Oracle® Revenue Management and Billing Cloud Service

Release 8.1.1

End-User Onboarding Using IAM

Revision 1.1

F76061-01

April 2023

ORACLE

Oracle Revenue Management and Billing Cloud Service End-User Onboarding Using IAM

F76061-01

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 document explains how to setup the security administrator account for the ORMB Cloud Service. It explains how to manage users and groups for the ORMB Cloud Service. In addition, it explains how to import and export bulk users and groups for the ORMB Cloud Service and how to use SAML on the Cloud environment for single sign-on.

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	Identity and Access Management with Identity Domains	Provides an overview for Oracle Cloud Infrastructure Identity and Access Management (IAM) with Identity Domains.
Section 2	Security Administrator Account	Describes how to setup a security administrator account for the ORMB Cloud Service.
Section 3	Managing Users	Describes how to manage users for the ORMB Cloud Service.
Section 4	Managing Groups	Describes how to manage groups for the ORMB Cloud Service.
Section 5	Managing Applications	Describes the pre-defined application roles and explains how to assign groups to an application.
Section 6	SAML Application	Explains how to use SAML on the Cloud environment for single sign-on.

Conventions

The following conventions are used across this document:

Convention	Meaning
boldface	Boldface indicates graphical user interface elements associated with an action, or terms defined in the text.

Convention	Meaning
italic	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.

Acronyms

The following acronyms are used in this document:

Acronym	Meaning
ORMB	Oracle Revenue Management and Billing
ORMBCS	Oracle Revenue Management and Billing Cloud Service
SSO	Single Sign-On
IDCS	Oracle Identity Cloud Service
IAM	Oracle Identity and Access Management
ID	Identity Domains
JWT	JSON Web Tokens
SAML	Security Assertion Markup Language
R8	Release 8
CSV	Comma-Separated Values
MFA	Multi-Factor Authentication
SP	Service Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
OCI	Oracle Cloud Infrastructure

Related Documents

You can refer to the following documents for more information:

Document Name	Description
Oracle Revenue Management and Billing Cloud Service Release 8.1.1 Release Notes	Lists the feature enhancements and client platforms and browsers that are supported in this release. It highlights different roles and responsibilities of Oracle and Customer in deploying, configuring, and maintaining the Oracle Revenue Management and Billing Cloud Service. It also highlights the known issues in this release.

Document Name	Description
Oracle Revenue Management and Billing Cloud Service Licensing Guide	Lists different features which are offered when you acquire a license for the following cloud services: • Oracle Financial Services Revenue Management and Billing • Oracle Insurance Revenue Management and Billing It also provides the licensing information of Oracle software and third-party JARs and components which are included in the above-mentioned cloud services.
Oracle Revenue Management and Billing Cloud Service REST Services Configuration Guide	Explains how to configure federated Web service login to access protected REST services on the ORMB Cloud environments.
Oracle Revenue Management and Billing Cloud Service SFTP Authentication and Access Permissions Guide	Explains how to configure SFTP authentication for the ORMB Cloud Service. It also explains how to access the SFTP server using WinSCP, how to create the directories and files on the SFTP server, and how to set the read, write, and execute permissions for a file or folder on the SFTP server.
Oracle Revenue Management and Billing Cloud Service SaaS Reporting using OAS	Provides an overview of the ORMB SaaS reporting architecture. It also explains how to use Oracle Analytics Server for ORMB SaaS reporting.
Oracle Revenue Management and Billing Cloud Service Federated Identity Configuration Using IAM	Provides an overview of federated SSO login. It explains how to configure federated SSO login with SAML for the ORMB Cloud Service.

Change Log

Revision	Last Update	Updated Section	Comments
1.1	05-Jul-2023	Related Documents	Added Information

Contents

1. Identity and Access Management with Identity Domains

This section provides an overview for Oracle Cloud Infrastructure Identity and Access Management (IAM) with Identity Domains. The Identity and Access Management tenancy is provided to the customer as part of the service subscriptions. The Identity and Access Management (IAM) is a built-in part of the Oracle Cloud Infrastructure and governs the access to the Oracle Cloud Infrastructure's resources along with Oracle Cloud Services. The Identity and Access Management components include:

- **Identity Domains** – Identity Domains are the part of IAM, where users and access to the Oracle Cloud Services are configured and managed. Each cloud service subscription includes at least one Identity Domain. The Identity Domains are managed exclusively by the customer. In ORMB, Cloud Service configurations are defined and maintained in an identity domain. An initial provision of the service results in all environments is connected to a single identity domain usually known as a Default Domain.
- **Application** - In ORMB Cloud Service, the application represents a single environment, either production or non-production. Applications are created through 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 the user with access to the component. Application roles are created through 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.

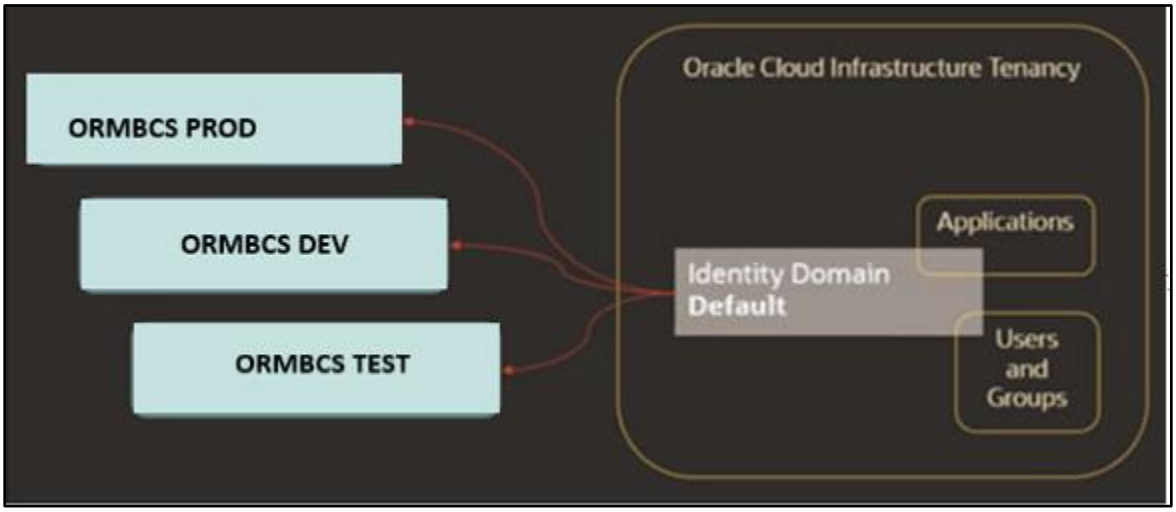

Figure 1: Identity Access Management with Identity Domains

This section provides an overview of the initial set up of your cloud server user community. It contains the following topics:

1.1 Activating the Security Administrator Account

Access the Oracle Identity Domain Console and perform the verification of the provisioned environments. Follow the steps described in the Security Administrator Account section.

1.2 Evaluating the Federated Single Sign-On Requirements

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

1.3 Modifying the Oracle Identity and Access Management Settings

Modify Oracle Identity and Access Management (IAM) 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 IAM Login page with your company's branding elements (optional).

1.4 Preparing the User Community

Determine the list of users who require access to the provisioned environments:

- 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 section describes how to setup the security administrator account. It contains the following topics:

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 service order is processed, the security administrator receives a cloud account activation email. The activation email contains:

- Activation URL
- The username and the temporary one-time password

To login first time to the Oracle Identity Domain Console, the security administrator should do the following:

1. Click the activation link received in the email or open the link in a browser. The **Login** page appears, as shown in the following figure:

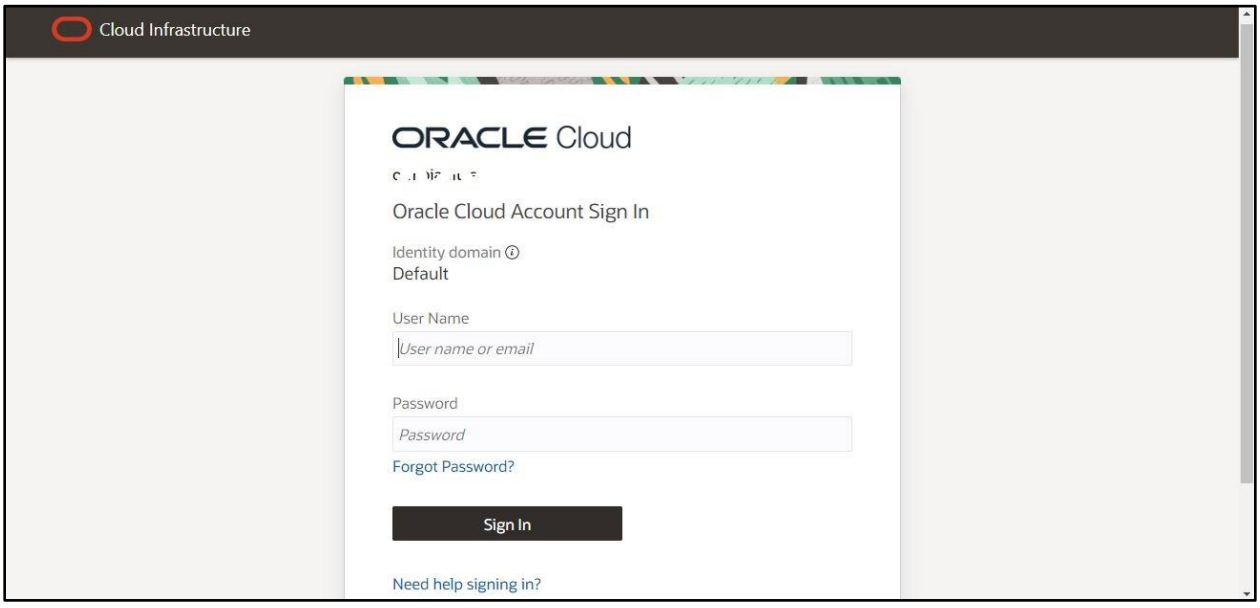

Figure 2: Login Page

2. Specify the username and temporary password in the respective fields.
3. Click **Sign In**. A message appears to create a new password.
4. Specify the new password in the respective field.
5. Confirm the new password and then click **Sign In**. The **Overview in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

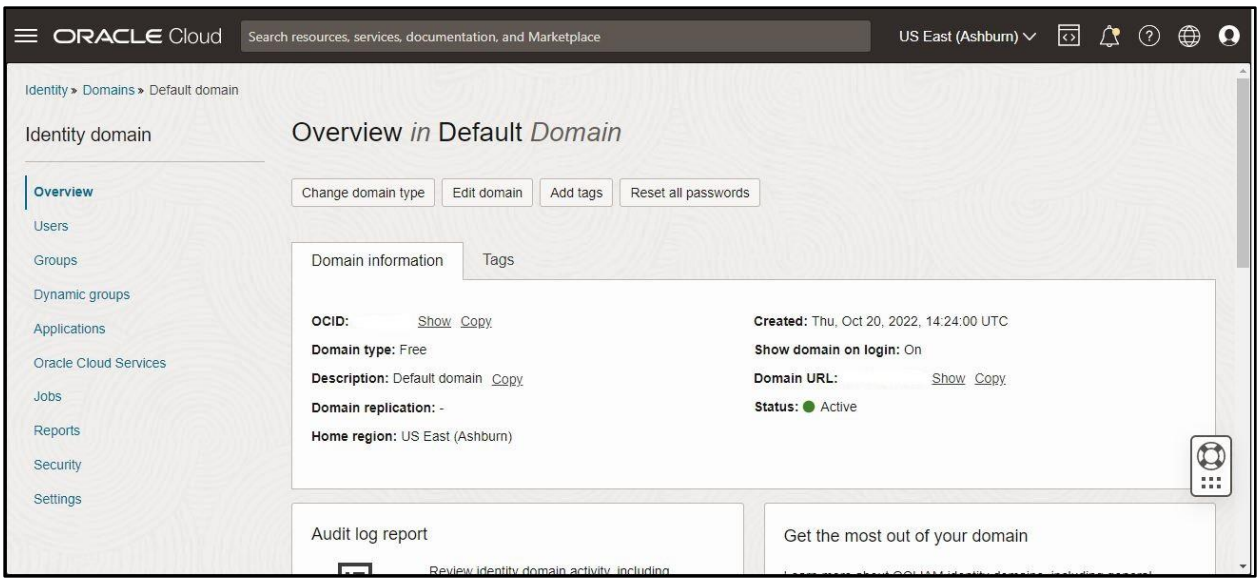

Figure 3: Overview in Default Domain Page

Subsequently, you can access the Oracle Identity Domain Console using the URL sent in the activation email communication.

2.2 Verifying the Security Administrator IAM Access

To verify the security administrator IAM access:

1. Open the **Oracle Identity Domain Console**. The **Overview in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

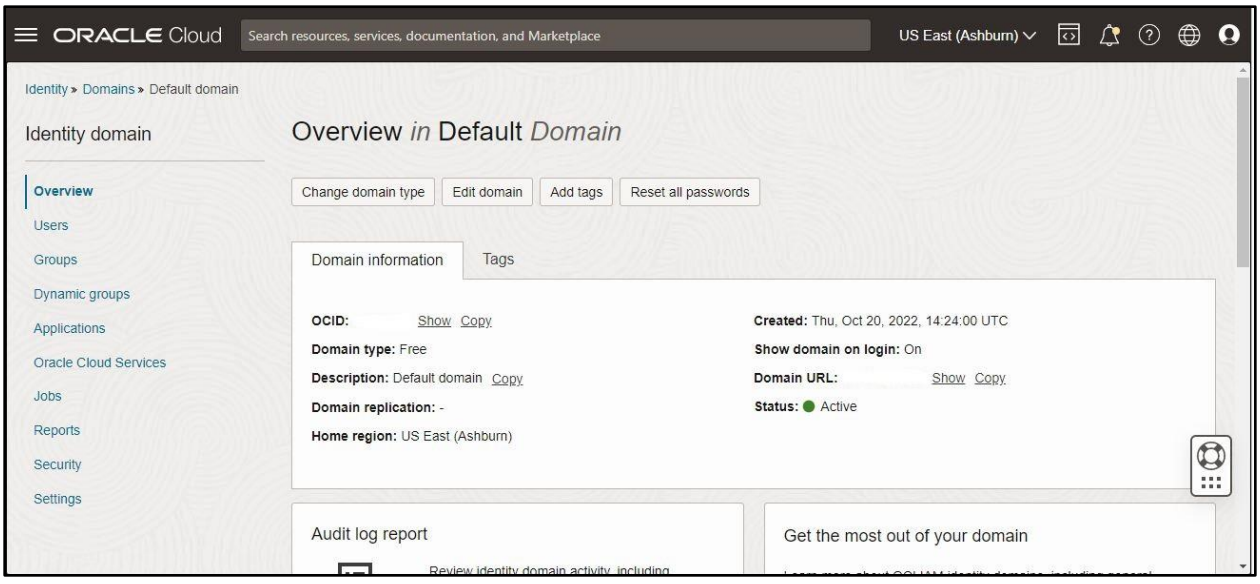

Figure 4: Overview in Default Domain Page

2. Click the **Security** option in the left navigation pane. The **Terms of use documents in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

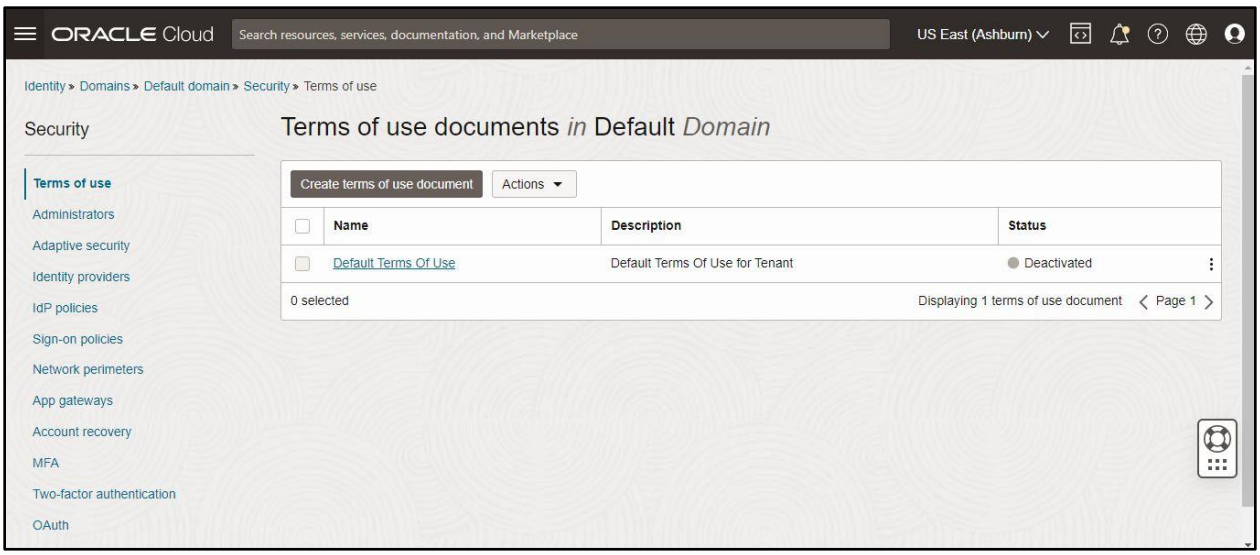

Figure 5: Terms of use documents in Default Domain Page

3. Click the **Administrators** option in the left navigation pane. The **Administrators in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

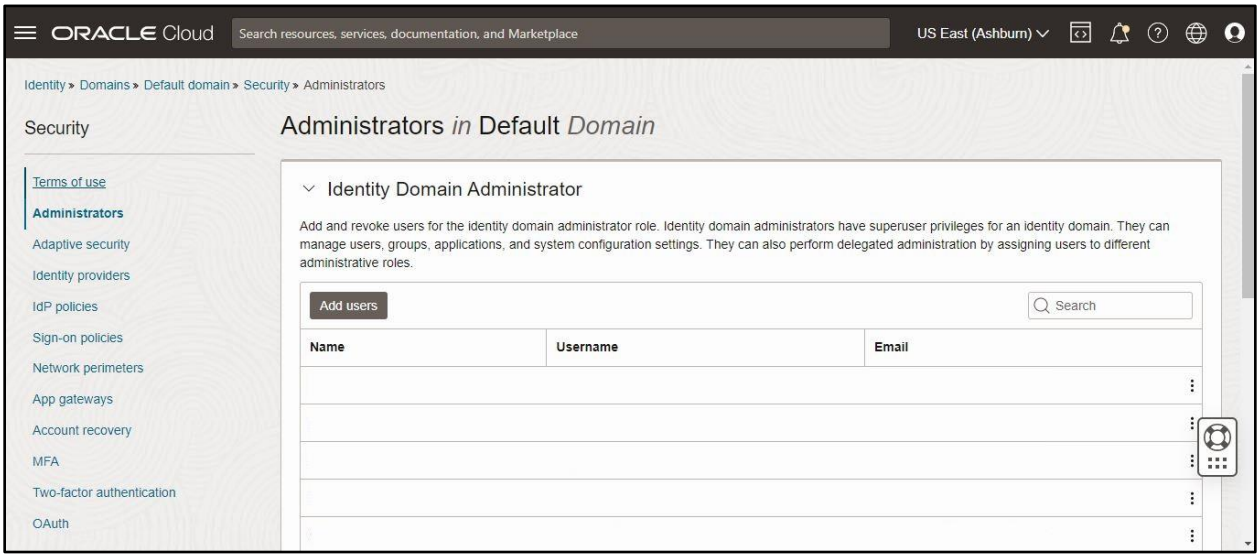

Figure 6: Administrators in Default Domain Page

4. Collapse the **Identity Domain Administrator** section.
5. Expand the **Security Administrator** section in the **Administrators in Default Domain** page. The details of the security administrator appear in the Oracle Identity Domain Console, as shown in the following figure:

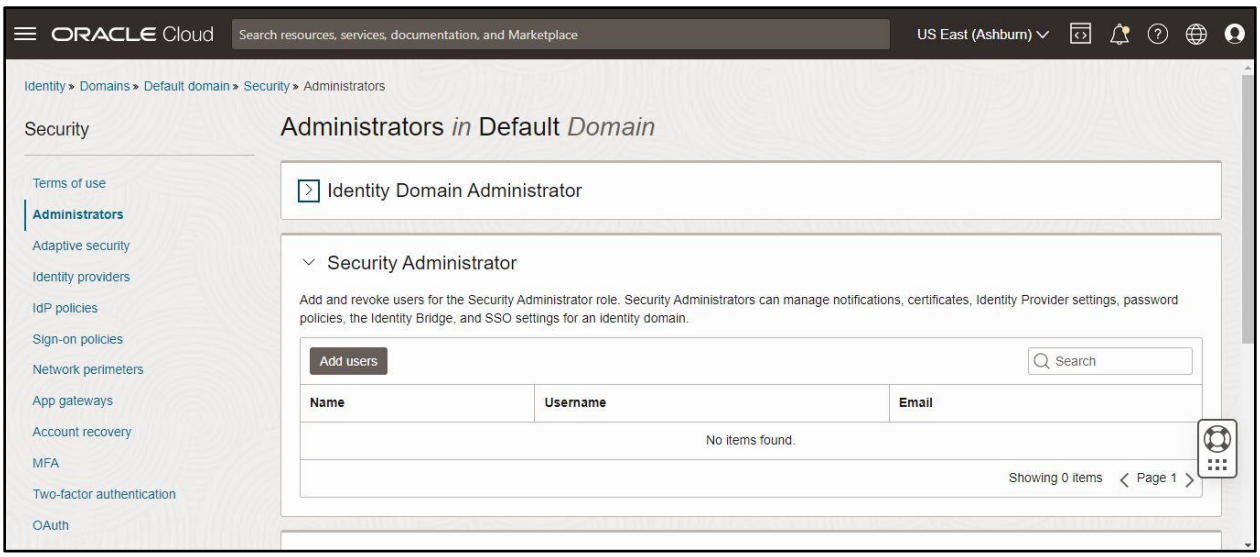

Figure 7: Security Administrator Details

6. Verify whether the security administrator's name appears in the **Security Administrator** list.

2.3 Verifying the Subscription Contents

To verify the subscription contents:

1. Click the **Applications** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Applications in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

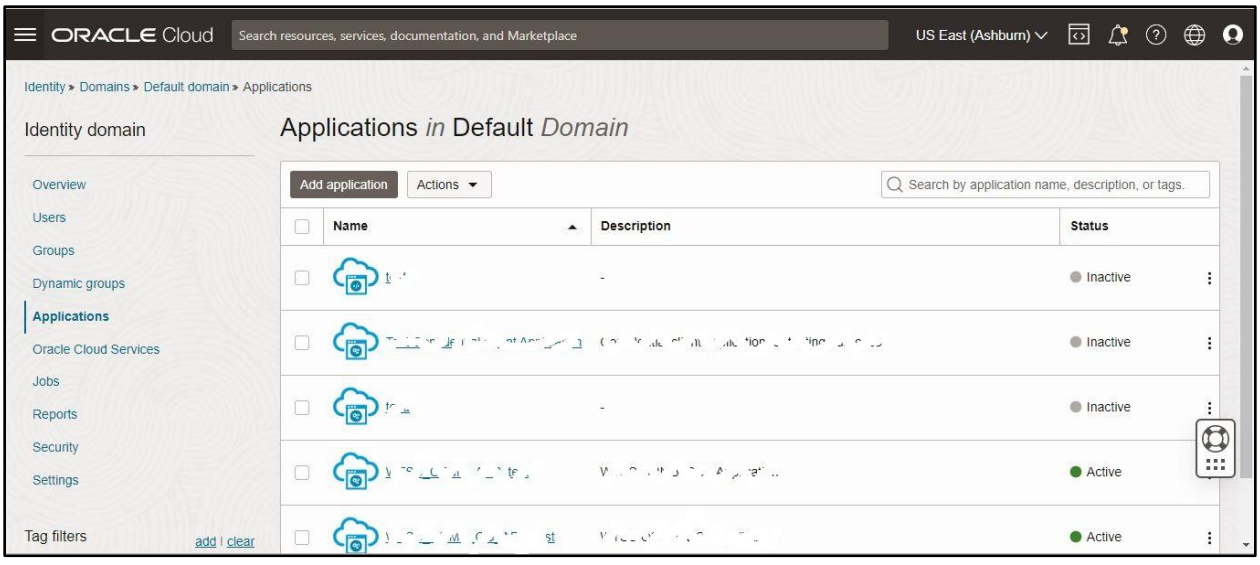

Figure 8: Applications in Default Domain Page

2. View the list of active and inactive applications in the **Applications in Default Domain** page.

Note: Oracle Revenue Management and Billing Cloud Service subscription contains at least one production and one or more non-production environments.

2.4 Exploring the Applications

To explore an application, click on any one of the available applications in the **Applications in Default Domain** page. An application represents a single environment and different application roles represent different components within the environment. To authorize a user's access to a certain component, you must assign the user account to the corresponding application role.

Note: Most of the application information is system-generated and read-only. Users can be assigned to the application roles only within the application.

3. Managing Users

This section describes how to manage Oracle Identity Cloud Service users. It contains the following topics:

3.1 Creating a User

You can create a new user only if you are a security administrator or an identity domain administrator. To create a new user:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

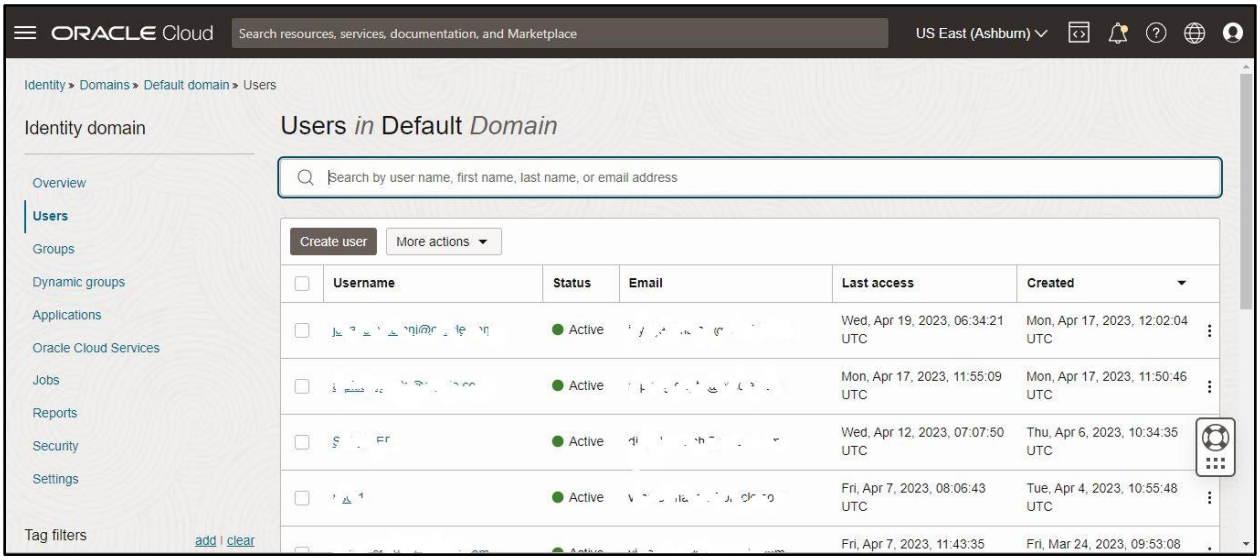

Figure 9: Users in Default Domain Page

2. Click **Create user** in the **Users in Default Domain** page. The **Create user** dialog box appears, as shown in the following figure:

Figure 10: Create User Dialog Box

3. Specify the first name, last name, and email address in the respective fields.
4. Ensure that the **Use the email address as the username** option is selected in the **Create user** dialog box.
5. In the **Groups** list, select the check box corresponding to the group to which you want to assign the user.

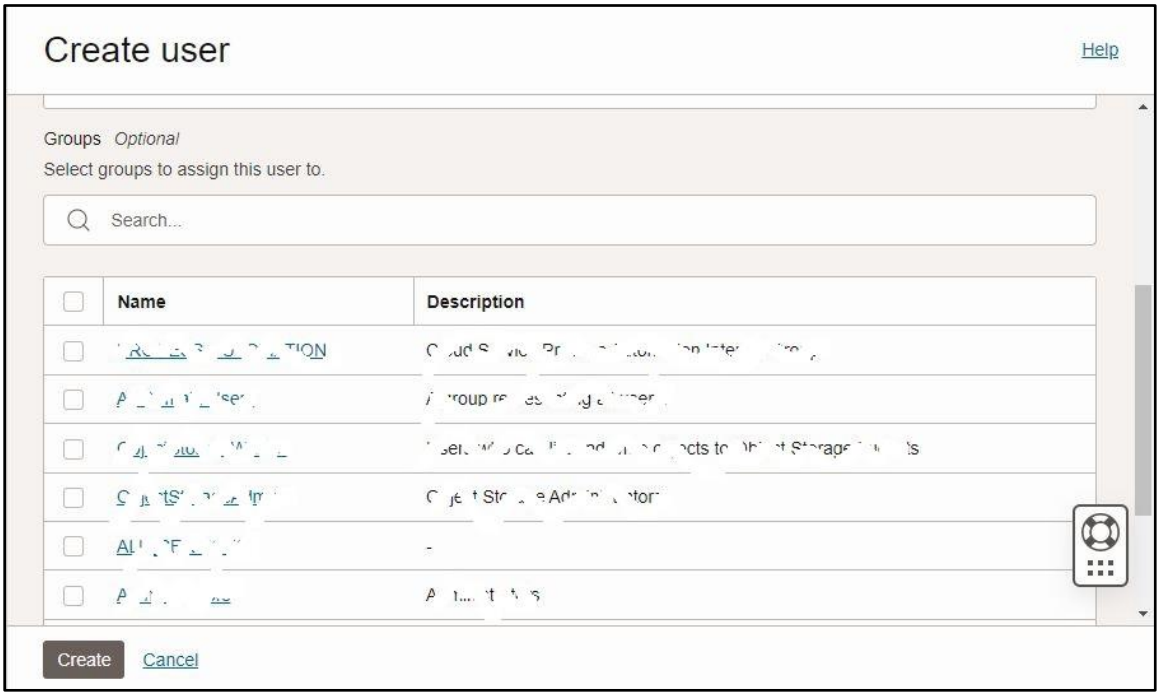

Figure 11: Assigning a User Account to a Group

Note: It is mandatory to assign the user to a group. You can assign a user to one or more groups. A group to which you want to assign the user should already be present in ORMB and it should have access to the **C1-USRLOGINDTLS** application service.

6. Click **Create**. The user is created and assigned to the respective group.

3.2 Activating an Inactive User

To activate an inactive user:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
2. Select the check box corresponding to an inactive user that you want to activate in the **Users in Default Domain** page.
3. Click **More actions**. A list appears, as shown in the following figure:

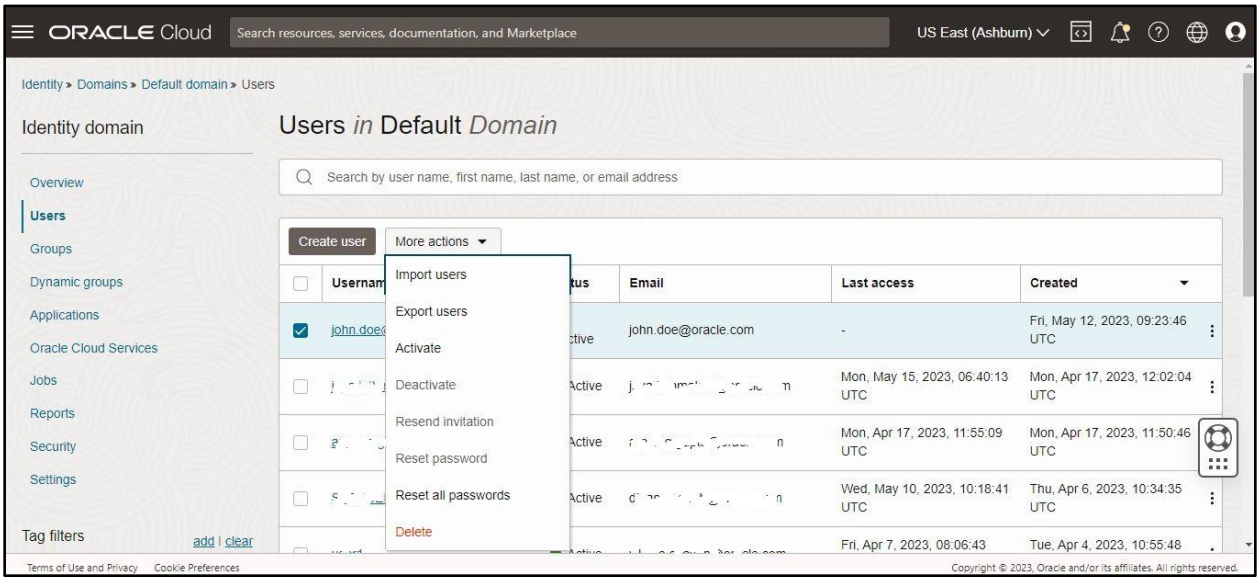

Figure 12: More Actions

4. Click the **Activate** option from the list. The **Confirm activation** dialog box appears, as shown in the following figure:

Figure 13: Confirm Activation Dialog Box

5. Click **Activate** to reinstate the access rights of the user. An email notification is sent to the user immediately after activating the account.

3.3 Assigning an Administrator Role to a User

By default, all users have self-service capabilities such as updating their profiles, resetting their passwords, and changing their email preferences. You might want to provide administrative capabilities to a user. For example, if you want a user to manage applications, you need to assign the application administrator role to the user.

A user can be assigned one or more administrator roles. The user inherits the privileges from the respective administrator role. If both the application administrator role and the user administrator role are assigned to a user, then the user can manage applications, users, groups, and group memberships.

Identity administration roles authorize users to manage configurations and administer an identity domain. Oracle Identity Domain Console contains the following administrator roles:

- **Identity Domain Administrator** - An identity domain administrators use the Infrastructure Classic Console or Applications Console to manage users and roles. An individual is granted an Identity Domain Administrator predefined role when an identity domain is set up for a service. However, if you want to create additional identity domain administrators or promote an existing user as an identity domain administrator, you can assign the Identity Domain Administrator role to the user. Identity domain administrators have superuser privileges for an identity domain. They can manage users, groups, applications, and system configuration settings. They can also perform delegated administration by assigning users to different administrative roles.
- **Security Administrator** – The security administrators can manage notifications, certificates, Identity Provider settings, password policies, the Identity Bridge, and SSO settings for an identity domain.
- **Application Administrator** – The application administrators can manage applications in identity domain. They can create, update, activate, deactivate, and delete applications. They can also grant and revoke applications for groups and users.
- **User Administrator** – The user administrators can manage users, groups, and group memberships for an identity domain.
- **User Manager** – The user manager can manage users of the selected groups.
- **Help Desk Administrator** - The help desk administrator can manage users of the selected groups.
- **Audit Administrator** – The audit administrator can generate audit reports for an identity domain.

To assign the security administrator role to a user, refer to the Assigning the Security Administrator Role to a User section. Similarly, you can assign other administrator roles to a user based on the requirements.

3.4 Assigning the Security Administrator Role to a User

To assign the Security Administrator role to a user:

1. Click the **Security** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Terms of use documents in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
2. Click the **Administrators** option in the left navigation pane. The **Administrators in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

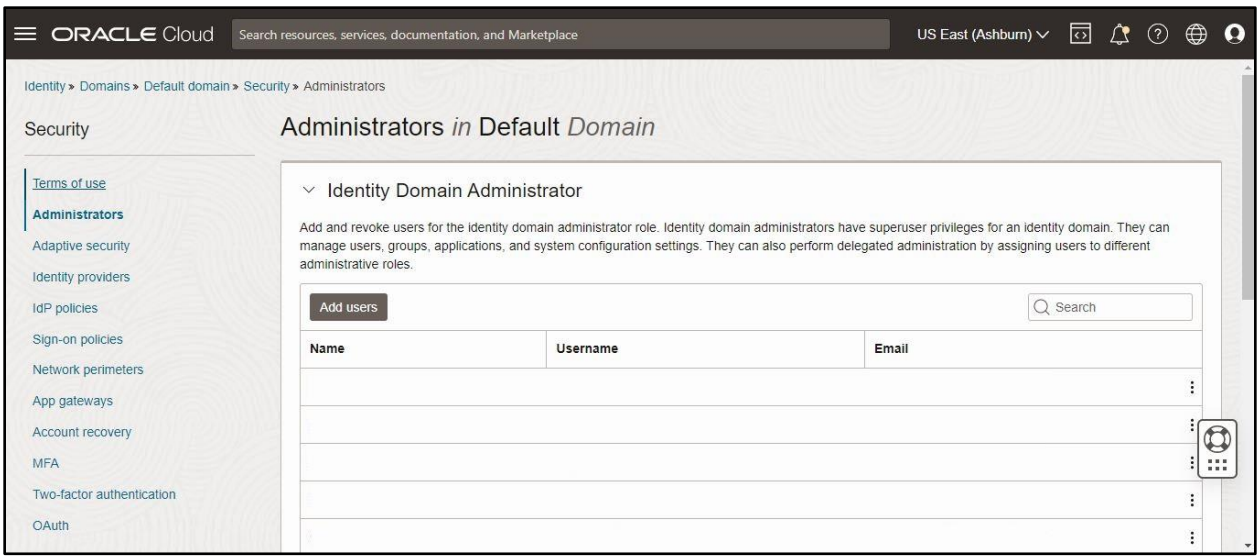

Figure 14: Administrators in Default Domain Page

3. Collapse the **Identity Domain Administrator** section.
4. Expand the **Security Administrator** section in the **Administrators in Default Domain** page. The details of the security administrator appear in the Oracle Identity Domain Console, as shown in the following figure:

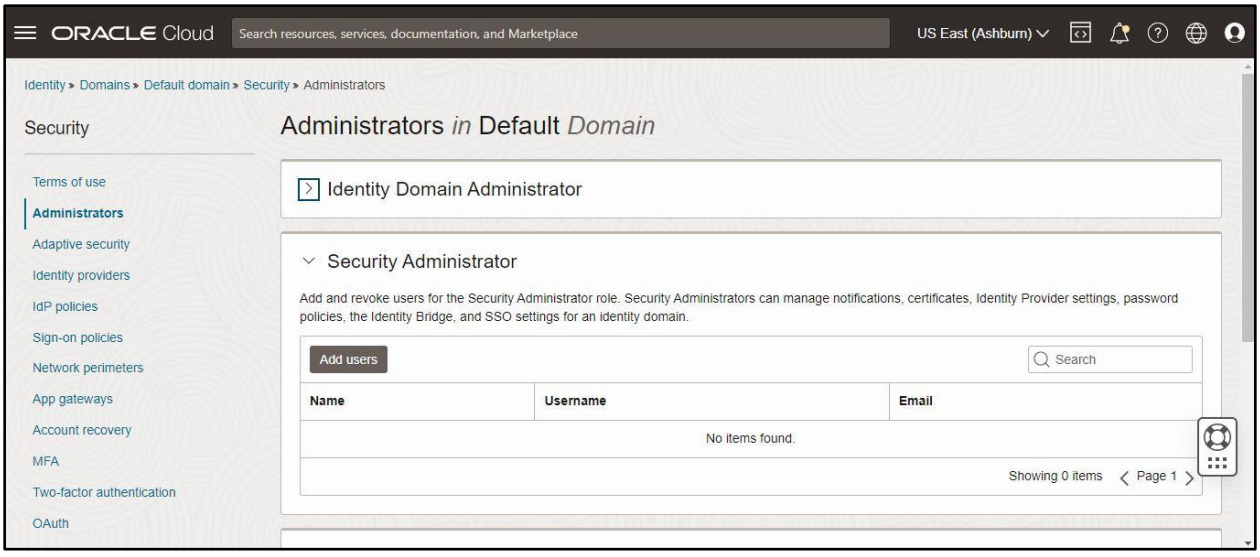

Figure 15: Security Administrator Details

5. Click **Add users** in the **Security Administrator** section. The **Add Security administrator** dialog box appears, as shown in the following figure:

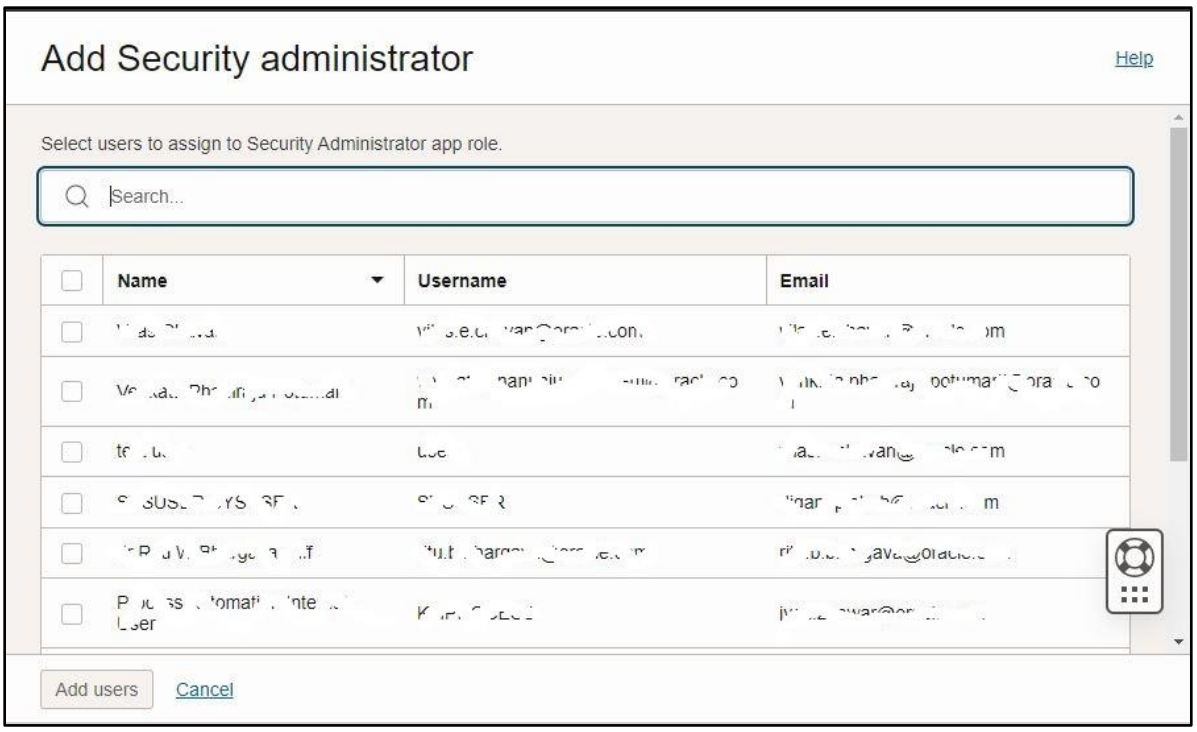

Figure 16: Add Security Administrator Dialog Box

6. If required, search the user to which you want to assign the security administrator role.
7. Select the check box corresponding to the user to which you want to assign the security administrator role and then click **Add users**. The user is assigned the security administrator role and is listed in the **Security Administrator** section.

3.5 Editing the Details of a User

To edit the details of a user:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
2. Click the link in the **Username** column corresponding to the user, whose details you want to edit, in the **Users in Default Domain** page. The respective user's information appears, as shown in the following figure:

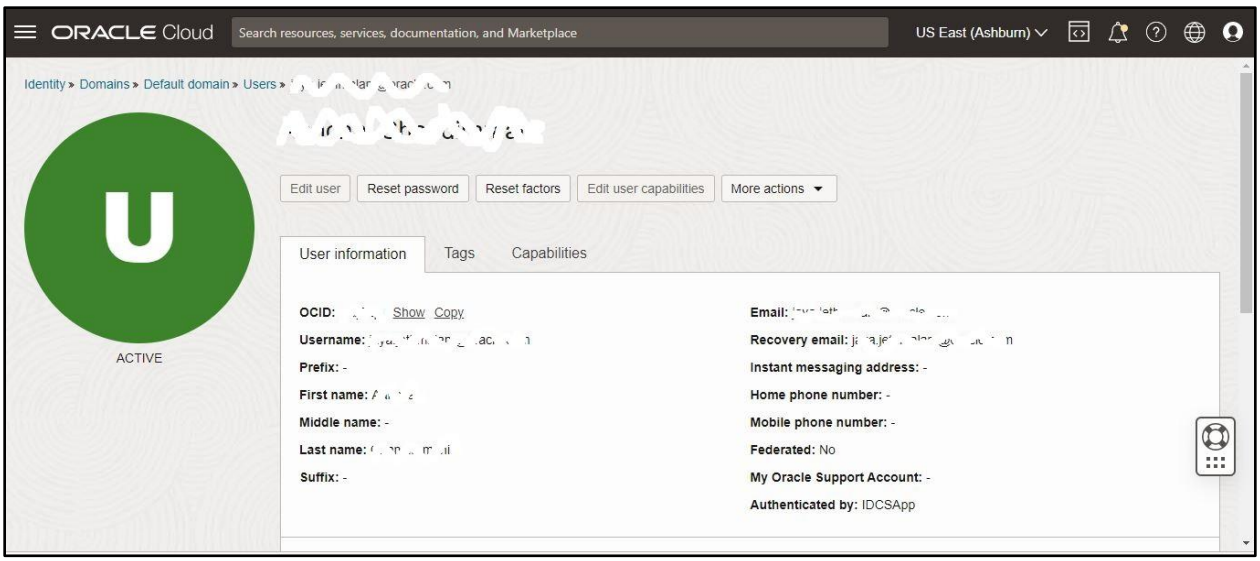

Figure 17: User Information

3. Click **Edit user**. The **Edit user** dialog box appears, as shown in the following figure:

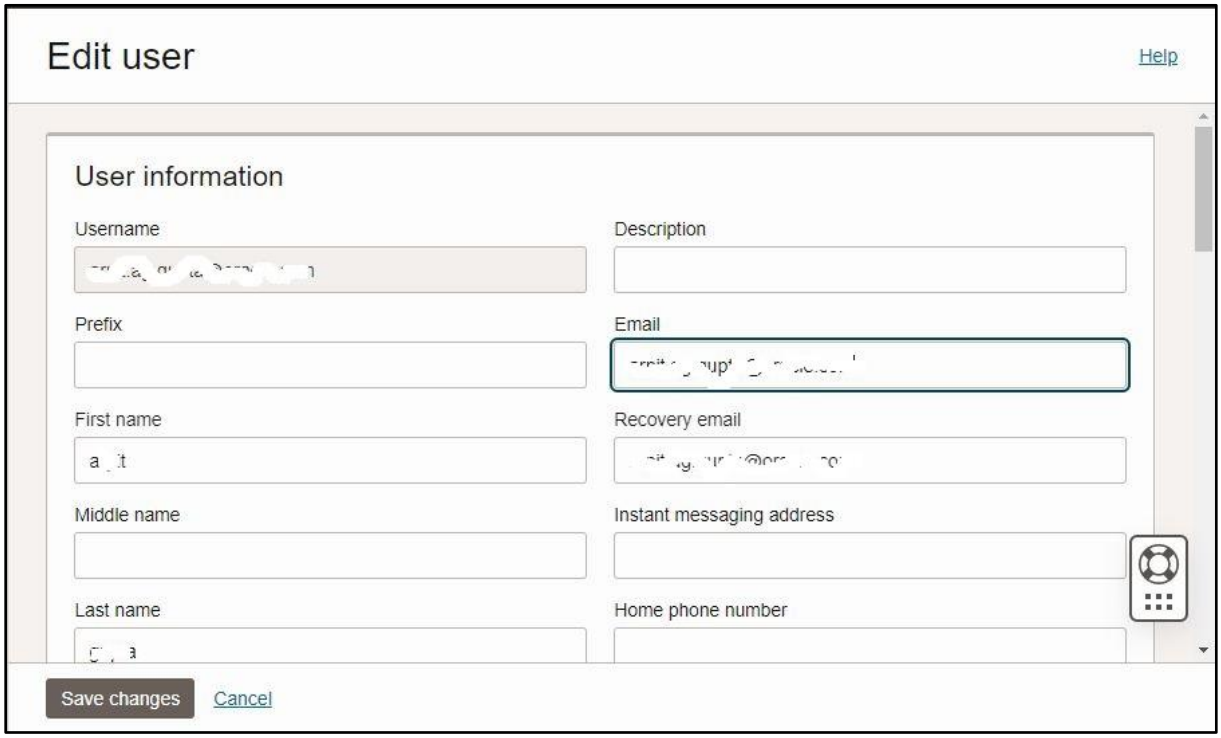

Figure 18: Edit User Dialog Box

4. Modify the required information and then click **Save changes**.

3.6 Deleting a User

To delete a user:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.

2. Select the check box corresponding to a user that you want to delete in the **Users in Default Domain** page.
3. Click **More actions**. A list appears, as shown in the following figure:

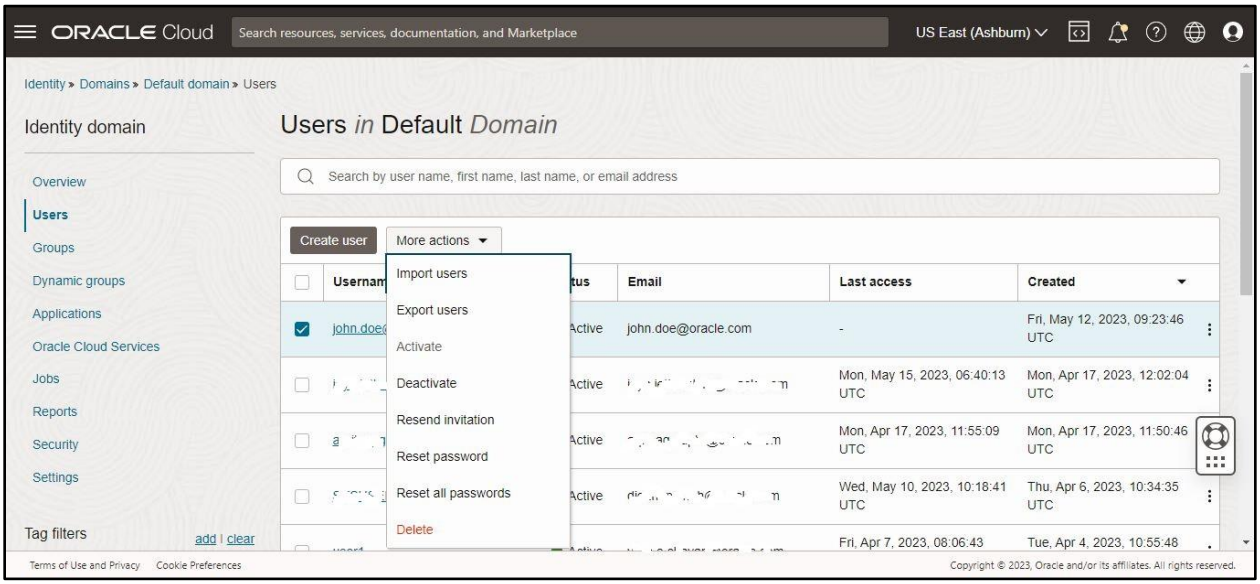

Figure 19: More Actions

4. Click the **Delete** option from the list. The **Delete user** dialog box appears, as shown in the following figure:

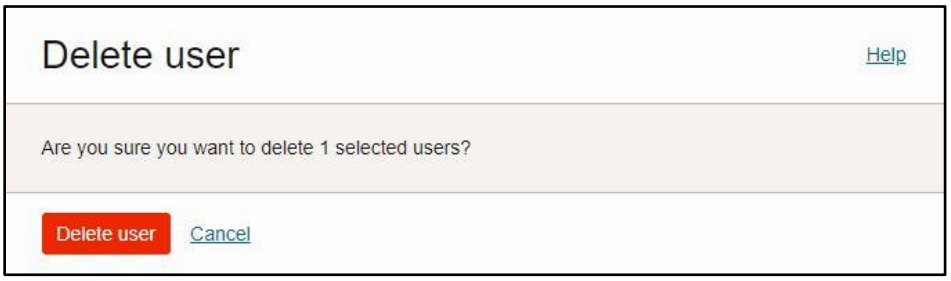

Figure 20: Delete User Dialog Box

5. Click **Delete user**. The user is permanently deleted from the system.

3.7 Resending an Invitation to a User to Activate their Account

Once a user is created, a welcome invitation is sent to the user, requesting that they activate the account. The new user must be activated before it can be used. If the user is not activated within a designated time, then the identity domain administrator can send another invitation to the user to activate the account.

Note: The initial email invitation gets expired after certain period.

To resend an invitation to a user to activate their account:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.

2. Select the check box corresponding to the user, to whom you want to resend the invitation, in the **Users in Default Domain** page.
3. Click **More actions**. A list appears, as shown in the following figure:

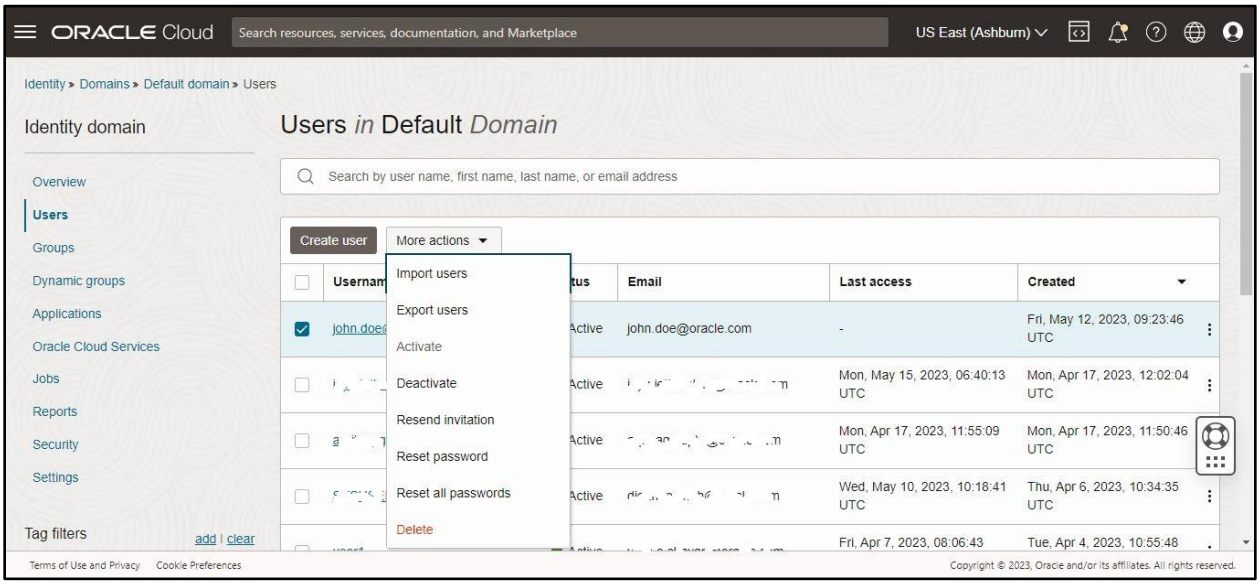

Figure 21: More Actions

4. Click the **Resend invitation** option from the list. The **Confirmation** dialog box appears, as shown in the following figure:

Figure 22: Confirmation Dialog Box

Note: If the user is already activated, the **Resend invitation** option is disabled.

5. Click **Send invitation**. The welcome invitation is sent to the user's email address.

3.8 Resetting Password for a User Account

You can reset the password of a single, multiple, or all the users at the same time. When you request a password change, a notification is sent to the user so that the user can provide a new password for the account. You cannot reset the passwords for the deactivated users.

To reset password for a user:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.

2. Select the check box corresponding to the user, whose password you want to reset, in the **Users in Default Domain** page.
3. Click **More actions**. A list appears, as shown in the following figure:

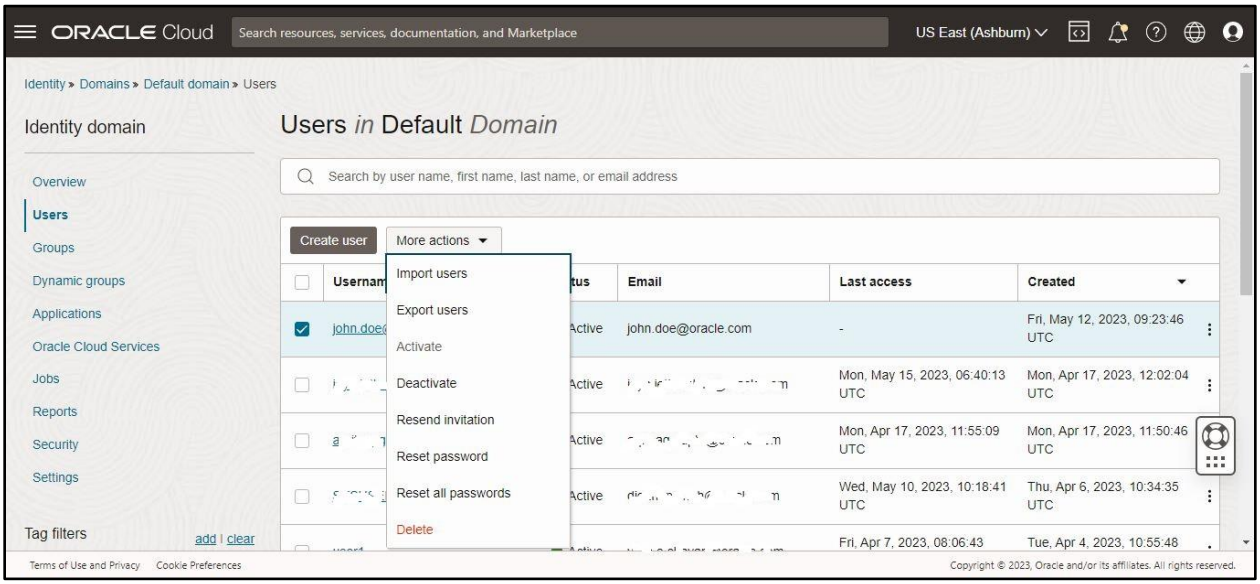

Figure 23: More Actions

4. Click the **Reset password** option from the list. The **Reset password** dialog box appears, as shown in the following figure:

Figure 24: Reset Password Dialog Box

5. Click **Reset password**. A password reset email notification is sent to the user.

Note: If you want to reset the password of all the users, select **Reset all passwords**. Then, in the **Reset all passwords** dialog box, click **Reset all passwords**.

3.9 Deactivating a User

You can temporarily deactivate a user. On deactivating a user, the access rights to Oracle Identity Cloud Service of the user are disabled. If the user deactivation tenure is longer than the password rotation period, the activation process resets the password.

To deactivate a user:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.

2. Select the check box corresponding to an active user that you want to deactivate in the **Users in Default Domain** page.
3. Click **More actions**. A list appears, as shown in the following figure:

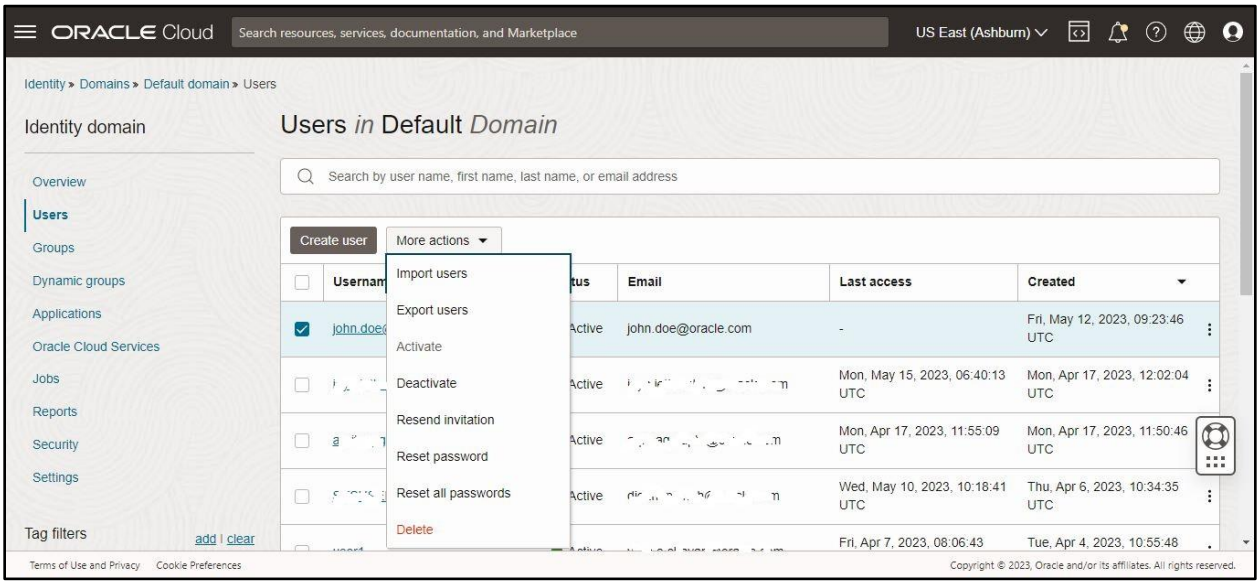

Figure 25: More Actions

4. Click the **Deactivate** option from the list. The **Confirm deactivation** dialog box appears, as shown in the following figure:

Figure 26: Confirm Deactivation

5. Click **Deactivate**. An email notification is sent to the user immediately after deactivating the account. Note that deactivated users are not able to login until you reactivate the user.

3.10 Importing Users

If you are an identity domain administrator or a user administrator, you can import users using a comma-separated values (CSV) file. Before you can import users, you must first create a CSV file that is properly formatted for the import process. To create a file for importing users:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
2. Click **More actions**. A list appears, as shown in the following figure:

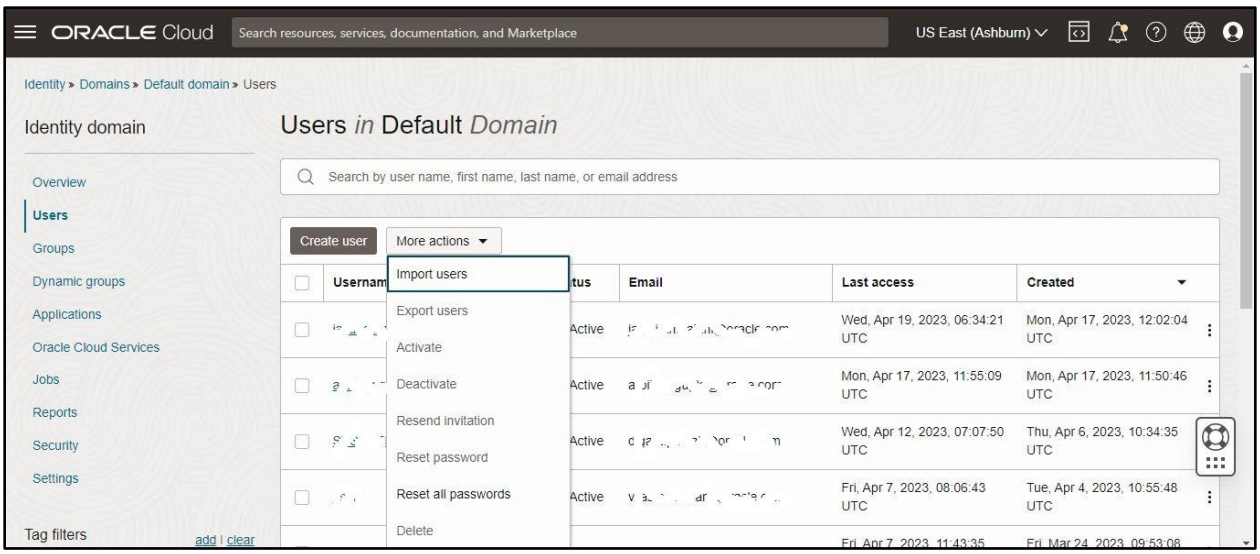

Figure 27: More Actions

3. Click the **Import users** option from the list. The **Import users** dialog box appears, as shown in the following figure:

Figure 28: Import Users Dialog Box

4. Click the **Download sample file** link. The **bulkImportSampleFilesCSV.zip** is downloaded.

Note: The sample files can be used as a template (or boilerplate) for creating the CSV file for importing data.

5. Unzip the **bulkImportSampleFilesCSV.zip** file. The contents include the following sample files:
   - AppRoleMembership.csv
   - Groups.csv

- Users.csv
- UsersAccounts.csv

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

Points to Note:

The maximum number of rows in the user import file must not exceed 1,00,000 and the import file size must not exceed 52 MB.

At a minimum, the file must have these exact column headings and distinct records with the unique combination of the following - User ID, Last Name, First Name, Work Email, Primary Email, Primary Email Type.

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.

The valid values for Primary Email Type are home, work, or other.

7. For each user, create a new row (line) and enter data into each column (field).

Note: Each row equals one record.

8. Save the file in the CSV format.
9. Open the CSV file with a text editor, such as Notepad.
10. Save the file with UTF-8 encoding.

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

To import users:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
2. Click **More actions**. A list appears.
3. Click the **Import users** option from the list. The **Import users** dialog box appears, as shown in the following figure:

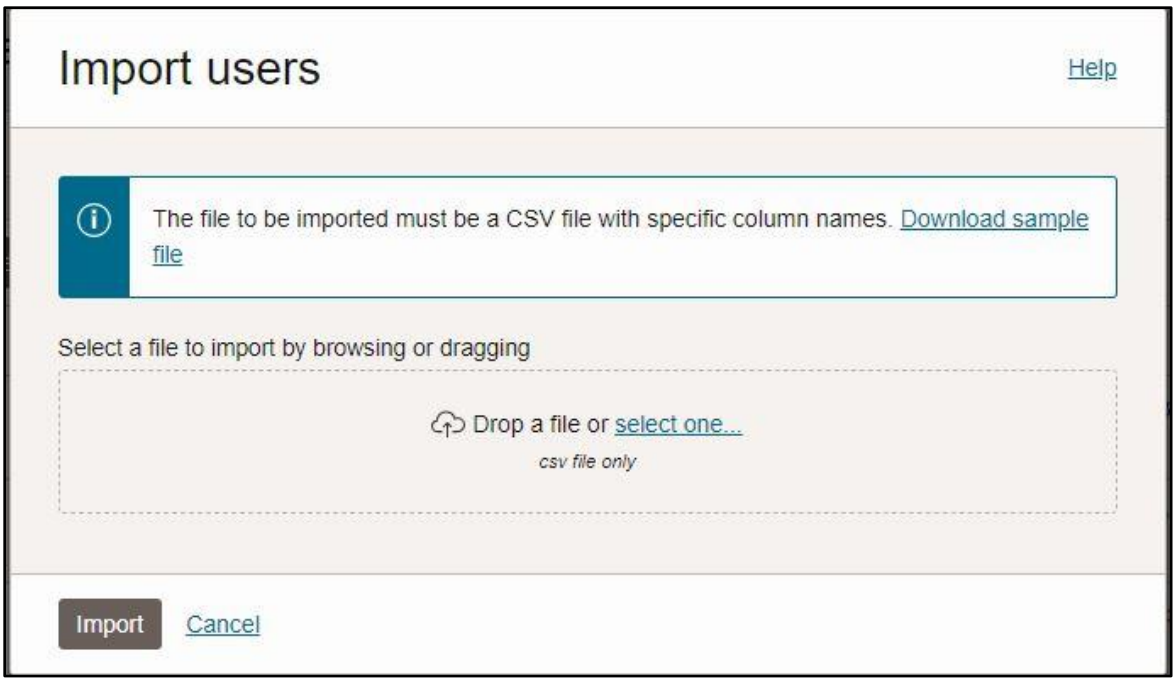

Figure 29: Import Users Dialog Box

4. Click the **select one** link. The **Open** dialog box appears, as shown in the following figure:

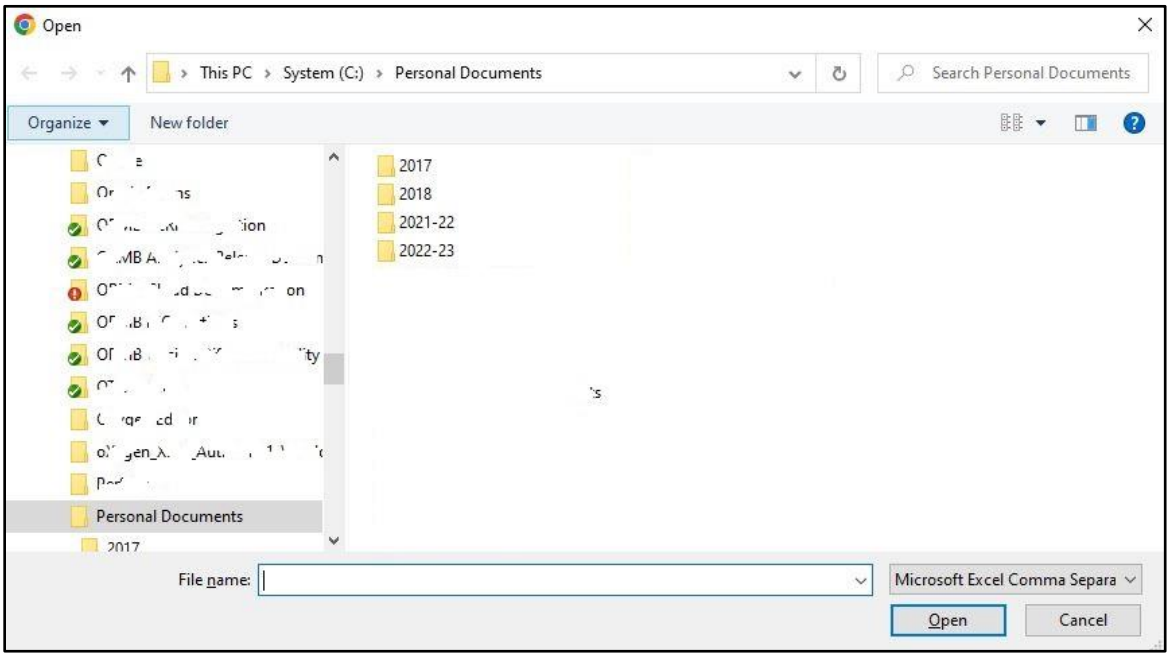

Figure 30: Open Dialog Box

5. Browse and select the file from where you want to import the user data and then click **Open**. The file is selected.
6. Click **Import**. A message appears indicating that the import process has started, as shown in the following figure:

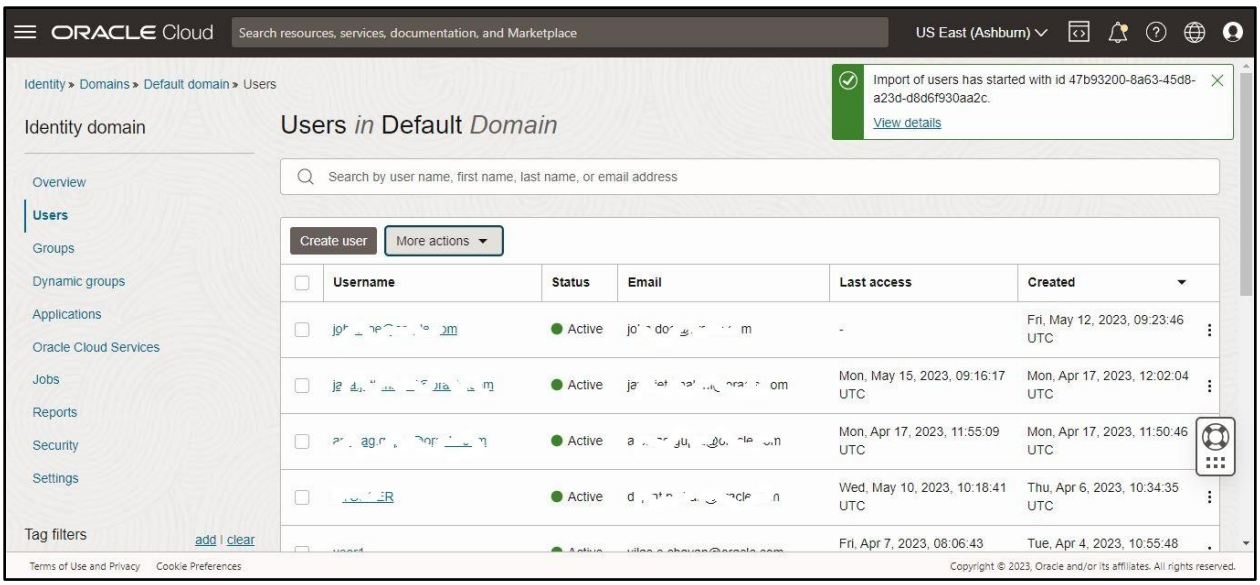

Figure 31: Information Message

7. Click **View details**. The **Job Details** screen appears, as shown in the following figure:

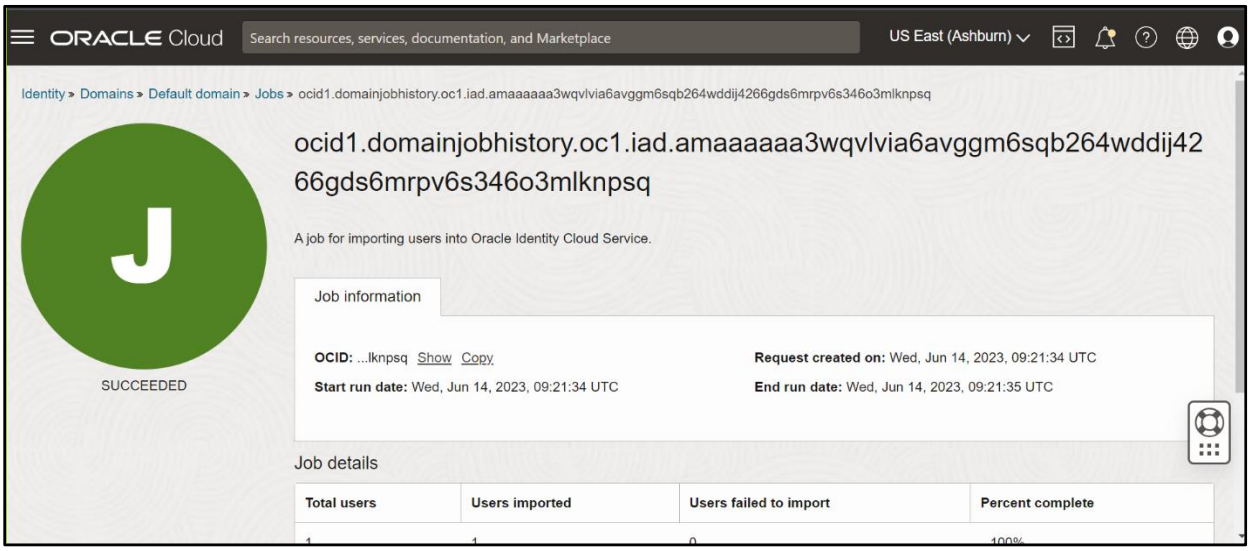

Figure 32: Job Details

Once the import process is complete, the **Job Details** screen displays the details, such as:

- Percent Completion
- Total Users
- Users Imported Successfully
- Users Failed to Import

3.11 Exporting Users Accounts

To export users:

1. Click the **Users** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Users in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
2. Select the check box corresponding to one or more users, whose details you want to export, in the **Users in Default Domain** page.
3. Click **More actions**. A list appears, as shown in the following figure:

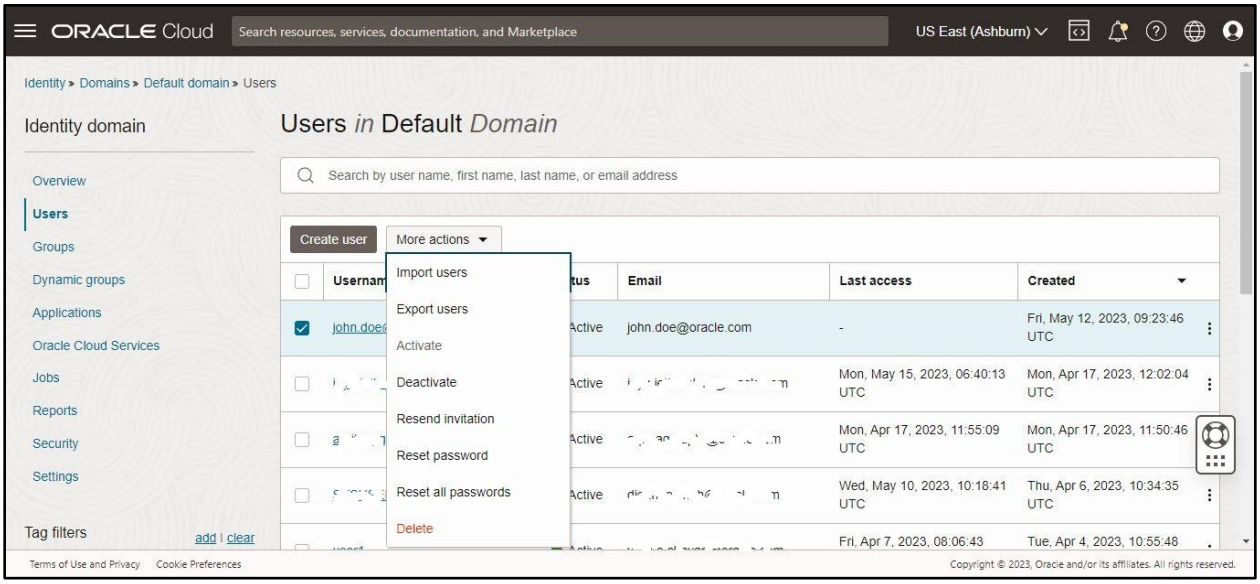

Figure 33: More Actions

4. Click the **Export users** option from the list. The **Export users** dialog box appears, as shown in the following figure:

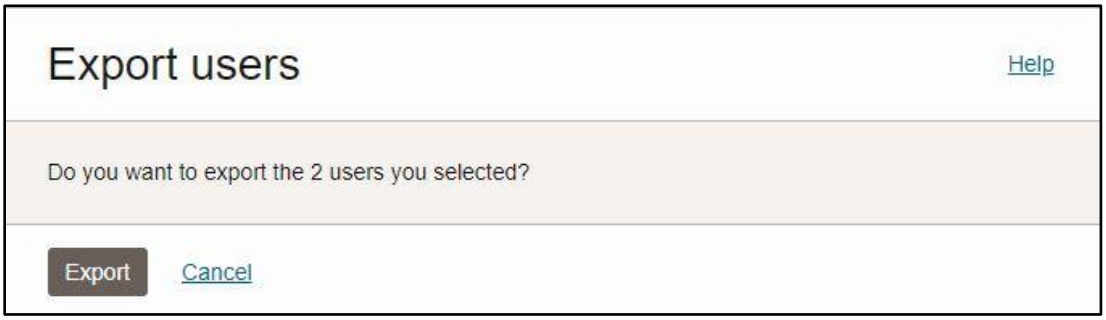

Figure 34: Export Users Dialog Box

5. Click **Export**. A message appears indicating that the export process has started, as shown in the following figure:

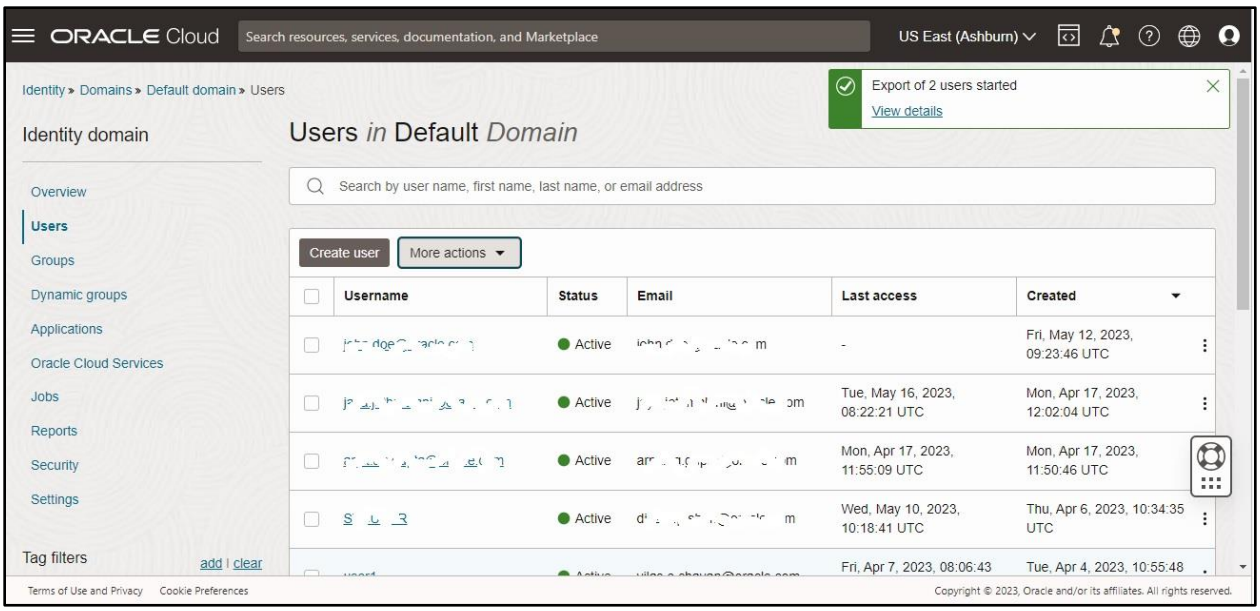

Figure 35: Information Message

6. Click **View details**. The **Job Details** screen appears, as shown in the following figure:

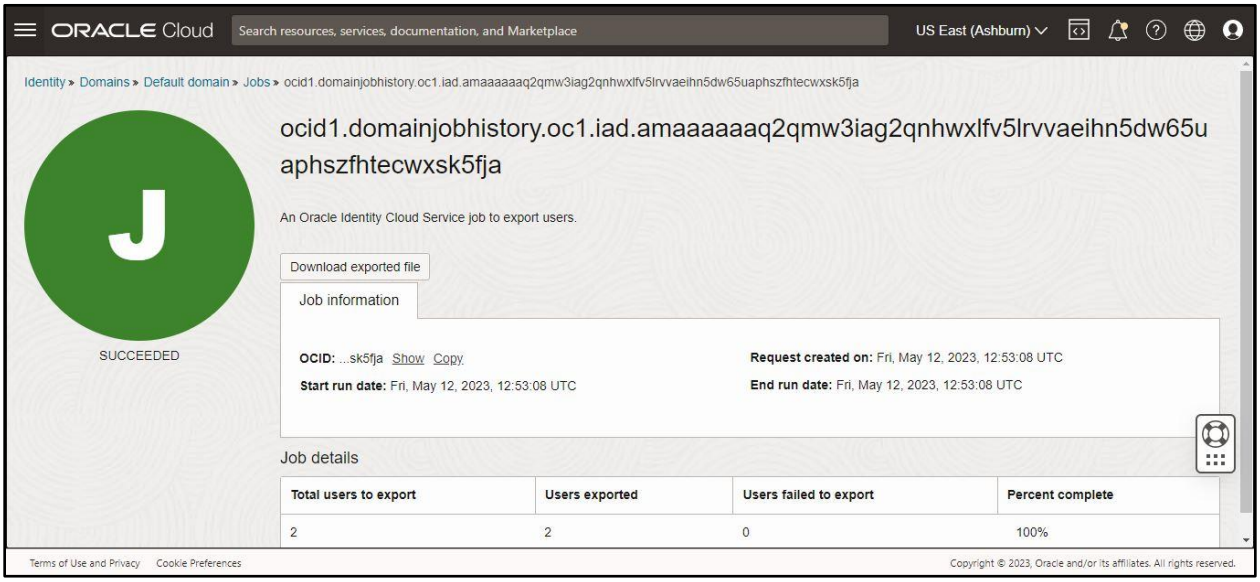

Figure 36: Job Details

Once the export process is complete, the **Job Details** screen displays the details, such as:

- Percent Completion
- Total Users
- Users Exported Successfully
- Users Failed to Export

4. Managing Groups

This section describes how to manage Oracle Identity Cloud Service groups. It contains the following topics:

4.1 Creating a Group

To create a group:

1. Click the **Groups** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Groups in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

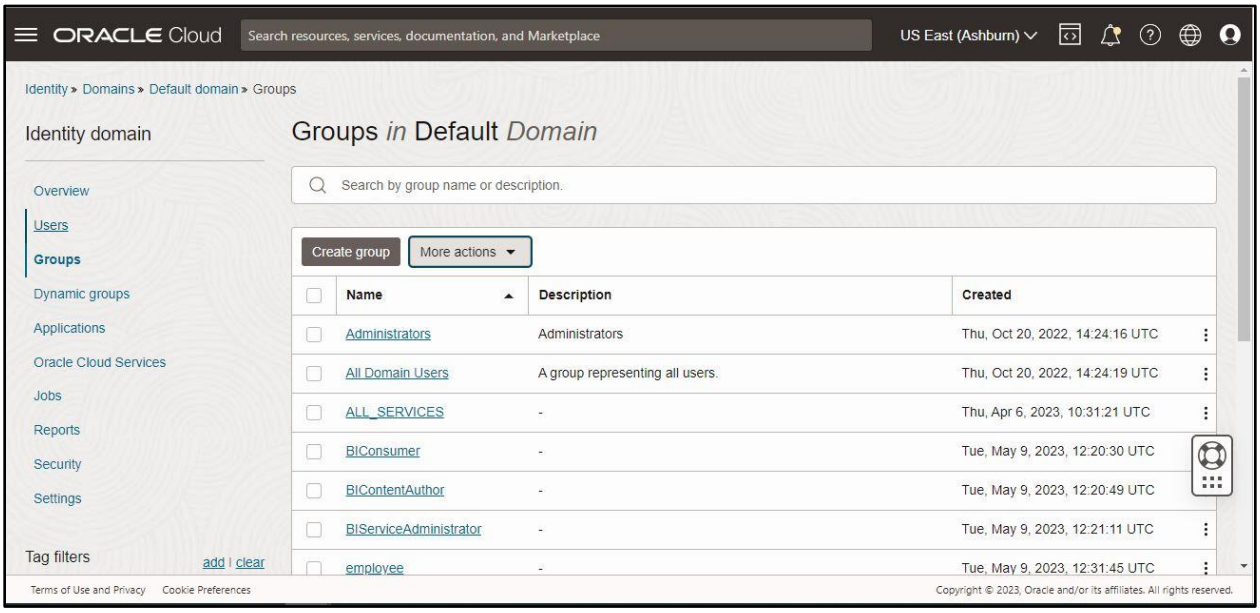

Figure 37: Groups in Default Domain Page

2. Click **Create group**. The **Create group** dialog box appears, as shown in the following figure:

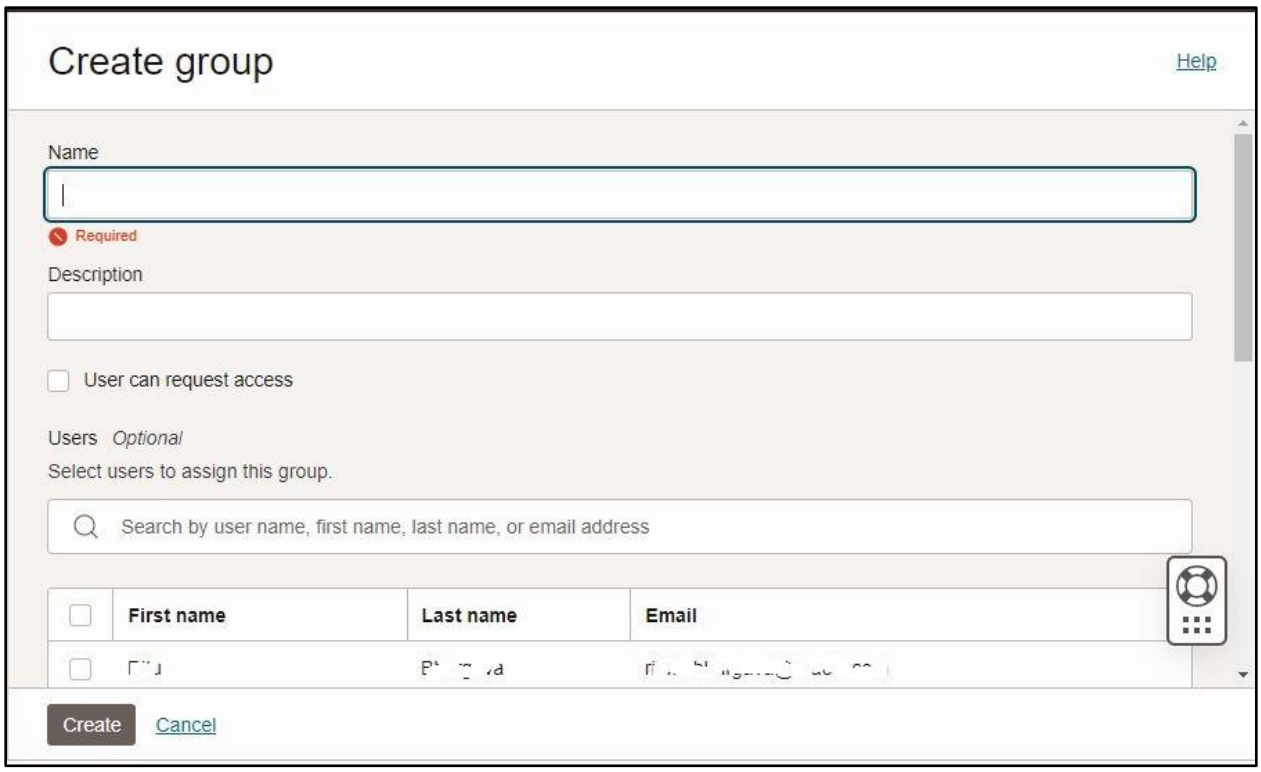

Figure 38: Create Group Dialog Box

3. Specify the group name and description in the respective fields.
4. Select the **User can request access** option if you want to allow the users to request access for this group.
5. Search for the user that you want to add in the group and then click the check box corresponding to the user.
6. Click **Create**. The group is created, and the user is assigned to the group.

4.2 Adding Users to a Group

To add users to an existing group:

1. Click the **Groups** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Groups in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
1. Click the link in the **Name** column corresponding to the group, whose details you want to edit, in the **Groups in Default Domain** page. The respective group's information appears, as shown in the following figure:

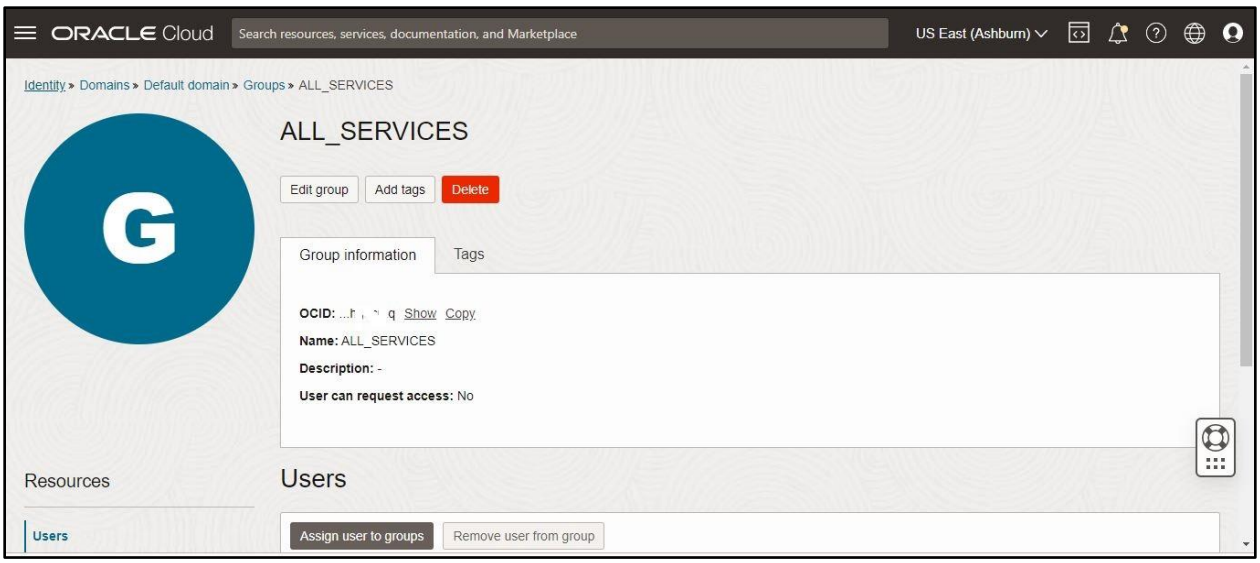

Figure 39: Group Details

2. Click the **Assign user to groups** button. The **Add users** dialog box appears, as shown in the following figure:

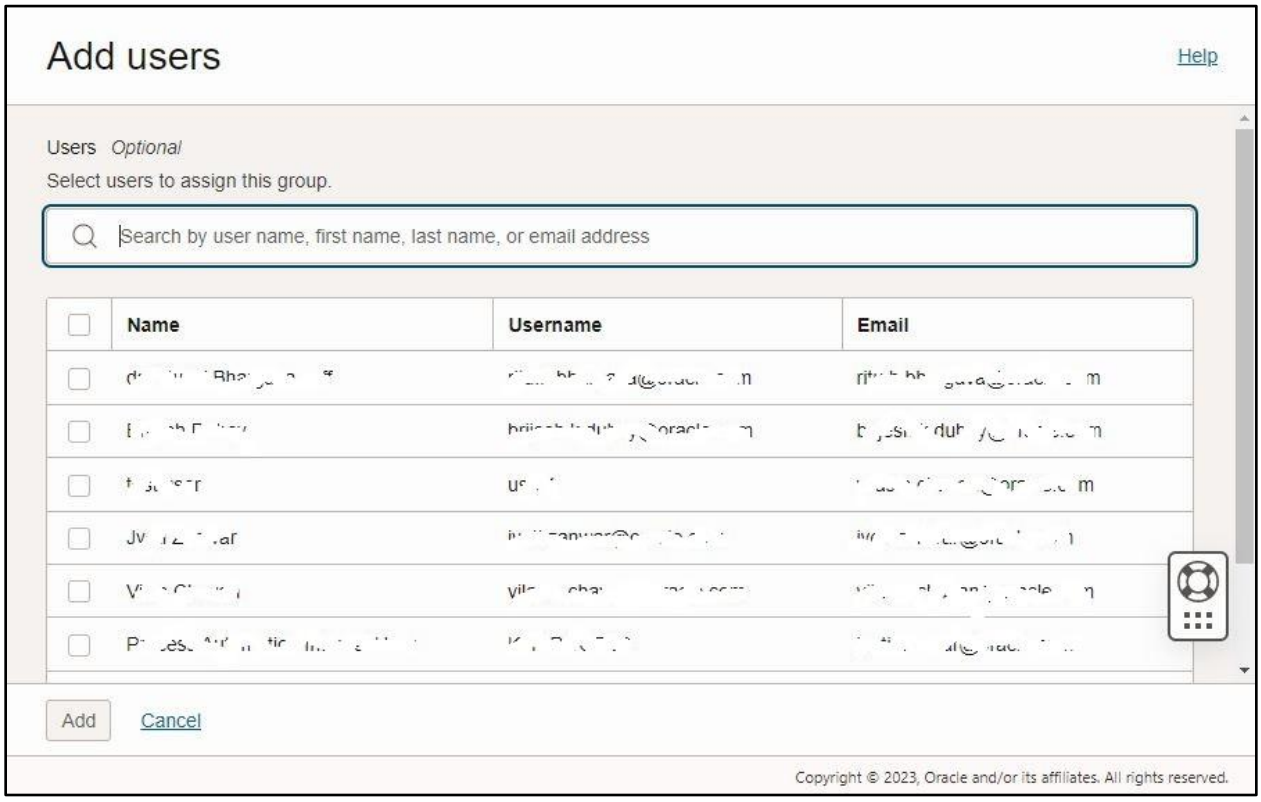

Figure 40: Add Users Dialog Box

3. Search for the user that you want to add in the group.
4. Select the check box corresponding to the user and then click **Add**. The user is added to the group.

4.3 Importing Groups

If you are an identity domain administrator or a user administrator, you can import groups using a comma-separated values (CSV) file. Before you can import groups, you must first create a CSV file that is properly formatted for the import process. To create a file for importing groups:

1. Click the **Groups** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Groups in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

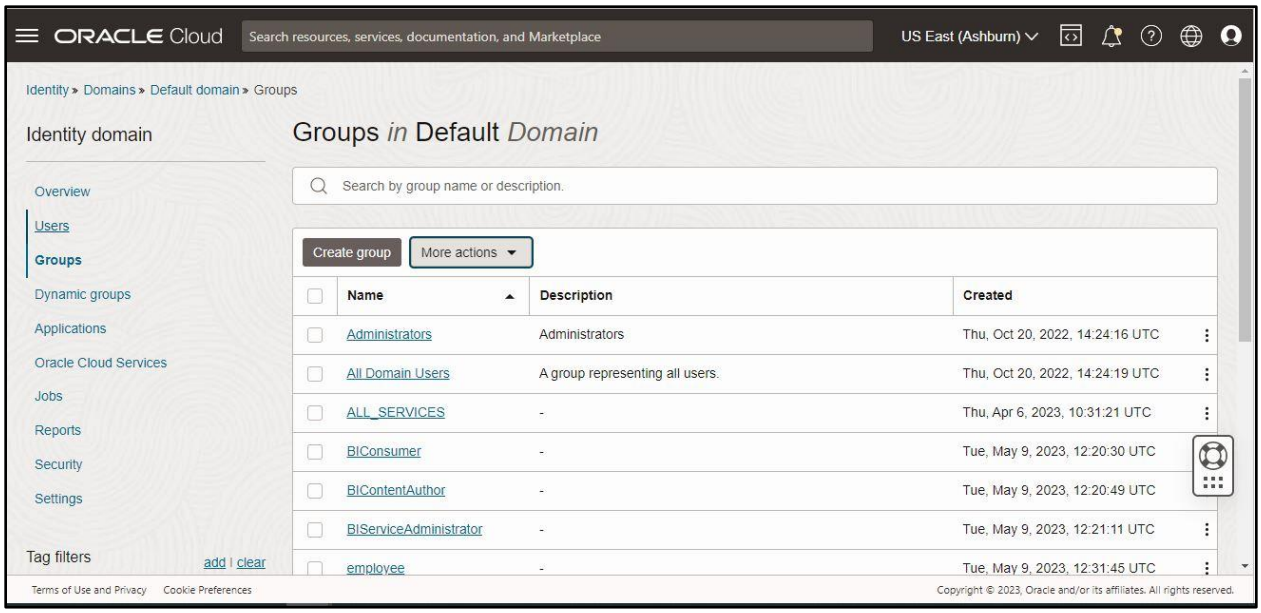

Figure 41: Groups in Default Domain Page

2. Click **More actions**. A list appears, as shown in the following figure:

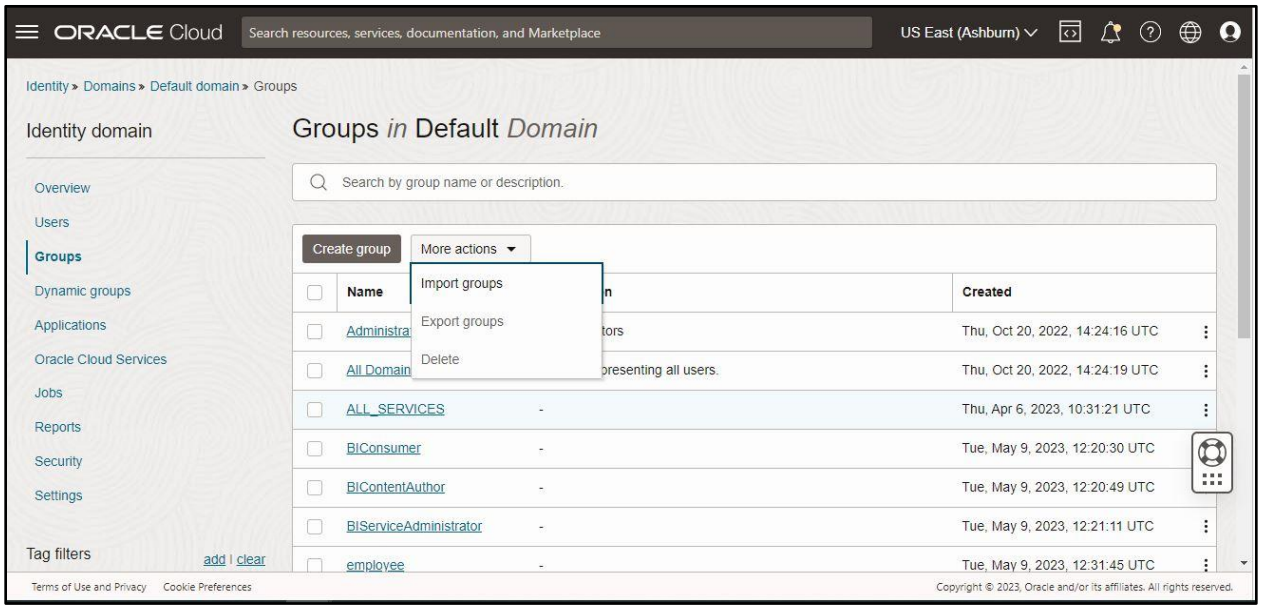

Figure 42: More Actions

3. Click the **Import groups** option from the list. The **Import groups** dialog box appears, as shown in the following figure:

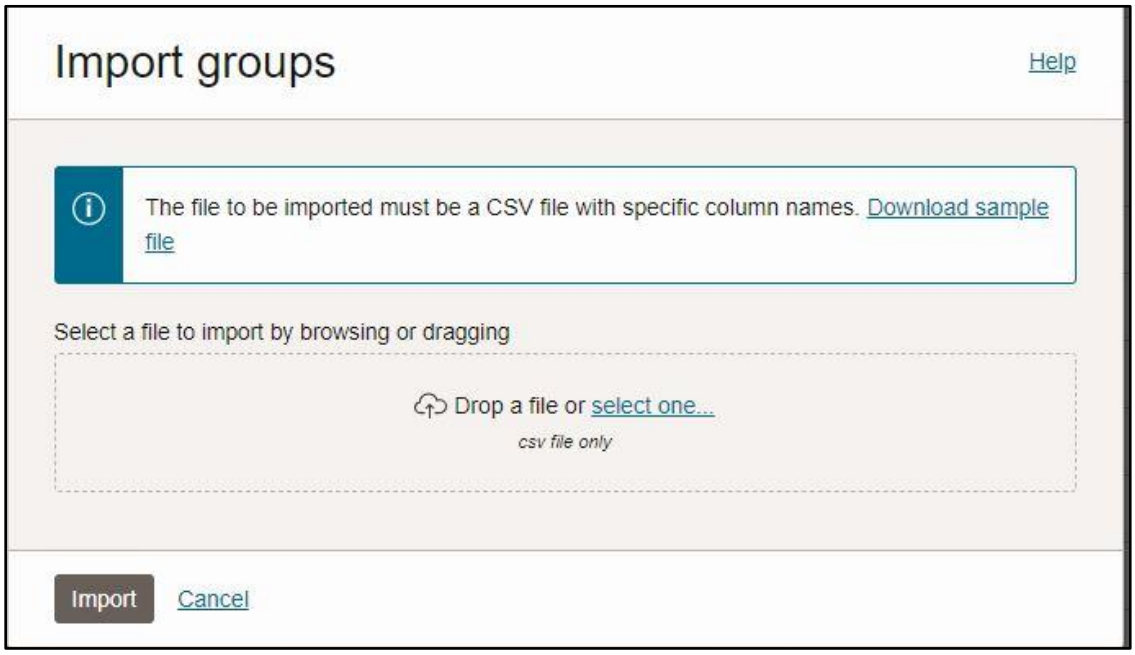

Figure 43: Import Groups Dialog Box

4. Click the **Download sample file** link. The **bulkImportSampleFilesCSV.zip** is downloaded.

Note: The sample files can be used as a template (or boilerplate) for creating the CSV file for importing data.

5. Unzip the **bulkImportSampleFilesCSV.zip** file. The contents include the following sample files:
   - AppRoleMembership.csv
   - Groups.csv
   - Users.csv
   - UsersAccounts.csv
6. Create an import file using the **Groups.csv** sample file. The **Groups.csv** file is a simple text file in a tabular format (comprising of rows and columns). The first row in the file defines the columns (fields) in your table.

Points to Note:

The maximum number of rows in the group import file must not exceed 1,00,000 and the import file size must not exceed 52 MB.

At a minimum, the file must have the following exact column headings - Display Name, Description, User Members.

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.

7. For each group, create a new row (line) and enter data into each column (field).

Note: Each row equals one record.

8. Save the file in the CSV format.
9. Open the CSV file with a text editor, such as Notepad.
10. Save the file with UTF-8 encoding.

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

To import groups:

11. Click the **Groups** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Groups in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
12. Click **More actions**. A list appears.
13. Click the **Import groups** option from the list. The **Import groups** dialog box appears, as shown in the following figure:

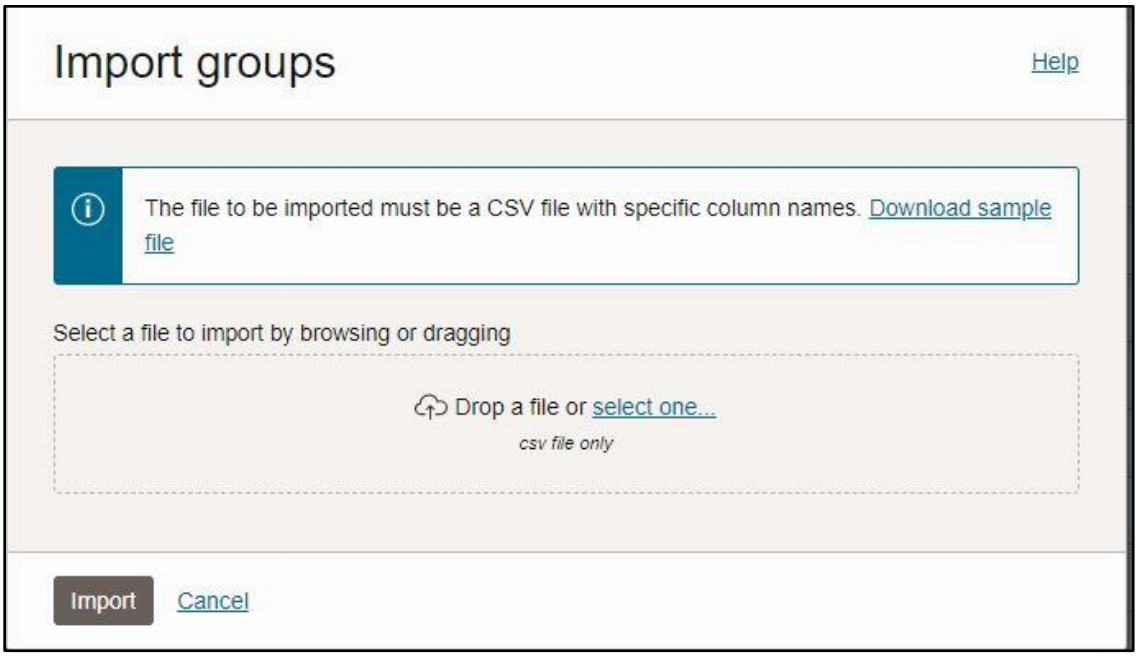

Figure 44: Import Groups Dialog Box

14. Click the **select one** link. The **Open** dialog box appears, as shown in the following figure:

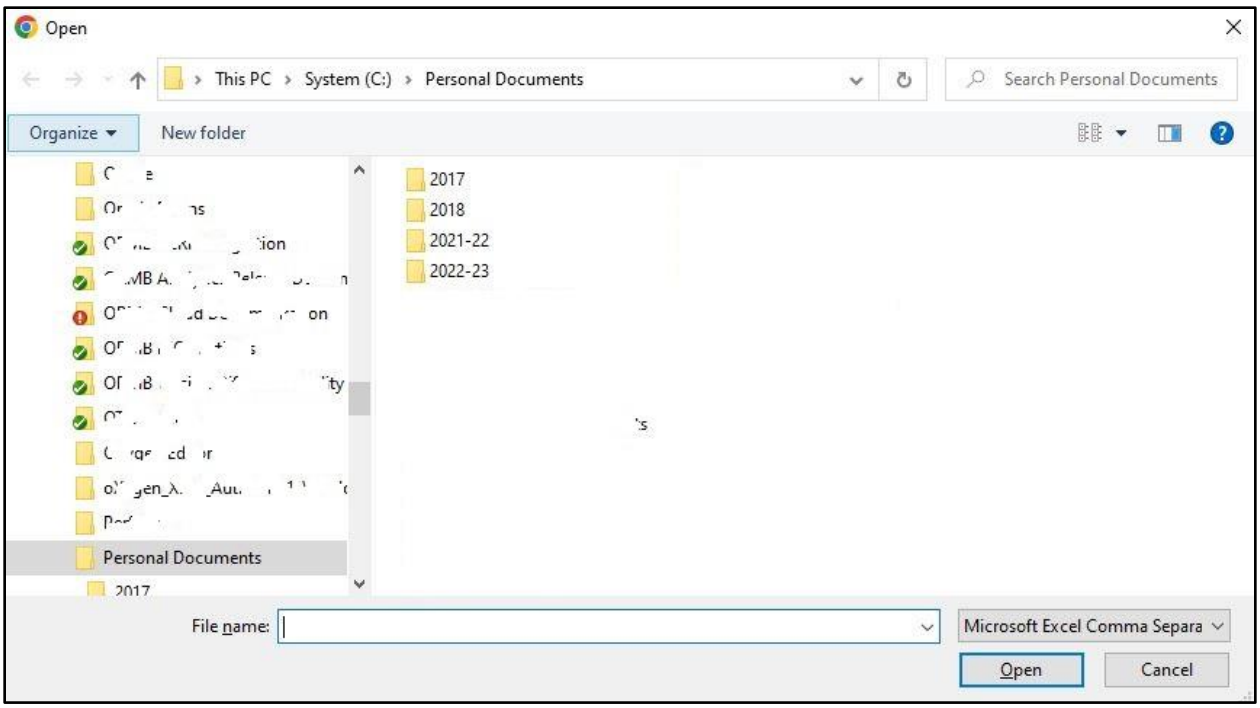

Figure 45: Open Dialog Box

15. Browse and select the file from where you want to import the group data and then click **Open**. The file is selected.
16. Click **Import**. A message appears indicating that the import process has started, as shown in the following figure:

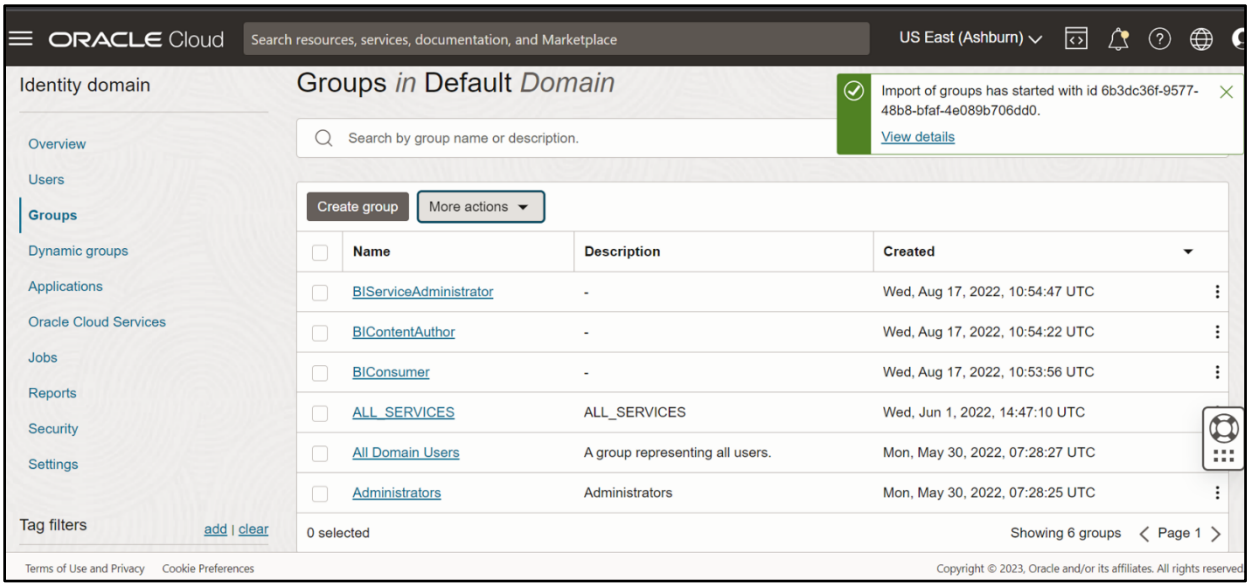

Figure 46: Information Message

17. Click **View details**. The **Job Details** screen appears, as shown in the following figure:

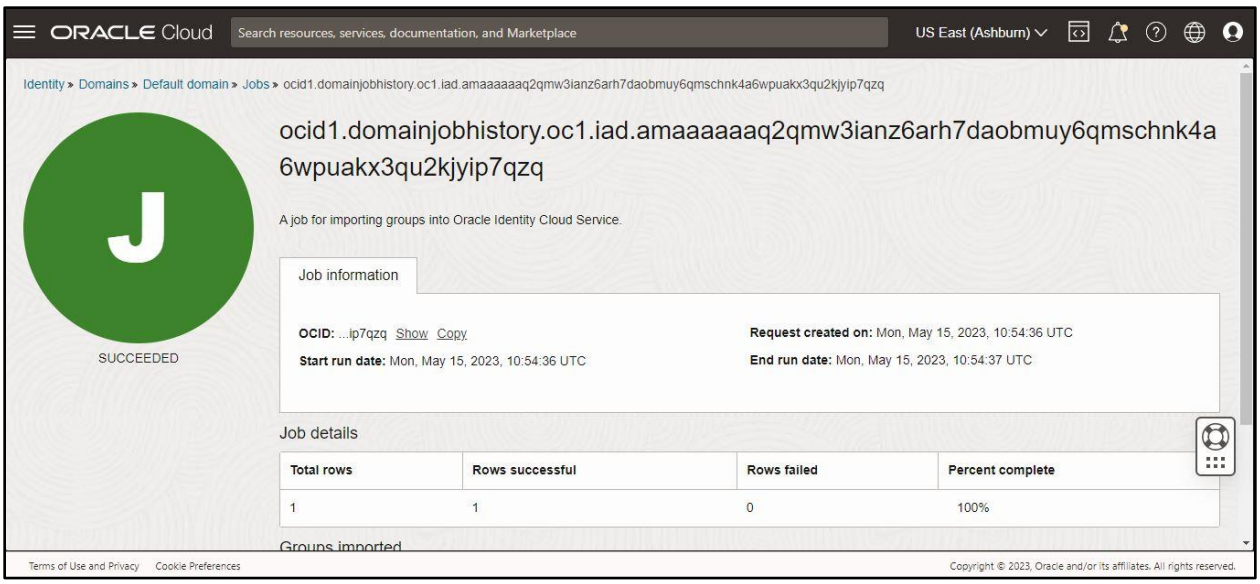

Figure 47: Job Details

Once the import process is complete, the **Job Details** screen displays the details, such as:

- Percent Completion
- Total Groups
- Groups Imported Successfully
- Groups Failed to Import

4.4 Exporting Groups

To export groups:

1. Click the **Groups** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Groups in Default Domain** page appears in the right pane of the Oracle Identity Domain Console.
2. Select the check box corresponding to one or more groups, whose details you want to export, in the **Groups in Default Domain** page.
3. Click **More actions**. A list appears, as shown in the following figure:

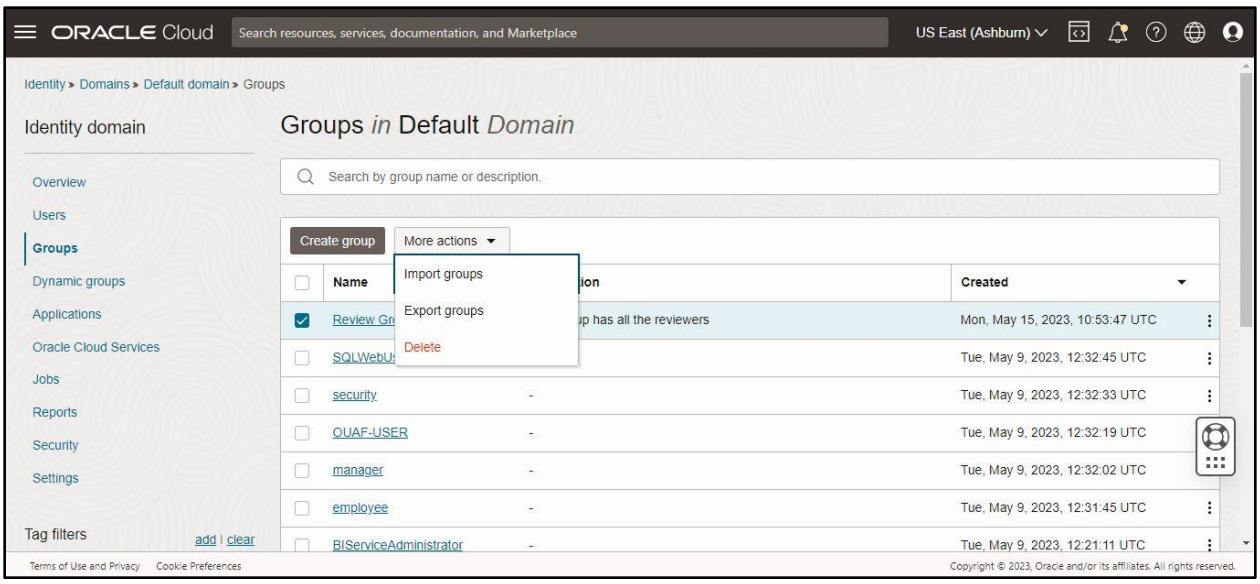

Figure 48: More Actions

4. Click the **Export groups** option from the list. The **Export groups** dialog box appears, as shown in the following figure:

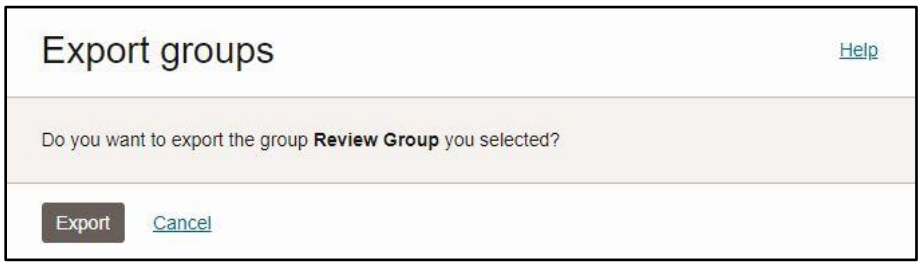

Figure 49: Export Groups Dialog Box

5. Click **Export**. A message appears indicating that the export process has started, as shown in the following figure:

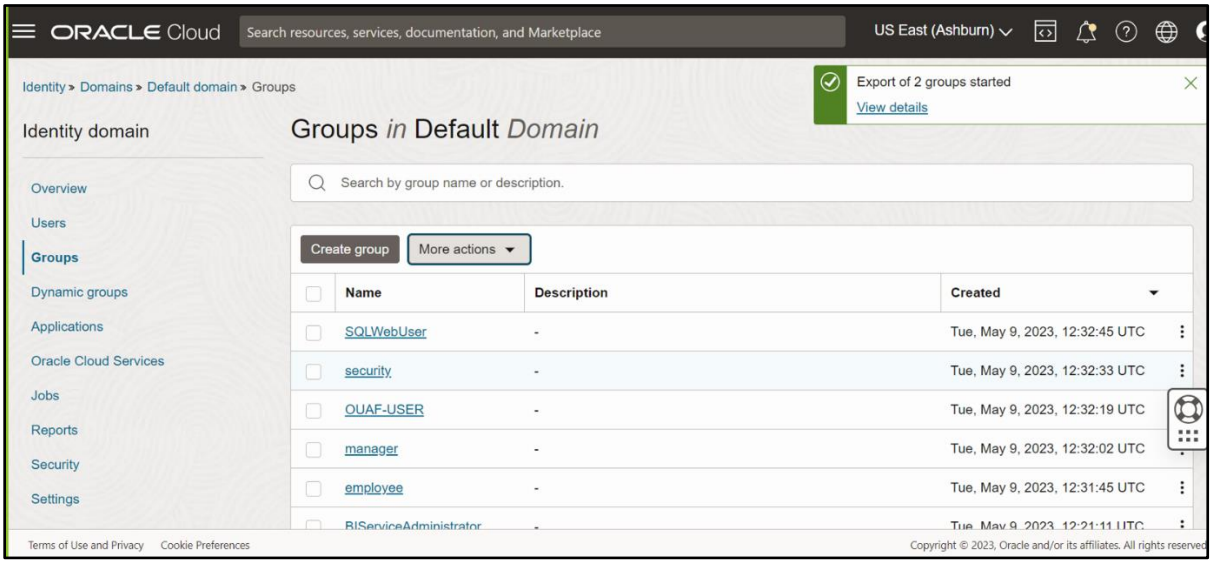

Figure 50: Information Message

6. Click **View details**. The **Job Details** screen appears, as shown in the following figure:

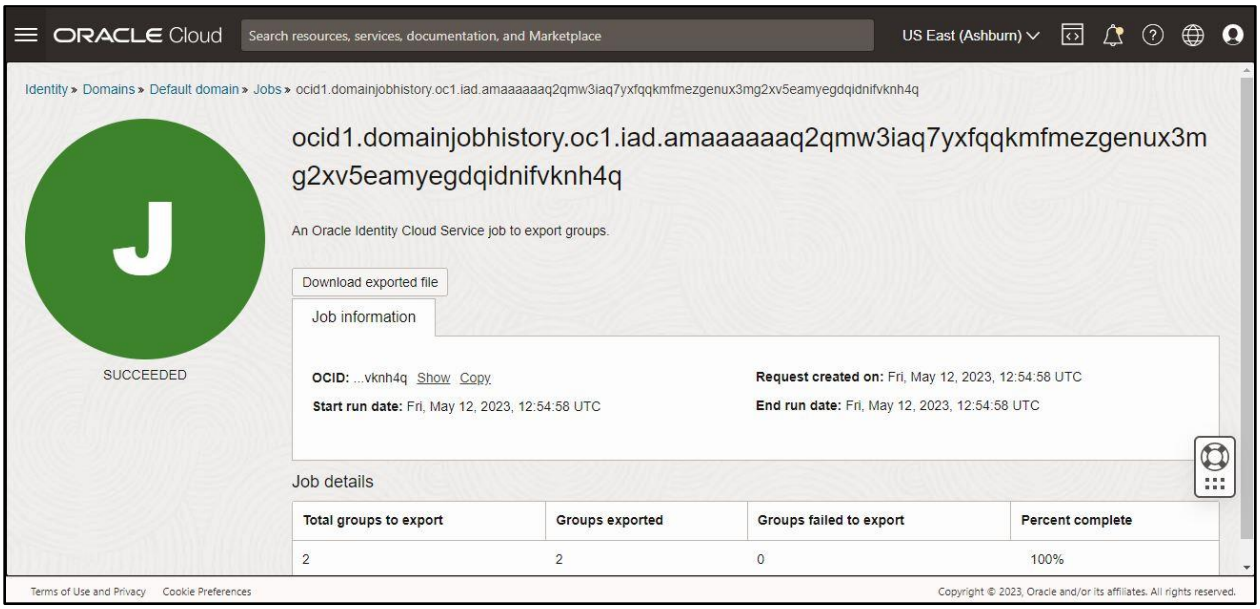

Figure 51: Job Details

Once the export process is complete, the **Job Details** screen displays the details, such as:

- Percent Completion
- Total Groups
- Groups Exported Successfully
- Groups Failed to Export

5. Managing Applications

Applications that represent provisioned services are pre-created during the service order processing. Application roles are also pre-configured. The administrator is authorized to activate or deactivate certain applications, assign users to application roles, and import and export the members of an application role.

This section contains the following topics:

5.1 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 superuser 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 for Multi-Factor Authentication (MFA).

5.2 Assigning Groups to an Application

To assign groups to an application:

1. Click the **Applications** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Applications in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

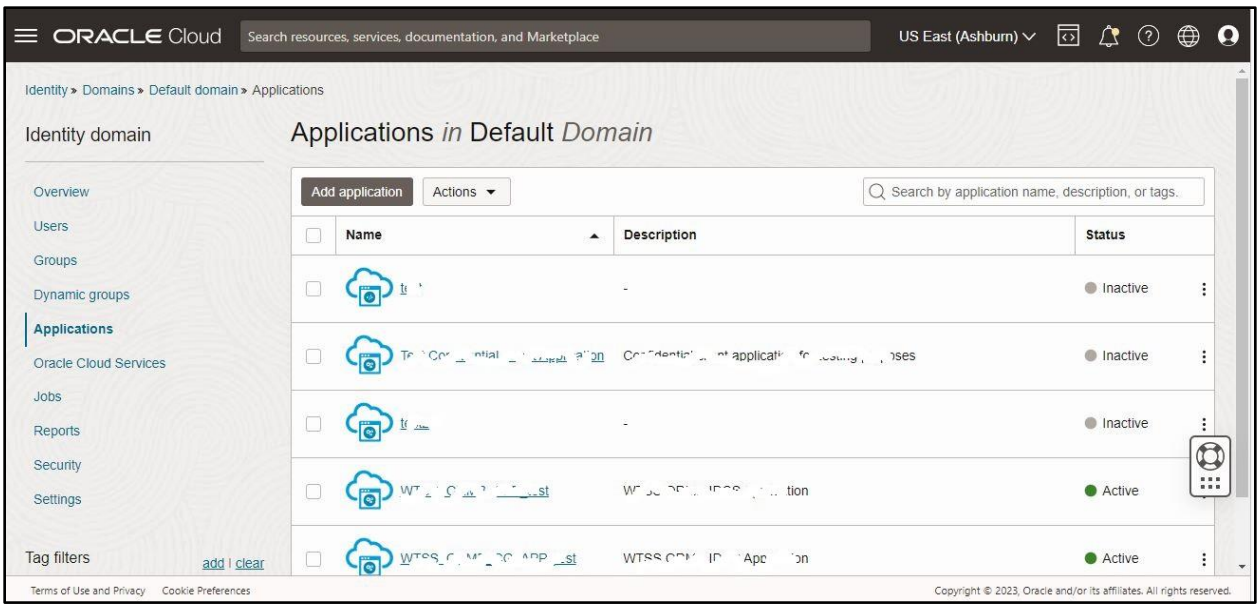

Figure 52: Applications in Default Domain Page

2. Click the link in the **Name** column corresponding to the application, whose details you want to edit, in the **Applications in Default Domain** page. The respective application's information appears, as shown in the following figure:

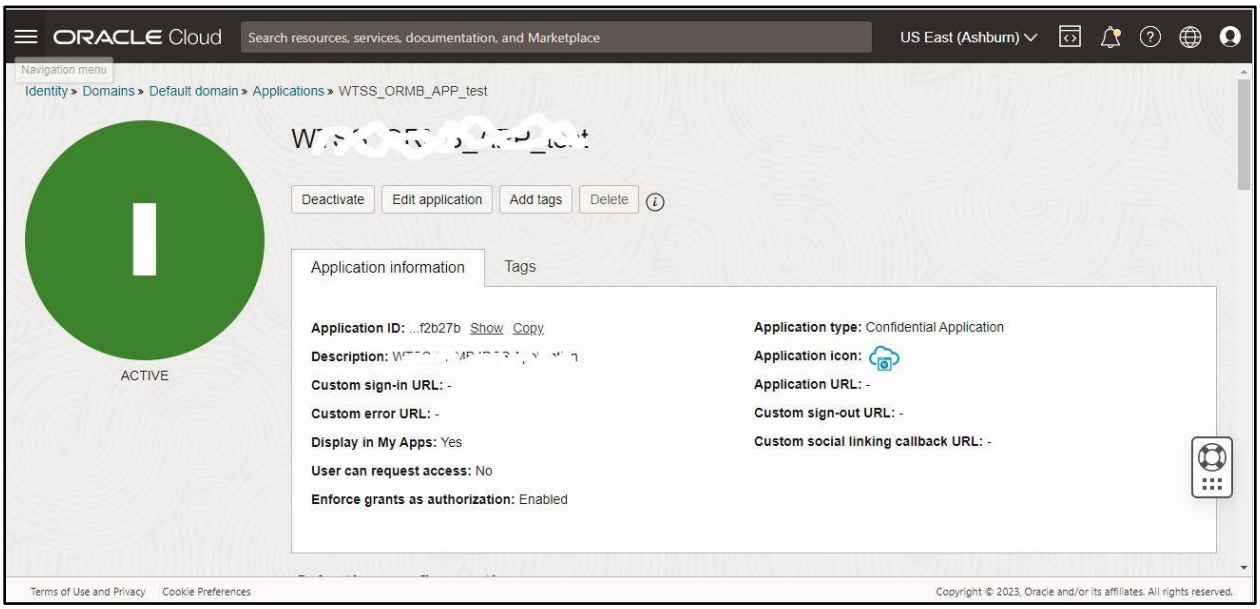

Figure 53: Application Information

3. Scroll down to view the **Resources** section in the left navigation pane, as shown in the following figure:

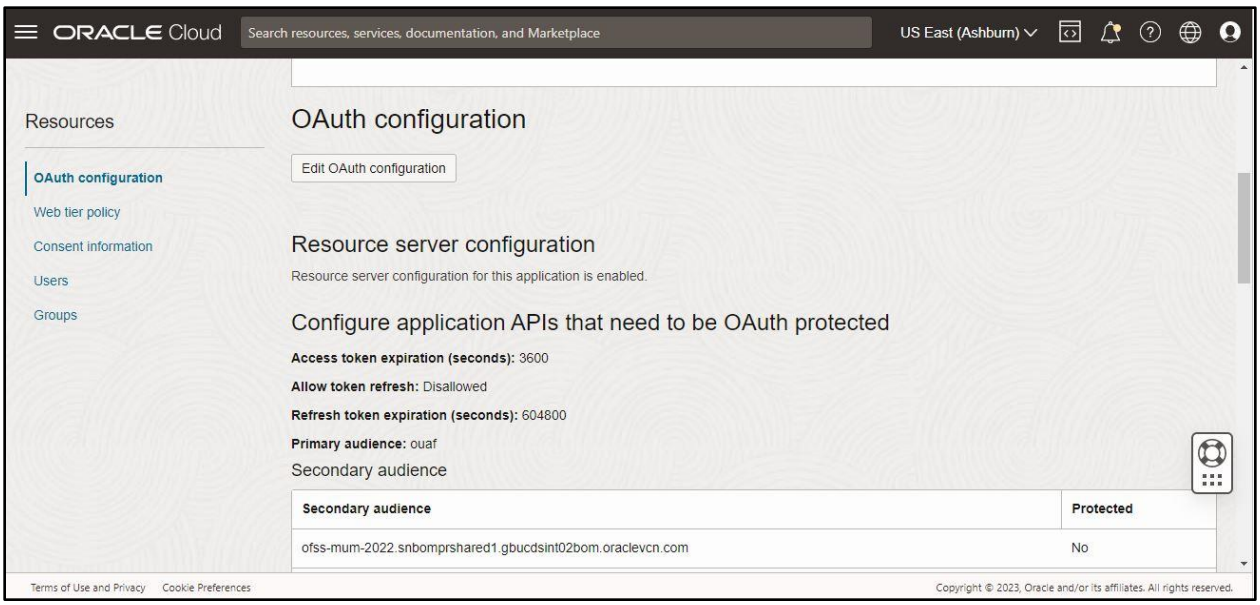

Figure 54: Resources Section

4. Click **Groups**. The **Groups** section appears in the right pane, as shown in the following figure:

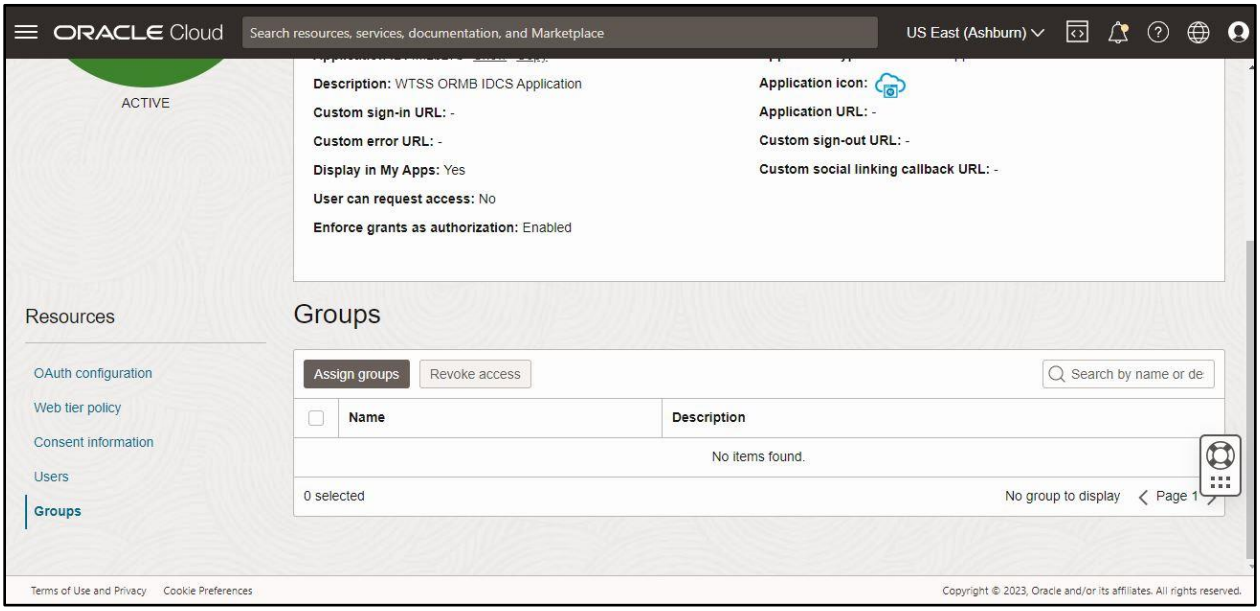

Figure 55: Groups Section

5. Click **Assign groups**. The **Assign groups** dialog box appears, as shown in the following figure:

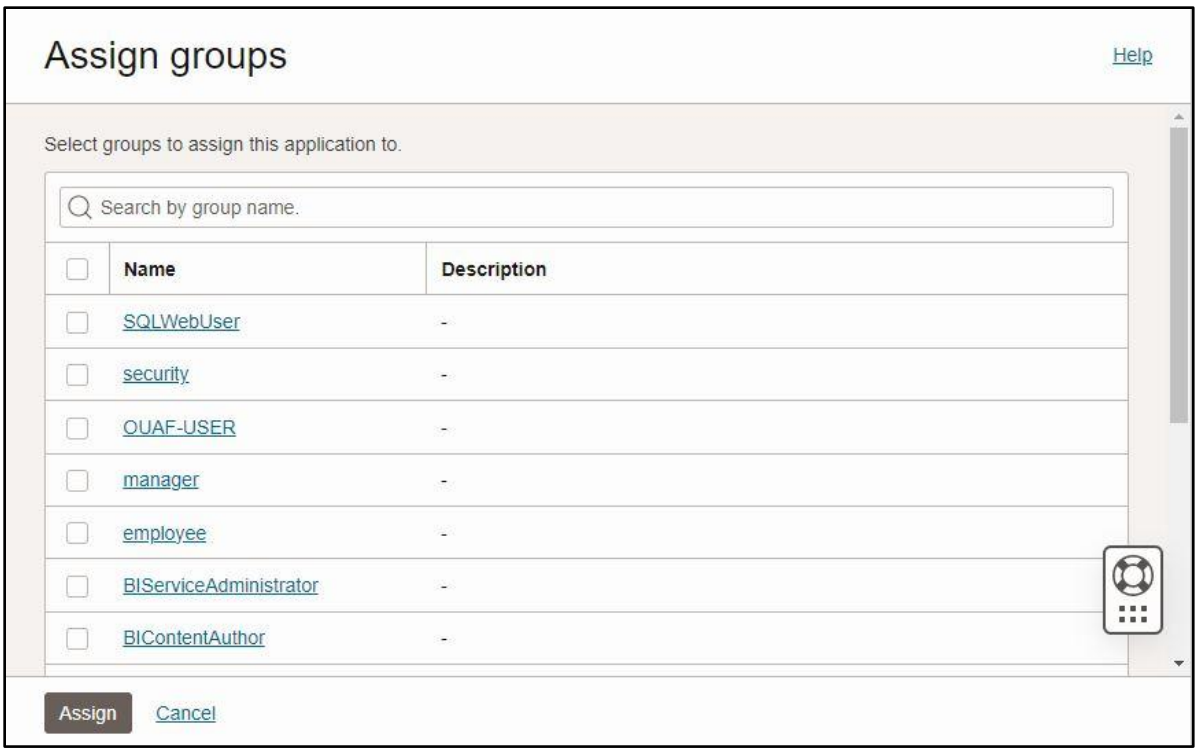

Figure 56: Assign Groups Dialog Box

6. Select the check box corresponding to the group that you want to assign to the application.
7. Click **Assign**. The group is assigned to the application.

6. SAML Application

This section explains 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. It contains the following topics:

6.1 Adding an SAML Application

To add an SAML application:

1. Click the **Applications** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Applications in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

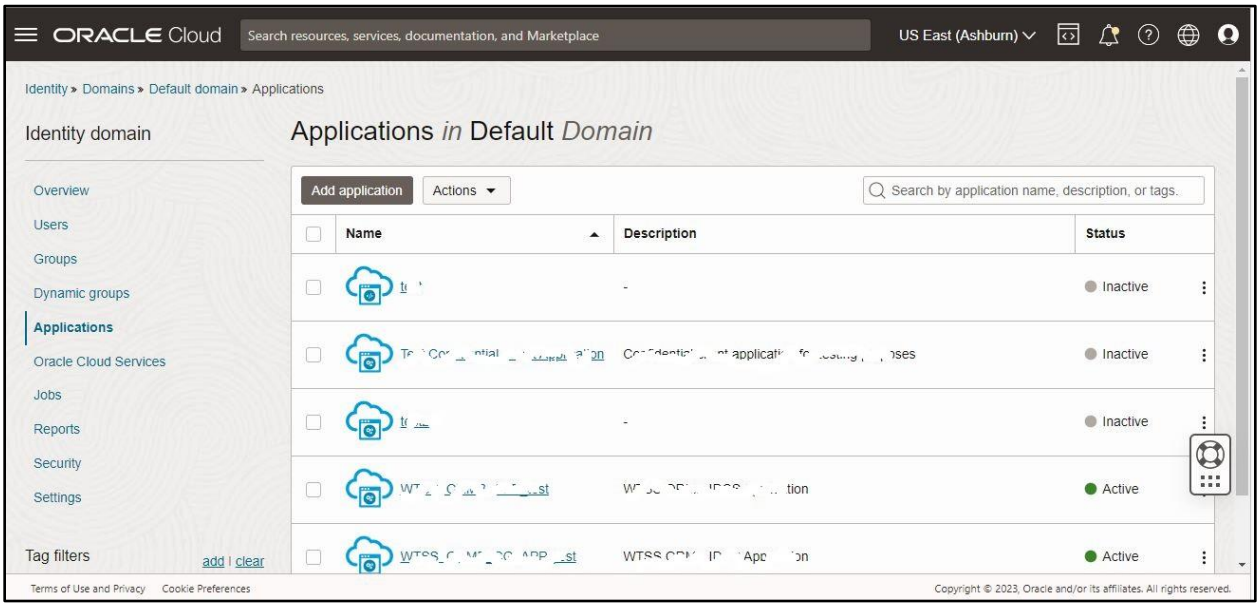

Figure 57: Applications in Default Domain Page

2. Click **Add application**. The **Add application** dialog box appears, as shown in the following figure:

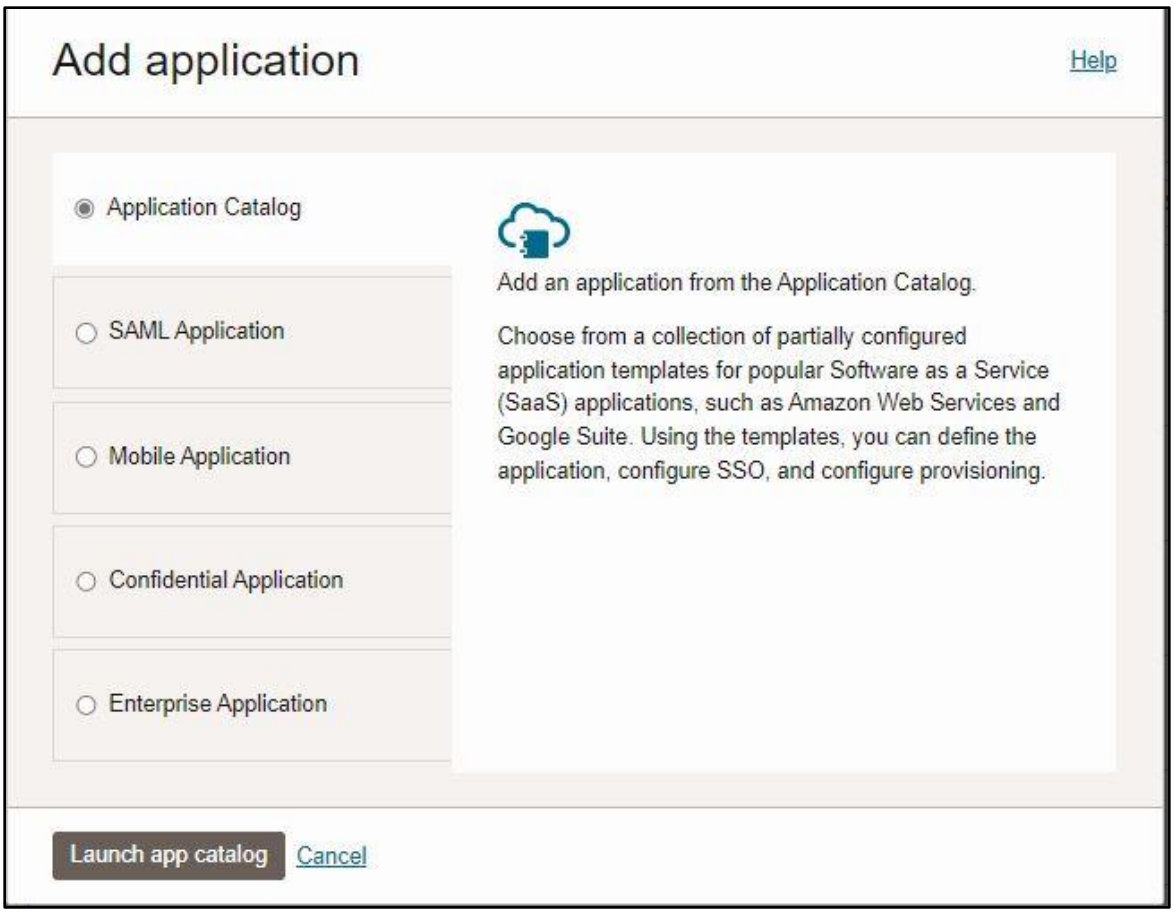

Figure 58: Add Application Dialog Box

3. Click the **SAML Application** option **i**n the **Add application** dialog box, as shown in the following figure:

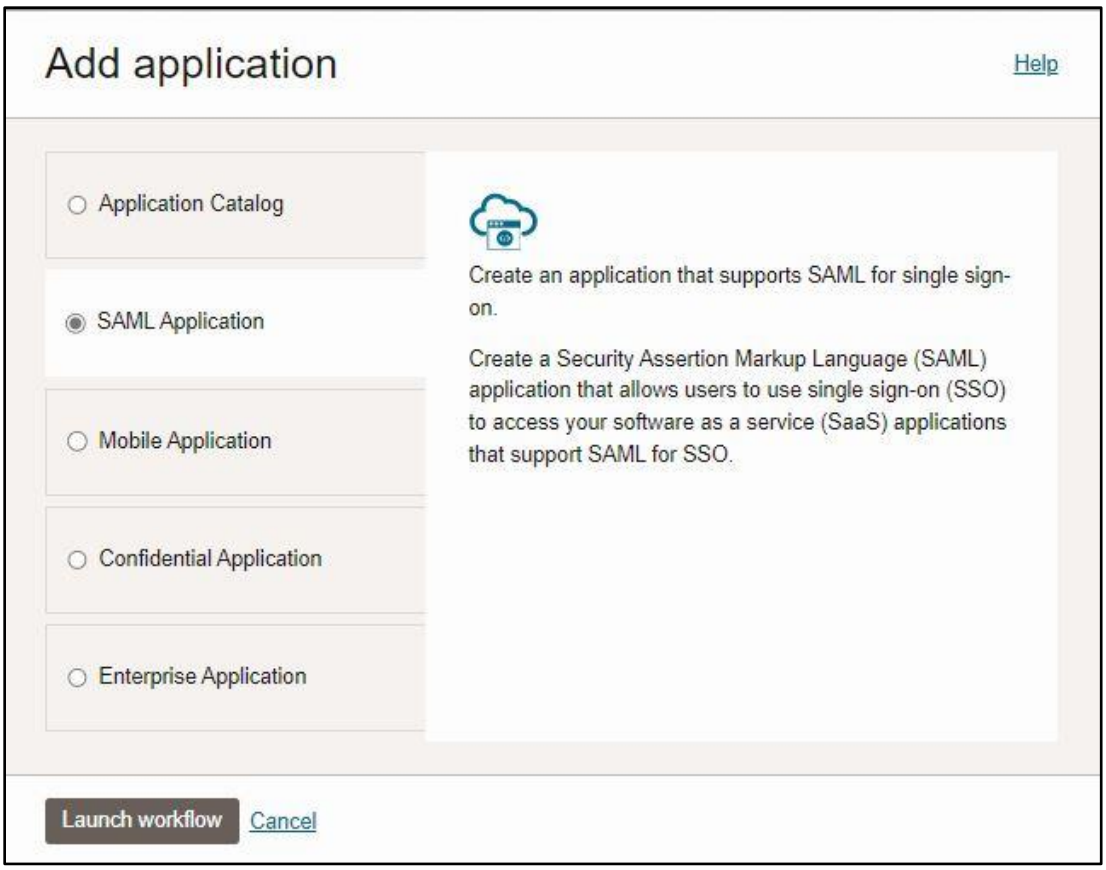

Figure 59: Add Application Dialog Box

4. Click **Launch workflow**. The **Add SAML Application** dialog box appears, as shown in the following figure:

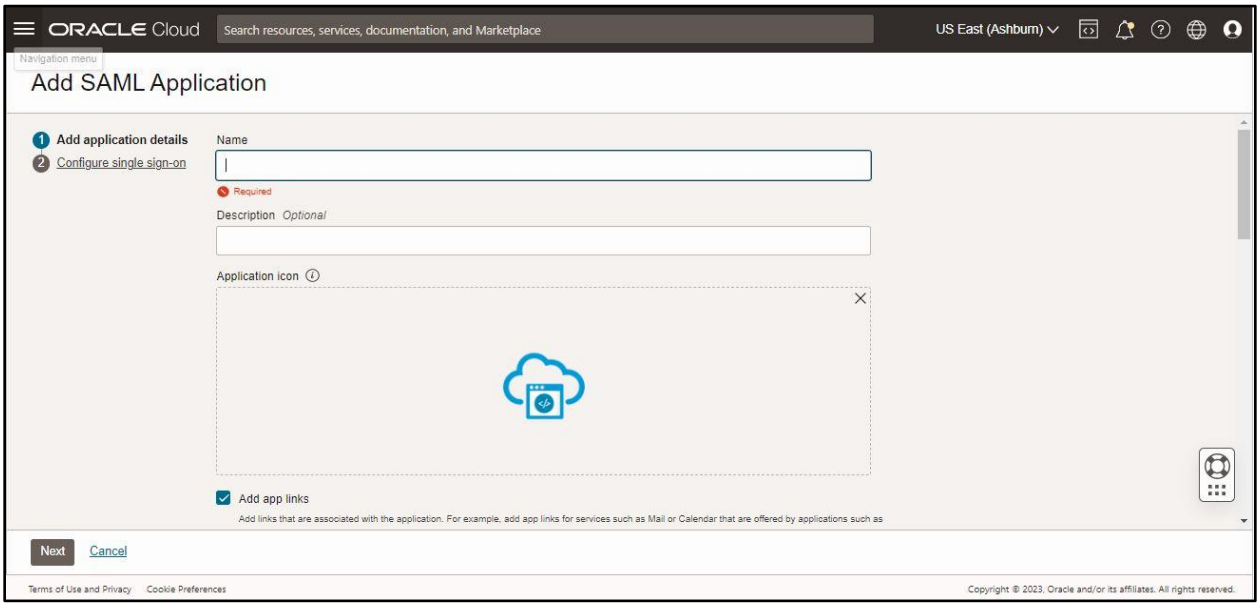

Figure 60: Add SAML Application

5. Specify the name and description for the SAML application in the respective fields.

Note: The description must not exceed 250 characters.

6. Scroll down to view the **App links** section in the **Add SAML Application** dialog box, as shown in the following figure:

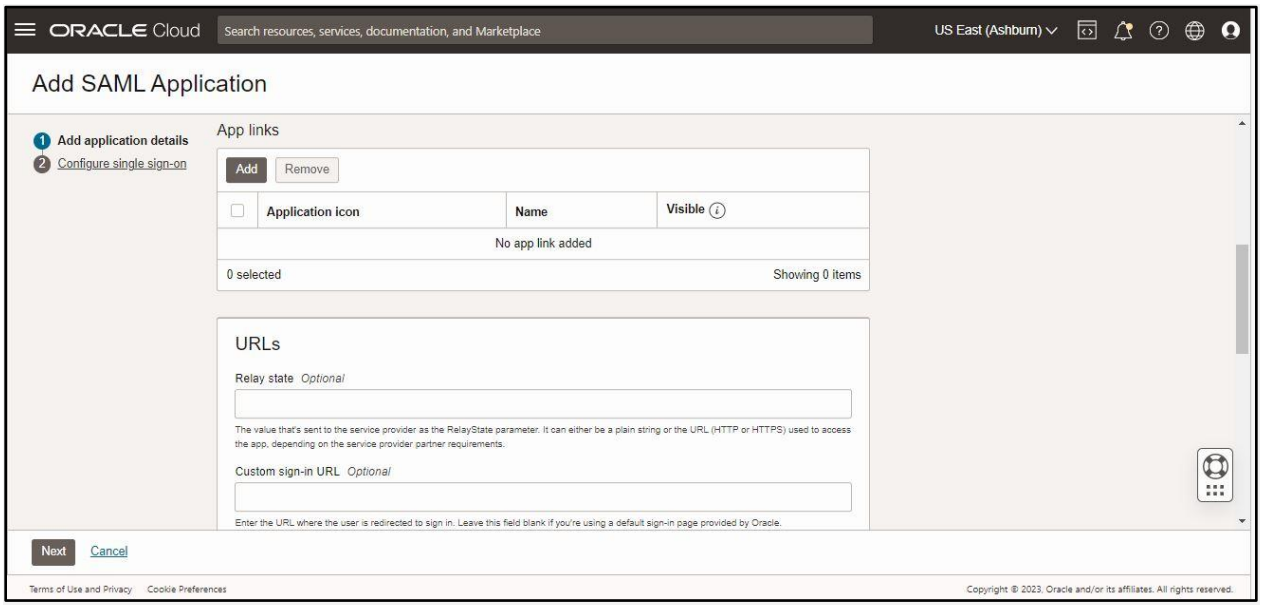

Figure 61: App links Section in Add SAML Application

7. Click **Add** in the **App links** section. The **Add app link** dialog box appears, as shown in the following figure:

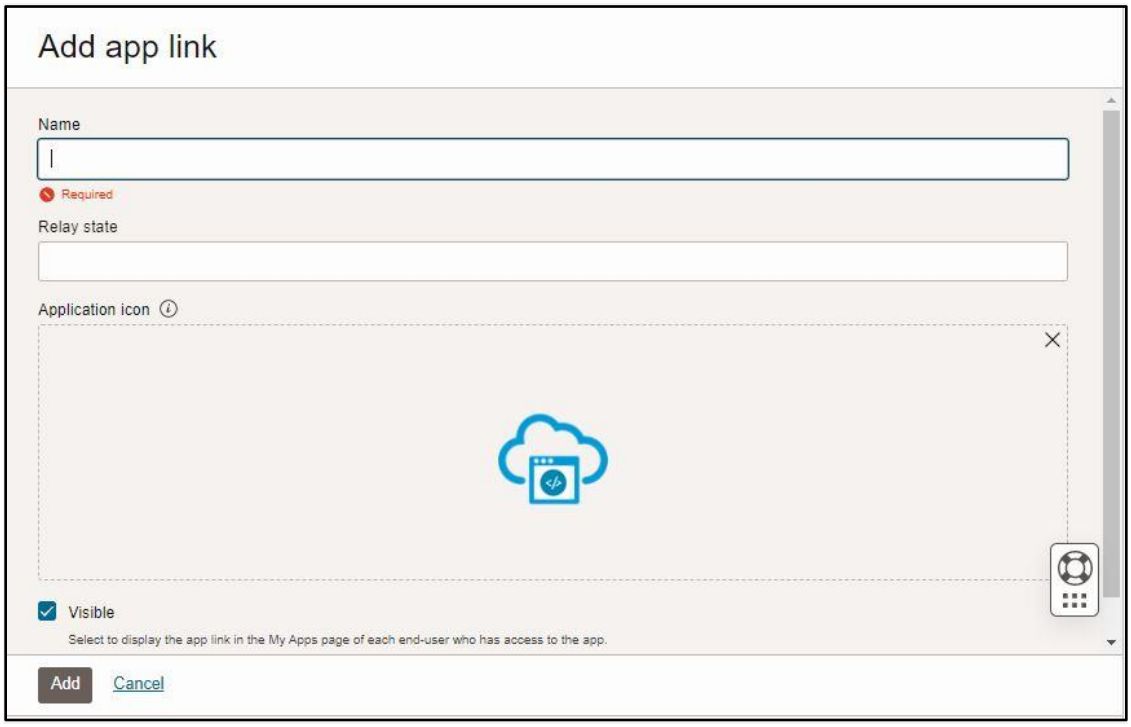

Figure 62: Add App Link Dialog Box

8. Specify the name of the application in the respective field.

9. In the **Relay state** field, specify a value which will be sent to the SAML Service Provider as the SAML RelayState parameter.
10. If required, you can change the icon for the SAML application.
11. Click **Add**. The app links for services that are offered by the application are added to the list.
12. Scroll down to view the **URLs** section in the **Add SAML Application** dialog box, as shown in the following figure:

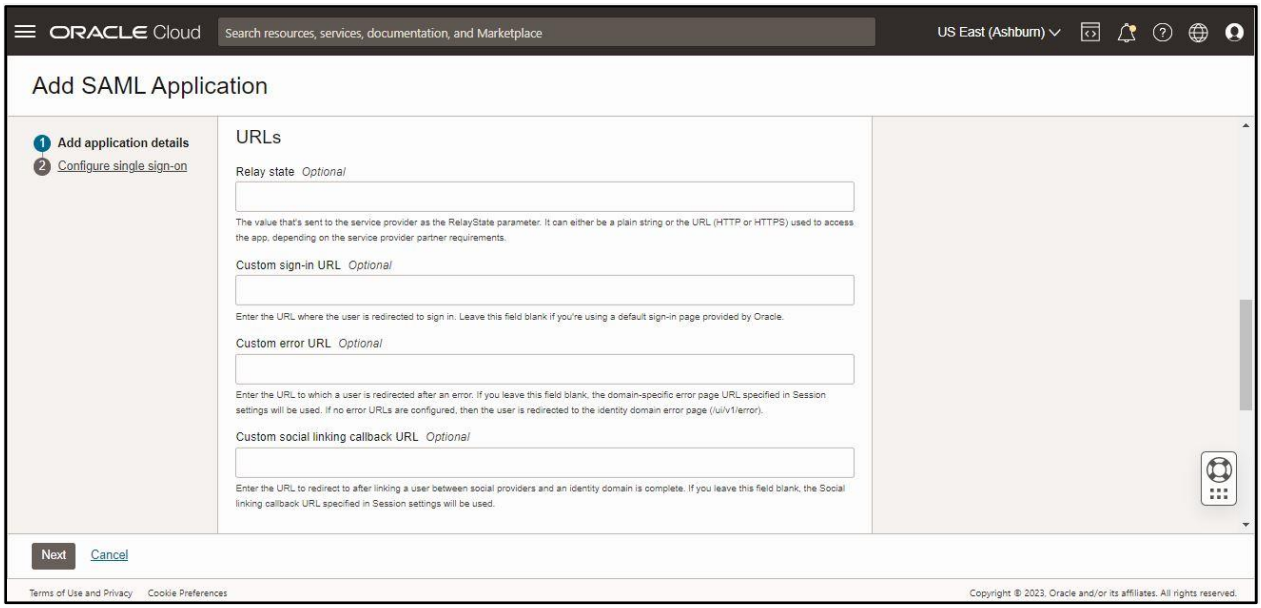

Figure 63: URLs Section in Add SAML Application

13. Specify a custom sign-in URL in the respective field.

Note: The **Custom sign-in URL** field is optional. If you are using the default login page provided by Oracle Identity Cloud Service, then leave the **Custom sign-in URL** field blank.

14. Specify a custom error URL, where you want to redirect the user in case of failure, in the respective field.

Note: The **Custom error URL** field is optional. However, if not specified, the tenant specific error page URL will be used. If both the error URLs are not configured, then the user will be redirected to the Oracle Identity Cloud Service Error Page (/ui/v1/error).

15. Specify a custom social linking callback URL in the respective field. This URL is used to redirect Oracle Identity Cloud Service after linking of a user between social providers and Oracle Identity Cloud Service is complete.

Note: The **Custom social linking callback URL** field is optional.

16. Scroll down to the bottom of the **Add SAML Application** dialog box, as shown in the following figure:

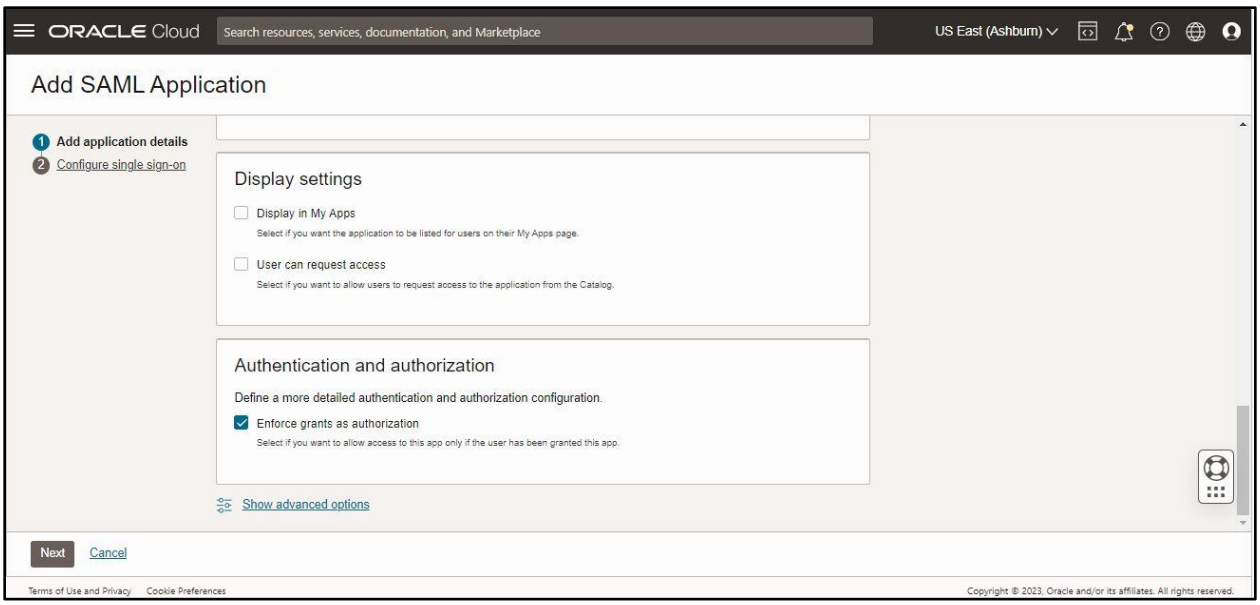

Figure 64: Display Settings Section in Add SAML Application

17. In the **Display settings** section, do the following:
    a. Select the **Display in My Apps** check box to indicate that you want to list the SAML application for users on their My Apps page.
    b. Select the **User can request access** check box if you want to allow users to request access to the application from the Catalog.

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

18. Click the **Show advanced** options link in the **Add SAML Application** page. The **Tags** section appears in the **Add SAML Application** dialog box, as shown in the following figure:

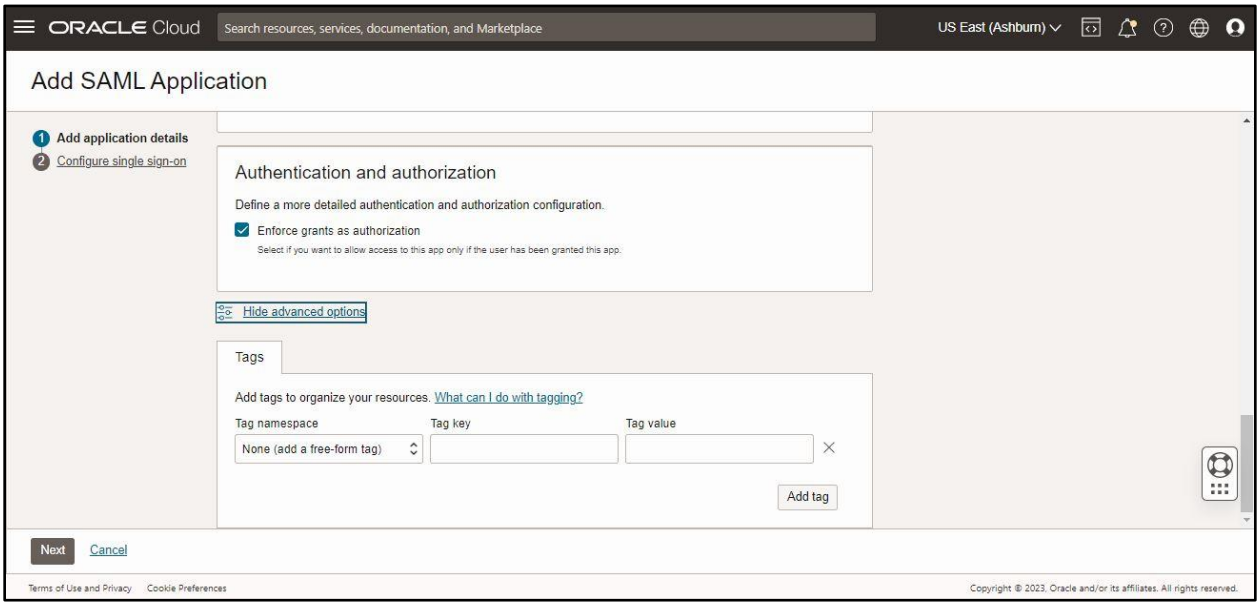

Figure 65: Tags Section in Add SAML Application

19. Add the required tags to your SAML application to organize and identify it.

20. Click **Next** to configure the SSO details for the SAML application. The **General** section in the **Add SAML Application** page appears, as shown in the following figure:

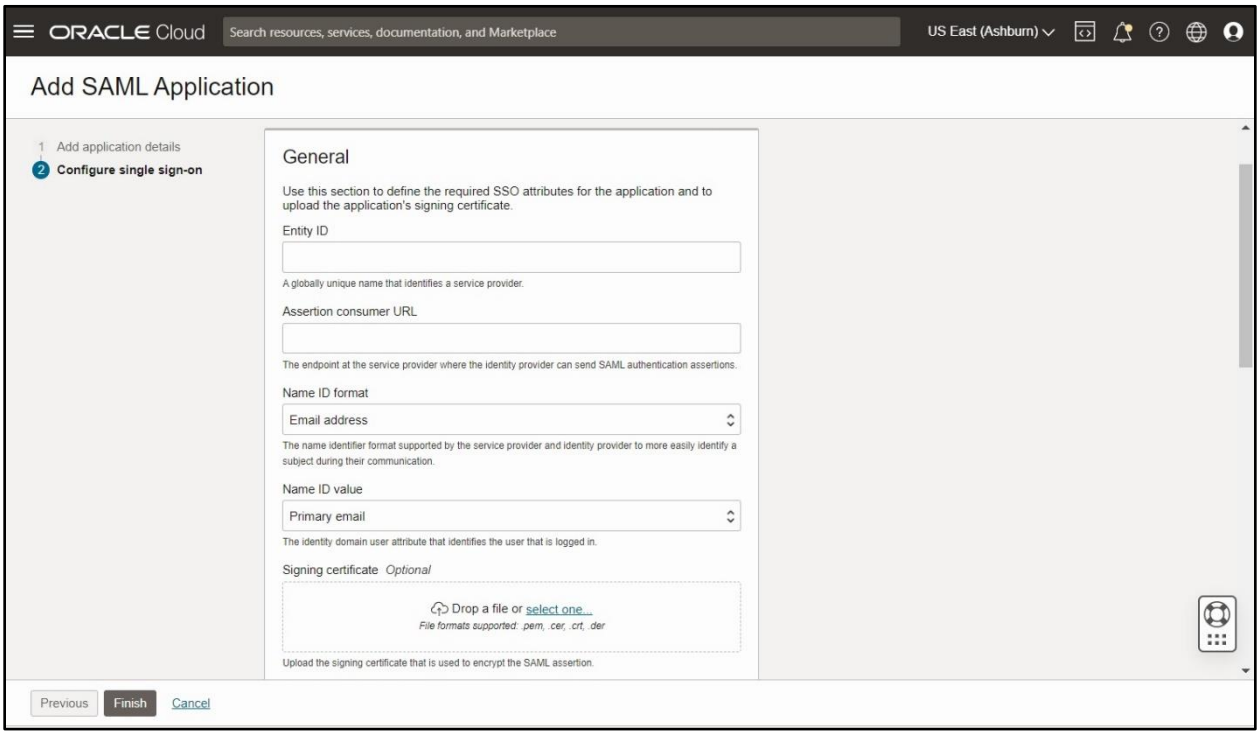

Figure 66: General Section

21. In the **General** section, do the following:
    a. Specify a globally unique name for the SAML entity in the respective field. This field usually contains the URL of an identity provider or a service provider.
    b. Specify the URL to which the SAML identity provider will send the SAML assertion in the respective field. This URL must either begin with the HTTP or HTTPS protocol.
    c. Select the **Unspecified** option from the **Name ID format** list. The name ID format is used by service and identity providers to easily identify a subject during their communication.
    d. Select the **User Name** option from the **Name ID value** list. It is used to identify the user who has logged into the application.
    e. Select or drag and drop the signing certificate that you want to use to encrypt the SAML assertion.
22. Scroll down to view the **Additional configurations** section in the **Add SAML Application** dialog box, as shown in the following figure:

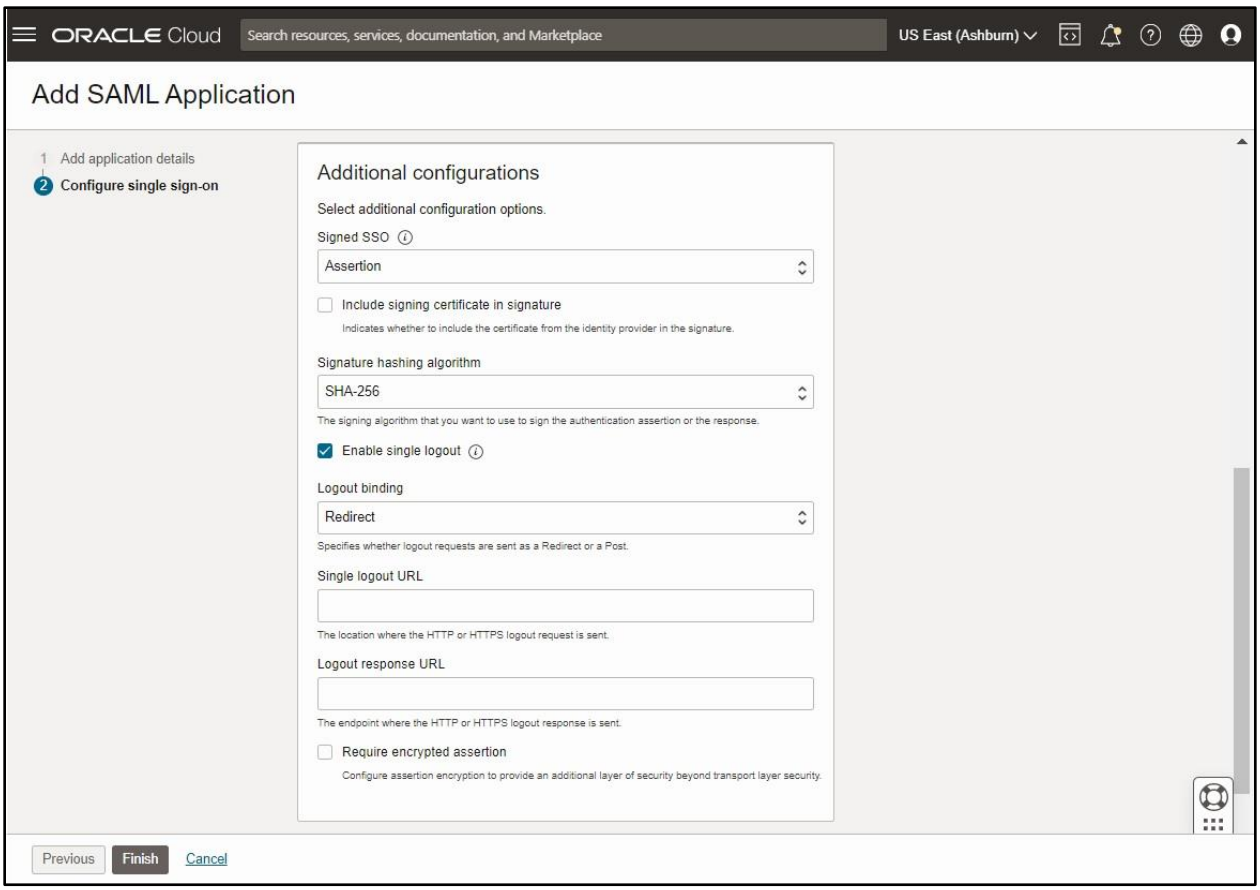

Figure 67: Additional Configurations in Add SAML Application

23. In the **Additional configurations** section, do the following:
    a. Select the **Assertion and Response** option from the **Signed SSO** list to indicate that you want the SAML assertion and response signed.
    b. Select the **Include signing certificate in signature** option to include the signing certificate in the signature.
    c. Select the **SHA-256** option from the **Signature hashing algorithm** list. It is used to generate a fixed 256-bit hash value.
    d. Do not select the **Enable single logout** option as we are not supporting single logout.
    e. If you want to encrypt the assertion, do the following:
        i. Select the **Require encrypt assertion** option. The following fields appear - Encryption Certificate, Encryption Algorithm, Key Encryption Algorithm.
        ii. Specify the encryption algorithm that you want to use for encrypting the SAML assertion in the respective field.
        iii. Upload the encryption certificate that you want to use to encrypt the SAML assertion.
        iv. Select the key encryption algorithm that you want to use to encrypt the SAML assertion.
    f. Scroll down to view the **Attribute configuration** section in the **Add SAML Application** dialog box, as shown in the following figure:

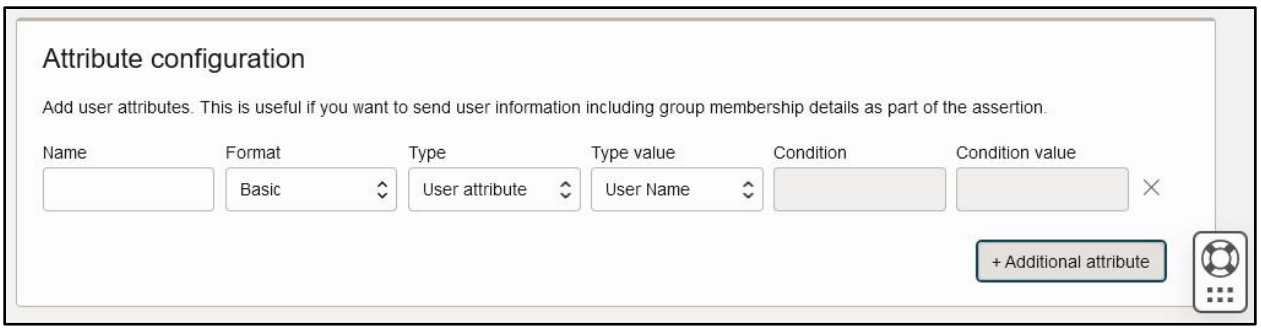

Figure 68: Attribute Configuration in Add SAML Application

24. Click **Additional attribute** in the **Attribute configuration** section to add user and group specific attributes to the SAML assertion. A dialog box appears where you can specify user-specific or group-specific attributes that you want to send as part of the SAML assertion.
25. In the dialog box , do the following:
    a. Specify the name of the SAML assertion attribute in the respective field.
    b. Select the format for the SAML assertion attribute from the respective field.
    c. Select the type based on which you will specify the value of the assertion attribute.
    d. Select or enter the value which you want to send as part of the assertion, based on the selected type.
26. When you are creating SAML application from scratch rather than using a pre-configured SAML application from the App Catalog, the **Authentication and Authorization** section appears. The **Enforce Grants as Authorization** option is selected by default. This option enables users to access only those applications for which you have granted access. If the option is selected, Oracle Identity and Access Management can control access to the SAML application based on the access granted to users and groups. If the option is not selected, any authenticated user has access to the application regardless of the assignment status.
27. To import the Identity and Access Management signing certificate into your application, click the **Download Signing Certificate** to download the certificate in the **PEM** format. This certificate is used by the SAML application to verify whether the SAML assertion is valid.
28. To import the **Identity and Access Management Identity Provider** metadata into your application, click the **Download Identity Provider Metadata** to download the metadata file in the **XML** format. The SAML application needs this information so that it can trust and process the SAML assertion that is generated by the **Identity and Access Management** as part of the federation process. This information includes the following:
    a. Profile and Binding support
    b. Connection Endpoints
    c. Certificate Information
29. Click **Finish**. The SAML application is created in a deactivated state.

6.2 Activating an SAML Application

To activate the SAML application:

1. Click the **Applications** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Applications in Default Domain** page appears in the right pane of the Oracle Identity Domain Console, as shown in the following figure:

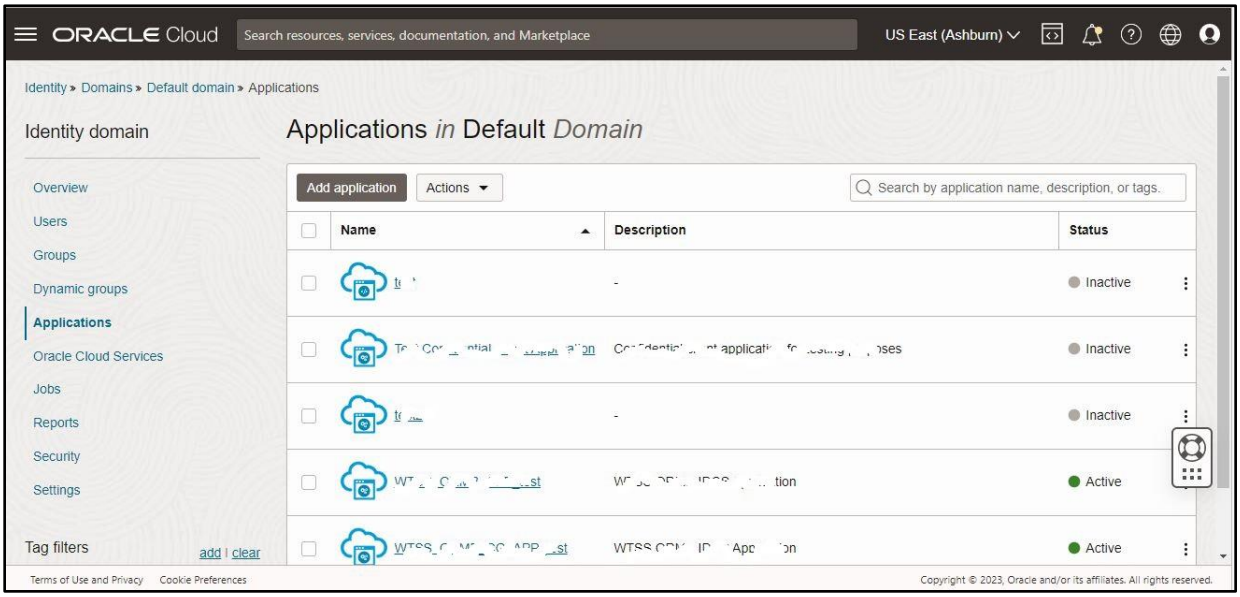

Figure 69: Applications in Default Domain Page

2. Select the check box corresponding to the deactivated SAML application that you want to activate.

Note: A grey circle indicates a deactivated SAML application, whereas green circle indicates an activated SAML application.

3. Click **Actions**. A list appears, as shown in the following figure:

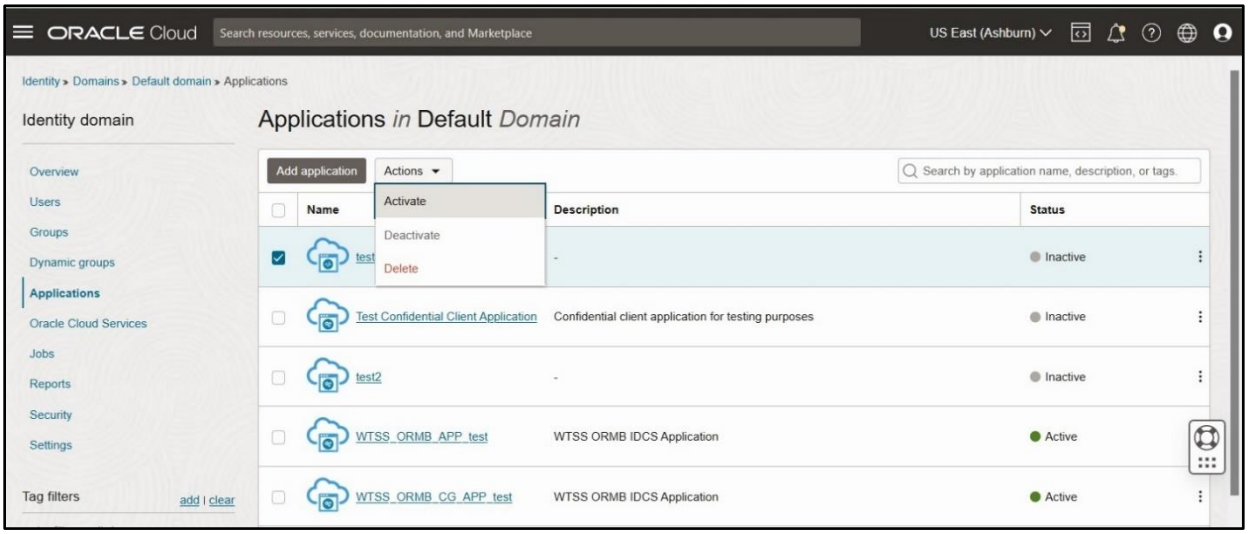

Figure 70: Activating an SAML Application

4. Click the **Activate** option from the **Actions** list. The **Activate application** dialog box appears, as shown in the following figure:

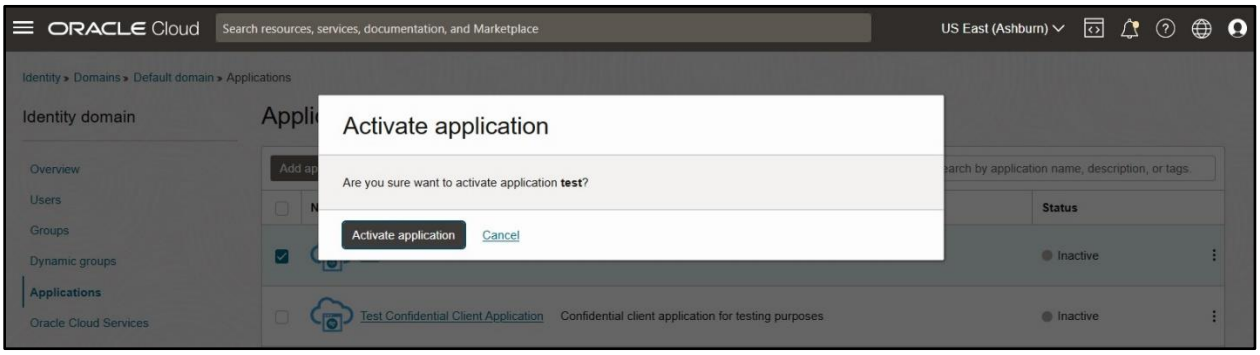

Figure 71: Activate Application Dialog Box

5. Click **Activate application**. The SAML application is activated.

Note: If you want to activate all the deactivated SAML applications, click the **Select All** check box and then activate.

6.3 Importing Metadata for the SAML Identity Provider

To import the metadata for the SAML Identity Provider:

1. Click the **Security** option in the left navigation pane of the **Oracle Identity Domain Console**. The **Terms of use Documents in Default Domain** page appears, as shown in the following figure:

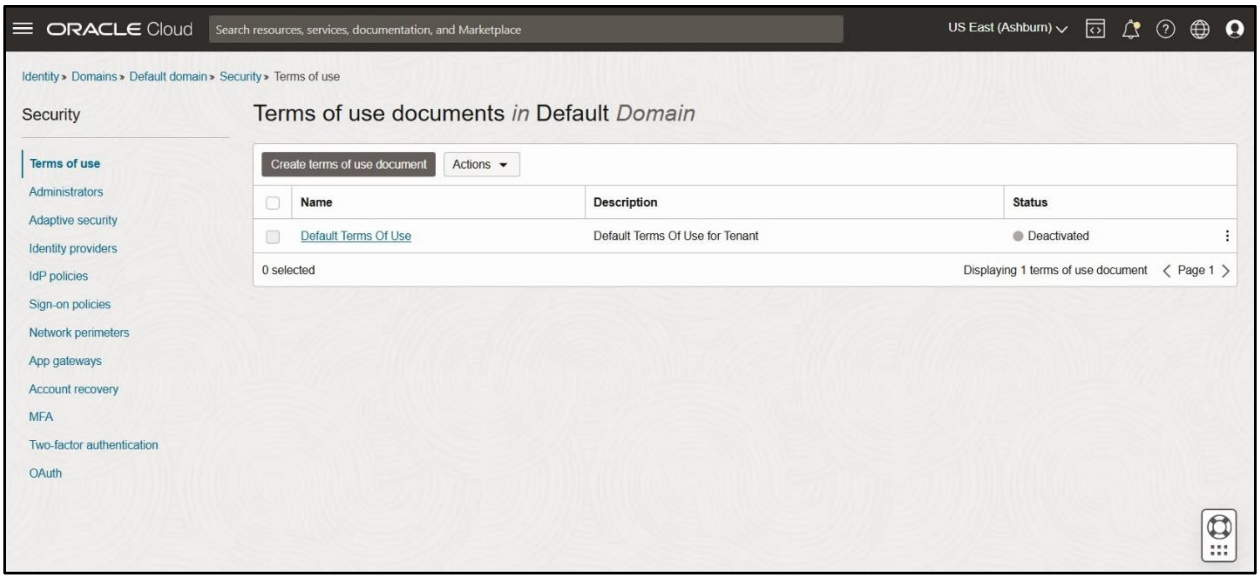

Figure 72: Terms of use documents in Default Domain

2. Click the **Identity providers** option in the left navigation pane of the **Oracle Identity Domain Console.** The **Identity providers (IdP) in Default Domain** page appears, as shown in the following figure:

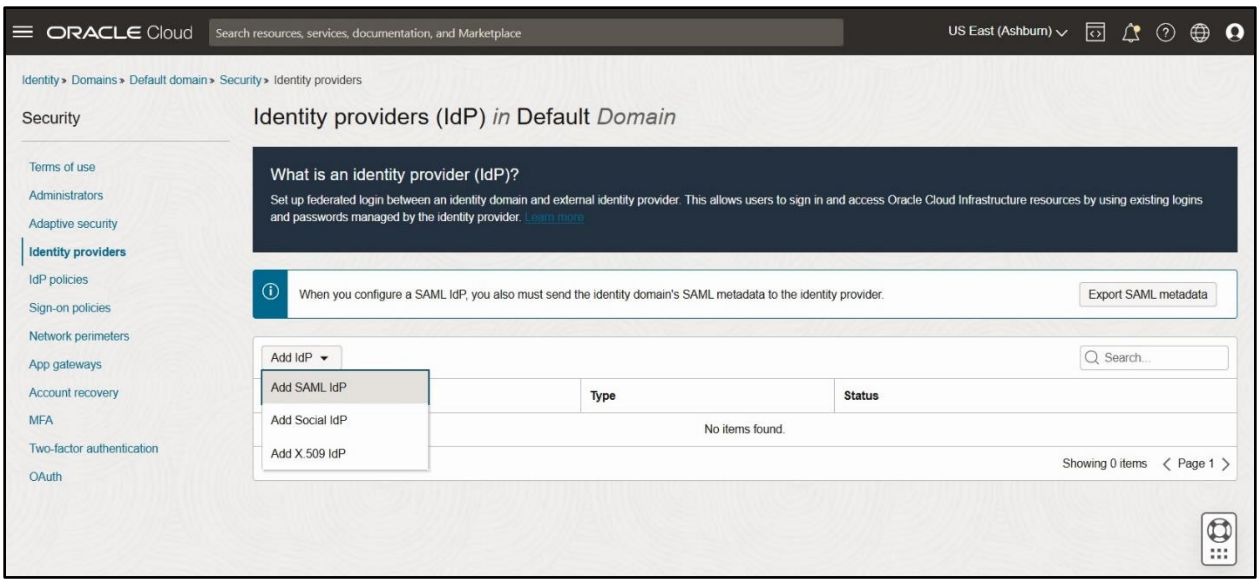

Figure 73: Identity Providers (IdP) in Default Domain

3. Select the **Add SAML IdP** option from the **Add IdP** list. The **Add SAML identity provider** page appears, as shown in the following figure:

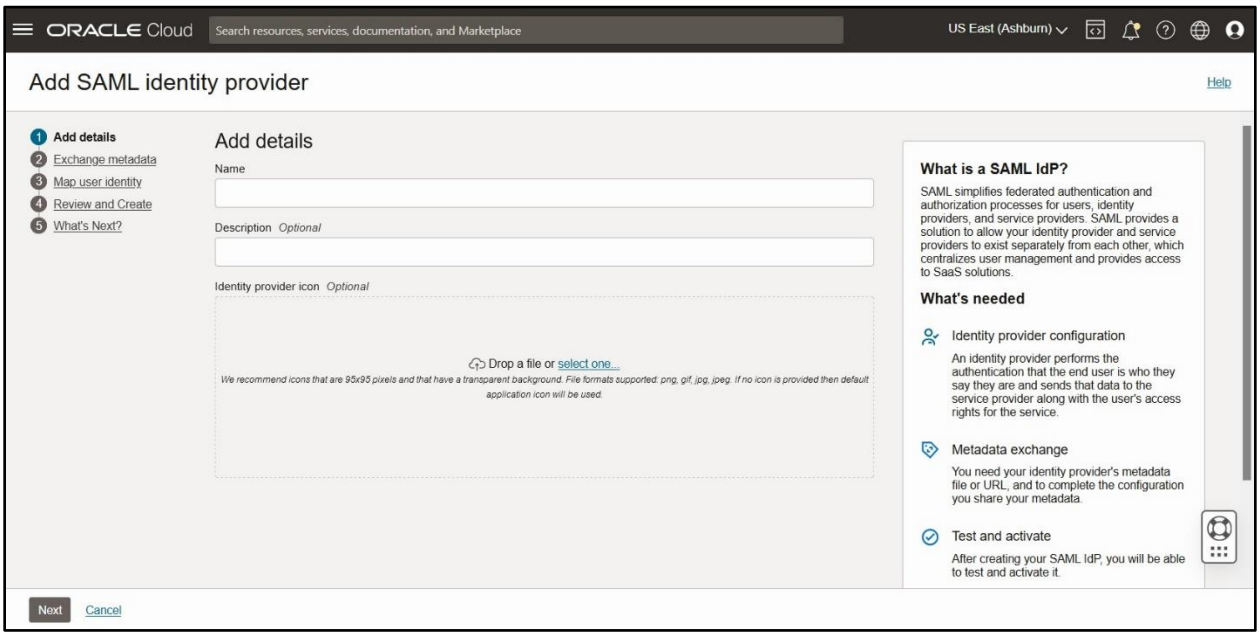

Figure 74: Add SAML Identity Provider

4. In the **Add details** section, do the following:
    a. Specify a suitable name for the identity provider in the respective field.
    b. Specify the description of the identity provider in the respective field.
    c. Select or drag and drop an icon which you want to upload for the application.

5. Click **Next**. The **Exchange metadata** page appears in the right pane, as shown in the following figure:

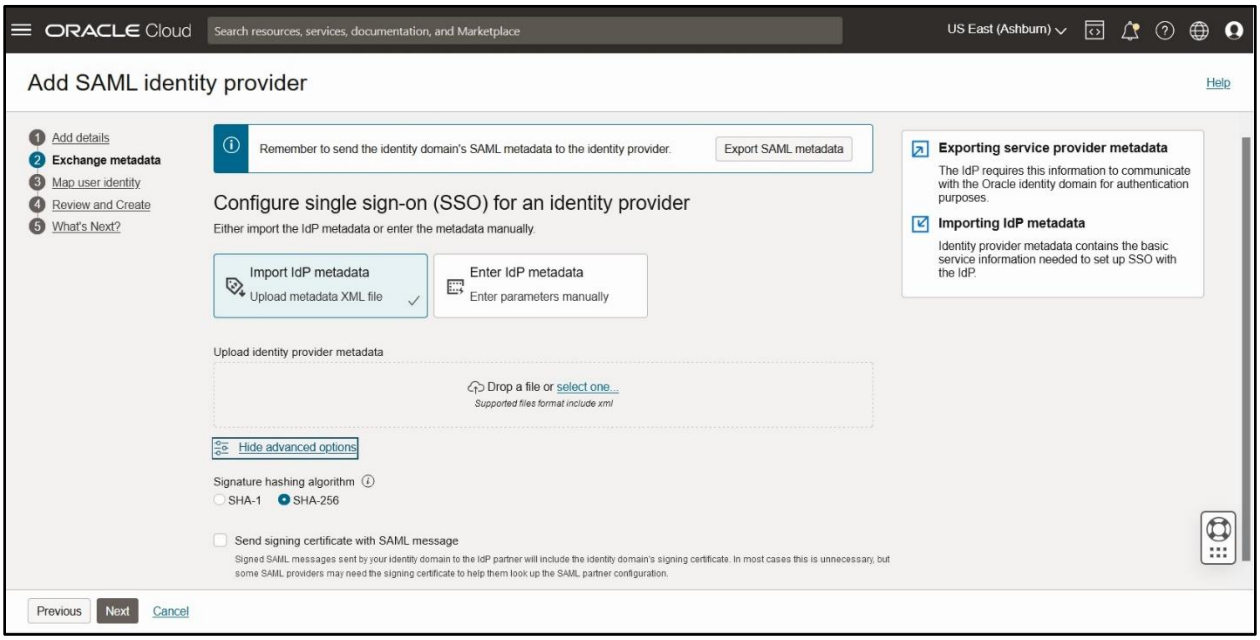

Figure 75: Exchange Metadata

6. In the **Configure single sign-on (SSO) for an identity provider** section, do the following:
    a. Click **Import IdP metadata** when you want to configure the SSO for an identity provider by importing the metadata file.
    b. Select or drag and drop the XML metadata file that you want to import.
    c. Click **Show advanced options**. The **Show advanced options** section appears.
    d. Select the appropriate signature hashing algorithm that you want to use to encrypt the signing certificate for an identity provider.
    e. Select the **Send signing certificate with SAML message** option to include a signing certificate to verify the signature of the messages for the identity provider.

Note: If you do not want to include a signing certificate with your identity provider, then do not select the **Send signing certificate with SAML message** option.

7. Click **Next**. The **Map user identity** page appears in the right pane from where you can map identify provider and identity domain user attributes.
8. Select the **Name ID** option from the **Identity provider user attribute** list.
9. Select the **Username** option from the **Identity domain user attribute** list.
10. Select the **Unspecified** option from the **Requested NameID format** list.
11. Click **Next**. The **Review and create** page appears in the right pane.
12. Review your SAML identity provider settings. If the settings are correct, click **Create**. A message appears indicating that the SAML identity provider is created.

Note: If you need to change the settings, click **Edit** next to the set of settings in the **Review and create** page.

13. Click **Test Login** to test the configuration settings for the identity provider, and then click **Next**.

14. Click **Activate** to activate the identity provider.
15. Click **Finish**.

