

Oracle® Revenue Management and Billing Cloud Services

Release 8

End User Provisioning Guide

Revision 1.1

F31935-01

August, 2020

Oracle Revenue Management and Billing End User Provisioning Guide

F31935-01

Copyright Notice

Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

Trademark Notice

Oracle, Java, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

License Restrictions Warranty/Consequential Damages Disclaimer

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 de-compilation of this software, unless required by law for interoperability, is prohibited.

Warranty Disclaimer

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.

Restricted Rights Notice

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

U.S. GOVERNMENT RIGHTS

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, documentation, and/or technical data delivered to U.S. Government end users are “commercial computer software” or “commercial technical data” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, documentation, and/or technical data shall be subject to license terms and restrictions as mentioned in Oracle License Agreement, and to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). No other rights are granted to the U.S. Government.

Hazardous Applications Notice

This software 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 in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Third Party Content, Products, and Services Disclaimer

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products, and services 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.

Preface

About This Document

This guide provides instructions for Security Administrators to set up user accounts for ORMB cloud services, managing the end-to-end lifecycle for user identity, and governing user authentication in ORMB applications. Identity management tasks include users and user group records, granting users and groups an access to the ORMB applications, and managing various security settings.

This guide also introduces working with Oracle Identity Cloud Service. Identity Cloud Service is provisioned to customers with subscriptions to ORMB cloud services (R8 onwards). Customers receive an instance of Identity Cloud Service (also referred to as Identity Cloud Service tenancy). Exclusively the customer manages the tenancy.

Intended Audience

This document is intended for the following audience:

- System Administrators
- Consulting Team
- Implementation Team

Organization of the Document

The information in this document is organized into the following sections:

Section No.	Section Name	Description
Section 1	Introduction	Provides an overview of the end user provisioning process, with references to additional information in the following chapters
Section 2	Security Administrator Account	Describes how to set up a security administrator account for user provisioning
Section 3	User Management Procedures	Describes general procedures related to managing users and groups
Section 4	User Provisioning for ORMB Cloud Services	Describes specific tasks related to user provisioning for Oracle Management and Billing Cloud service

Conventions

The following conventions are used across the document:

Convention	Meaning
boldface	Boldface indicates graphical user interface elements associated with an action, or terms defined in the text.
<i>italic</i>	Italic indicates a document or book title.
monospace	Monospace indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or information that an end-user needs to enter in the application.

Change Log

Revision	Last Update	Updated Section	Comments
1.1	27 Aug 2020	4.3, Appendix	Added sections 4.3 and Appendix

Contents

1.	Introduction.....	1
1.1	Identity Cloud Service Tenancy	1
1.2	Overview.....	2
1.2.1	Activate Security Administrator Account.....	2
1.2.2	Evaluate Federated Single Sign-On Requirements	2
1.2.3	Modify Oracle Identity Cloud Service Settings	2
1.2.4	Prepare User Community	2
2.	Security Administrator Account.....	3
2.1	Setting Up the Security Administrator Account	3
2.2	Verifying Security Administrator Identity Cloud Service Access	3
2.3	Verifying Subscription Contents	4
2.4	Exploring Applications	4
3.	User Management Procedures.....	5
3.1	Setting Up a New User.....	5
3.1.1	Add User Details.....	5
3.2	Setting Up a New Security Administrator.....	6
3.2.1	Security Administrator	6
3.2.2	Identity Administrator	7
3.3	Updating or Removing a User	7
3.3.1	Update User Details	7
3.3.2	Remove User	8
3.4	Managing Groups	8
3.4.1	Add Groups	8
3.4.2	Add Users.....	8
3.5	Advanced User and Access Management - Identity Cloud Service Admin Console.....	9
3.5.1	Managing Users	9
3.5.2	Managing Groups.....	9
3.5.3	Managing Applications.....	10
3.6	Bulk User and Group Import/Export	10
3.6.1	Downloading the CSV templates	10
3.6.2	Bulk User Import	10
3.6.3	Bulk User Export.....	12
3.6.4	Bulk Group Import	12
3.6.5	Bulk Group Export.....	12
3.7	Adding Groups in Application.....	13
3.8	Pre-Defined Application Roles.....	13
4.	SAML Application.....	15

4.1	Adding SAML Application	15
4.2	Importing metadata for a SAML Identity Provider	17
4.3	Adding Identity Provider to IDP Policies.....	18
Appendix A :	REST API for Identity Cloud Service	19
A.1	Creating Group in IDCS using Rest Call.....	19
A.1.1	Group.json.....	19
A.1.2	To Create a Test Group	19
A.2	Creating A User In IDCS Using Rest Call.....	20
A.2.1	User.json	20
A.2.2	Commands To A Create User	20
A.3	Adding User To A Group	20
A.3.1	Addusertogroup.json	20
A.3.2	Commands To Add a User To a Group.....	21

1. Introduction

End user provisioning involves creating user records and granting appropriate access for users of Oracle Revenue Management and Billing (ORMB).

1.1 Identity Cloud Service Tenancy

Identity cloud service tenancy is provided to the customer as part of the service subscriptions. The following configurations are defined in Identity Cloud Service:

- **Application:** In ORMB Cloud services, the application represents a single environment: either Production or non-Production. Applications are created by the subscription provisioning process.
- **Application Role:** In ORMB cloud service, the Application Role represents an entitlement to access a component within the environment. Assigning a user to an Application Role provides this user with access to this component. Application Roles are created by the subscription provisioning process.
- **User:** Users represent a human or non-human entity that is accessing the environment. User records are created and managed by the Security Administrator.
- **Group:** Groups comprise of one or more users. Groups are created and managed by the Security Administrator.

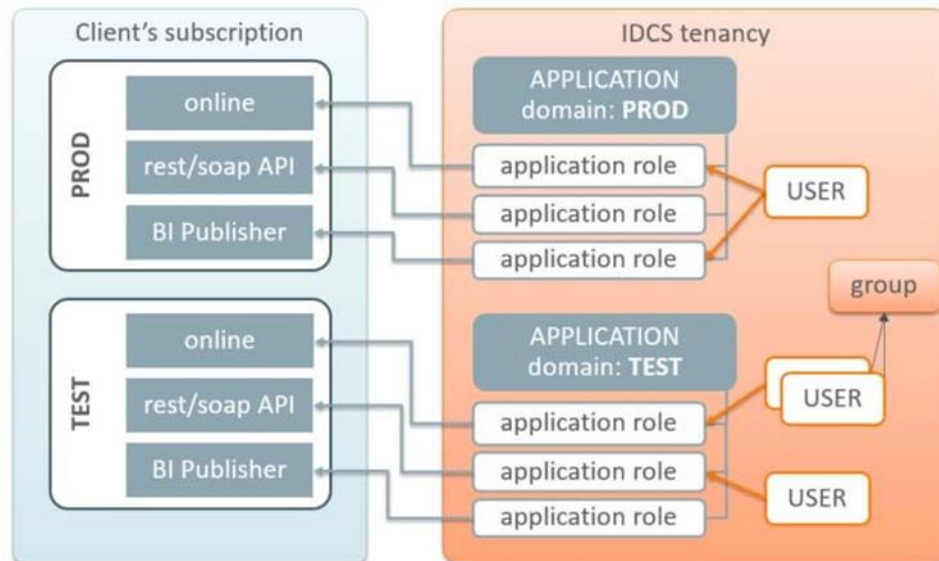


Figure 1: IDCS Tenancy

1.2 Overview

This section provides an overview of the initial set up of your cloud server user community including:

- Activate Security Administrator Account
- Evaluate Federated Single Sign-On Requirements
- Modify Oracle Identity Cloud Service Settings
- Prepare User Community

1.2.1 Activate Security Administrator Account

Access the Oracle Identity Cloud Service (IDCS) Admin console and perform the verification of the provisioned environments. Follow the steps described in Chapter 3: Security Administrator Account.

1.2.2 Evaluate Federated Single Sign-On Requirements

If you are using IDCS as your only identity management system, proceed with adjusting the IDCS cloud settings followed by the user community setup. Otherwise if the user identities are managed by an existing enterprise identity management system then evaluate any Federated Single Sign-On (SSO) requirements.

1.2.3 Modify Oracle Identity Cloud Service Settings

Modify Oracle Identity Cloud Service (IDCS) settings as follows:

- Define user naming conventions and decide whether the email address will be used as the user name. If not, you may want to include user name in the communication emails.
- Update the notifications further to include additional details; for example, the contact information of the technical support team.
- Evaluate the default Password Policy and amend according to your organization's requirements.
- Customize the look of the IDCS login page with your company's branding elements (optional).

1.2.4 Prepare User Community

- Determine the list of users who require access to the provisioned environment(s):
 - Provide access to the non-production environments for key members of the implementation team
 - Provide access to the production environment users

2. Security Administrator Account

This chapter describes how to set up a security administrator account for user provisioning, including:

- Setting Up the Security Administrator Account
- Verifying Security Administrator Identity Cloud Service Access
- Verifying Subscription Contents
- Exploring the Applications

2.1 Setting Up the Security Administrator Account

The account for the Security Administrator is created during the tenancy provisioning. The customer provides the name and the email address of the intended security administrator as part of the service order. Once the order is completed the Security Administrator receives a cloud account activation email.

The activation email contains:

- Activation URL
- The user name and the temporary one-time password

Security administrators should use the following procedure for first time logging into the Oracle Cloud Account Portal:

1. Press the activation link or copy the link into the internet browser's address. You will be redirected to the login page.
2. Enter the user name and the temporary password.
3. Follow the prompts to create a new permanent password. This redirects you to the Oracle Cloud Account Portal dashboard.

2.2 Verifying Security Administrator Identity Cloud Service Access

Expand the Security option on the navigation pane and click Administrators.

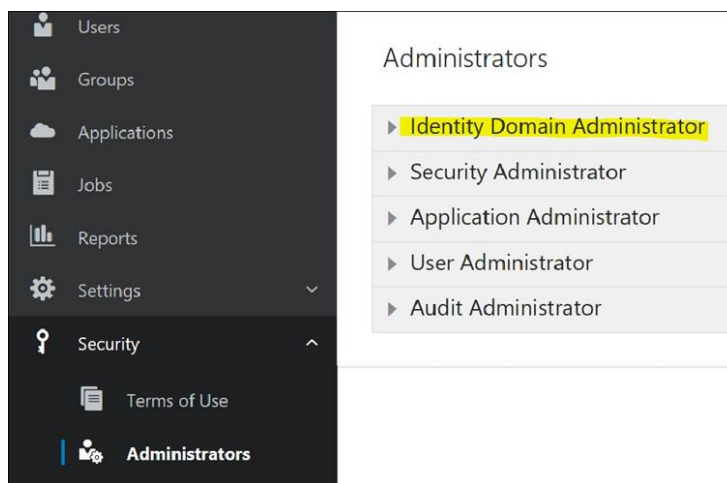


Figure 2: Identity Domain Administrator

On the Administrators page, click Identity Domain Administrator and verify that your name is on the list of Identity Domain Administrators.

2.3 Verifying Subscription Contents

Click Applications on the navigation pane. The main panel displays a list of available applications. Oracle Management and Billing Cloud service subscription contains at least one production and one or more non-production environments.

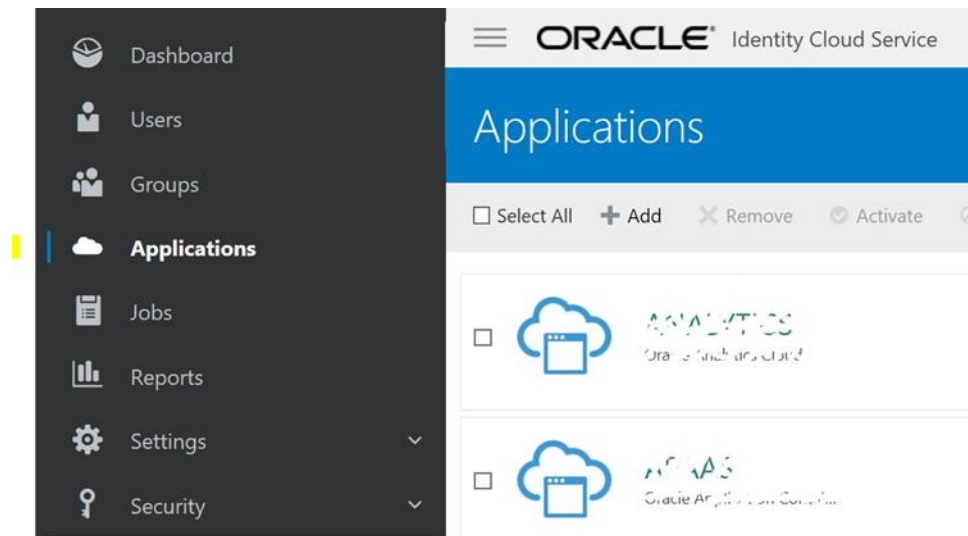


Figure 3: Applications

2.4 Exploring Applications

Click on one of the applications on the list and display the single application. Most of the information is system-generated and read-only. Users can be assigned to Application Roles within the application.

While the application represents a single environment, the different Application Roles represent different components within the environment. In order to authorize a user's access to a certain component, the user has to be assigned to a corresponding Application Role.

3. User Management Procedures

This chapter contains general procedures related to managing users and groups, including:

- Setting Up a New User
- Setting Up a New Security Administrator
- Updating or Removing a User
- Managing Groups
- Advanced User and Access Management - Identity Cloud Service Admin Console
- Adding groups in application
- Pre-defined Applications role

3.1 Setting Up a New User

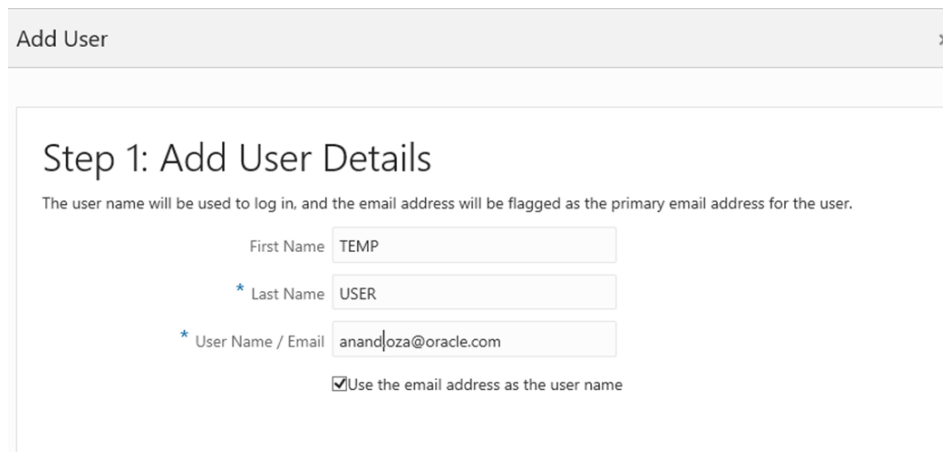
Click Add on the Users tab of the User Management portal to set up a new user.

3.1.1 Add User Details

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. Use following steps to add user:

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Users, and then click Add.
2. In the **First Name** and **Last Name** fields of the Add User window, enter the user's first and last name.
3. Leave the "Use the email address as the user name" check box selected.
4. In the Email field, enter the email address for the user account.
5. To assign the user account to a group, click next. Otherwise, click Finish.

Important: It is mandatory to assign a User Group to a user and that the User group (which is being assigned) must already be present (if not, then create it) in ORMB and that the User group must have access to C1-USRLOGINDTLS Application service.



Add User

Step 1: Add User Details

The user name will be used to log in, and the email address will be flagged as the primary email address for the user.

First Name

* Last Name

* User Name / Email

Use the email address as the user name

Figure 4: Add User Details

6. In the Add User window, select the check box for each group that you want to assign to the user account. Click Finish.

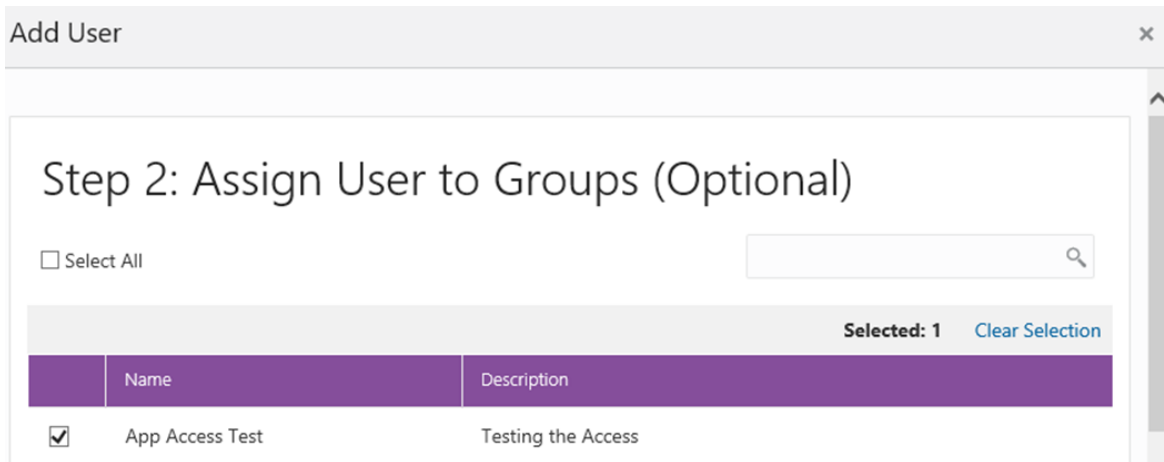


Figure 5: Assign User to Groups

7. Activating a user account reinstates the access rights of the user account for Oracle Identity Cloud Service.
 - a. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
 - b. Select the check box for each deactivated user account that you want to activate. To activate all deactivated user accounts, search for accounts with a status of Inactive and then select the Select All check box.
 - c. Click Activate.
 - d. In the Confirmation window, click OK.

3.2 Setting Up a New Security Administrator

The new security administrator is configured as follows:

1. Add a new user record as shown above.
2. Grant administrative role(s) to the new user.

3.2.1 Security Administrator

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Security.
2. Click Administrators (the user with the gear icon in the Security menu).
3. Click a security role title (for example, Security Administrator), and then click Add.
4. Search and select the users you want to assign as administrators, and then click OK.

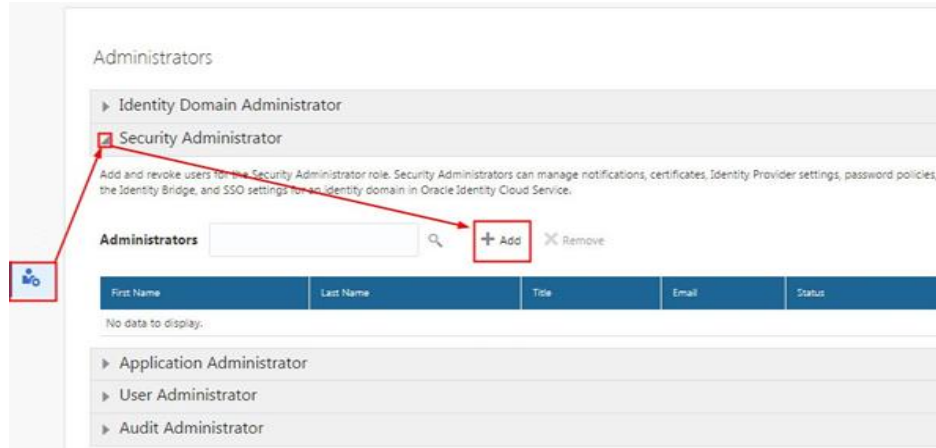


Figure 6: Security Administrator

3.2.2 Identity Administrator

Identity administration roles authorize users to manage configurations and administer Identity Cloud Service. There are various level of access:

- User Administrators are allowed to create and manage users and groups.
- The Application Administrator role is limited to the Application configuration and lifecycle.
- Audit and Security Administrator roles provide access to basic security settings and Identity-related reports.
- The Identity Domain Administrator role includes all of the above.

In order to grant administrative role to the user in Identity Cloud Service:

1. Filter the services list and locate an Identity Cloud service.
2. Select one or more roles from the list or click Add Admin Roles to add all available roles at once.

3.3 Updating or Removing a User

User records are displayed on the User Management portal.

3.3.1 Update User Details

To update details for a user, select the user or click on the action menu icon to open the user record and update the user information as appropriate.

Figure 7: Account Information

Note: First and Last names are editable. The email address is editable only if not used as user name (login)

3.3.2 Remove User

To remove a user, click Remove from the menu.



Figure 8: Removing a User

Note: Removing a user is irreversible.

3.4 Managing Groups

Click the Groups tab on the User Management portal. The portal displays a list of all available group.

3.4.1 Add Groups

You can create groups in Oracle Identity Cloud Service. Use following steps to add Groups:

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Groups.
2. Click Add.
3. In the Name and Description fields of the Add Group window, enter the name and descriptive information about the group.
4. To allow users to request access to this group, click “User can request access”.
5. To assign user accounts to the group, click Next. Otherwise, click Finish.
6. Select the check box for each user account that you want to assign to the group, and then click Finish.

Note: To search for user accounts to assign to the group, , enter all or part of the beginning of the user names, first names, or last names of the user accounts that you want to locate in the search field, and click Enter.

3.4.2 Add Users

To add users to a group, click on the group name on the list or use the Edit menu action. The portal displays the selected group record. Click the Users tab, then click Add Users to add one or multiple users to the group.

3.5 Advanced User and Access Management - Identity Cloud Service Admin Console

Use the Identity Cloud Service admin console to manage applications, perform advanced user management and administer general and security settings also view basic reports.

3.5.1 Managing Users

Users can be added and maintained via Identity Cloud Service admin console. Access the Users portal from the Identity Cloud Service admin console dashboard or from the navigation bar.

Select one or more users from the list, and select the appropriate action. In addition to add and remove, the following actions are also available:

- Resend Invitation
- Reset Password
- Activate/Deactivate User
- Update User information and preferences (on individual User record)
- Unlock User (on individual User record)

The screenshot shows the user management interface for a user named Amar Babu. The header includes the user's initials 'AB', name 'Amar Babu', and status 'Active' with a 'Reset Password' link. Below the header are tabs for 'Details', 'Groups', and 'Access'. The 'Details' tab is active, showing 'Account Information' with an 'Update User' button. The form contains the following fields:

* User Name	odrdiev	* Email	amar.babu@oracle.com
Prefix		Recovery Email	amar.babu@oracle.com
First Name	Amar	Instant Messaging Address	
Middle Name		Home Phone Number	

Figure 9: Managing a User

3.5.1.1 Resend Invitation to Service

The initial email invitation to access the service is sent to the user immediately upon user record creation. This invitation is expired after certain period of time.

3.5.1.2 Reset Password

Resets a single, multiple, or all passwords. Users will receive a password reset email notification immediately

3.5.1.3 Activate/Deactivate User

User can be temporarily activated or deactivated. The email notification is sent to the user immediately. If the deactivation lasts longer than the password rotation period the activation will cause password reset..

3.5.2 Managing Groups

Users and groups can be added and maintained using the Identity Cloud Service admin console. Access the Groups portal from the Identity Cloud Service admin console dashboard or from the navigation bar.

Select one or more entries from the list. In addition to add and remove, the following actions are available:

- Import Groups
- Export Groups

3.5.3 Managing Applications

The applications that represent the provisioned services are pre-created during the service order processing. The Application Roles are also pre-configured.

The administrator is authorized to activate or deactivate certain applications, assign users to Application Roles and also perform import and export of application role's members.

3.6 Bulk User and Group Import/Export

3.6.1 Downloading the CSV templates

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Click Import.
3. Click Download sample file.

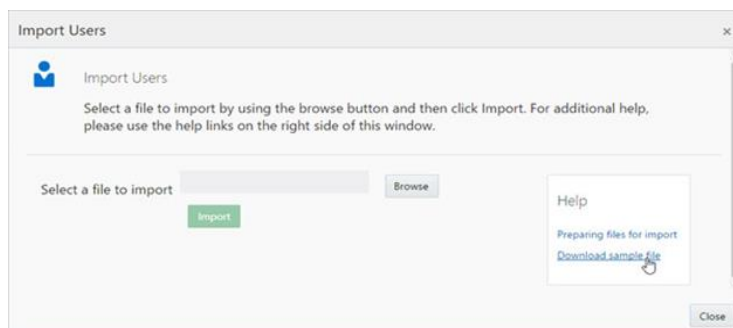


Figure 10: Download Sample File

Note: The sample files can be used as a template (or boilerplate) for creating your own user's CSV file for import.

4. Save the bulkImportSampleFilesCSV.zip file to your local disk and minimize your browser.
5. Extract the bulkImportSampleFilesCSV.zip file contents. The bulkImportSampleFilesCSV.zip file contains CSV templates for importing users (Users.csv) and groups (Groups.csv) to Oracle Identity Cloud Service.

Note: CSV file downloading procedure in case of Bulk group import is same as Bulk User import.

3.6.2 Bulk User Import

If you are an identity domain administrator or a user administrator, you can batch import user accounts using a comma-separated values (CSV) file. Before you can import user accounts, first create a CSV file that is properly formatted for the import process. To create and prepare a file for import, follow these steps:

1. Create an import file using the Users.csv file. The Users.csv file is a simple text file in a tabular format (rows and columns). The first row in the file defines the columns (fields) in your table.

Note: The maximum number of rows in the user import file must not exceed 100,000 and the import file size must not exceed 52 MB. Save the file with UTF-8 for encoding. At a minimum, the file must have these exact column headings and the fields in these columns must be unique.

2. For each account, create a new row (line) and enter data into each column (field). Each row equals one record.
3. The IDs of the users that you want to import into Oracle Identity Cloud Service must contain at least three characters. The names of the groups that you want to import into Oracle Identity Cloud Service must contain at least five characters.
4. When importing users, the attribute **Recovery** cannot be specified as one of valid values for Primary Email Type. The valid values for Primary Email Type are home, work, or other.
5. If you are uploading a CSV file with modified email addresses, make sure to include the Primary Email Type attribute in the template's header to trigger the change. For each user with a modified email address, add an appropriate value (either home, work, or other) in the Primary Email Type column.

Note: Save the file with UTF-8 for encoding. If you do not save the file in a CSV format with UTF-8 encoding, the import fails. Saving the file in UTF-8 format ensures that non-English characters display properly.

6. For each account, create a new row (line) and enter data into each column (field). Each row equals one record.
7. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
8. Click Import.
9. In the Import Users dialog box, click Browse to locate and select the CSV file that contains the user accounts to import.
10. Click Import.

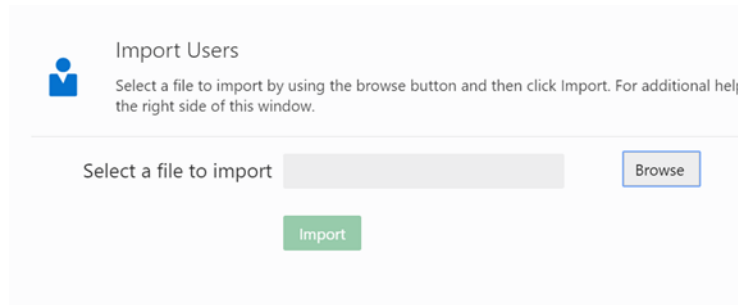


Figure 11: Import Users

11. Once the import is complete, the screen displays details of the import like:
 - Percent Complete
 - Total Users
 - Users Imported
 - Users Failed to Import

Note: Click on 'Users Failed to Import' for details of each user that failed import. Please note that Oracle Identity Cloud Service handles user errors individually during the import.

3.6.3 Bulk User Export

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click Users.
2. Click Export.
3. You can Export all users or the one you have selected.
4. After selecting Export you will get the job id and also receive one mail.
5. Go to job id and exported users will be visible.

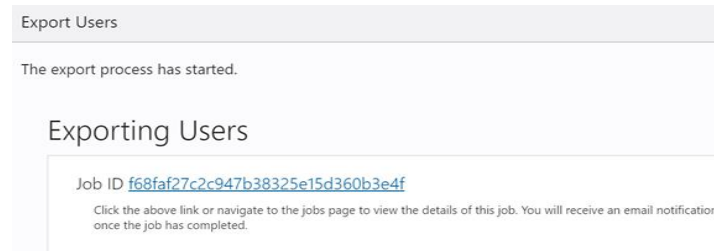


Figure 12: Exporting Users

3.6.4 Bulk Group Import

1. In the Oracle Identity Cloud Service console, expand the Navigation Drawer, and then click Groups.
2. Click Import.
3. Click Browse.
4. Select the CSV file with your groups for import.
5. Click Import.

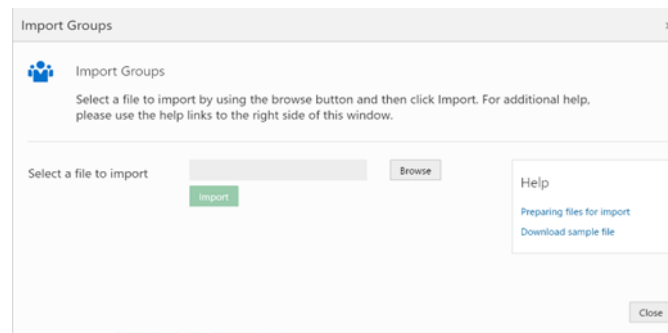


Figure 13: Import Groups

After uploading the file, Oracle Identity Cloud Service displays a Job ID for import processing. If the job completes with error, click on View Details see the error message that helps to identify the reason for failure.

3.6.5 Bulk Group Export

1. In the Identity Cloud Service console, expand the Navigation Drawer, and then click group.
2. Click Export.
3. You can Export all group or the one you have selected.
4. After selecting Export you will get the job id and also receive one mail.
5. Go to job id and exported Group will be visible.

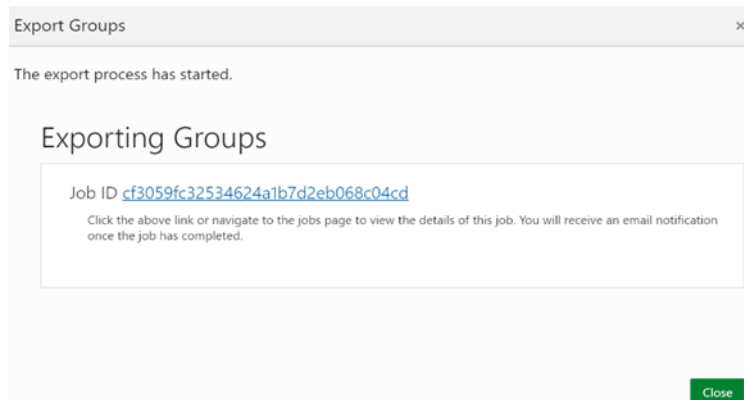


Figure 14: Exporting Groups

3.7 Adding Groups in Application

1. Go to application and go to group tag.
2. Click on assign and then we can add single or multiple groups and click ok.

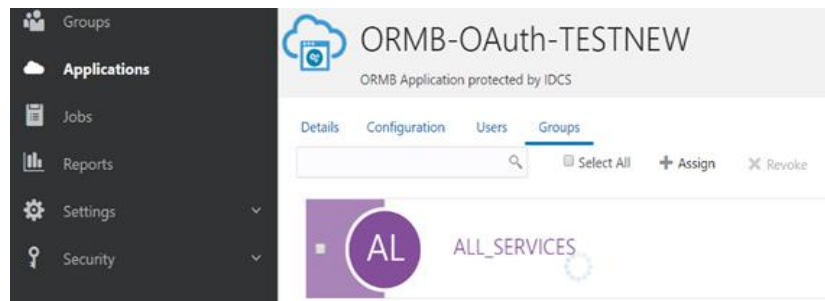


Figure 15: Adding Groups

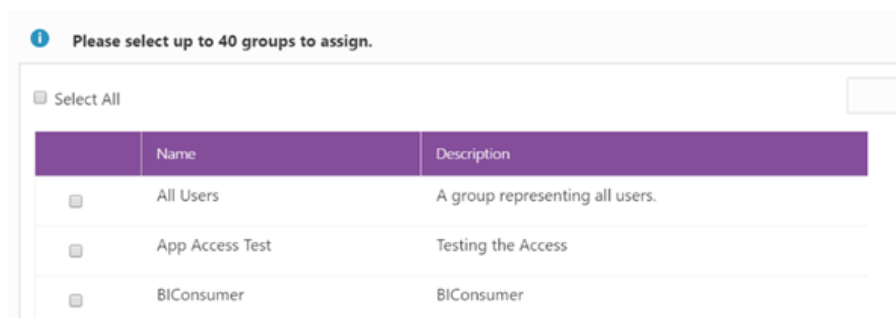


Figure 16: Selecting Groups

3.8 Pre-Defined Application Roles

The following roles are pre-defined in the Applications that represent Oracle Management and Billing Cloud service environments. Each role represents an entitlement within the environment and grants user an access to a certain component:

Administrator Role	Privileges
Identity domain administrator	Has super user privileges for an identity domain in Oracle Identity Cloud Service
Security administrator	Manage Oracle Identity Cloud Service system configuration and security settings for an identity domain in Oracle Identity Cloud Service
Application administrator	Manage Oracle Identity Cloud Service applications
User administrator	Manage users, groups, and group memberships for an identity domain in Oracle Identity Cloud Service
User manager	Manage all users or users of selected groups in Oracle Identity Cloud Service
Audit administrator	Run reports for an identity domain in Oracle Identity Cloud Service
Users	Users can update their profiles, reset their passwords, change their email preferences, link their social accounts to Oracle Identity Cloud Service, request access to groups and applications, view their access requests, access groups and applications assigned to them, and enroll in Multi-Factor Authentication (MFA).

4. SAML Application

This chapter provides a detailed idea about how to create a Security Assertion Markup Language (SAML) application and grant it to users so that your users can single sign-on (SSO) into your SaaS applications that support SAML for SSO.

4.1 Adding SAML Application

1. In the Identity Cloud Service console, expand Navigation Drawer, and then click Applications.
2. Click Add.
3. In the Add Application window, click SAML Application.
4. In the App Details section of the Add SAML Application page, provide values for the following fields:
 - a. In the Name field, enter a name for the application.
 - b. In the Description field, enter 250 or fewer characters to provide a description of the application.
 - c. Click Upload to add an icon for your application.
 - d. In the Application URL / Relay State field, enter a value, which will be sent to the SAML SP (Service Provider) as the SAML Relay State parameter.
 - e. In the Custom Login URL field, specify a custom login URL. However, if you are using a default login page provided by Oracle Identity Cloud Service, then leave this field blank.
 - f. In the Custom Logout URL field, specify a custom logout URL. However, if you are using a default login page provided by Oracle Identity Cloud Service, then leave this field blank.
 - g. In the Custom Error URL field, enter the error page URL to which a user has to be redirected, in case of a failure. This is an optional field. However, if not specified, the tenant specific Error page URL will be used. If both the error URLs are not configured, then the error will be redirected to the Oracle Identity Cloud Service Error Page (/ui/v1/error).
 - h. In the Linking callback URL field, enter the URL that Oracle Identity Cloud Service can redirect to after linking of a user between social providers and Oracle Identity Cloud Service is complete. This is an optional field.
5. In the Tags section of the Add SAML Application page, click Add Tag to add tags to your SAML application to organize and identify it. This is optional.
6. In the Display Settings sections of the Add SAML Application page, make the following selections:
 - a. Select Display in My Apps check box to specify whether you want the SAML App to be listed on the My Apps page.
 - b. Select the User can request access check box if you want the app to be listed in the Catalog. This option allows end users to request access to the app from their My Apps page by clicking Add and then selecting the app from the Catalog.

Note: Do not forget to activate the application (after completing setup) so that users can request access.

7. Click Next to configure SSO details for the SAML application.
8. In the General section of the SSO Configuration page, define the following:

- a. **Entity ID:** Enter a globally unique name for a SAML entity. It usually takes a URL of an identity provider as a value.
 - b. **Assertion Consumer URL:** Enter the URL to which the SAML identity provider will send the SAML assertion. This URL must begin with either the HTTP or HTTPS protocol.
 - c. **NameID Format:** Select the type of format is “Unspecified” to use for the NameID.
 - d. **NameID Value:** Select the NameID Value to identify the user that is logged in. Chose available option “User Name”.
 - e. **Signing Certificate:** Upload the signing certificate that is used to encrypt the SAML assertion.
9. Expand Advanced Settings on the SSO Configuration page, and then use the following to define a more fine-grained SAML configuration:
- a. **Signed SSO:** Select Assertion and Response to indicate that you want the SAML assertion and response signed.
 - b. **Include Signing Certificate in Signature:** Select the check box to include the signing certificate in the signature.
 - c. **Signature Hashing Algorithm:** Select SHA-256.
 - d. **Enable Single Logout:** We are not supporting single logout.
 - e. **Encrypt Assertion:** Select if you want to encrypt the assertion, and then define the encryption algorithm that you want to use and upload the encryption certificate.
 - f. **Encryption Certificate link:** Used to upload the encryption certificate that is used to encrypt the SAML assertion.
 - g. **Encryption Algorithm:** Select which encryption algorithm you want to use to encrypt the SAML assertion.
 - h. **Key Encryption Algorithm:** Select which key encryption algorithm you want to use to encrypt the SAML assertion.
10. Expand Attribute Configuration on the SSO Configuration page to add user-specific and group-specific attributes to the SAML assertion.
11. Click the plus sign next to Attributes, and then use the following table to specify the user attribute that you want to include.
12. When you are creating SAML app from scratch rather than creating a preconfigured SAML app created from the App Catalog, the Authentication and Authorization section appears. The Enforce Grants as Authorization check box is selected by default. This check box enables users to access only the application that you assigned or granted access to. If the check box is selected, Oracle Identity Cloud Service can control access to the SAML application based on grants to users and groups. If the check box is not selected, any authenticated user has access to the application regardless of the assignment status.
13. To import the Identity Cloud Service signing certificate into your application, click Download Signing Certificate to first download the certificate file in PEM format. This certificate is used by the SAML application to verify that the SAML assertion is valid.
14. To import the Identity Cloud Service Identity Provider metadata into your application, click Download Identity Provider Metadata to first download the metadata file in XML format. The SAML application needs this information so that it can trust and process the SAML assertion that is generated by Identity Cloud Service as part of the federation process. This information includes, for example, profile and binding support, connection endpoints, and certificate information.

15. Click Finish. The application is added in a deactivated state. To activate the application, click Activate, and then click OK in the Confirmation window.

4.2 Importing metadata for a SAML Identity Provider

1. In the Identity Cloud Service console, expand the Navigation Drawer, click Security, and then click Identity Providers.
2. Click Add SAML IDP. The Add Identity Provider wizard appears.
3. Use the following values to populate the Details pane of the wizard, and click Next:
 - a. **Name:** Enter the name of the IDP.
 - b. **Description:** Enter explanatory information about the IDP.
 - c. **Icon:** Click Upload to add an icon that represents the IDP.
4. Use the following values to populate the Configure pane of the wizard, and click Next:
 - a. **Import Identity Provider metadata:** Click this button because you want to configure SSO for the IDP by importing metadata for it.
 - b. **Metadata:** Click Upload. Select the XML file that contains the metadata for the IDP that you want to import.
 - c. **Signature Hashing Algorithm:** From the menu, select the secure hash algorithm used to encrypt the signing certificate for the IDP.
 - By default, select the **SHA-256** algorithm.
 - If the IDP does not support SHA-256, then select SHA-1.
 - d. **Include Signing Certificate:** To include a signing certificate with your IDP, select this check box. The signing certificate is used to verify the signature of the messages for the IDP. If you do not want to include a signing certificate with your IDP, then leave the check box deselected.
5. Use the following values to populate the Map pane of the wizard, and click Next:
 - a. **Identity Provider User Attribute:** Select the attribute value received from the IDP that can be used to uniquely identify the user. Select "Name ID"
 - b. **Oracle Identity Cloud Service User Attribute:** Select the attribute in Oracle Identity Cloud Service to which you are mapping the attribute received from the IDP. Select "Username".
 - c. **Requested NameID Format:** select "Unspecified".
6. Use the following table to populate or reference the Export pane of the wizard, and click Next:
 - a. **Service Provider Metadata:** To export metadata for Oracle Identity Cloud Service, click Download. Then, import this metadata into the IDP.
 - b. **Provider ID:** The Uniform Resource Identifier (URI) that uniquely identifies the identity domain. There is a one-to-one relationship between the provider ID and the IDP because the provider ID identifies the IDP uniquely. Because of this relationship, only one IDP can be defined in Oracle Identity Cloud Service with a given provider ID.
 - c. **Assertion Consumer Service URL:** The Uniform Resource Locator (URL) of the service that receives and processes assertions from the IDP
 - d. **Logout Service Endpoint URL:** The URL of the service that receives and processes logout requests from the IDP.
 - e. **Logout Service Return URL:** The URL of the service that receives and processes logout responses from the IDP.

- f. **Service Provider Signing Certificate:** To download a signing certificate for the IDP, click Download. Select the file that contains the signing certificate. This certificate is used to verify requests and responses signed by Oracle Identity Cloud Service.
 - g. **Service Provider Encryption Certificate:** To download an encryption certificate for the IDP, click Download. Select the file that contains the encryption certificate. The IDP can use this certificate to encrypt the assertion.
7. In the Test pane of the wizard, click Test Login to test the configuration settings for the IDP.
 8. Click Next.
 9. In the Activate pane of the wizard, click Activate to activate the IDP.
 10. Click Finish.

4.3 Adding Identity Provider to IDP Policies

An identity provider policy allows identity domain administrators, security administrators, and application administrators to define which identity providers are visible in the Sign In page either when they're accessing a specific app or attempting to access resources that are protected by Oracle Identity Cloud Service.

Oracle Identity Cloud Service also uses identity provider policies to determine whether users authenticate into Oracle Identity Cloud Service through identity providers or with a local authentication factor.

1. In the Identity Cloud Service console, go to the Navigation Drawer and select **Security, IDP Policies**. This shows the list of IDP Policies on the right hand side pane.
2. Click on **Default Identity Provider Policy**.
3. Go to **Identity Providers** tab and click on **Assign**. This opens the Assign Identity Providers pop up and lists the identity providers available in IDCS.
4. Select the SAML Identity Provider created in section [4.2](#) and click OK. This assigns the Identity Provider to the IDP Policy.

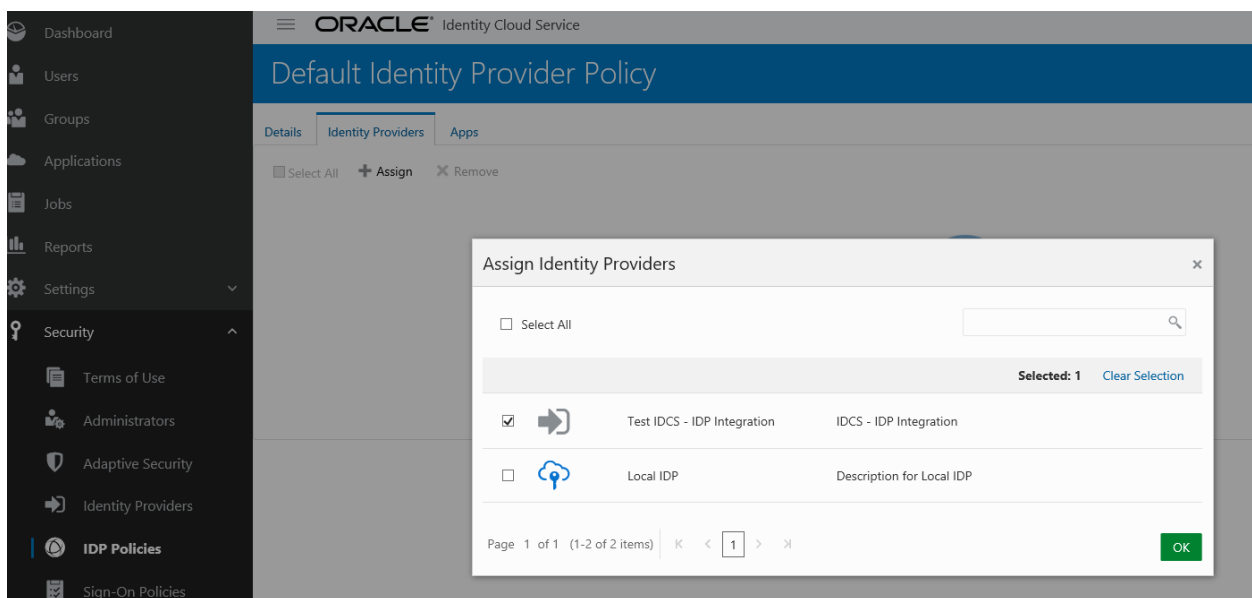


Figure 17: Assign Identity Providers

Appendix A : REST API for Identity Cloud Service

You can find an exhaustive list of REST endpoints at:

<https://docs.oracle.com/en/cloud/paas/identity-cloud/rest-api/rest-endpoints.html>

Below are a few examples of REST APIs for Identity Cloud Service.

A.1 Creating Group in IDCS using Rest Call

A.1.1 Group.json

```
{
  "displayName": "Test_Group",
  "externalId": "123456",
  "urn:ietf:params:scim:schemas:oracle:ids:extension:group:Group": {
    "creationMechanism": "api",
    "description": "This is test group"
  },
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:Group",
    "urn:ietf:params:scim:schemas:oracle:ids:extension:group:Group",
    "urn:ietf:params:scim:schemas:extension:custom:2.0:Group"
  ]
}
```

A.1.2 To Create a Test Group

A.1.2.1 To Get An Access Token

```
curl -k -X POST -u "client_id:client_secrets"
-d "grant_type=client_credentials&scope=urn:opc:idm:__myscopes__" "https://tenant-base-url/oauth2/v1/token" -o access_token.json
```

A.1.2.2 To Create A Group

```
curl -k -v -X POST -H "Content-Type:application/scim+json"
-H "Authorization: Bearer `cat access_token.json | cut -d : -f2-2 | cut -d , -f1 | tr -d '"'`" "https://tenant-base-url/admin/v1/Groups" -d"@group.json"
```

A.2 Creating A User In IDCS Using Rest Call

A.2.1 User.json

```
{
  "schemas": ["urn:ietf:params:scim:schemas:core:2.0:User"],
  "userName": "testuser",
  "name": {
    "familyName": "test_user",
    "givenName": "test_user",
    "middleName": "test_user"
  },
  "emails": [{
    "value": "test@test.com",
    "type": "work",
    "primary": true
  }]
}
```

A.2.2 Commands To A Create User

A.2.2.1 To Get Access Token

```
curl -k -X POST -u "client_id:client_secrets"
-d "grant_type=client_credentials&scope=urn:opc:idm:__myscopes__" "https://tenant-base-url/oauth2/v1/token" -o access_token.json
```

A.2.2.2 To Create User

```
curl -k -v -X POST -H "Content-Type:application/scim+json"
-H "Authorization: Bearer `cat access_token.json | cut -d : -f2-2 | cut -d , -f1 | tr -d '\n'" "https://tenant-base-url/admin/v1/Users" -d"@user.json"
```

A.3 Adding User To A Group

If you want to add existing user to group, use the sample below

A.3.1 Addusertogroup.json

```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "add",
      "path": "members",
      "value": [
        {
          "value": "useridvalue",
          "type": "User"
        }
      ]
    }
  ]
}
```

In place of `useridvalue`, place the user id that you want to add.

A.3.2 Commands To Add a User To a Group

A.3.2.1 To Get Access Token

```
curl -k -X POST -u "client_id:client_secrets"  
-d "grant_type=client_credentials&scope=urn:opc:idm:__myscopes__" "https://tenant-base-url/oauth2/v1/token" -o access_token.json
```

A.3.2.2 To Add User To The Group

```
curl  
-X PATCH  
-H "Content-Type:application/scim+json"  
-H "Authorization: Bearer `cat access_token.json | cut -d : -f2-2 | cut -d , -f1 | tr -d '`'"`"  
https://tenant-base-url/admin/v1/Groups/<ID>  
-d @Addusertogroup.json
```