2 access token to use for authorization. The access token provides a session (with scope and expiration) that your client application can use to invoke the OFSLL API Services in SaaS environment.

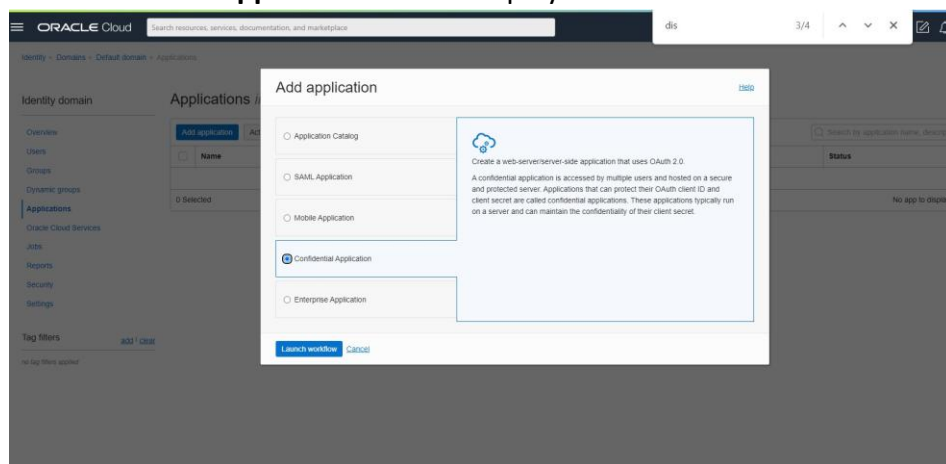
The following sections walk you through the steps required to use an OAuth client with Oracle Identity Cloud Service to access the OFSLL REST APIs:

3.1. Setup the OAuth Clients in Identity Cloud Service & OFSLL

3.1.1. Register a Confidential Application in Oracle Identity Cloud Service (Identity Cloud Service)

To create and register a confidential application:

1. In the OCI Console (<https://cloud.oracle.com>), expand the Navigation Drawer, select Identity & Security, Navigate to the **Identity** screen, click **Domains**. Under **Domains**, click **Default domain**.
2. Under **Default domain**, click **Applications**, and then click **Add**.
3. Select **Confidential Application** as the type of application. The **Confidential Application** screen displays.



4. Enter an application name (for example: PROD_OFSLL_OAUTH_CLIENT1) and a description, and then click **Next**. The **configure OAuth** screen displays.

Cloud Service User Provisioning

ORACLE Cloud

Search resources, services, documentation, and marketplace

Add Confidential Application

- 1 Add application details
- 2 **Configure OAuth**
- 3 Configure policy

Resource server configuration

☐ Configure this application as a resource server now ☒ Skip for later

Client configuration

☒ Configure this application as a client now ☐ Skip for later

Authorization

Allowed grant types ⓘ

☐ Resource owner ☐ Authorization code

☒ **Client credentials** ☐ Implicit

☐ JWT assertion ☐ SAML2 assertion

☐ Refresh token ☐ TLS client authentication

☐ Device code

☐ Allow HTTP URLs ⓘ

Redirect URL Optional ⓘ

5. On the configure OAuth screen, define below parameters:

- a) Resource server configuration as **Skip for later**.
- b) Client configuration: Select Authorization as **Client credentials**.
- c) At the bottom of the page under the Resources section, click on **Add Scope**.

The **Add Scope** screen displays.

ORACLE Cloud

Search resources, services, documentation, and marketplace

Add Confidential Application

- 1 Add application details
- 2 **Configure OAuth**
- 3 Configure policy

Bypass consent

☐ Turn on Bypass consent to overwrite the Require consent attribute

Client IP address

☐ Anywhere ☐ Restrict by network perimeter

Token issuance policy

Authorized resources ⓘ

☐ All ☐ Specific

☒ **Add resources**

Add resources if you want your application to access the API

Resources

☐ **Resource**

0 Selected

☐ **Add app roles**

Add the application roles to assign to this application. For example, the application.

Add scope

Search by application name, description, or tags.

<input type="checkbox"/>	Name
<input type="checkbox"/>	BotSaaSAuto
<input type="checkbox"/>	CloudPortalResourceApp
<input type="checkbox"/>	COMPUTEAREMETAL
<input type="checkbox"/>	DATABASEAREMETAL
<input type="checkbox"/>	DIS-IAD-FSGBU-PRD
<input type="checkbox"/>	EXADATABM
<input type="checkbox"/>	INTEGRATIONCAUTO
<input type="checkbox"/>	OCMSApp
<input type="checkbox"/>	OCNSApp
<input type="checkbox"/>	OFSLLCS_APP_DEV
<input checked="" type="checkbox"/>	OFSLLCS_APP_PRD
<input type="checkbox"/>	OMCEXTERNAL
<input type="checkbox"/>	PSMApp-cacct-8d7fdee52df7467abd436f50b91d6243

d) Select the OFSLL Application Resource for the environment that you want to create (for

example: FSGBU_OFSLCS_APP_PROD), and then click on **Add**.

e) Continue clicking **Next** until the user reach the **Finish** screen.

The **Configure policy** screen displays.

f) Click **Finish** to complete the process.

The following screen displays.

g) Make note (using your preferred note utility) of the Client ID and the Client Secret that appear in confirmation window, and then click **Close**.

6. Click **Activate** in the upper-right section of the page to activate the application.

Note: Do not grant any Identity Cloud Service Admin API roles.

3.1.2. Create OAuth Client User in OFSLL

1. Create a User in the OFSLL system by taking the Username and OAuth Client ID values from [Step 2.1.1.](#)
2. Select the appropriate Responsibility code as per the Client Access level. OFSLL Authorizes the client REST API requests based on the authorization code defined in this screen.

3.2. Access the OFSLL REST APIs with Access Token

3.2.1. Base64 Encode the Client ID and Client Secret

You must encode the client ID and client secret when you include it in a request for an access token.

1. Generate Base64 encoding of the above OAuth Client application's client ID and client secret.

Concatenate the client ID and client secret like ClientID: ClientSecret. The values of client ID and client secret are the values that the system generated as part of [Step 2.1.1](#). Then generate Base64 encoding of ClientID: ClientSecret. You can use your preferred tool to generate Base64 encoding. If you don't have one, then you can use <https://www.base64encode.org/>

2. Copy the encoded data.

3.2.2. Obtain an Access Token for accessing the OFSLL REST API

The next step in this process is to request the access token.

1. Launch a command prompt (You could use POSTMAN or any similar REST API clients).
2. Enter the cURL command below, replacing the text in brackets (< >) with the appropriate values:

Text in Brackets	Value
base64encoded clientid:secret	Replace with the encoded credentials that you generated in the Base64 Encode the client ID and client secret section.
Identity Cloud Service_Service_Instance	Replace with your Oracle Identity Cloud Service URL (for example: <a href="https://<Identity Cloud Service-Service-Instance>.identity.oraclecloud.com">https://<Identity Cloud Service-Service-Instance>.identity.oraclecloud.com).
OFSLL_App_Instance	Replace with your SaaS Environment OFSLL Application Load Balancer Name (for example: https://CUSTOMERCODE-ENVCODE-ofsllfsl.oracleindustry.com)

```
curl --location --request POST 'https://<Identity Cloud Service_Service_Instance>/oauth2/v1/token' \
--header 'Content-Type: application/x-www-form-urlencoded;charset=UTF-8' \
--header 'Authorization: Basic <base64encoded clientid:secret>' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'scope=https://<OFSLL_App_Instance>/ofsllcs'
```

3. Copy the **access_token** value from the response. Make sure to copy only the actual token, which is the access_token value between the quotation marks:

```
Status: 200
"access_token":"eyJ4NXQiOiI4Wk. . ."
"token_type":"Bearer",
"expires_in":3600
```

Note: The response includes the expires_in: 3600 parameter. This means that your token is no longer valid after one hour from the time it is generated. After one hour, you must refresh the token or get a new access token.

3.2.3. Make a REST Request to the OFSSL Environment

After you obtain the OAuth 2.0 access token, you can use the token in a cURL command to send a REST request to the OFSLL Service REST API. The following service command is used to fetch lookups Details in OFSLL Cloud Service.

```

c
envcode> curl -X GET -H 'Authorization: Bearer <access token>' -H 'Content-Type: application/json' -H 'ofsll_access_token: \
OfsllRestWS/service/api/v1/etup/lookups?lookupsType=ACC_STATUS_CD' \
--header 'ofsll_access_token: \' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer '

```

4. Bulk Import User Accounts in Identity Cloud Service

Oracle Identity Cloud Service provides an option to create users in bulk using a comma-separated values (CSV) file. This feature can be leveraged for OFSLL Cloud Service for migrating users from any other source system to Identity Cloud Service in a bulk manner.

Reference the following URL for complete details:

<https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/csgsg/import-batch-users-cloud-account-identity-cloud-service.html>

5. References

<https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm>