

Oracle® Hospitality OPERA Cloud Identity Management Administrator Guide



Release 24.1
F96310-01
June 2024



Copyright © 2024, 2024, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 Overview

2 Managing IAM Administrator Roles

IAM Administrator Roles	2-1
Managing Administrator Roles	2-3
Navigating to Administrator Roles	2-3
Searching for Existing Administrator Roles	2-4
Managing Administrator Role Memberships	2-4

3 Managing Groups

Groups in OPERA Cloud Identity Management	3-1
Navigating to the Group Management Page	3-1
Creating a Custom Group	3-2
Searching for Groups	3-3
Group Profile Management	3-3
Assigning and Removing Group Membership	3-3
Deleting a Group	3-4

4 Managing Users

Navigating to the User Management Page	4-1
Creating a User	4-1
Searching for Users and Performing User Actions	4-3
User Profile Management	4-4
Editing a User	4-5
Resetting a User Password	4-6
Changing Primary Work Location for a User	4-7
Deleting a User	4-9

Preface

Oracle Hospitality OPERA Cloud Identity Management users are authorized to access the following modules and features:

- Oracle Hospitality OPERA Cloud Identity Management

Purpose

This guide explains how to manage Identity and Access Management (IAM) administrators, groups, and users in OPERA Cloud Identity Management using the OPERA Cloud Identity Management Portal.

Audience

This document is intended for OPERA Cloud Services application administrators.

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at the following URL:

<https://iccp.custhelp.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screenshots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at <http://docs.oracle.com/en/industries/hospitality/>.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc=docacc>.

Revision History

Date	Description of Change
June 2024	Initial publication

1

Overview

This guide explains how to manage Identity and Access Management (IAM) administrators, groups, and users in OPERA Cloud Identity Management using the OPERA Cloud Identity Management Portal.

2

Managing IAM Administrator Roles

IAM Administrator Roles

Identity and Access Management (IAM) administrator roles in OPERA Cloud Identity Management provide capabilities in OPERA Cloud Identity Management portal for managing users, groups, user group memberships and managing Oracle support access.

IAM administrator roles can be used for controlling access to capabilities only within OPERA Cloud Identity Management Portal.

The three IAM administrator roles available in OPERA Cloud Identity Management are as follows:

- IAMADMIN
- IAMUSERMANAGER
- IAMHELPDESK

IAM administrator roles are always associated to an enterprise, chain, or a property where scope of user and group data can be managed by members of that IAM. The Administrator role in the OPERA Cloud Identity Management Portal is always based on the associated enterprise, chain, or property.

Table 2-1 Administration Capabilities in OPERA Cloud Identity Management Portal

View User Information Administrator Role Name	Create User and Delete User	Activate/Deactivate User and Edit User	Unlock User/Reset Factors/Reset Password/Resend Invitation	Manage User Group Membership	View Groups	Create Custom Groups and Delete Custom Groups	Manage Group User Membership	Manage Admin Roles	Manage Oracle User Access
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ADMIN	No	Yes	Yes	Yes	Yes	No	Yes	No	No
ADMIN USER	No	No	Yes	No	Yes	No	No	No	No
ADMIN HELP DESK									



Note:

The IAMADMIN Administrator Role is automatically assigned for the CHAIN-ADMIN or PROPERTY-ADMIN group member for that respective chain or property.

Managing Administrator Roles

This section contains steps for managing IAM administrator roles in OPERA Cloud Identity Management portal.

The IAMADMIN role membership is required for managing administrator roles in OPERA Cloud Identity Management Portal.

Navigating to Administrator Roles

1. Log in to OPERA Cloud Identity Management portal using a user who is an IAMADMIN role member.

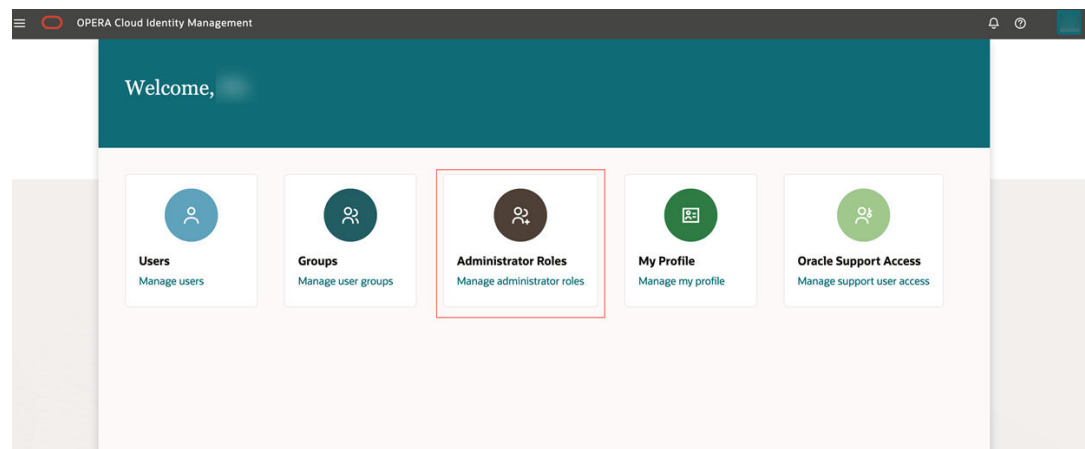


Note:

During provisioning of OPERA Cloud, the Enterprise administrator along with the Chain administrator and Property administrator are created in the customer's OCI IAM Identity Domain, and those users automatically get assigned the IAMADMIN role in OPERA Cloud Identity Management.

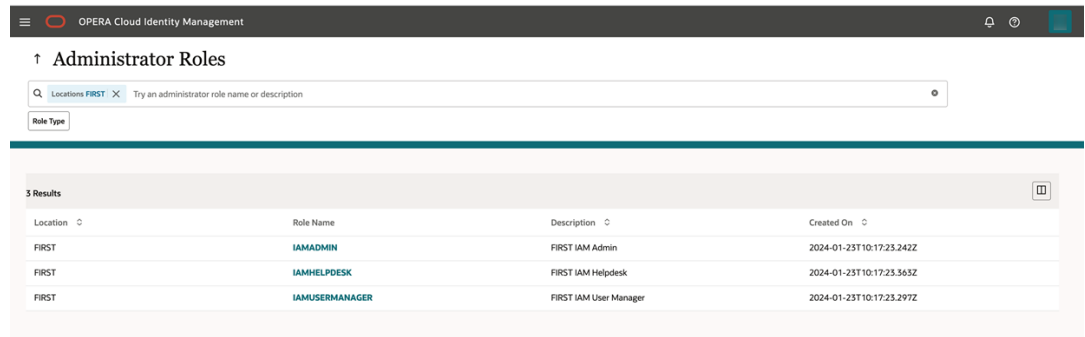
The home page is visible on successful login and the home page includes the tile for Administrator Roles.

2. Click the **Administrator Roles** tile on the home page to open the OPERA Cloud Identity Management Administrator Roles page.



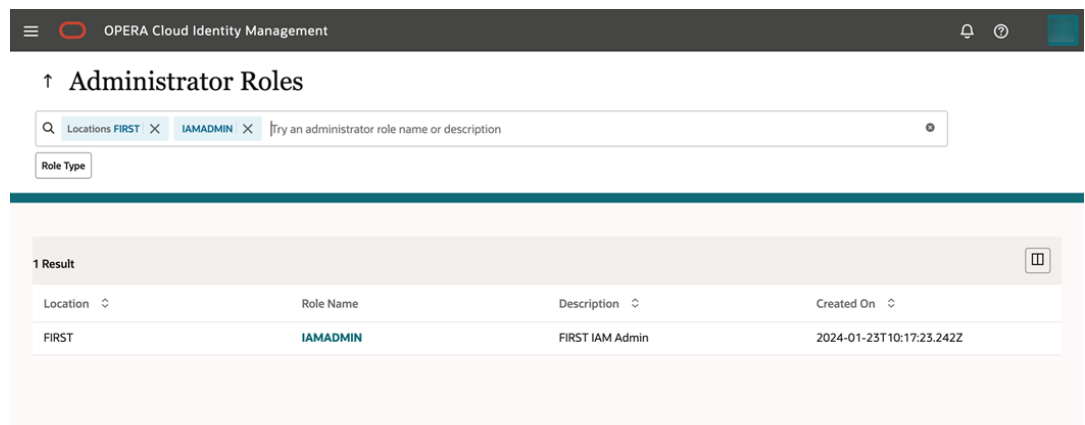
- The Administrator Roles page consist of a search bar and displays the Administrator Roles for your location.

- The search bar can be used to filter administrator roles based on locations and role name.



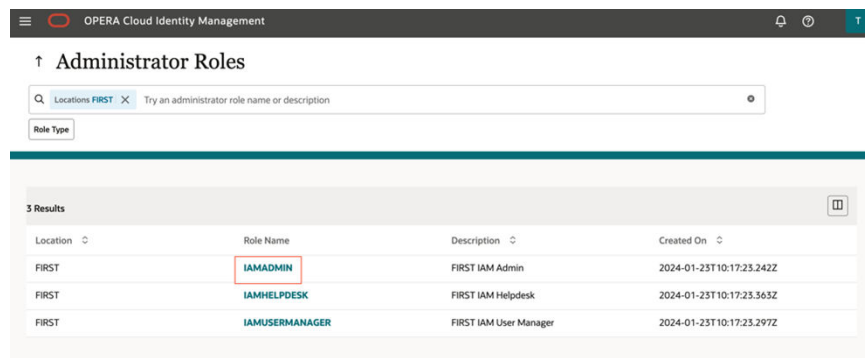
Searching for Existing Administrator Roles

- Click the **Locations** filter chip in the search bar for filtering roles based on locations.
- Type the **role name** or **description** to further filter the results based on a combination of location and role name.

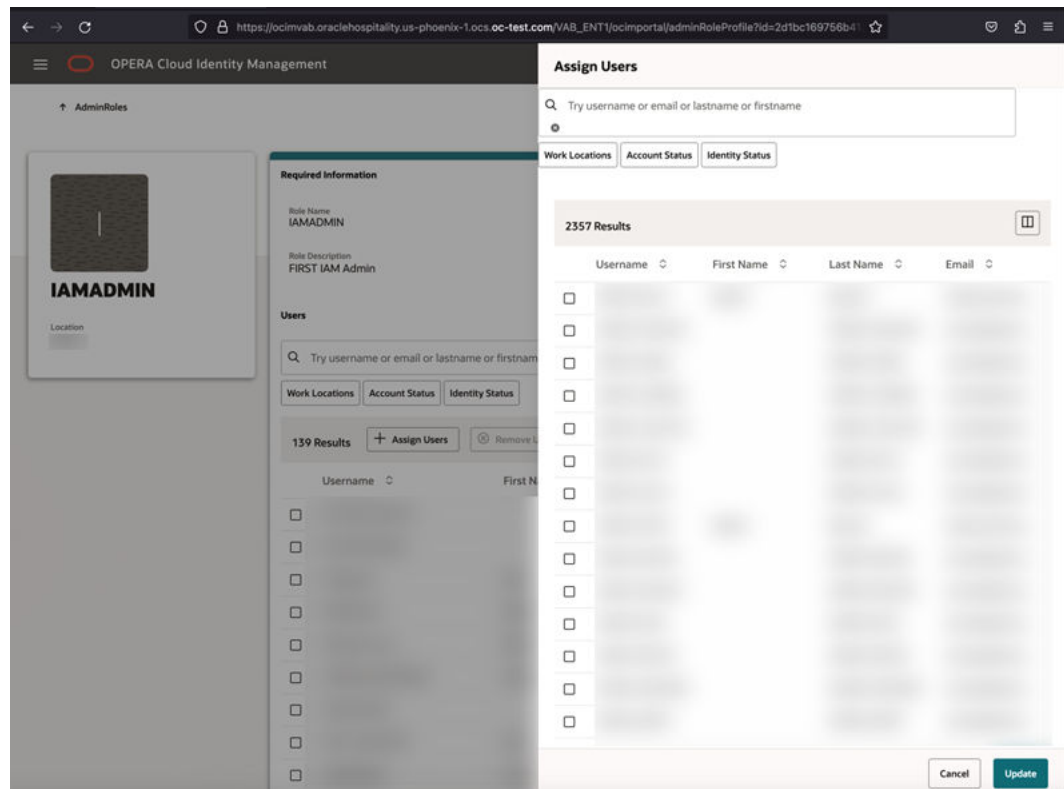


Managing Administrator Role Memberships

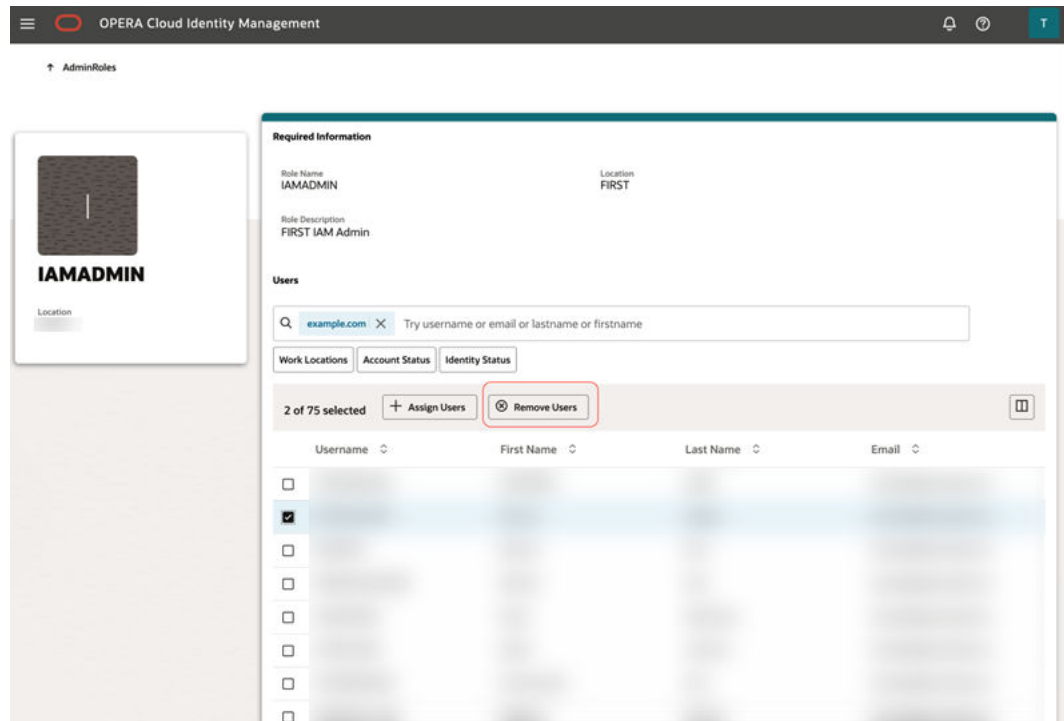
- You can click the respective role name to manage the administrator role membership.



- On clicking the administrator role name, the respective administrator role profile page opens.
 - Administrator Roles Profile page consist of a search bar and a table listing members of that role which also supports filtering.
 - Administrator Roles Profile also consist of buttons to Assign Users and Remove Users to the role.
2. Click **Assign Users** to add users to that administrator role. The assign users section opens on the same page.



3. Select a user and click **Update** to assign that user to the role.
4. Once on the Administrator Roles Profile page, select any user and click **Remove User** to remove that user from the role.



3

Managing Groups

Groups in OPERA Cloud Identity Management

OPERA Cloud applications use groups for authorizing users. These groups are stored in a customer's OCI IAM Identity Domains and managed using OPERA Cloud Identity Management Portal.

This section provides steps for managing groups in OPERA Cloud Identity Management portal.

OPERA Cloud Identity management consist of two types of groups:

1. **Seeded Groups** are groups available out of the box in OPERA Cloud Identity Management and are associated with chains and properties. Seeded groups are created in a customer's OCI IAM Identity Domains during chain or property provisioning in OPERA Cloud applications. These group cannot be deleted using the OPERA Cloud Identity Management Portal.

The following groups are seeded groups in OPERA Cloud Identity Management:

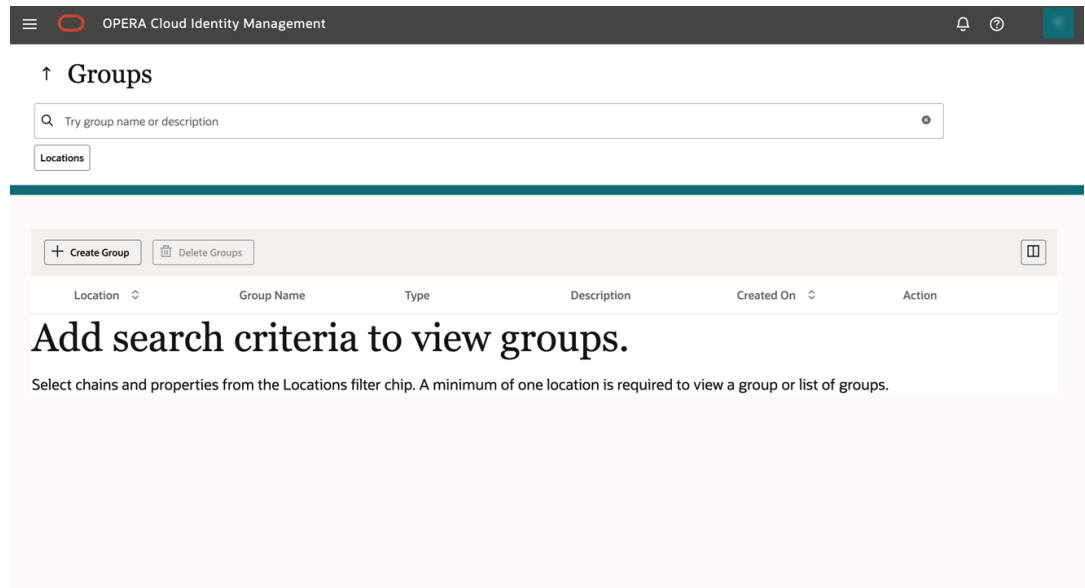
- ADMIN
- OPERACASHIER
- HDP_CHANNELMANAGEMENT
- HDP_ADMIN
- DEVELOPERPORTALACCESS
- CCTRANS
- CCCONF
- PPCONF
- OC_RNA-APPADMIN
- OC_RNA-REPORTINGADMIN
- OC_RNA-BIADMIN
- OC_RNA-CHAINADMIN
- GUESTEXPERIENCE

2. **Custom Groups** are those groups created by customer administrators based on their access control requirements. Custom groups must be mapped to permissions in OPERA Cloud Role Manager.

Navigating to the Group Management Page

1. Log in to OPERA Cloud Identity Management as an administrator.
2. Click the **Groups** tile on the home page.

The Group Management page consists of a search bar and a table listing all the groups pertaining to a location.



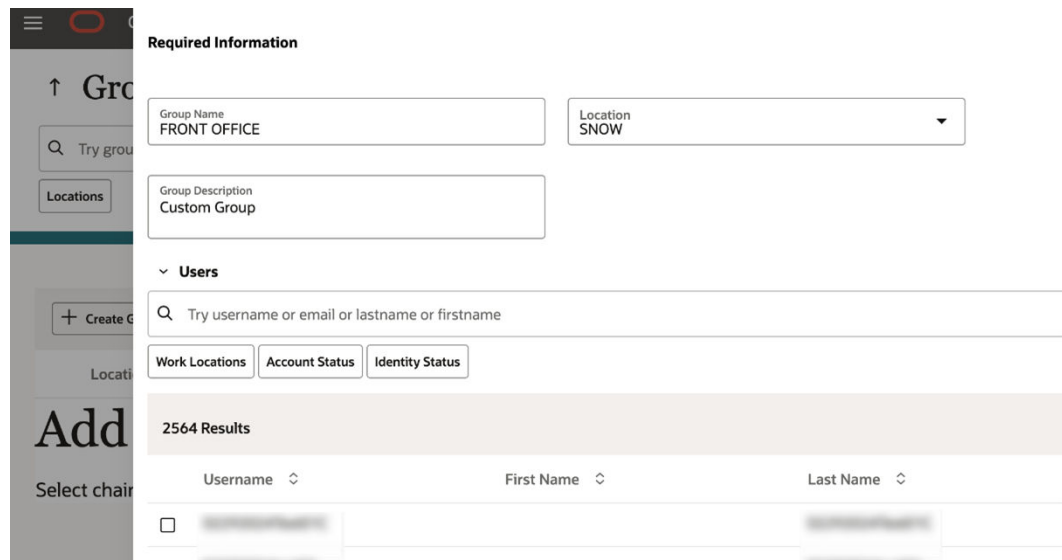
Creating a Custom Group

1. Click the **Create Group** button on the Group Management page.
2. Enter the custom **Group Name**.

Note:

Empty spaces will be replaced with underscores.

3. Select a location from the location list of values.
4. Optionally, you can also select users for assigning group membership.
5. Click **Submit** to create the custom group.



Searching for Groups

- Click **Locations** and select the location to search the associated groups for that location. Optionally, you can also search based on group name or even group description.

↑ Groups

Locations FIRST × ADMIN × Try group name or description

4 Results + Create Group Delete Groups

Location	Group Name	Type	Description	Created On	Action
FIRST	ADMIN	Read Only	FIRST	2024-01-23T10:18:02.9...	
<input type="checkbox"/> FIRST	HDP_ADMIN	Editable	FIRST	2024-01-26T10:33:15.1...	
<input type="checkbox"/> FIRST	ITADMIN	Editable	FIRST	2024-01-25T06:05:35.4...	
<input type="checkbox"/> FIRST	VAFIRST_ADMINUG	Editable	FIRST	2024-01-25T06:05:34.9...	

Note:

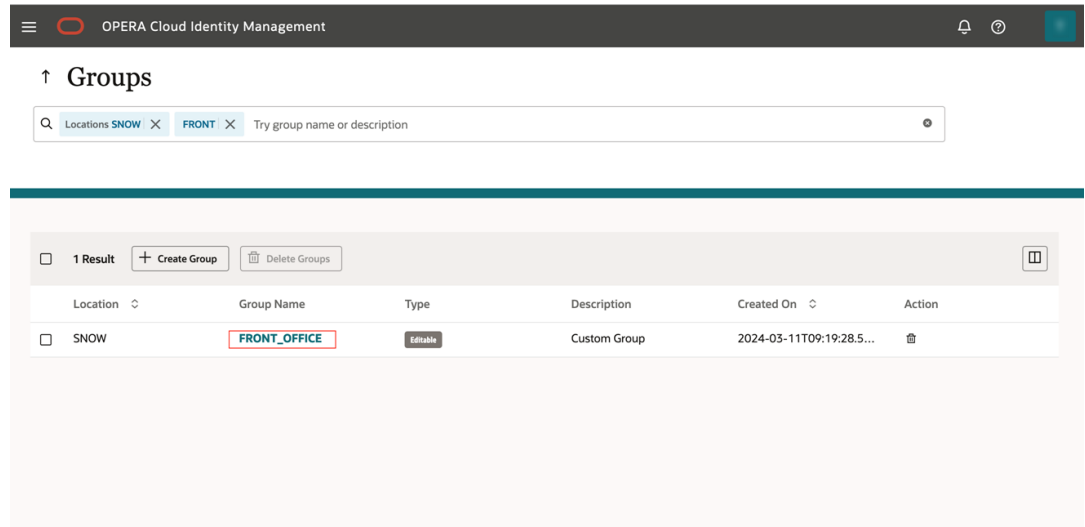
Seeded Groups are denoted as “Read Only” and Customer Groups are denoted as “Editable.”

Group Profile Management

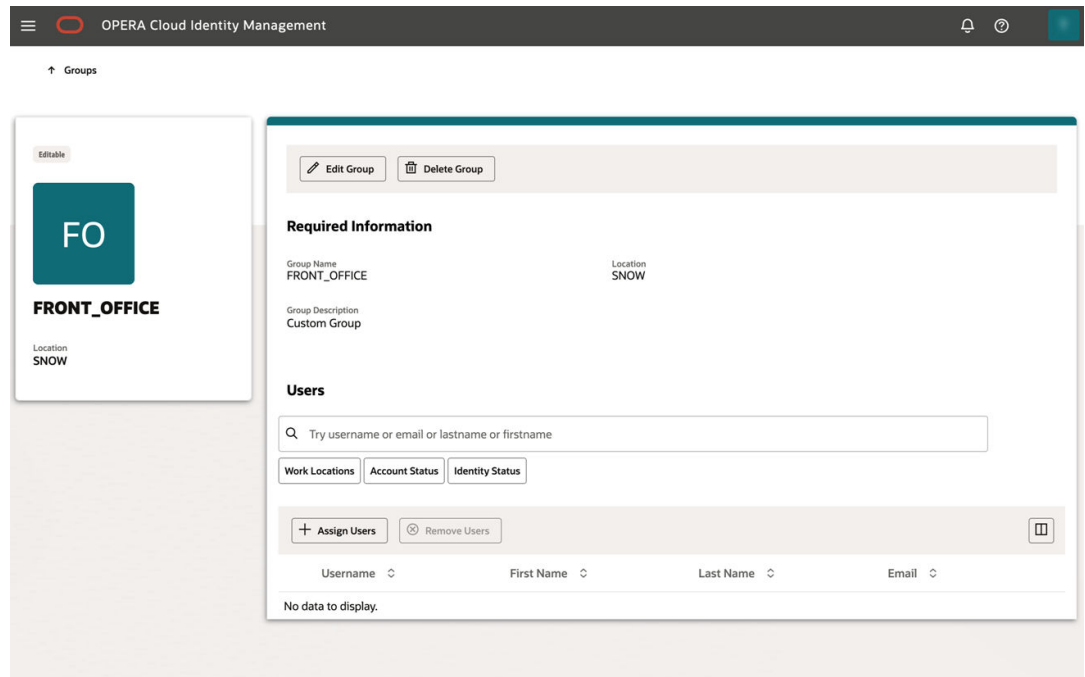
This page allows administrators to edit group description, assign user group membership, and remove user group membership.

Assigning and Removing Group Membership

1. Click the **Group Name** to open the group profile page.



Group details such as group description, associated location, and group memberships can be viewed on this page. Group membership also supports searching filters to filter users in the group membership table.




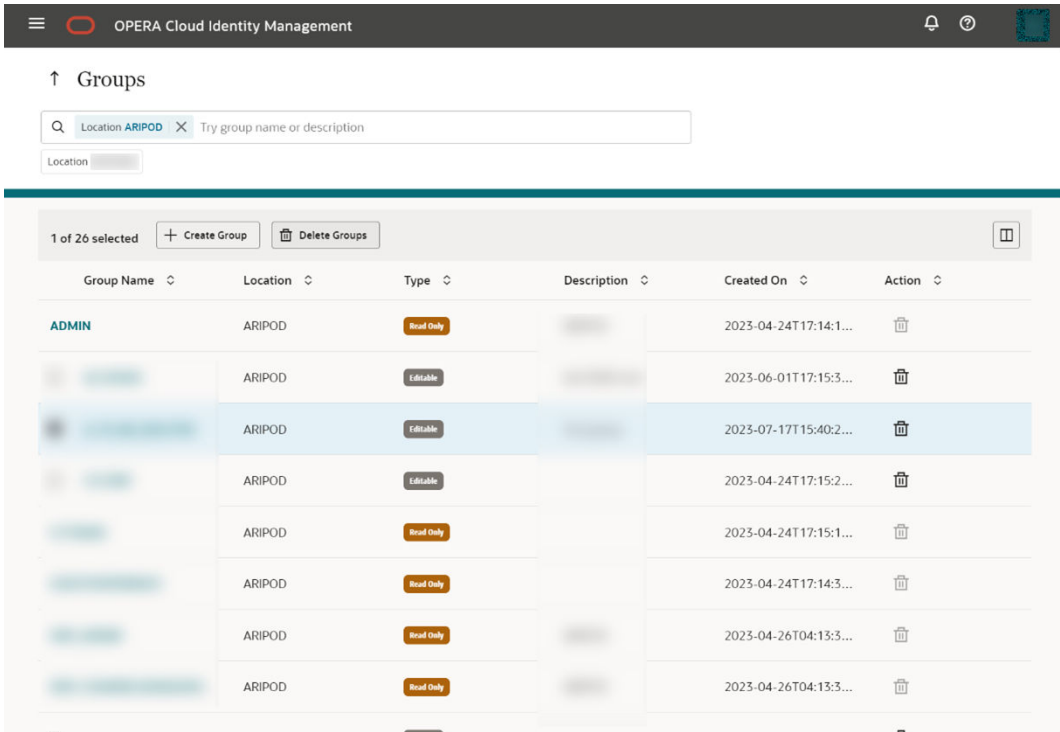
2. Click **Edit Group** to edit the group description.
3. Click **Assign Users** to assign user group membership in the group. Select the user and click **Update** to assign the group membership.
4. Select a user in the group membership table and click the **Remove Users** button to delete that user group membership.

Deleting a Group

1. Search for groups on the Group page.

2. Select group(s) and click the **Delete Groups** button to delete the group.

 **Note:**
Seeded groups cannot be deleted in the OPERA Cloud Identity Management portal and only custom groups can be deleted.

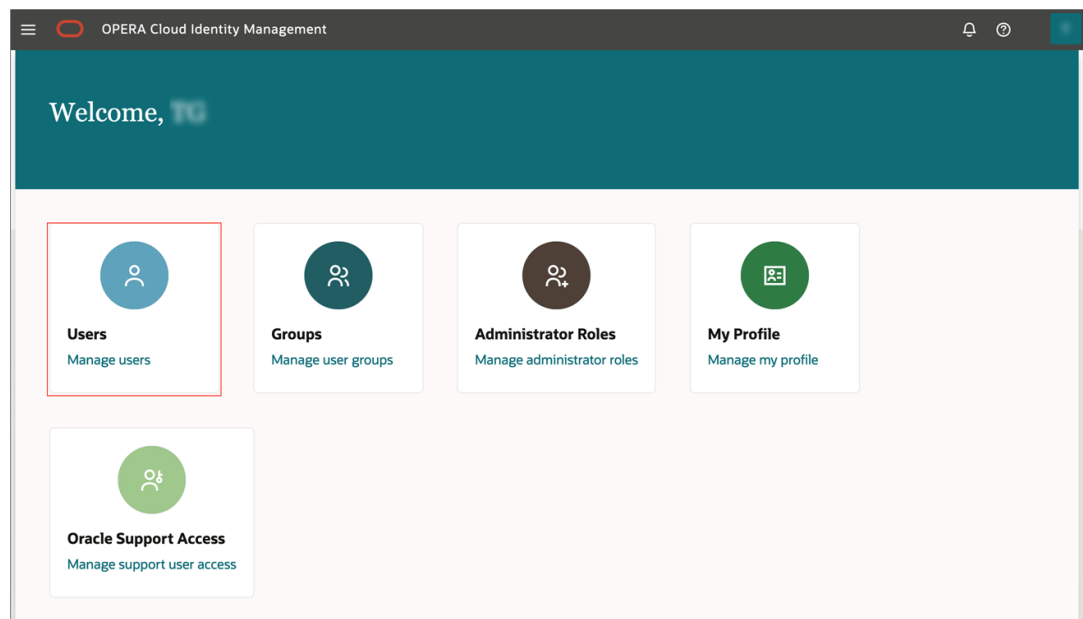


4

Managing Users

Navigating to the User Management Page

1. Log in to OPERA Cloud Identity Management as an administrator.
2. Click the **Users** tile on the homepage.



The User Management page consists of a search bar and a table listing all the users pertaining to a location.

Creating a User

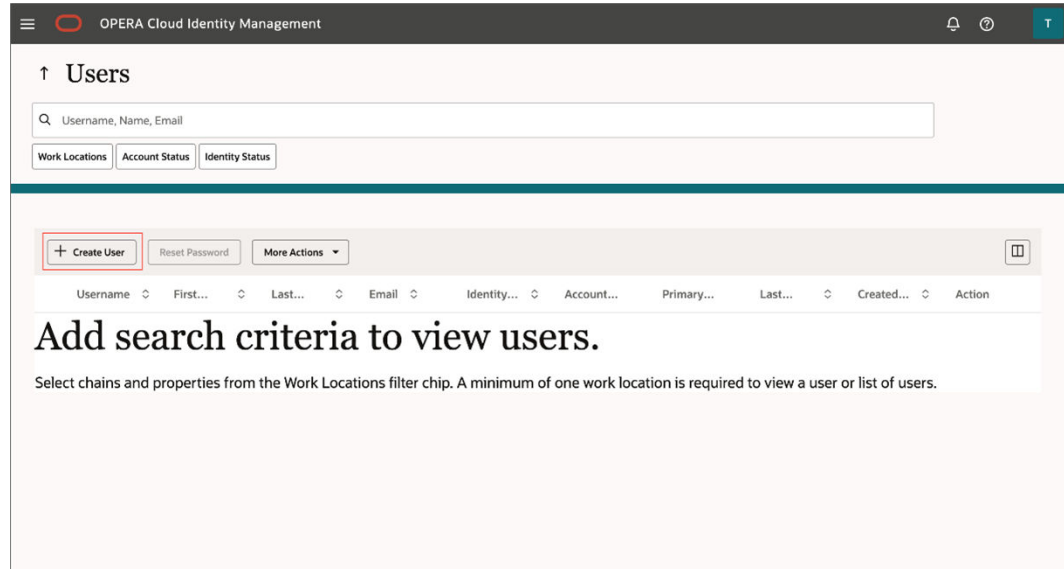
During a new employee or contractor onboarding in a chain or property, the administrator can create the user account in OPERA Cloud Identity Management using the OPERA Cloud Identity Management portal.

 **Note:**

Only respective IAMADMIN role members associated to the enterprise or a chain or a property in OPERA Cloud Identity Management can create a user in OPERA Cloud Identity Management Portal. Chain and property ADMIN group members are by default IAMADMIN administrator role members in OPERA Cloud Identity Management.

Follow the below steps to create a user account in the OPERA Cloud Identity Management portal.

1. Click the **Create User** button on the User Management page. A create user prompt appears.



2. The Create User prompt consists of the below user fields for creating a user:
 - **Last Name**
 - **Email Address**
 - **Username**
 - **Primary Work Location:** This is the chain or property code representing the location where the user works.
 - **Optional:** You can add additional information in the Additional Information section.
 - **Optional:** You can search for and select groups to which you can add the user during the user creation process.

Create a user also allows assigning of group membership during user creation. Groups can be searched and selected to be assigned during user creation.

3. Click **Create** to create the user.

Create User

Required Information

Last Name Required Email Address Required Username Required

Primary Work Location Required

Additional Information

Groups

Try a group name or description

Location SHSTGE3

366 Results

Name	Location	Description
ADMIN	316	316
ANSHULTEST	316	TEST anshul
CCCONF	316	

Cancel Create

Searching for Users and Performing User Actions

1. Click **Locations** and select the location to search for the associated users in that location. Optionally, you can also search user(s) based on username, name or even user email address.
2. Select users from the search result and perform actions on those user(s) by clicking **More Actions**.

The screenshot displays the OPERA Cloud Identity Management interface. At the top, there is a navigation bar with the OPERA logo and the text 'OPERA Cloud Identity Management'. Below this, the page title is 'Users'. A search bar is present with the placeholder text 'Username, Name, Email'. Below the search bar, there are two filter buttons: 'Account Status Locked' and 'Identity Status Active'. The main content area shows a summary of '285 Results' and three action buttons: '+ Create User', 'Reset Password', and 'More Actions'. Below this is a table with the following columns: Username, First Name, Last Name, Email, Primary Location, and Action. The table contains six rows of user data, with the last row showing 'ARIPOD3' in the Primary Location column. Each row has a checkbox on the left and a three-dot menu icon in the Action column.

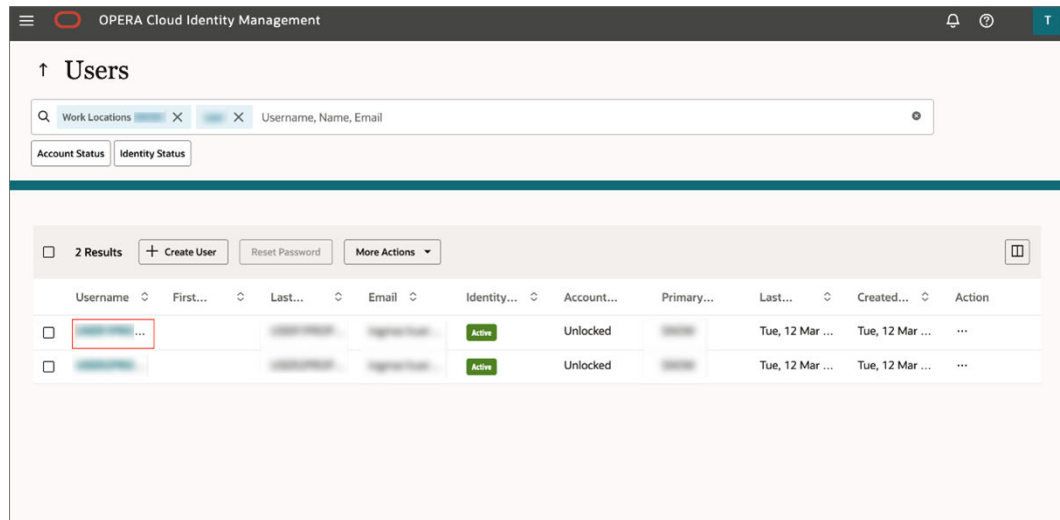
- Alternatively, click the **Action** column for a user row to perform actions on that respective user.

User Profile Management

The User Profile Management page enables administrators to edit a user description, assign user group membership, remove user group membership, and perform certain actions on the user.

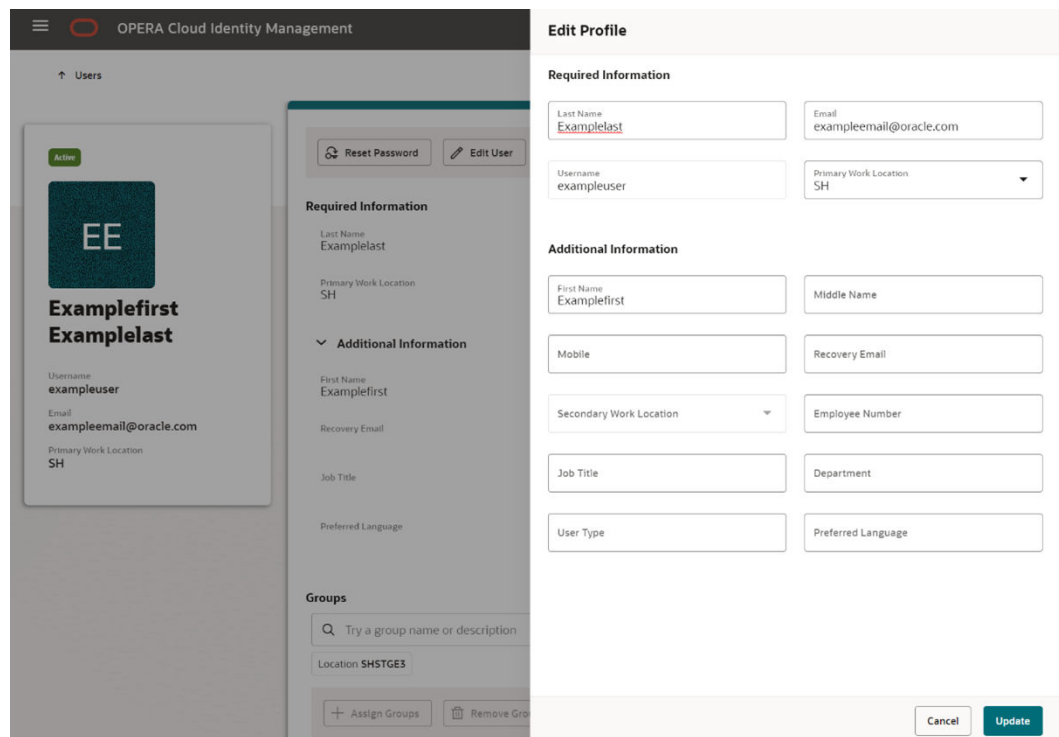
On the User Profile Management page, you can do the following:

- Reset the password for the user
- Edit the user details
- Access the following actions:
 - Reset Factors
 - Unlock Account
 - Deactivate user
 - Delete user



Editing a User

1. Click **Username** to open the User Profile page.
2. Click **Edit User** to open the prompt to edit user fields.
3. Edit the following details as needed:
 - **Last Name**
 - **Email Address**
 - **Username**
 - **Primary Work Location**: This is the chain or property code representing the location where the user works.
 - **Optional**: You can add additional information in the Additional Information section.
 - **Optional**: You can search for and select groups to which you can add the user during the user creation process.
4. Click **Update** to update the user.



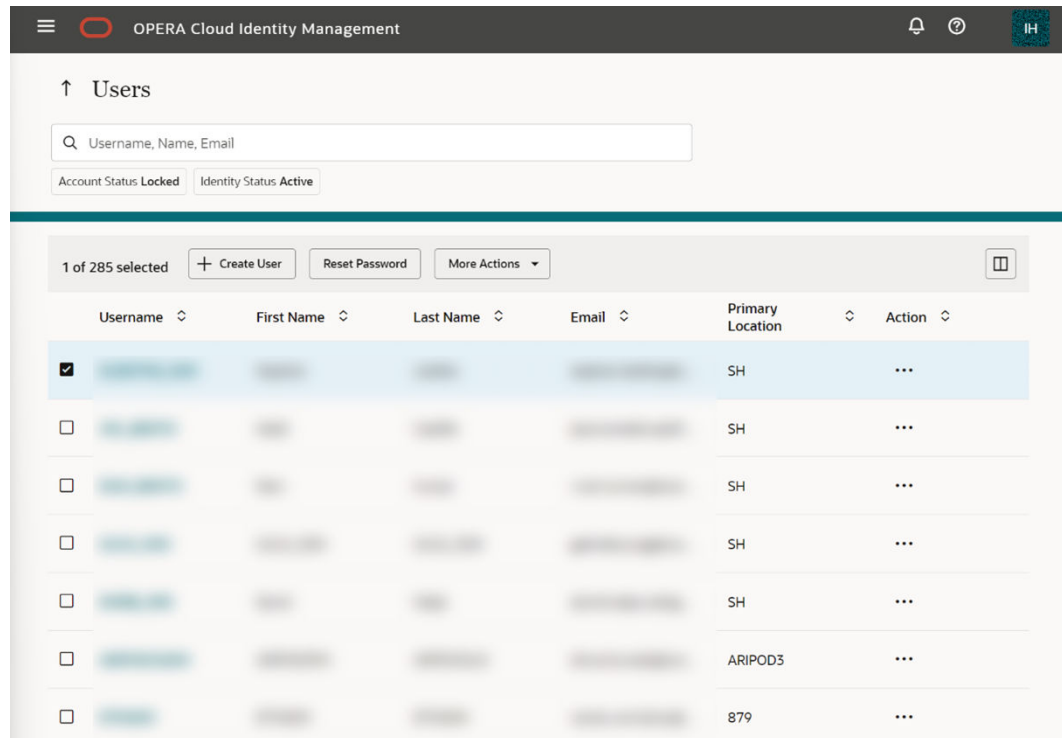
5. Click **More Actions** to perform various user actions.

Resetting a User Password

1. Click **Username** to open the User Profile page.
2. Select one or multiple users. After your selection, the Reset Password button appears.
3. Click the **Reset Password** button to reset the passwords for all selected users.
 - Users receive an email that allows them to enter a new password.

Note:

Administrators cannot reset the passwords for deactivated user accounts.



The screenshot displays the OPERA Cloud Identity Management interface. At the top, there is a navigation bar with the OPERA logo and the text "OPERA Cloud Identity Management". Below this, the page title "Users" is shown with an upward arrow. A search bar is present with the placeholder text "Username, Name, Email". Below the search bar, there are two filter buttons: "Account Status Locked" and "Identity Status Active". The main content area shows a table of users. The table has columns for "Username", "First Name", "Last Name", "Email", "Primary Location", and "Action". The first row is selected, and the "Primary Location" is "SH". The table also shows "1 of 285 selected" and buttons for "+ Create User", "Reset Password", and "More Actions".

Changing Primary Work Location for a User

During an employee or contractor transfer from one property or chain to another, OPERA Cloud Identity Management supports changing a user's primary working location to a new location, so the new location's administrator can manage the user.

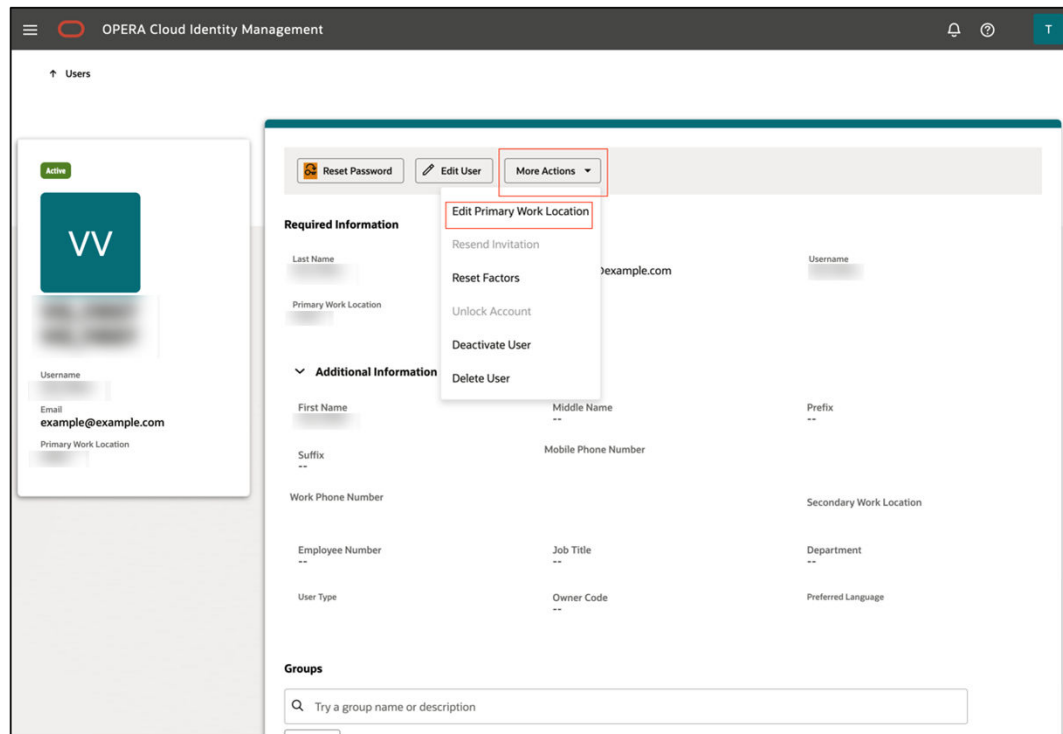


Note:

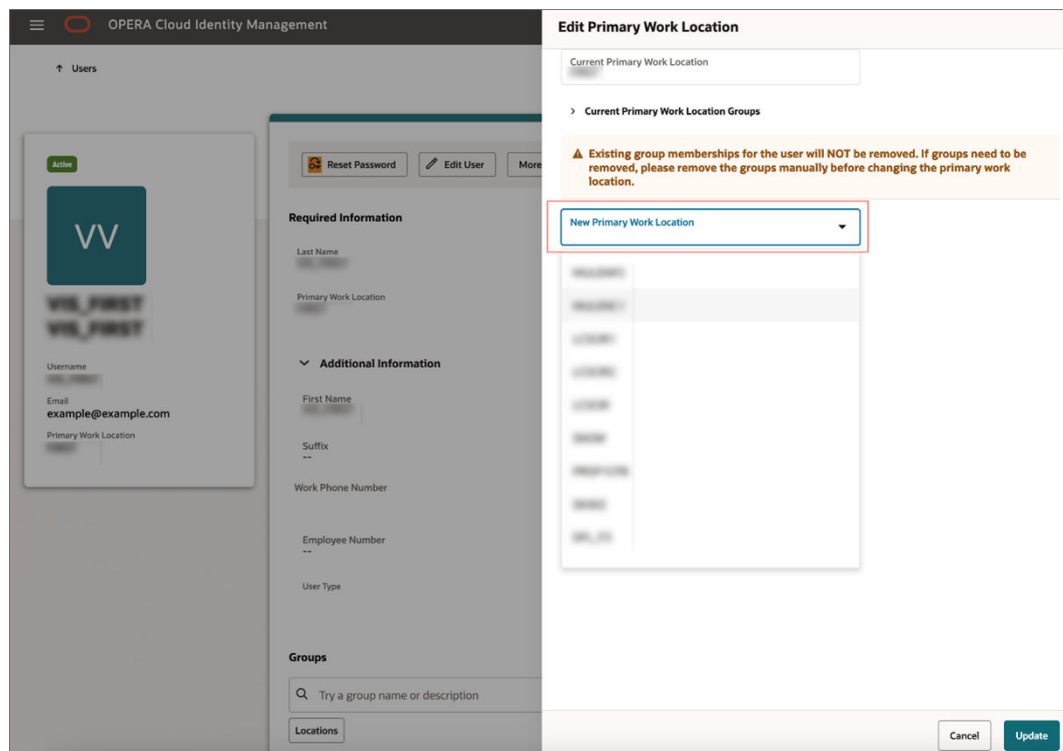
Only a chain IAM administrator or enterprise IAM administrator in OPERA Cloud Role Manager can perform this operation.

Follow the below steps to update a user's primary work location.

1. On the User Profile page for a user, click **More Actions** and then click **Edit User Primary Work Location**.



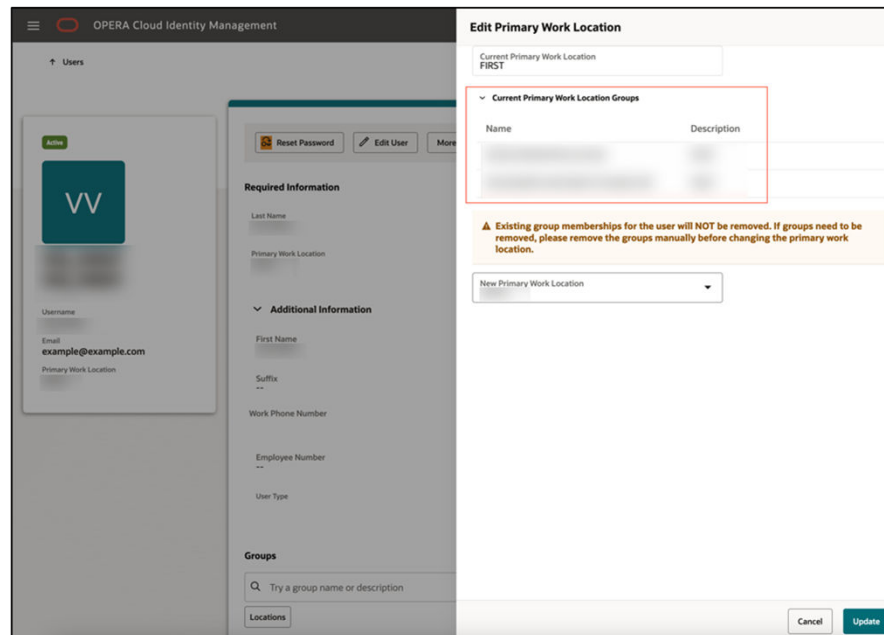
2. Click **New Primary Work Location** to select the new primary work location from the list of values, which is depicted as Chain followed by its properties.



3. Click **Current Primary Work Location Groups** to view group memberships for that user associated with the current primary work location.

 **Note:**

Before you update the primary work location, it is highly recommended that you remove group memberships for the user associated with the current primary work location.



4. Click **Update** to update the User Primary Work Location.

Deleting a User

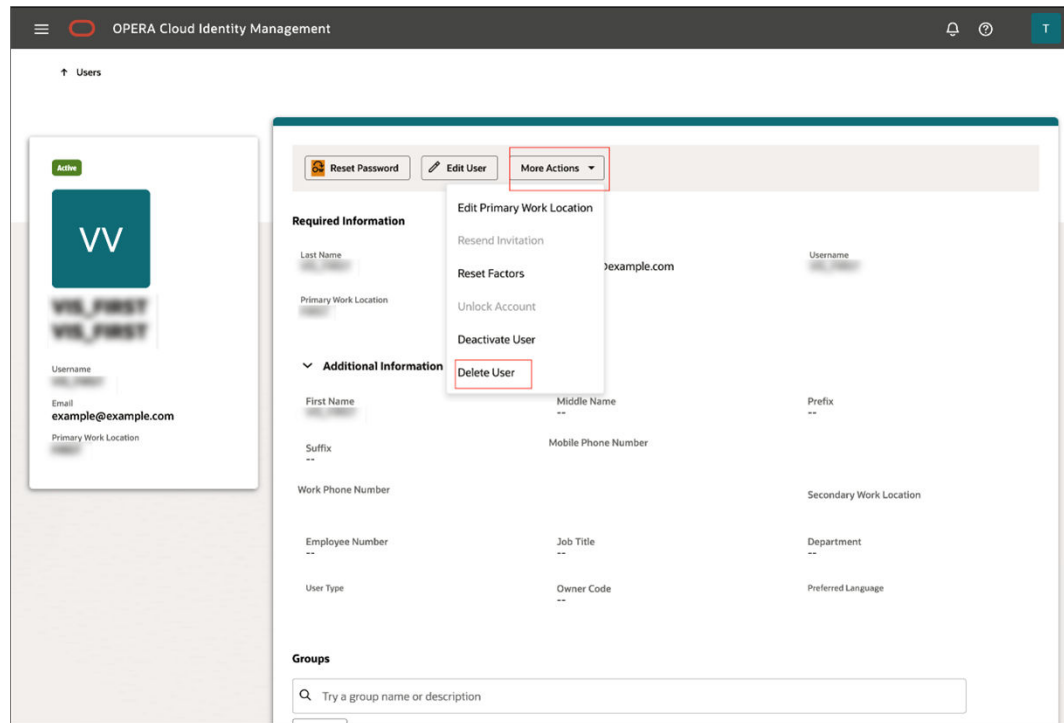
During user termination, OPERA Cloud Identity Management supports deleting user accounts in the OPERA Cloud Identity Management portal.

 **Note:**

Only respective IAMADMIN role members associated to the enterprise or a chain or a property in OPERA Cloud Identity Management can delete a user in OPERA Cloud Identity Management Portal. Chain and property ADMIN group members are by default IAMADMIN administrator role members in OPERA Cloud Identity Management.

Follow the below steps to delete user accounts in OPERA Cloud Identity Management.

1. On the User profile page for a user, click **More Actions** and then click **Delete User**.



2. Click **Delete** to delete the user account.