Oracle® Hospitality OPERA Cloud Identity Management

Administrator Guide

Release 25.2
G33329-02
July 2025

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide, Release 25.2

G33329-02

Contents

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 2025	Initial publication
July 2025	Added HDP_CLUSTERMGMT to seeded groups list.

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

Keyboard Navigation Shortcuts

In the OPERA Cloud Identity Management portal, you can use keyboard shortcuts as an alternative to using your mouse. The following keyboard shortcuts are supported:

Filter Chips in Search Bars

- **Tab** — Press to access.
- **Enter** — Press to open the filter chip and to select.
- **Arrow keys** — Press to navigate.
- **Back Space** — Press to remove or clear search.
- **Ctrl+A** — Press to select all the chosen values in the Search field.
- **Delete** — Press to clear search after selecting all chosen values in Search field using Ctrl + A.
- **Esc** — Press to close.

Data Tables

- **Tab** — Press to access.
- **Arrow keys** — Press to navigate.
- **Space** — Press to select or unselect the record(s).
- **Enter** — Press to hold the record selection and to access the action items.
- **Esc** — Press to unhold the record selection.

Page Level Actions

- **Tab** — Press to access.
- **Enter**— Press to open and to select.
- **Arrow keys** — Press to navigate.
- **Esc** — Press to close.

Edit Drawers

- **Enter**— Press to open the drawer and to select.
- **Esc** — Press to close the drawer.
- **Tab** — Press to access.
- **Arrow keys** — Press to navigate.
- **Space** — Press to select or deselect the record(s).

Multi Select Fields

- **Tab** — Press to access.
- **Arrow keys** — Press to navigate.
- **Enter** — Press to select.
- **Esc** — Press to close.

3

Managing IAM Administrator Roles

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.

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 3-1 Administration Capabilities in OPERA Cloud Identity Management Portal

Administrator Role Name	View User	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
IAMADMIN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IAMUSERMANAGER	Yes	No	Yes	Yes	Yes	Yes	No	Yes	No	No
IAMHELPDESK	Yes	No	No	Yes	No	Yes	No	No	No	No

> **Note:**
>
> The IAMADMIN Administrator Role is automatically assigned for the ENTERPRISE-ADMIN, CHAIN-ADMIN or PROPERTY-ADMIN group member for that respective chain or property.

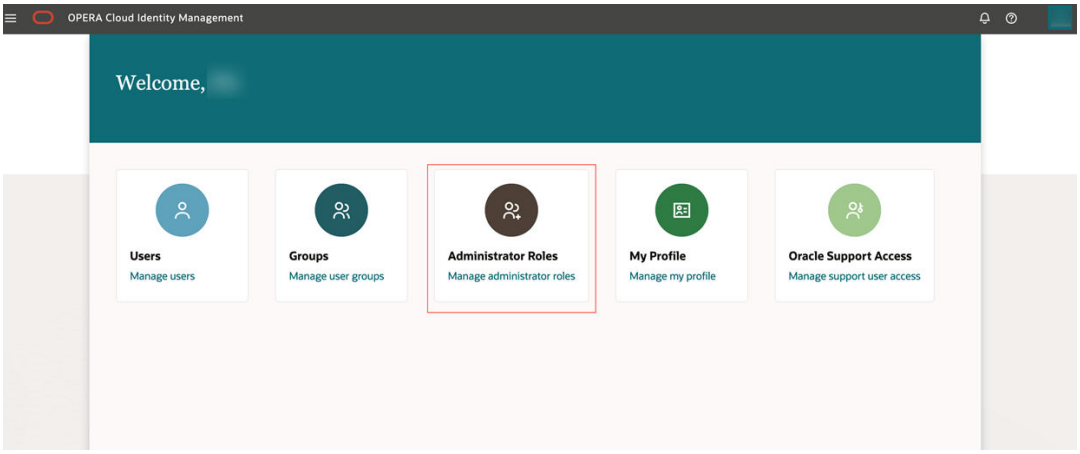
Navigating to Administrator Roles

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

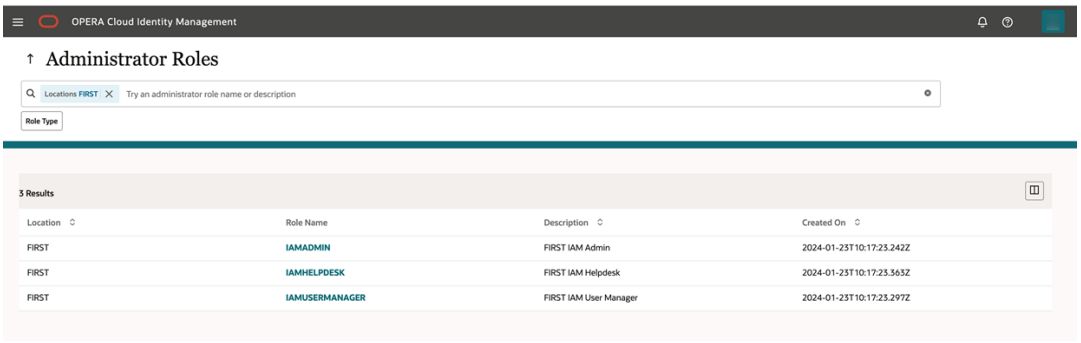
   > **Note:**
   >
   > During provisioning of OPERA Cloud, the Enterprise administrator along with the Chain administrator and Property administrator are created in the customer's OCI IAM Identity Domain, and those users automatically get assigned the IAMADMIN role in OPERA Cloud Identity Management.

   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.

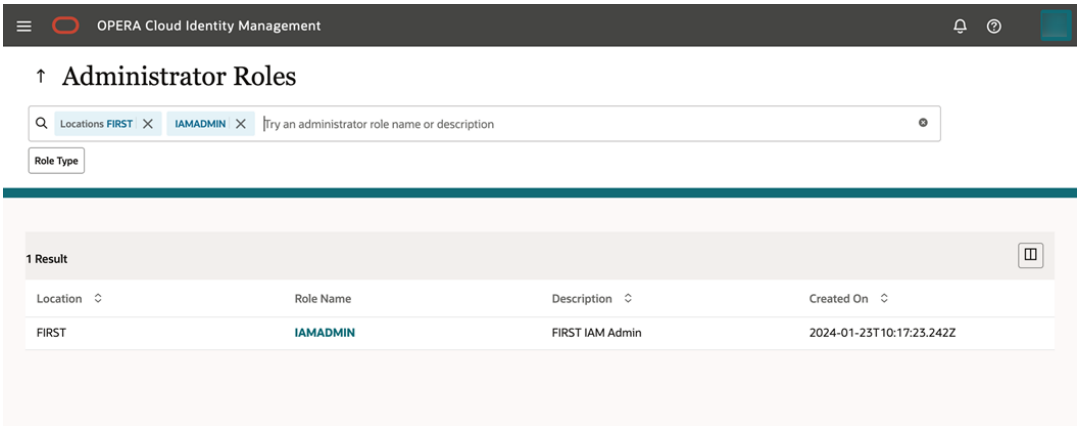


- The Administrator Roles page consist of a search bar and displays the Administrator Roles for your location.
- The search bar can be used to filter administrator roles based on locations and role name.



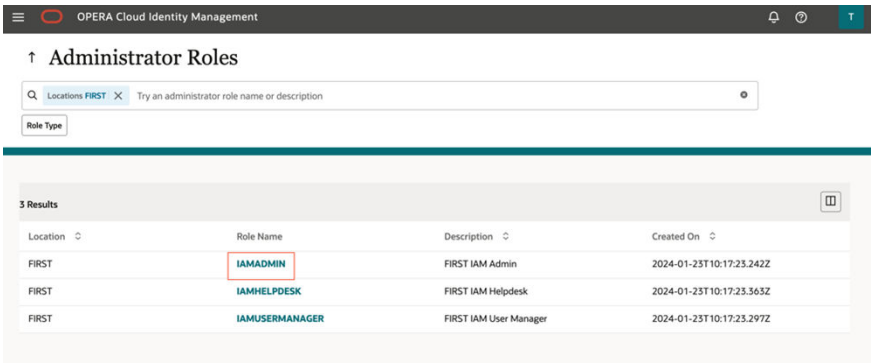
Searching for Existing Administrator Roles

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



Managing Administrator Role Memberships

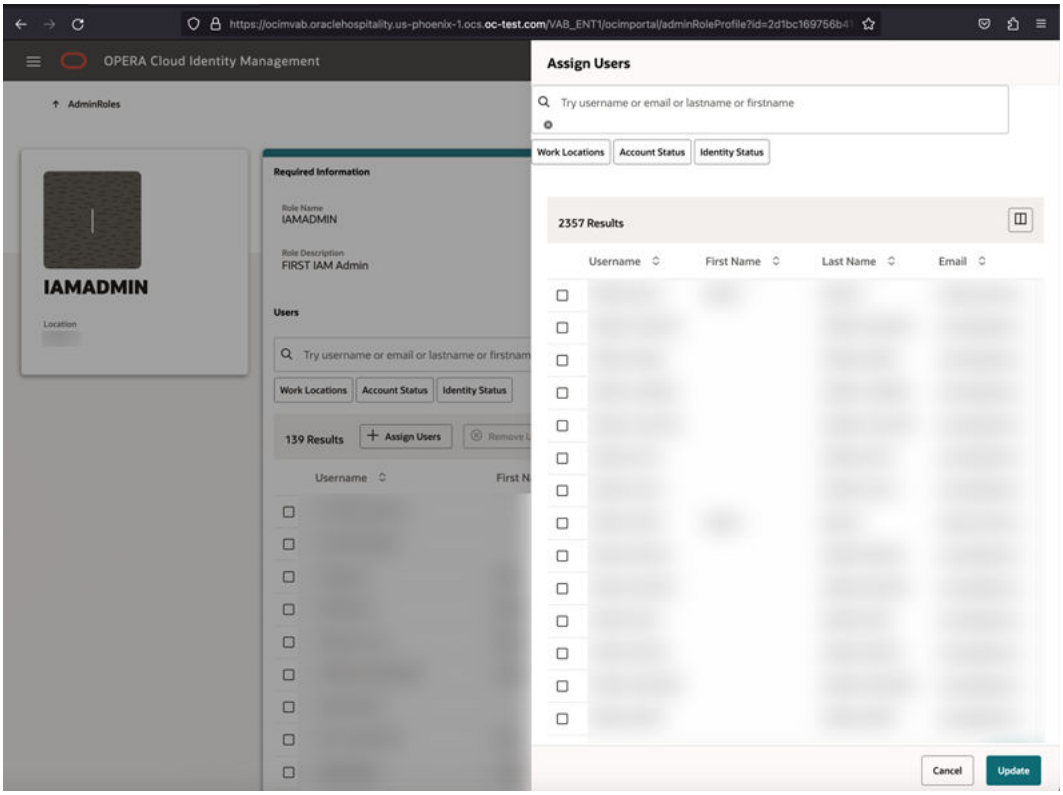
1. You can click the respective role name to manage the administrator role membership.



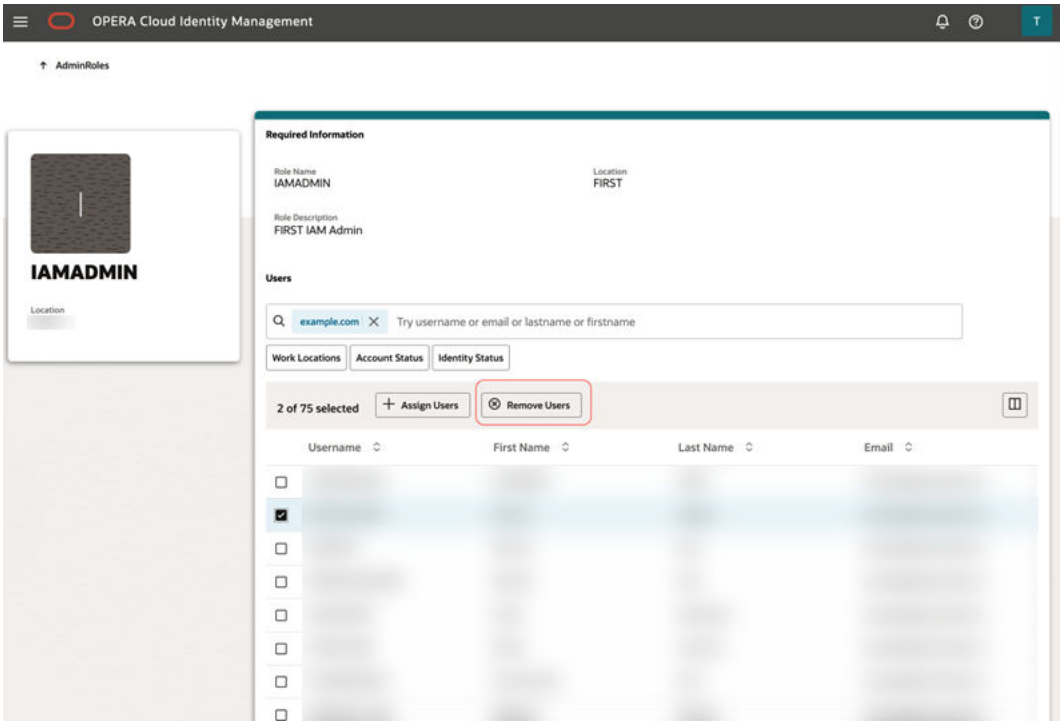
- On clicking the administrator role name, the respective administrator role profile page opens.

- 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.


OPERA Cloud Identity Management
AdminRoles
IAMADMIN
Location
Required Information
Role Name
IAMADMIN
Location
FIRST
Role Description
FIRST IAM Admin
Users
example.com
Try username or email or lastname or firstname
Work Locations
Account Status
Identity Status
2 of 75 selected
Assign Users
Remove Users
Username
First Name
Last Name
Email

4

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
   - HDP_CLUSTERMGMT
   - DEVELOPERPORTALACCESS
   - CCTRANS
   - CCCONF
   - PPCONF
   - OC_RNA-APPADMIN
   - OC_RNA-REPORTINGADMIN
   - OC_RNA-BIADMIN
   - OC_RNA-CHAINADMIN
   - GUESTEXPERIENCE
   - RNAACCESS

> **Note:**
>
> OC_RNA groups are only visible in Reporting and Analytics in the location "OC_RNA."

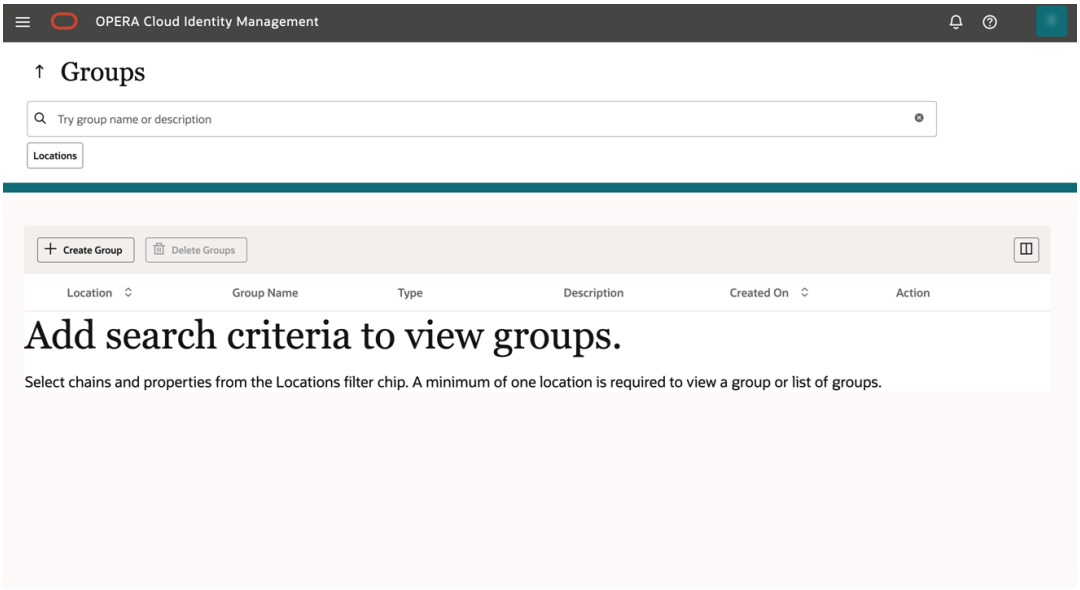
> **Note:**
>
> For more information on the seeded groups listed, refer to the respective Hospitality Cloud Product documentation.

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.

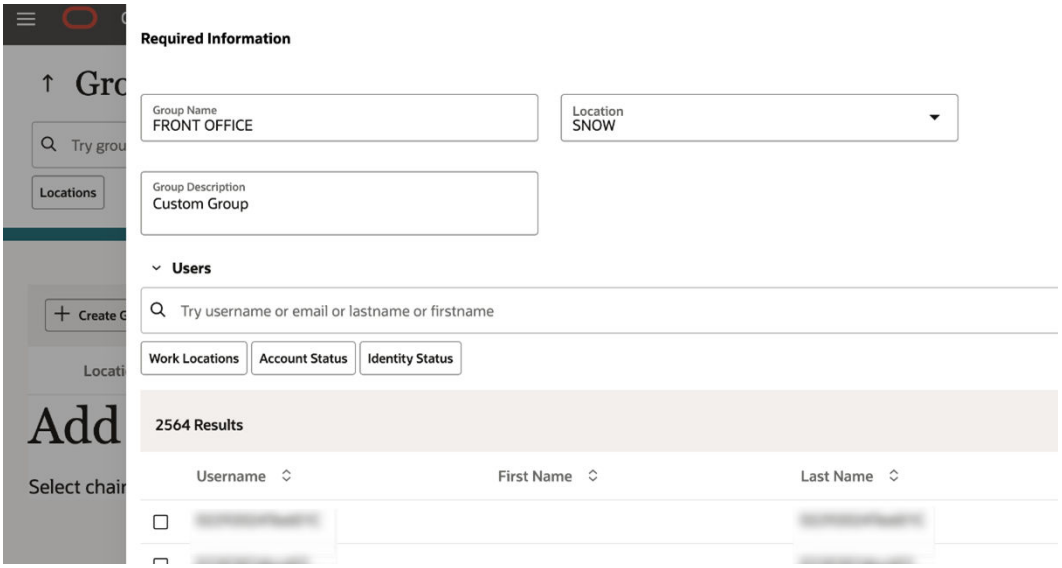


Creating a Custom Group

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.

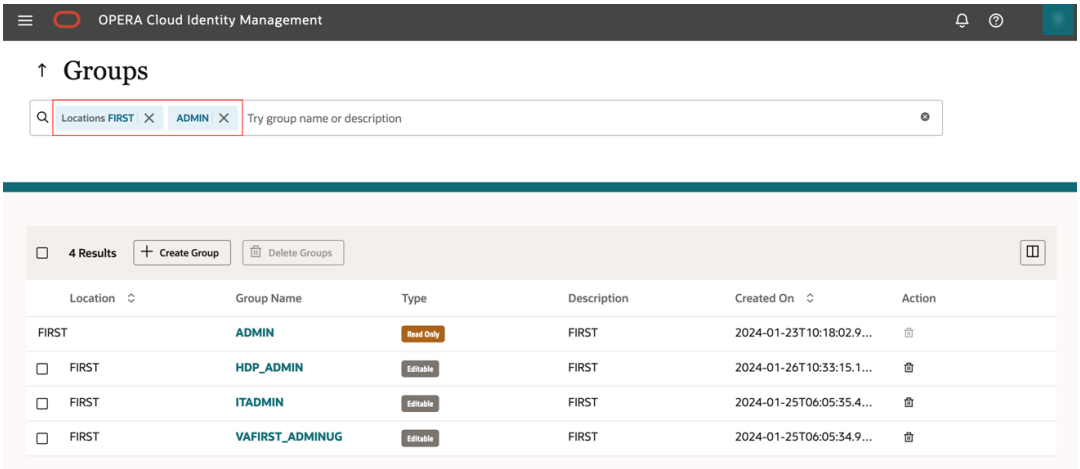
3. Select a location from the location list of values.
4. Optionally, you can also select users for assigning group membership.
5. Click **Submit** to create the custom group.



Searching for Groups

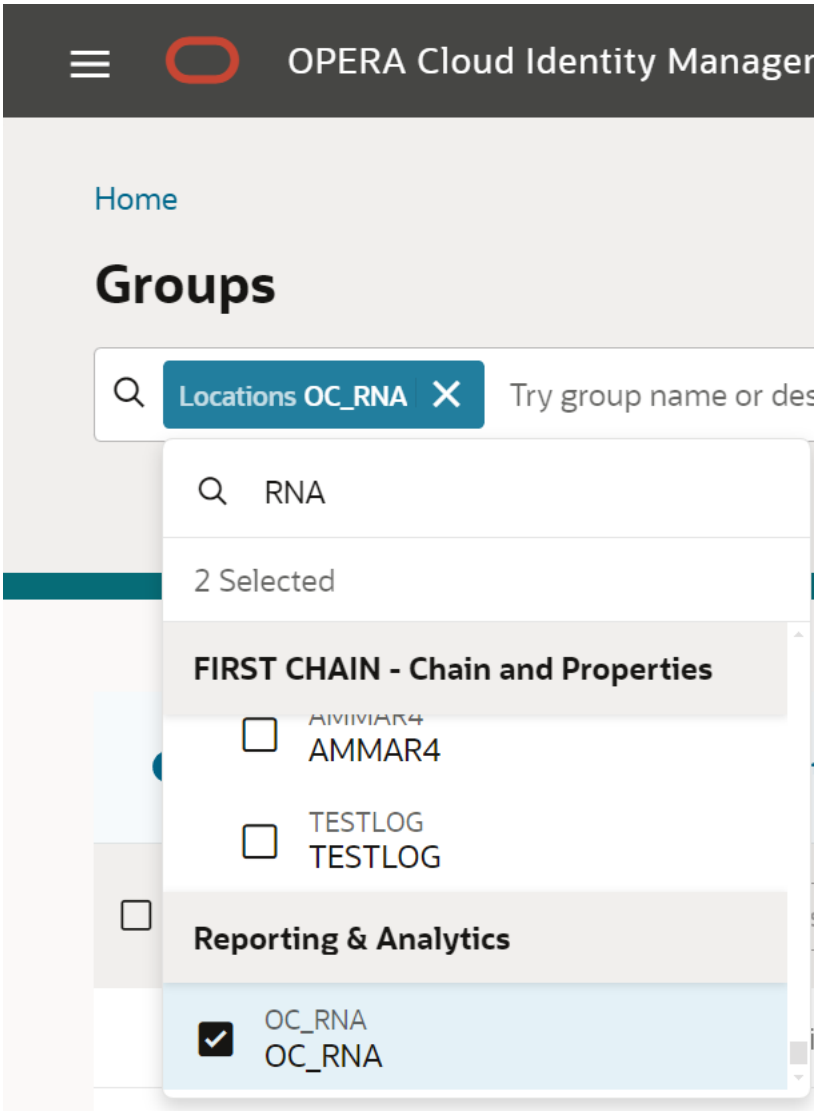
1. Click **Locations** and select the location to search the associated groups for that location.

   Optionally, you can also search based on group name or even group description.



> **Note:**
>
> Seeded Groups are denoted as “Read Only” and Customer Groups are denoted as “Editable.”

2. To search for Reporting and Analytics groups, click **Locations** and select the location **OC_RNA**.

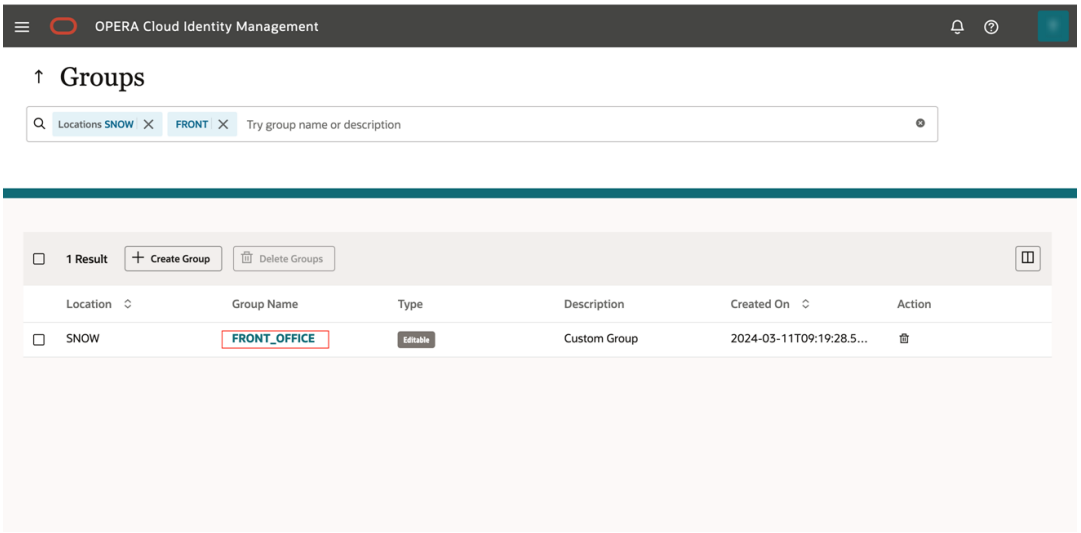


Group Profile Management

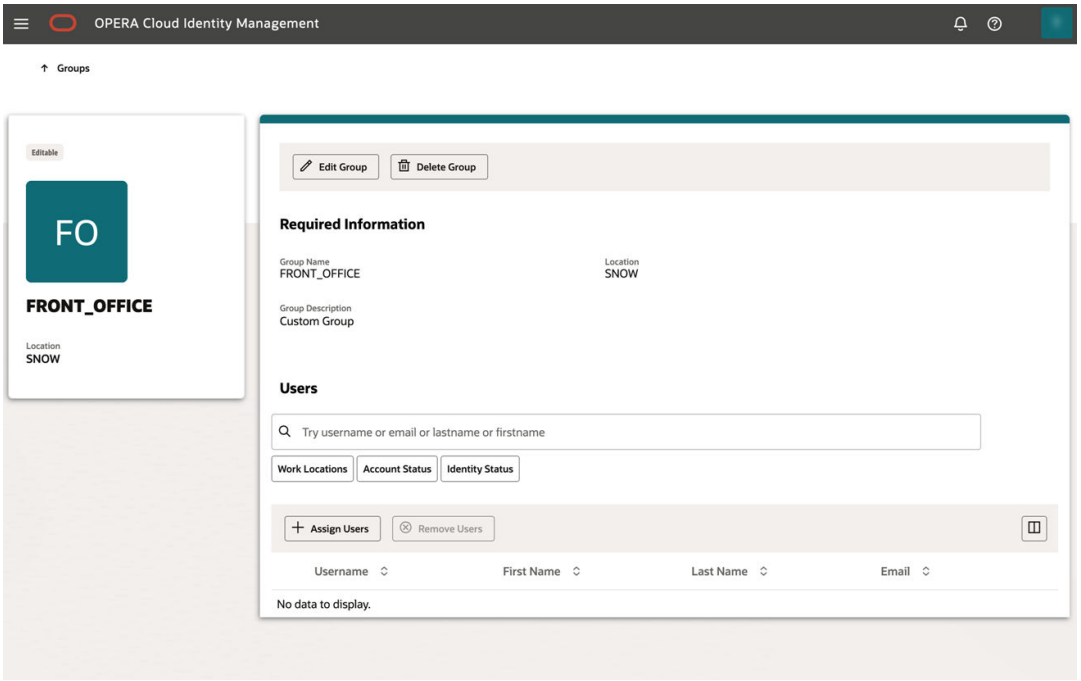
This page allows administrators to edit group description, assign user group membership, and remove user group membership.

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 filer users in the group membership table.



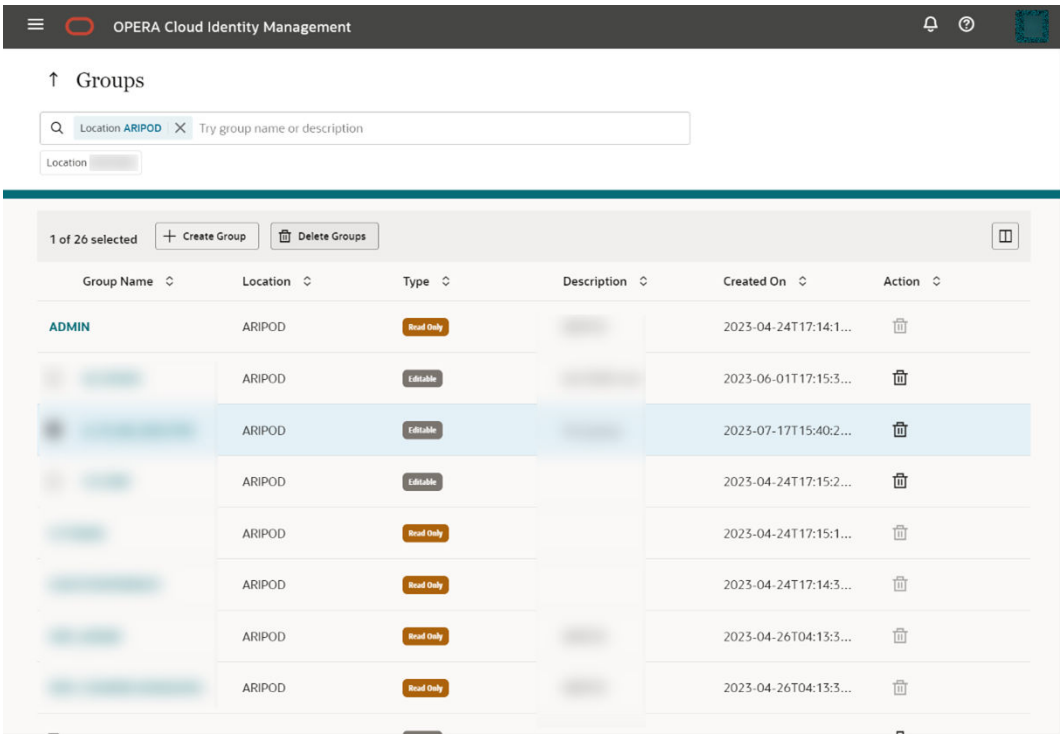
2. Click **Edit Group** to edit the group description.
3. Click **Assign Users** to assign user group membership in the group. Select the user and click **Update** to assign the group membership.
4. Select a user in the group membership table and click the **Remove Users** button to delete that user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

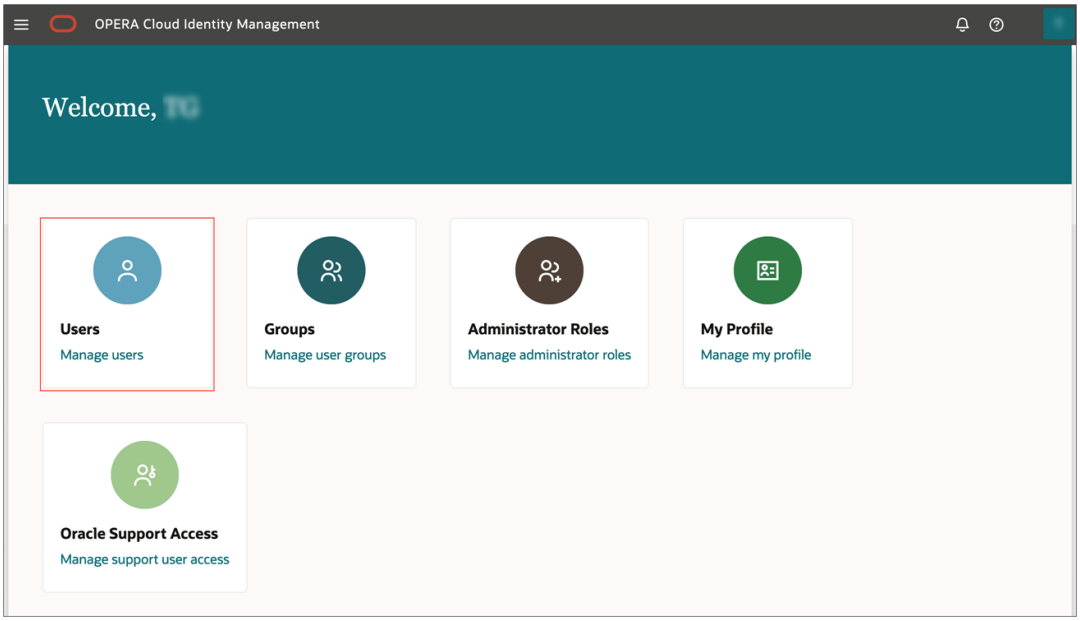


5

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.

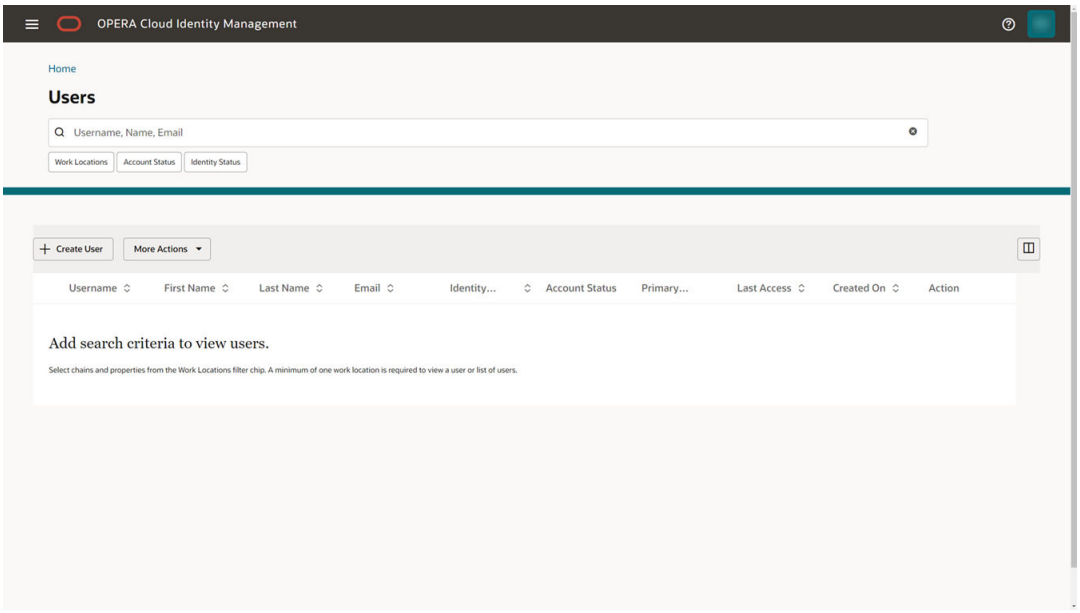
Creating a User with Email Address

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.

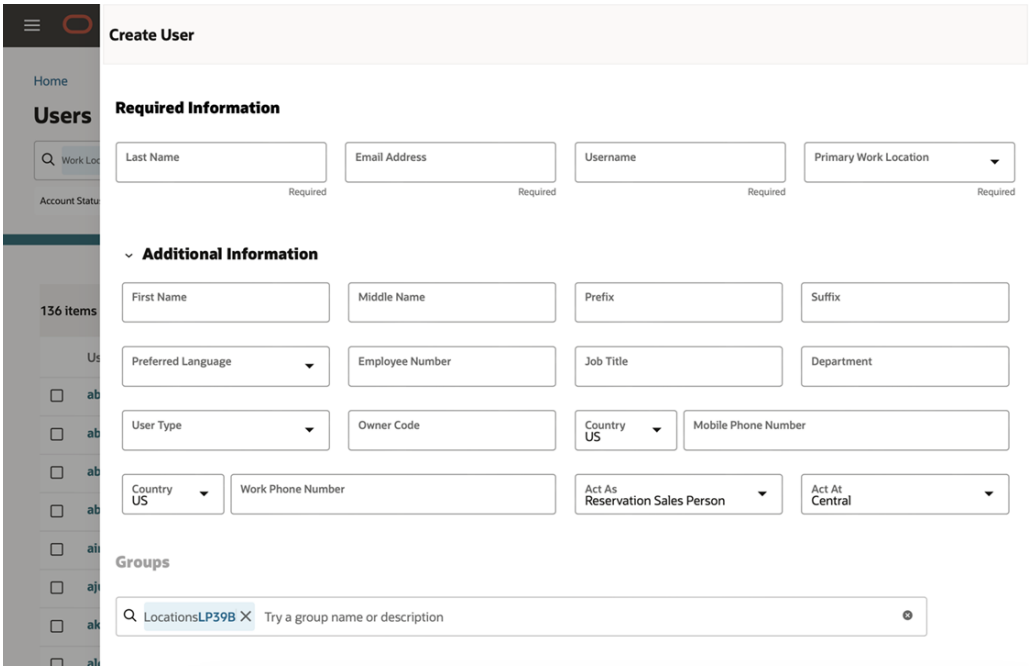
> **Note:**
>
> Only respective IAMADMIN role members associated to the enterprise or a chain or a property in OPERA Cloud Identity Management can create a user in OPERA Cloud Identity Management Portal. Enterprise, chain, and property ADMIN group members are by default IAMADMIN administrator role members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



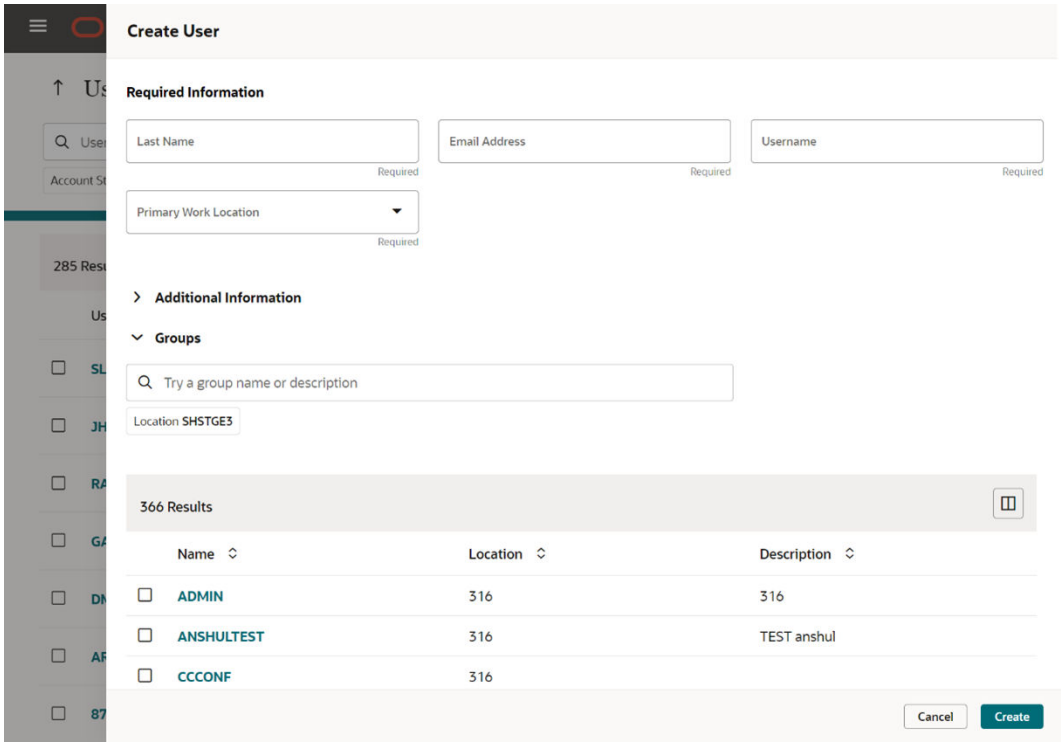
2. The Create User prompt consists of the below user fields for creating a user:
   - **Last Name**
   - **Email Address**
   - **Username**
   - **Primary Work Location**: This is the chain or property code representing the location where the user works.
   - **Optional**: You can add additional information in the Additional Information section. You can set values for the user's **Act As** and **Act At** fields while creating a new user in the OPERA Cloud Identity Management portal.



- **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.



Creating a User without Email Address

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. Enterprise, chain, and property ADMIN group members are by default IAMADMIN administrator role members in OPERA Cloud Identity Management.

In OPERA Cloud Identity Management, you can configure the domain to allow user creation without an email requirement. This is valuable for environments where users do not have an email account and allows these users to be managed in OPERA Cloud Identity Management.

> **Note:**
>
> For users without an email address, the administrator must create a temporary password for the user and must provide the user with the Login URL, the username, and the temporary password. The new user can log in with these credentials and will be prompted to create a password for future login to the user account.

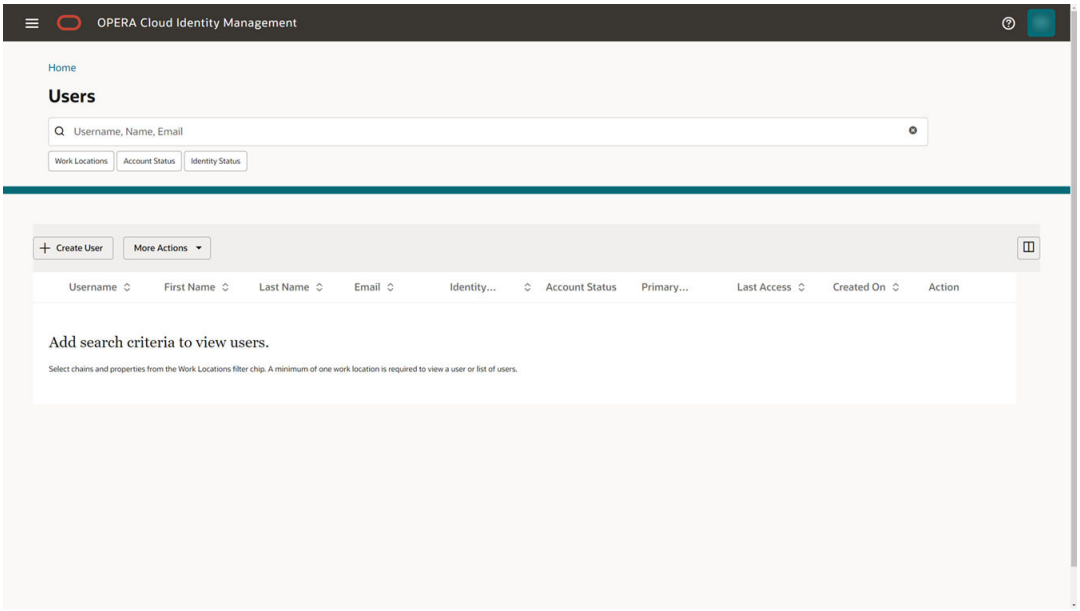
For users without an email address, communication related to the user account activation and the forgot password process must be managed with manual communication (that is, by text, in writing, verbal, and so on) between the OPERA Cloud Identity Management Administrator and the user since these users do not have an email address that can be used for communication.

> **Note:**
>
> Once an environment is configured with non-mandatory email for users and any user exists without email, you should not reactivate the mandatory email requirement unless all users have been given an email address.

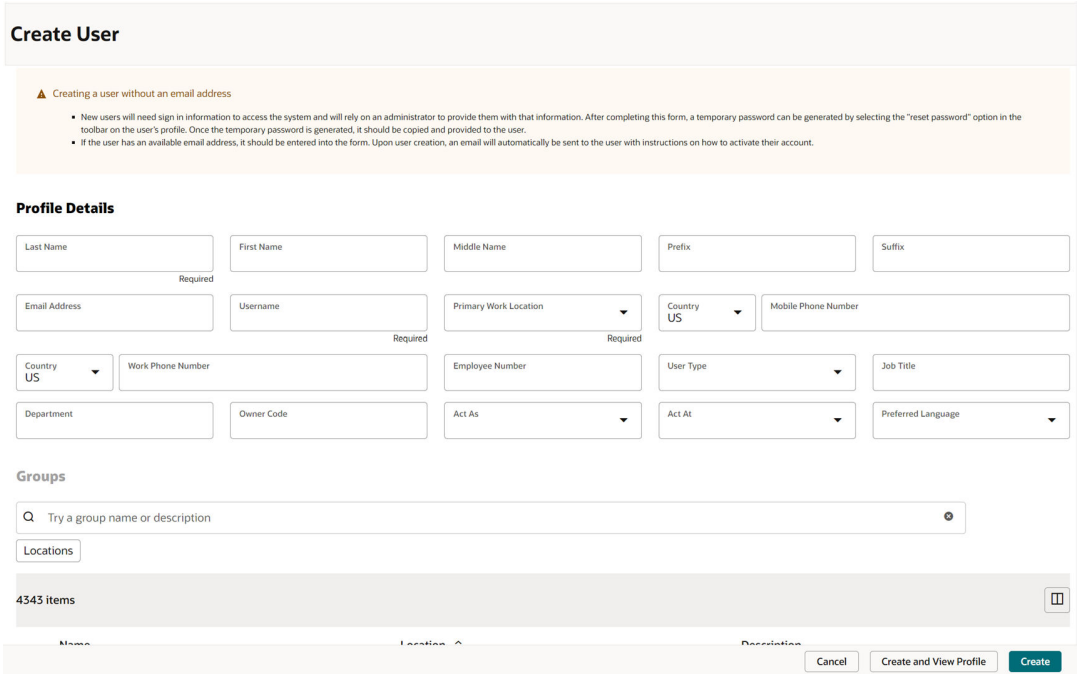
Follow the below steps to create a user account in the OPERA Cloud Identity Management portal.

> **Note:**
>
> You can create users with an email address, even if the domain has been configured to allow user creation without email addresses. When you create a user with an email address, the user receives an activation email, and the forgot password process will use this email address.

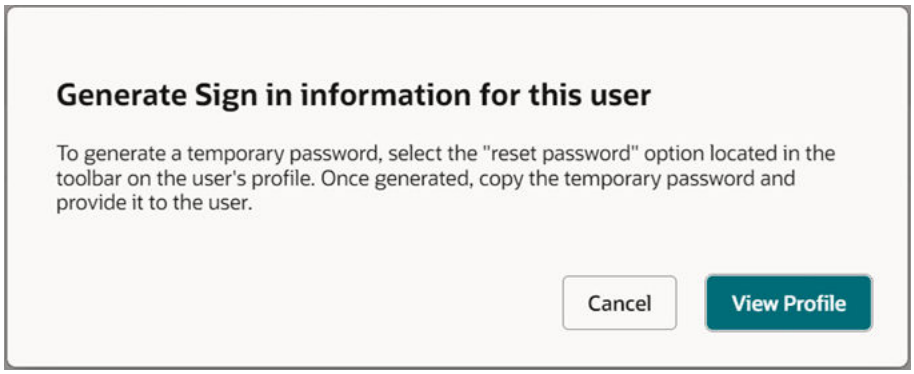
1. Click the **Create User** button on the User Management page. A create user prompt appears.



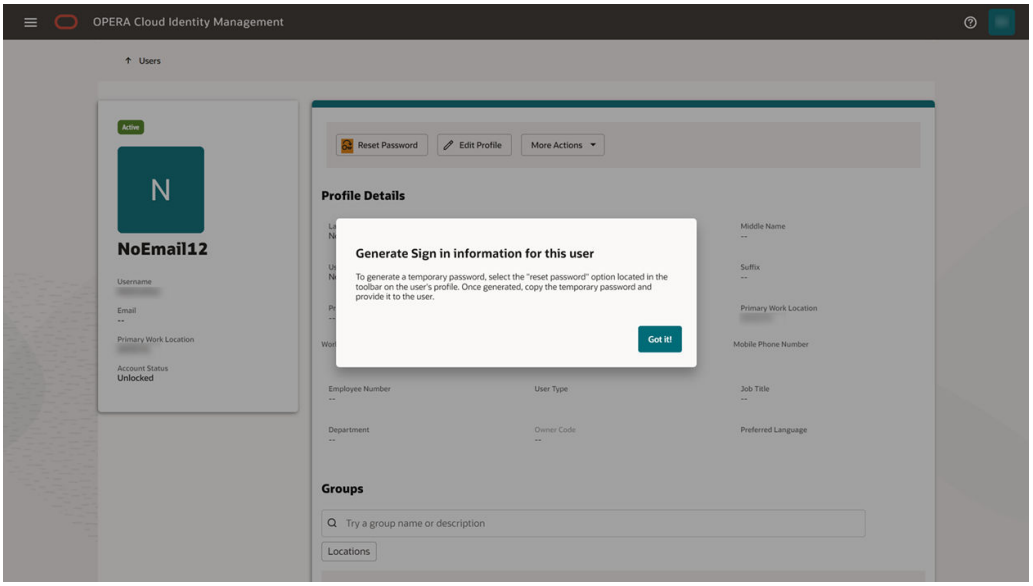
2. The Create User prompt consists of the below user fields for creating a user:
   - **Last Name**
   - **Email Address**: (optional) If added, user creation follows the regular user creation process with email.
   - **Username**
   - **Primary Work Location**: This is the enterprise, chain, or property code representing the location where the user works.
   - **Optional**:You can add additional user details.
   - **Optional**: You can search for and select groups to which you can add the user during the user creation process.
3. Click **Create** to create the user or click **Create and View Profile** to finalize the user creation process.



4. If you created a user without an email address and clicked **Create**, you will see the user listing screen and an information pop-up showing information related to 'Generate Sign in information for this user.' Clicking the **View Profile** button opens the newly created user profile and allows the admin to generate the user sign in details.



- If you create a user without an email address and click **Create and View Profile**, the user profile screen and an information screen appear with instructions for generating a temporary password for the user.



5. Generate sign-in information for users without an email.

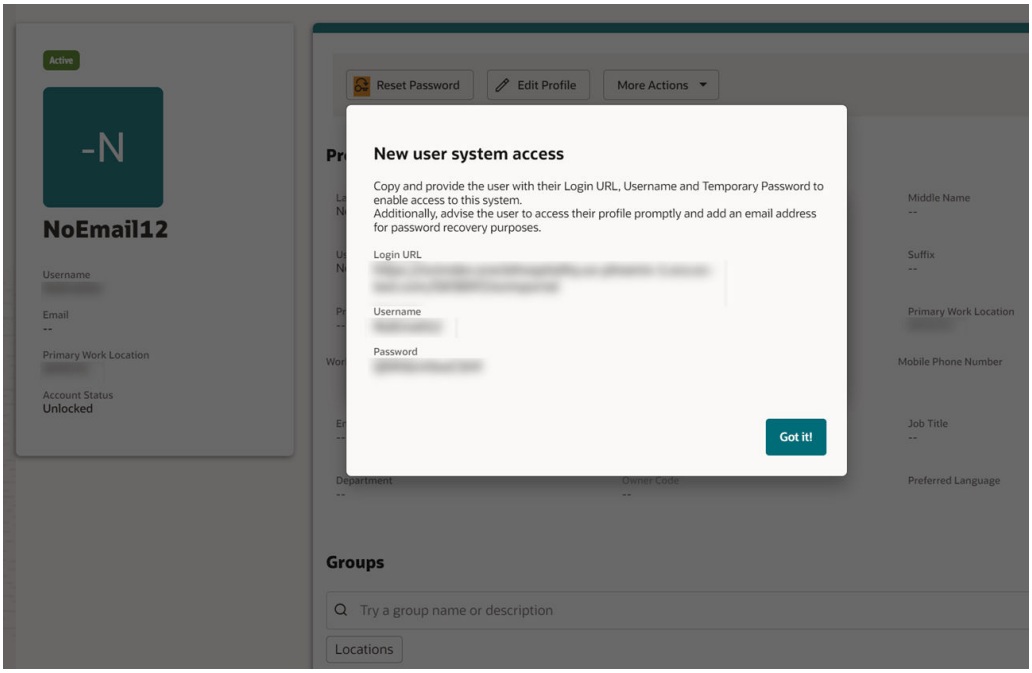
> **Note:**
>
> For users without an email address, the administrator must create a temporary password for the user. Once the temporary password is created, the administrator must provide the user with the Login URL, the username, and the temporary password. The new user can log in with these credentials and is prompted to create a new password for future login to the user account.

When an administrator accesses a profile without an email address, information appears on how to generate sign-in information for the user.

a. To generate sign-in information for the user, on the user profile, click **Reset Password**.

   An information screen appears with the following details:

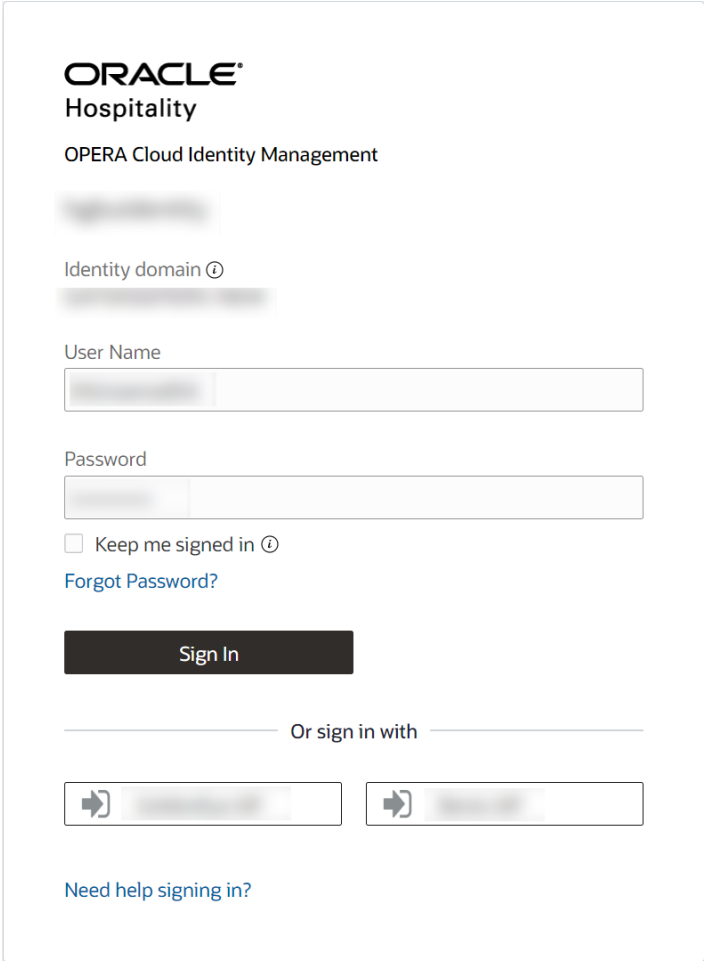
   - OPERA Cloud Identity Management portal URL
   - Username
   - Password



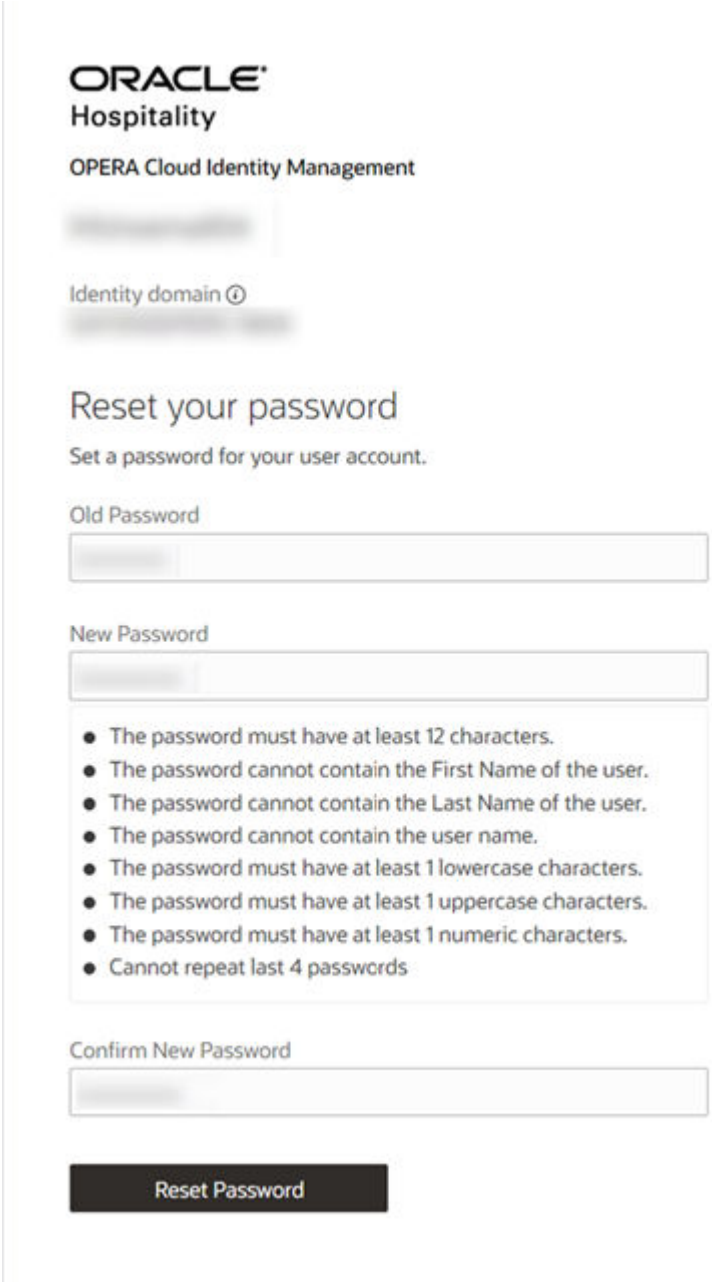
b. The administrator is required to provide the generated access details to the user through manual communication methods, such as text, written correspondence, or verbal communication, as these users do not possess an email address for correspondence. The administrator should advise the user to login with the provided credentials and create an own password.

6. User login and password reset:

   - After the user has obtained the sign-in information from the administrator, the user can log in with the provided information.



- The login with the temporary password prompts the user to reset the password to a password of choice. The old (temporary password) is required in this process.



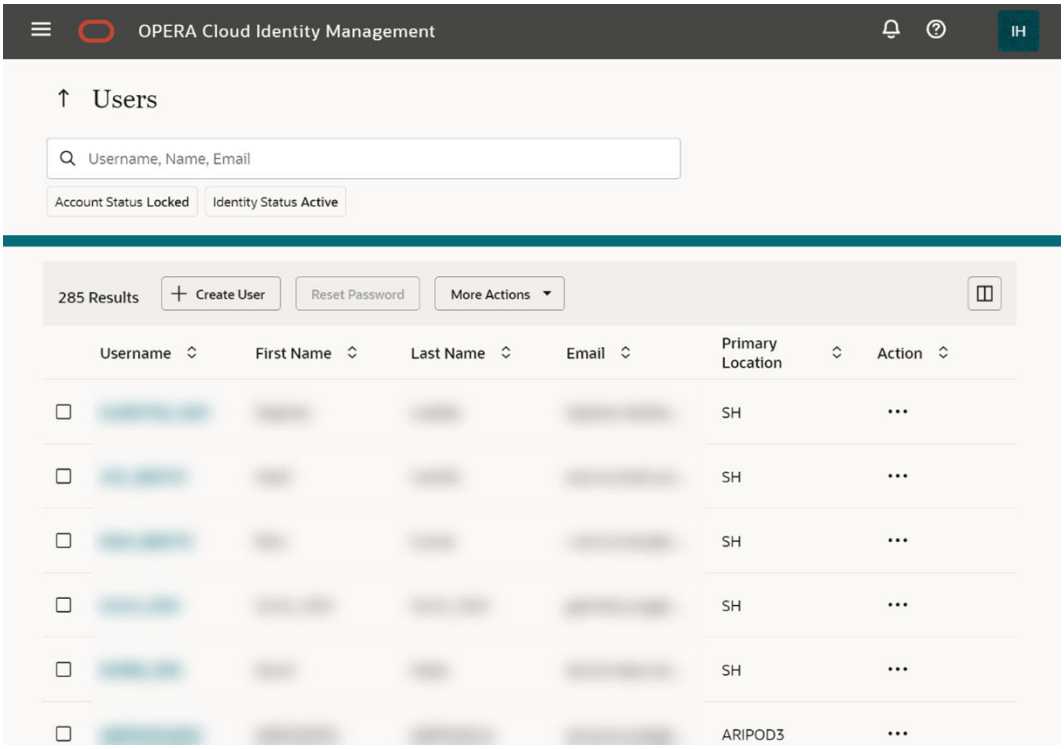
- The user can now log in with this password to the OPERA Cloud applications for which access has been granted.

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**.



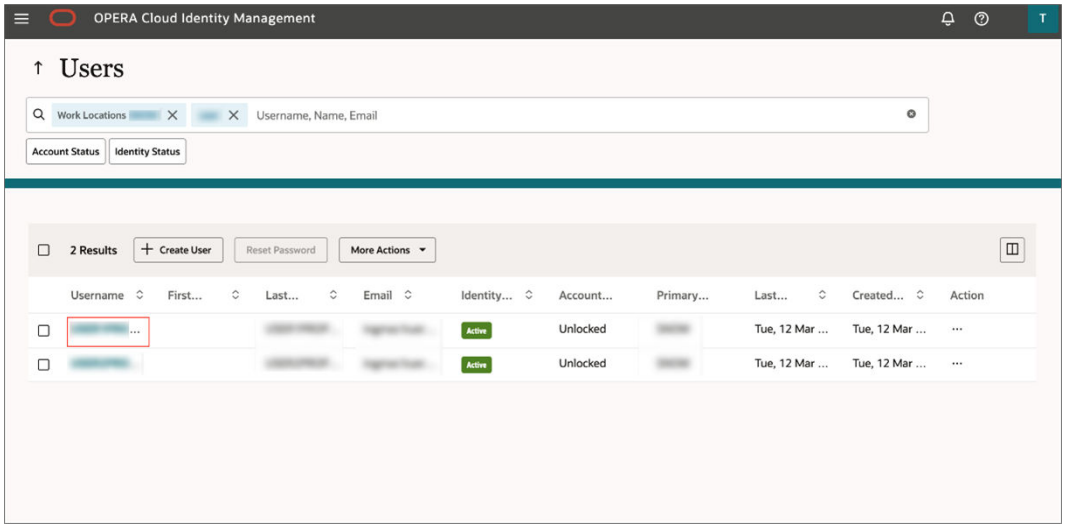
3. Alternatively, click the **Action** column for a user row to perform actions on that respective user.

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.

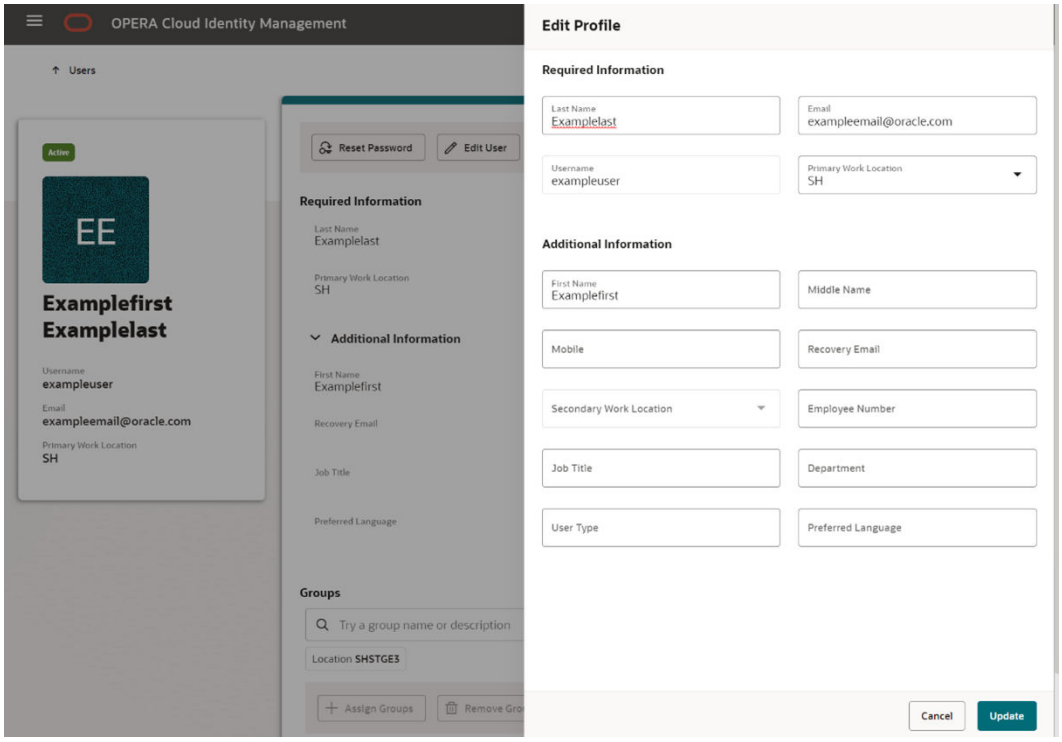
On the User Profile Management page, you can do the following:

- Reset the password for the user
- Edit the user details
- Access the following actions:
  - Reset Factors
  - Unlock Account
  - Deactivate user
  - Delete user
- Assign/Remove group memberships



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. Adjust the editable fields 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

Resetting Password for User

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.

Resetting Password for a User without an Email Address

1. Click the **Username** of the user to open the User Profile page.
2. Click the **Reset Password** button to create a temporary password that must be shared with the user.
3. The user can log in with the temporary password and will be prompted to create a new password for future login to the user account.

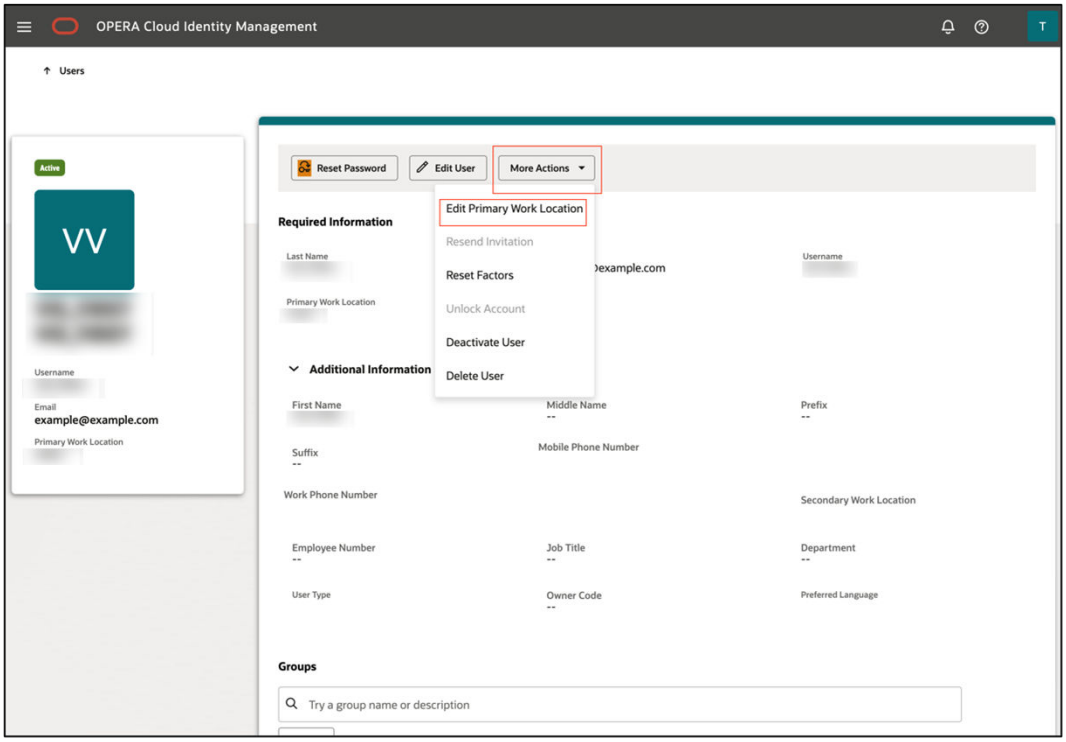
Changing Primary Work Location for a User

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.

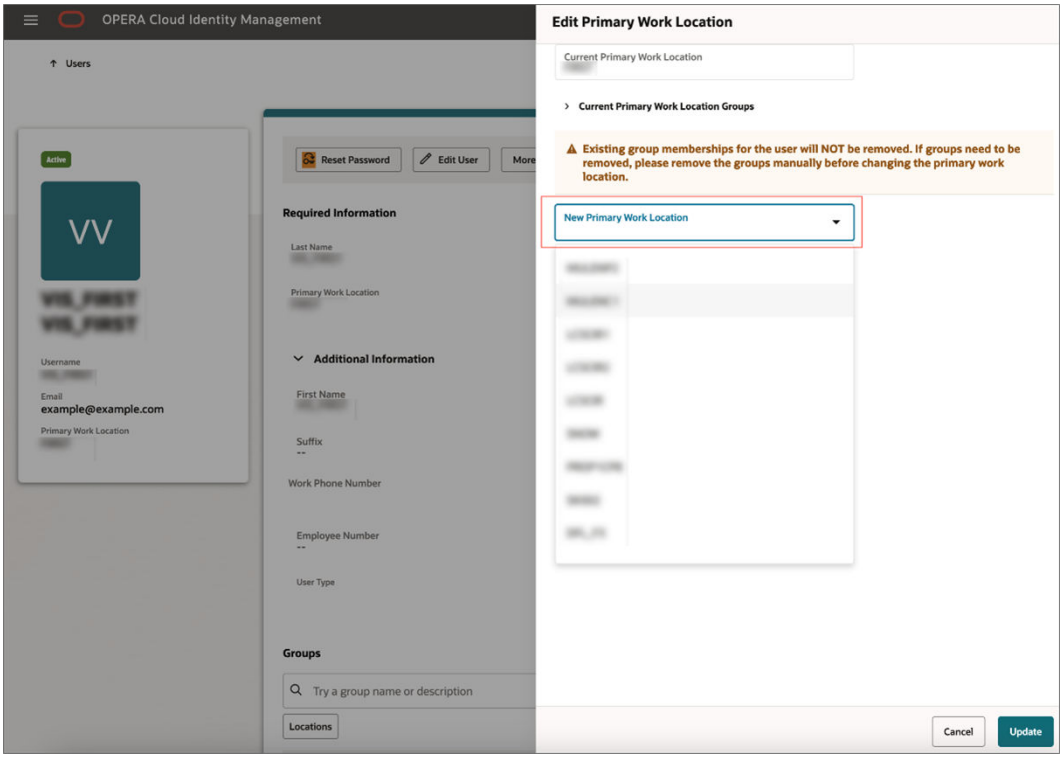
> **Note:**
>
> Only a chain IAM administrator or enterprise IAM administrator in OPERA Cloud Role Manager can perform this operation.

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**.

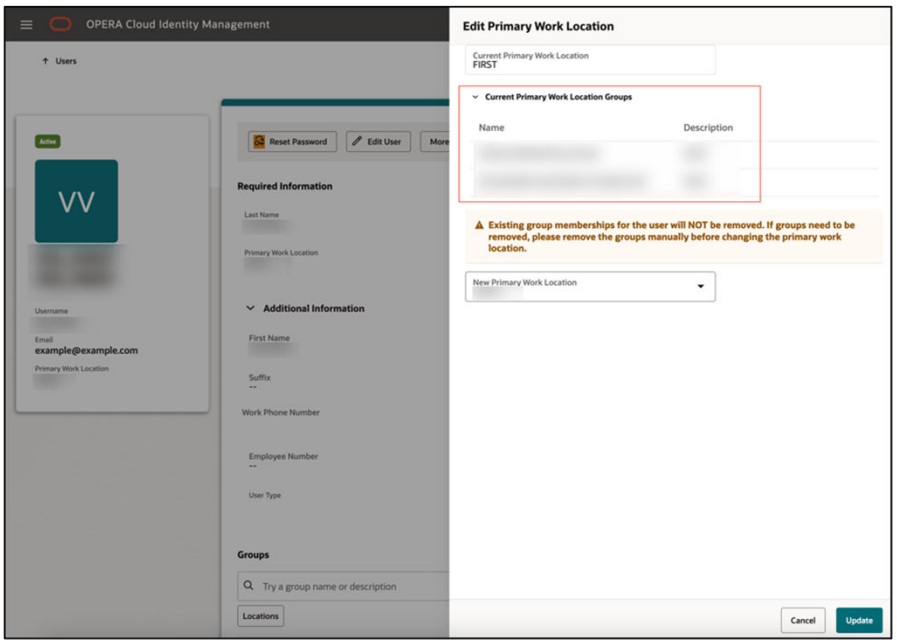


2. Click **New Primary Work Location** to select the new primary work location from the list of values, which is depicted as Chain followed by its properties.



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.

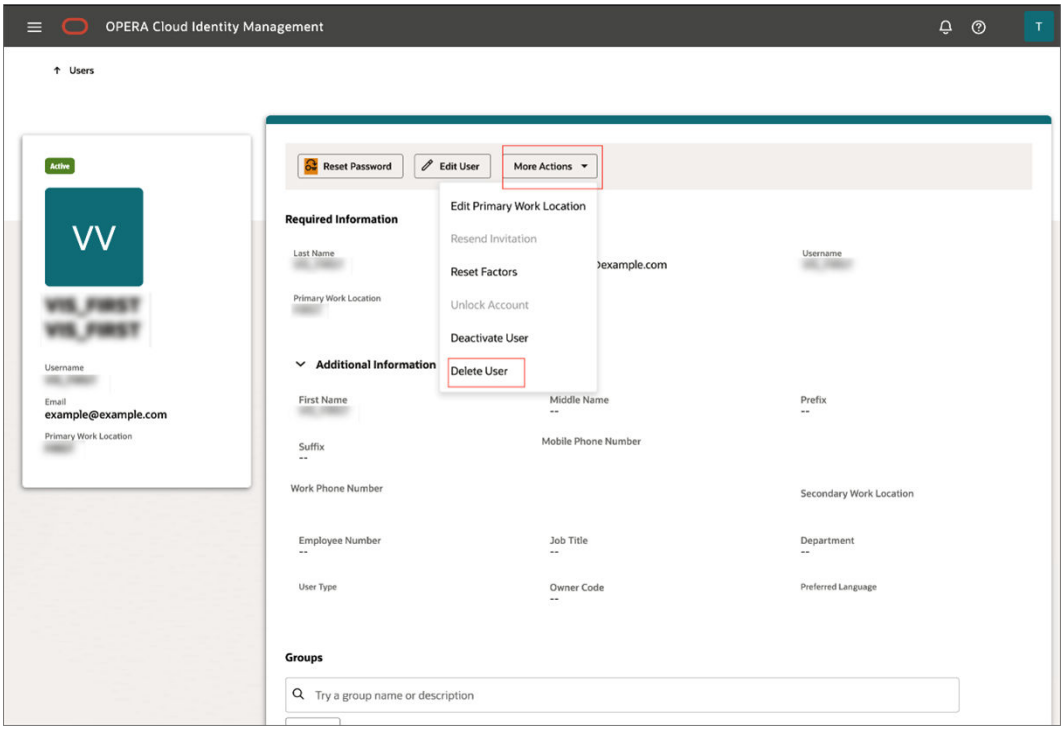
Deleting a User

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. Enterprise, 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.

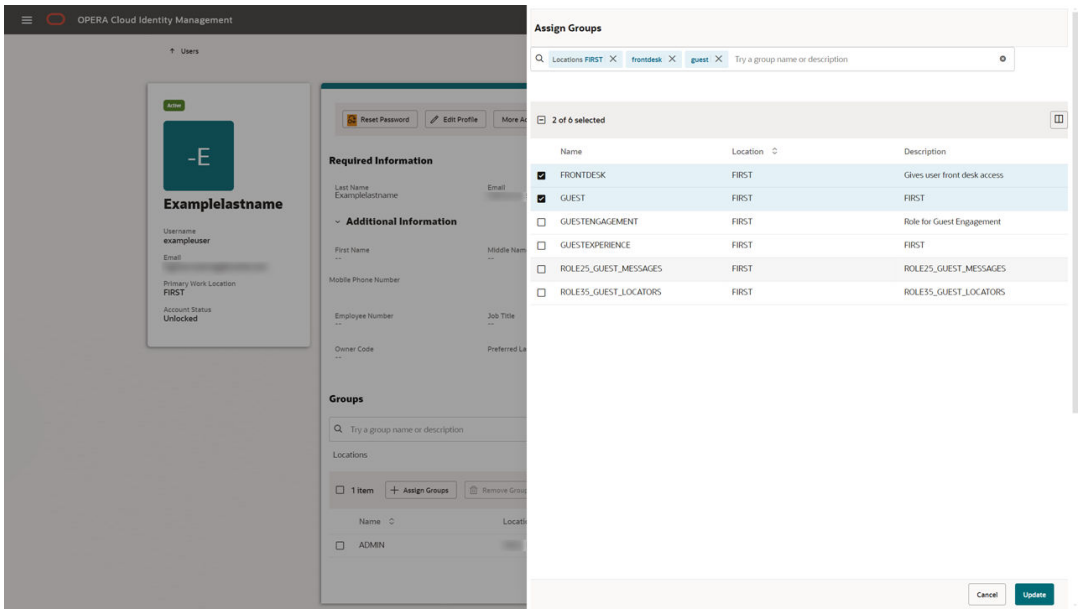
Assigning and Removing Group Membership

In the Groups section of the User Profile screen, you see the group memberships that are currently assigned to the user.

Assigning Groups

1. To assign an additional group to the user, select **Assign Groups**.

2. Search for and select one or multiple groups and select the **Update** button in the Assign Groups drawer.



Note:

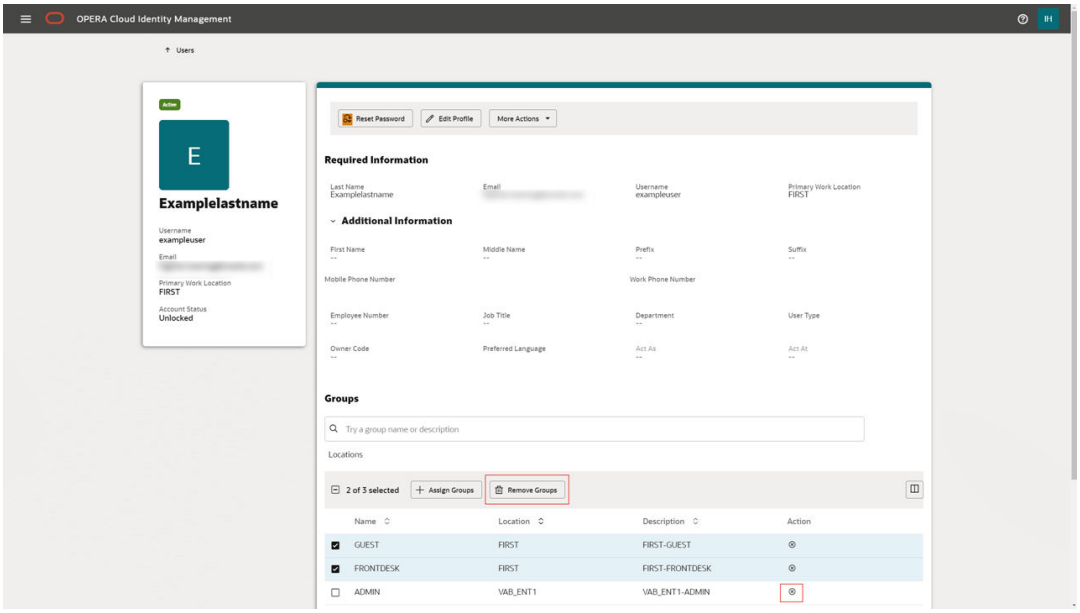
OC_RNA Location Search

To search for Reporting and Analytics groups:

- Click **Locations** and select the location **OC_RNA** (available for Enterprise and Chain administrators).

Removing Groups

1. To remove one group from the user, select the **Delete** icon in the **Action** column of the Groups table.
2. To remove multiple groups from the user at once, check all groups to be removed and select the **Remove Groups** button above the groups table.


OPERA Cloud Identity Management
Users
Active
E
Examplelastname
Username
exampleuser
Email
Primary Work Location
FIRST
Account Status
Unlocked
Reset Password
Edit Profile
More Actions
Required Information
Last Name
Examplelastname
Email
Username
exampleuser
Primary Work Location
FIRST
Additional Information
First Name
Middle Name
Prefix
Suffix
Mobile Phone Number
Work Phone Number
Employee Number
Job Title
Department
User Type
Owner Code
Preferred Language
Act As
Act At
Groups
Try a group name or description
Locations
2 of 3 selected
Assign Groups
Remove Groups
Name
Location
Description
Action
GUEST
FIRST
FIRST-GUEST
FRONTDESK
FIRST
FIRST-FRONTDESK
ADMIN
VAB_ENT1
VAB_ENT1-ADMIN

6

Managing Oracle Users

Introduction

OPERA Cloud Identity Management provides the capability of Oracle Corporate single sign-on (SSO). Oracle users (specifically Oracle HGBU users) can use SSO to access customer OPERA Cloud environments.

This guide provides the steps for granting the DATAACCESS, SENSITIVEDATAACCESS, ENTDATAACCESS, and ENTSENSITIVEDATAACCESS roles to Oracle users, so they can access customer environments. It is at the customer's discretion to grant this role to users.

Process Overview

The below processes are designed for Oracle users to gain access to customer OPERA Cloud environments.

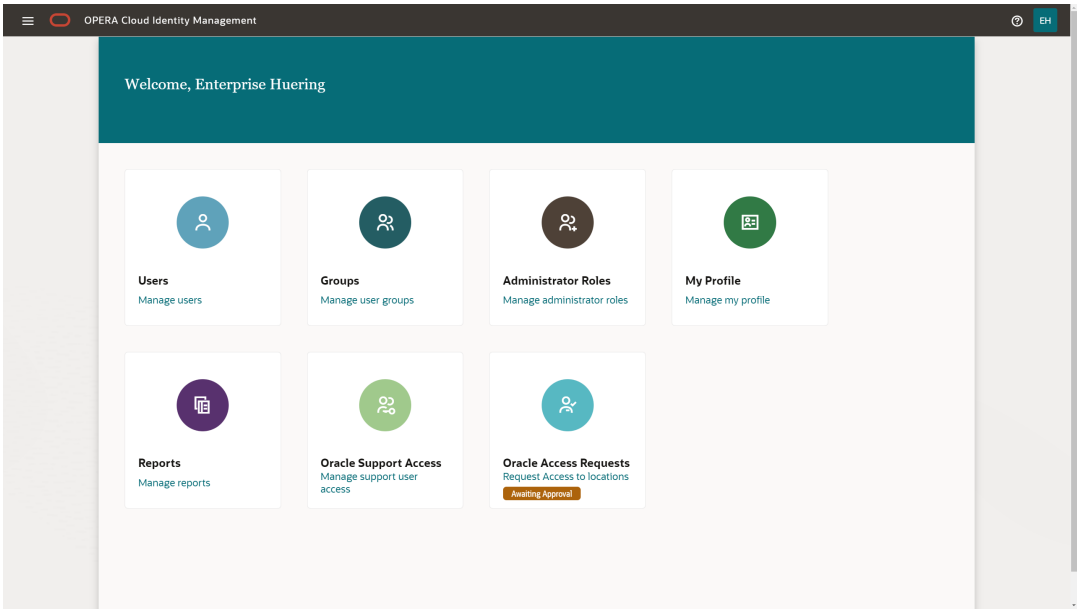
- Customers can assign DATAACCESS, SENSITIVEDATAACCESS, ENTDATAACCESS, and ENTSENSITIVEDATAACCESS role memberships to an Oracle user for a specified duration, which can range from 1 to 180 days. Unless modified, the default duration for Oracle Support grants is set to 7 days.
- Oracle users can manually communicate to customers through email or through an Oracle support SR to assign DATAACCESS, SENSITIVEDATAACCESS, ENTDATAACCESS, and ENTSENSITIVEDATAACCESS role memberships to the relevant property/chain in that customer OPERA Cloud environment.
- Oracle users receive a notification when a customer assigns DATAACCESS, SENSITIVEDATAACCESS, ENTDATAACCESS, and ENTSENSITIVEDATAACCESS role memberships to them through the OPERA Cloud Identity Management portal.

Managing Oracle Support User Access

The below section describes the steps required for granting DATAACCESS, SENSITIVEDATAACCESS, ENTDATAACCESS, and ENTSENSITIVEDATAACCESS role membership to Oracle users.

Navigating to Oracle Support Access

1. After logging in to OPERA Cloud Identity Management, you will see the OPERA Cloud Identity Management homepage that allows access to different functionality areas, based on your roles.
    - The homepage includes a tile to open the Oracle Support Access area.
2. Select the **Oracle Support Access** tile to open the OPERA Cloud Identity Management Oracle Support User Access area.

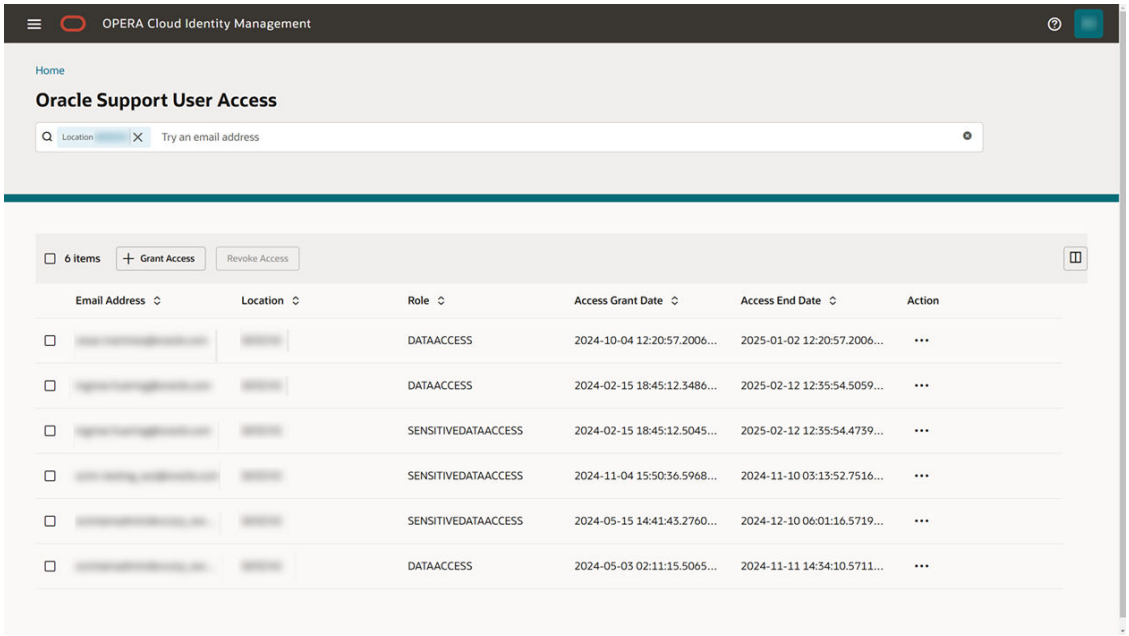


Granting, Extending, and Revoking Access to Oracle Support Users

After selecting the **Oracle Support Access** tile, the Oracle Support User Access page opens. This page shows you existing and active Oracle Support Users for all locations to which you have administrative access.

From the Oracle Support User Access page, you can do the following:

- Search for existing Oracle Support User access
- Grant access to users
- Edit access duration



Searching for Existing Oracle Support User Access

Use the search filter to search for users with existing grants for Oracle Support User access.

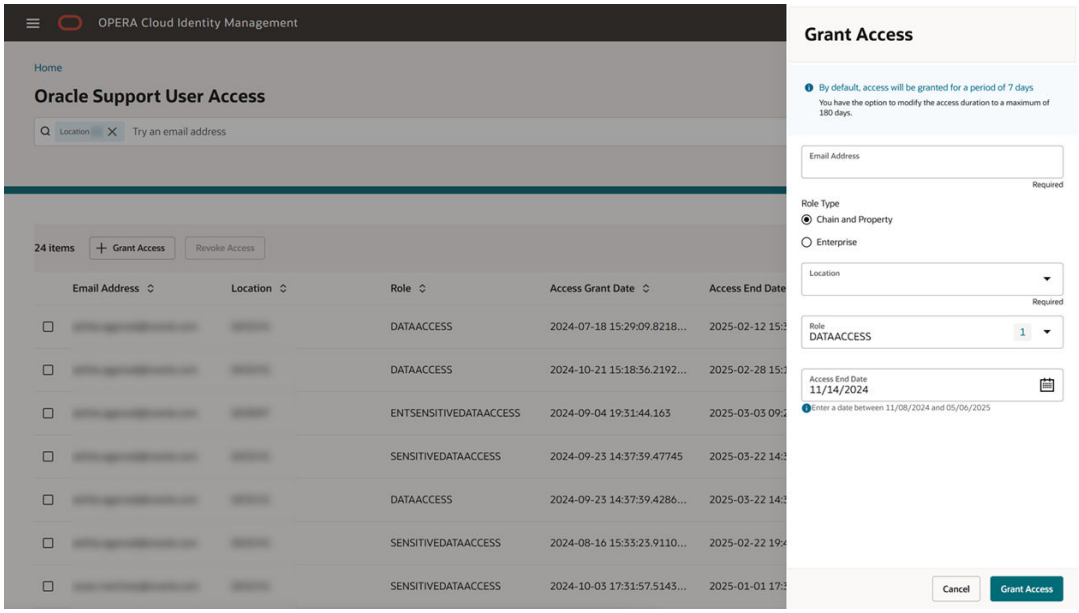
The search result table will refresh and show the users that are matching the search criteria.

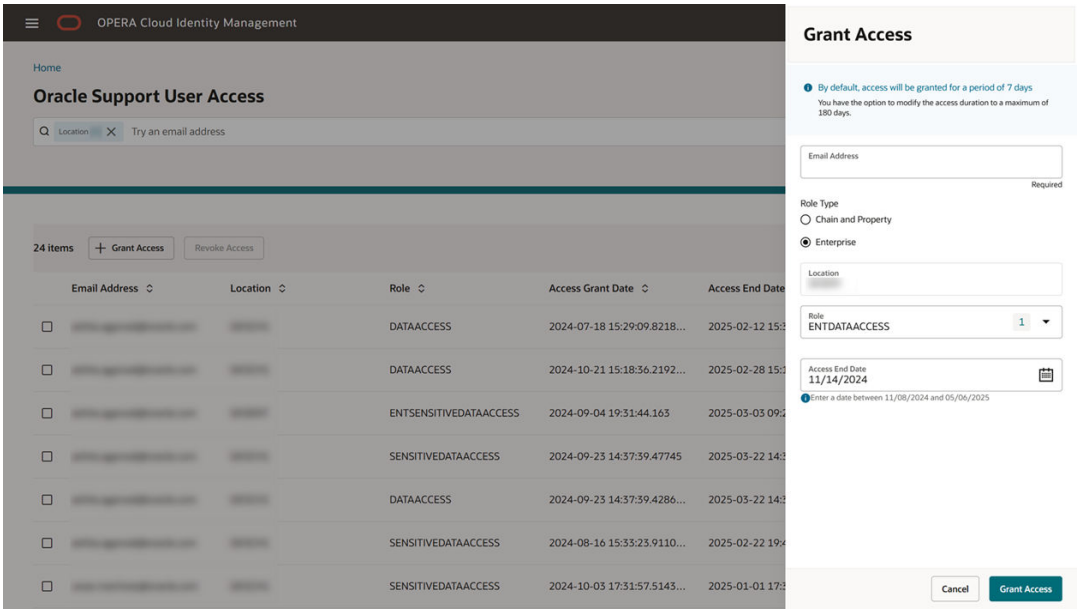
Only users for locations to which the logged in user has administrative access will show.

Granting Access to Users

1. Select the **Grant Access** button to grant Oracle Support User Access to a user.
   A 'Grant Access' drawer opens that enables you to enter the required details for the new Oracle Support User Access grant.
2. Select between the Chain/Property role type (DATAACCESS, SENSITIVEDATAACCESS roles) and Enterprise role type (ENTDATAACCESS, ENTSENSITIVEDATAACCESS roles).

> **Note:**
>
> Only enterprise level administrators see the option to select the enterprise role type.
>
> The DATAACCESS and SENSITIVEDATAACCESS roles give support access to the OPERA Cloud system. The ENTDATAACCESS, ENTSENSITIVEDATAACCESS roles EXCLUSIVELY give support access to the Enterprise Management application and not to the OPERA Cloud systems.





3. Enter the following details:
   - **Email Address** (must end with @oracle.com)
   - **Location** (that is, a chain or property code; if enterprise role type is selected, your enterprise code will be pre-populated)
   - **Role** (Chain/Property: DATAACCESS, SENSITIVEDATAACCESS; Enterprise: ENTDATAACCESS, ENTSENSITIVEDATAACCESS)
   - **Access End Date** (By default, the end date will be 7 days in the future. You can update the Access End Date to any date between 1 and 180 days in the future.) Click the **Grant Access** button when you are ready to grant access to the user. The user is granted support access to the locations for the selected roles until the Access End Date.

> **Note:**
>
> If the user already has access to any of the selected locations, an attempt is made to extend this existing access until the new Access End Date (with a maximum total access duration of 180 days). If the combined duration of the extended access exceeds 180 days, the request fails and the existing access grant for the respective location and role is not changed.

4. Select the **Grant Access** button when you are ready to grant access to the user. The user will be granted support access for 180 days to the selected locations for the selected roles.

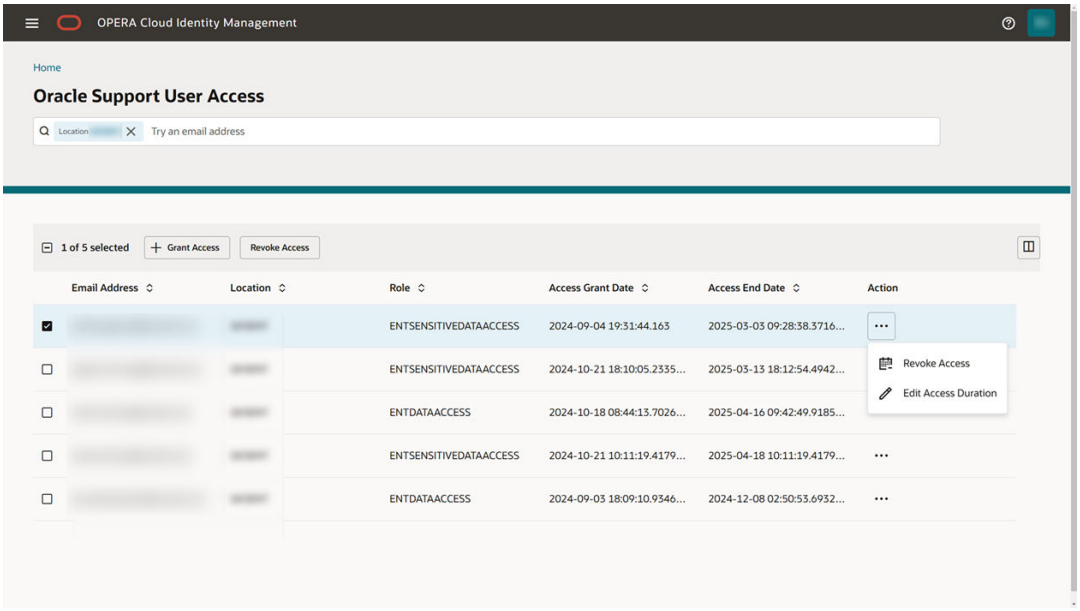
> **Note:**
>
> If the user has existing access to any of the selected locations, the existing access in these locations will be REPLACED with the new access granted to the user.

Editing Access Duration for Users

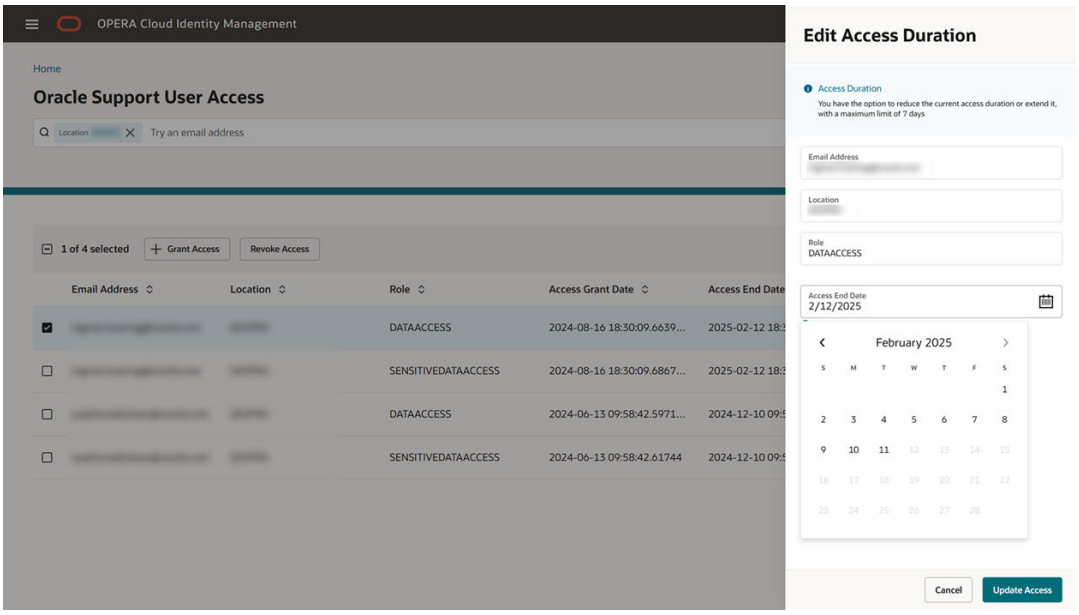
You can edit existing Oracle support user access from the Oracle Support User Access page for any user with an active support access. The maximum access duration is 180 days from the point of time the access started.

You can use the row-level action on the Oracle Support User Access table to edit the user's access duration.

1. Click the ellipsis icon under the **Action** column and select **Edit Access Duration**.



2. Select a new **Access End Date** from the calendar.



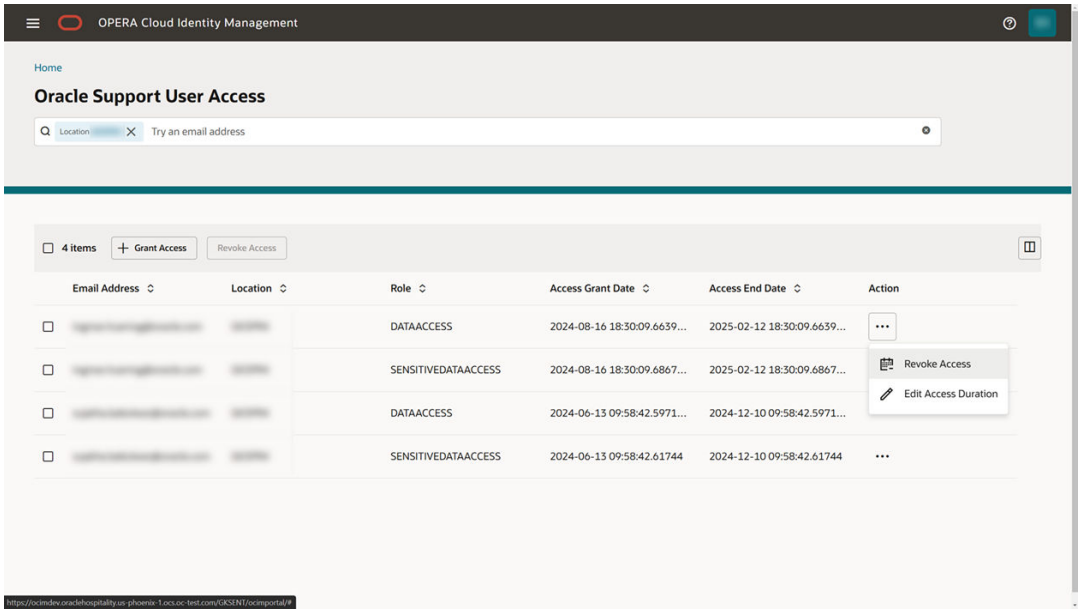
3. Click **Update Access**.

Revoking Access for Users

1. You can revoke an existing Oracle support user access from the Oracle Support User Access page for any user with active support access.
2. Revoking access for one or multiple users will IMMEDIATELY revoke the existing access.
3. You have two options to revoke a user's grant:
   - Revoking access for an individual user
   - Revoking access for multiple users

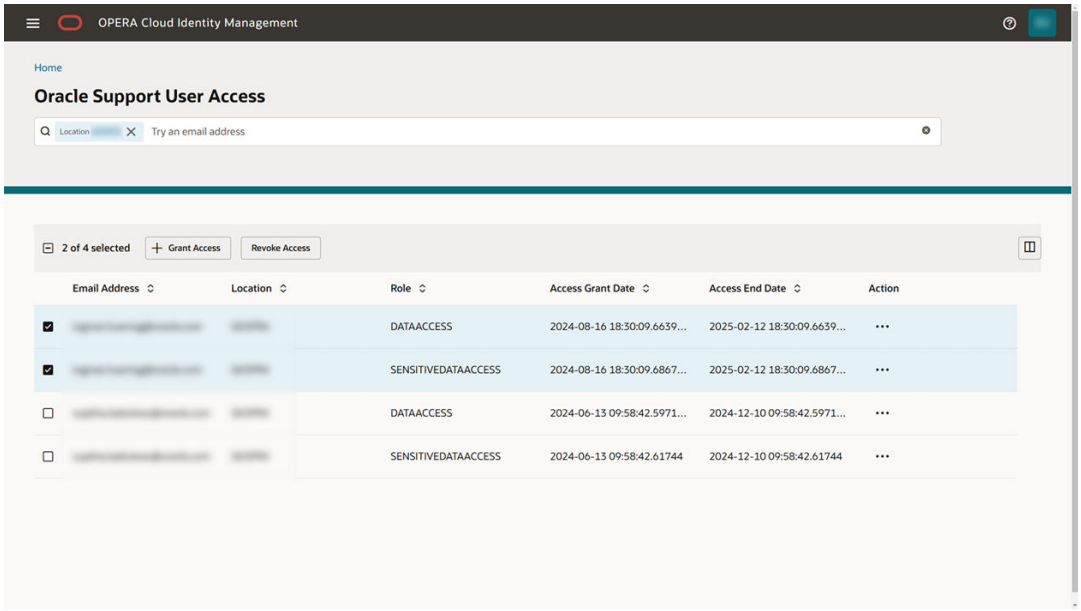
Revoking Access for an Individual User

1. You can use the row-level action on the Oracle Support User Access table to revoke the user's access.
2. Click the icon in the Action column and select Revoke Access.
3. Confirm the pop-up message to revoke the user access IMMEDIATELY.



Revoking Access for Multiple Users

1. You can select multiple users on the Oracle Support User Access table to revoke the user access for multiple users at the same time.
   After you select users on the Oracle Support User Access table, the top menu button "Revoke Access" is enabled.
2. Click the **Revoke Access** button.
3. Confirm the pop-up message to revoke the user access IMMEDIATELY for all selected users.


OPERA Cloud Identity Management
Home
Oracle Support User Access
Location
Try an email address
2 of 4 selected
Grant Access
Revoke Access
Email Address
Location
Role
Access Grant Date
Access End Date
Action
DATAACCESS
2024-08-16 18:30:09.6639...
2025-02-12 18:30:09.6639...
SENSITIVEDATAACCESS
2024-08-16 18:30:09.6867...
2025-02-12 18:30:09.6867...
DATAACCESS
2024-06-13 09:58:42.5971...
2024-12-10 09:58:42.5971...
SENSITIVEDATAACCESS
2024-06-13 09:58:42.61744
2024-12-10 09:58:42.61744


Revoke Access?
Access roles granted to the selected users at the associated locations will be immediately revoked.
Cancel
Revoke

7

Managing Oracle Support Access Requests

OPERA Cloud Identity Management provides a self-service approval workflow for Oracle Support Users access requests.

Oracle Support Users can request access for support roles, such as DATAACCESS, SENSITIVEDATAACCESS, ENTDATAACCESS, ENTSENSITIVEDATAACCESS, and respective customer administrators can approve/deny this request based on their discretion.

> **Note:**
>
> The DATAACCESS and SENSITIVEDATAACCESS roles give support access to the OPERA Cloud system. The ENTDATAACCESS, ENTSENSITIVEDATAACCESS roles EXCLUSIVELY give support access to the Enterprise Management application and not to OPERA Cloud systems.

These support roles provide the Oracle Support User with support access in OPERA Cloud Services, and it is recommended that customers review such support requests before approving/denying the request.

Oracle Support Access Request can be approved only by a customer's respective enterprise, chain, or property administrator in OPERA Cloud Identity Management Portal.

Navigating to Oracle Access Requests

1. Log in to OPERA Cloud Identity Management portal.

   In the OPERA Cloud Identity Management portal, you will see a tile for Oracle Access Requests.

   > **Note:**
   >
   > You must have administrative role membership in OPERA Cloud identity Management Portal to see the tile.

2. Select the **Oracle Access Requests** tile.

Oracle Access Requests Screen Overview

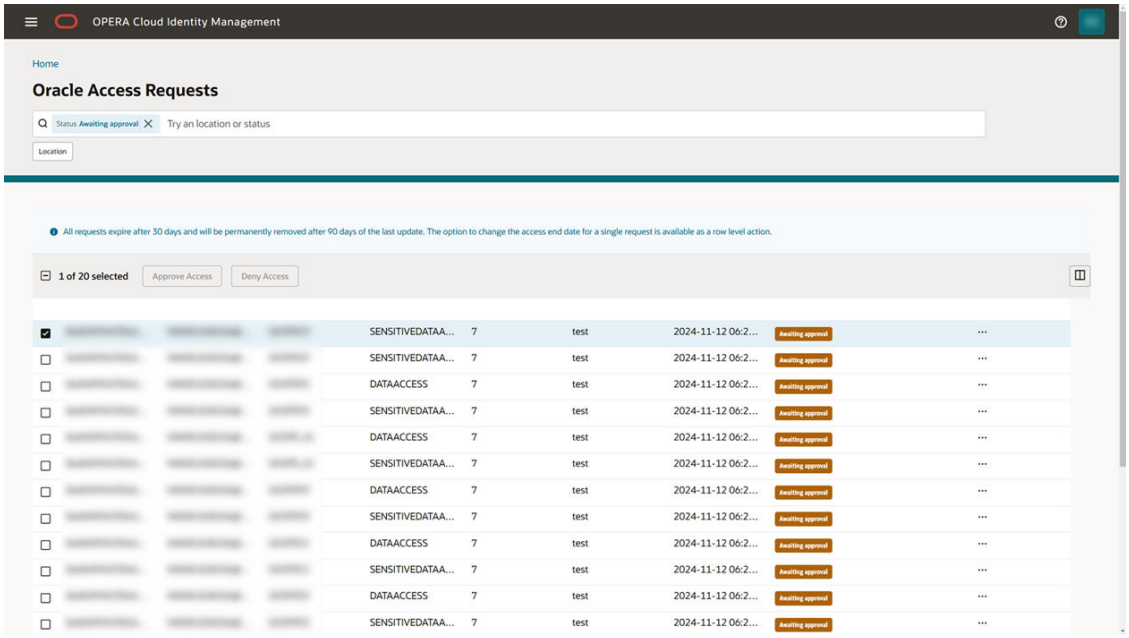
The Oracle Access Requests screen:

- Shows you details for all your access requests received within the last 90 days.
- Defaults the request status filter to support requests that are in "Awaiting Approval" status.
- Sorts the list of requests to the longest waiting requests to show on top.

> **Note:**
>
> You can only act on requests in “Awaiting Approval” status.

- Allows you to respond to one or multiple requests.

> **Note:**
>
> Requests not responded to within 30 days will expire and can no longer be acted on.



Approving a Single Request

1. To approve an Oracle Access Request with the row level action, click the ellipsis (“…”) under the Action column.
2. Click **Approve Access**.

   An ‘Approve Access’ drawer opens and shows the access details. The Access End Date is pre-populated with the date corresponding to the requested duration of the support access. (Access start date will be the point in time that the request is being approved in determined by the approval.)
3. Confirm by clicking **Approve request** in the Approve Access drawer.

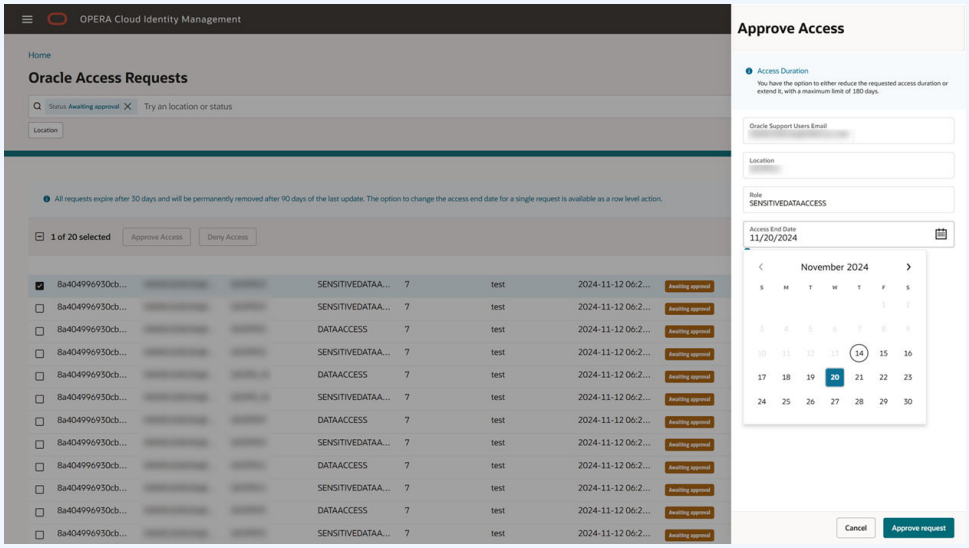
   You have successfully granted the requested support access for the selected row.

Note:

If the user already has access to a requested location and role, an attempt is made to extend this existing access by the requested access duration (with a maximum total access duration of 180 days). If the extended access exceeds 180 days, the request fails and the existing access grant for the respective location and role is not changed.

Note:

You can see all active support access grants in the Oracle Support Access tile. This shows all the currently active Oracle support access for locations to which you have administrative access.



Approving Multiple Requests

1. To approve one or multiple Oracle Access Requests with the page level action, first select the checkbox for all requests that you want to approve at the same time.

Note:

You can select up to a maximum of 20 requests at one time.

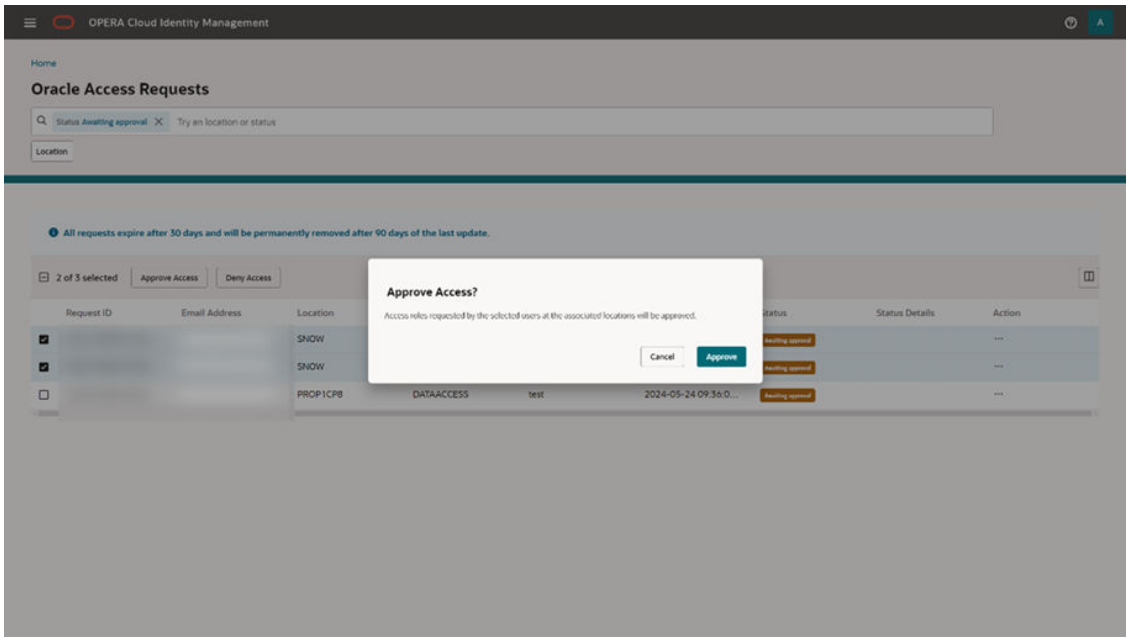
> **Note:**
>
> If you approve multiple requests, you cannot adjust the individual Access End dates for the individual requests, and all requests are processed with the requested duration.

2. Click the page level **Approve Access** button.
3. Confirm by clicking the **Approve** button in the “Approve Access?” dialogue.

For the selected requests, you have successfully granted the requested support access to the selected Oracle user.

> **Note:**
>
> If the user already has access to a requested location and role, an attempt is made to extend this existing access by the requested access duration (with a maximum total access duration of 180 days). If the extended access exceeds 180 days, the request fails and the existing access grant for the respective location and role is not changed.

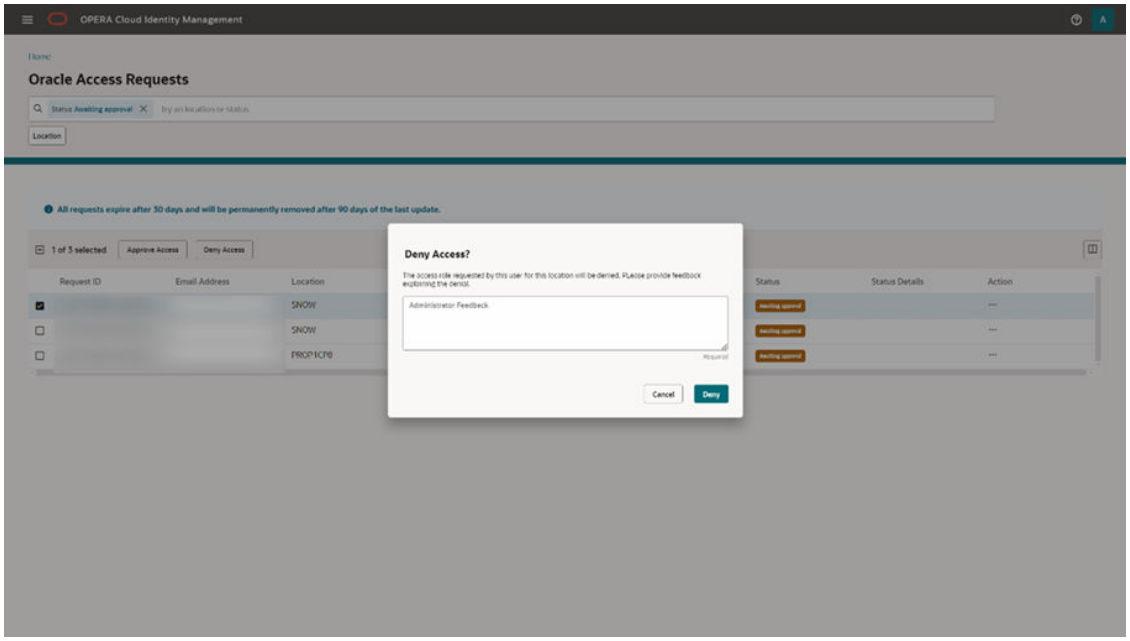
> **Note:**
>
> You can see all active support access grants in the Oracle Support Access tile. This shows all the currently active Oracle support access for locations to which you have administrative access.



Denying a Single Oracle Access Request

1. To deny an Oracle Access Request with the row level action, click the ellipsis (“…”) under the Action column.
2. Click **Deny Access**.
3. Provide a justification (required) to the requesting user explaining why the request was denied and confirm by clicking the **Deny** button on the “Deny Access?” dialogue.

You have successfully denied the requested support access for the selected row.



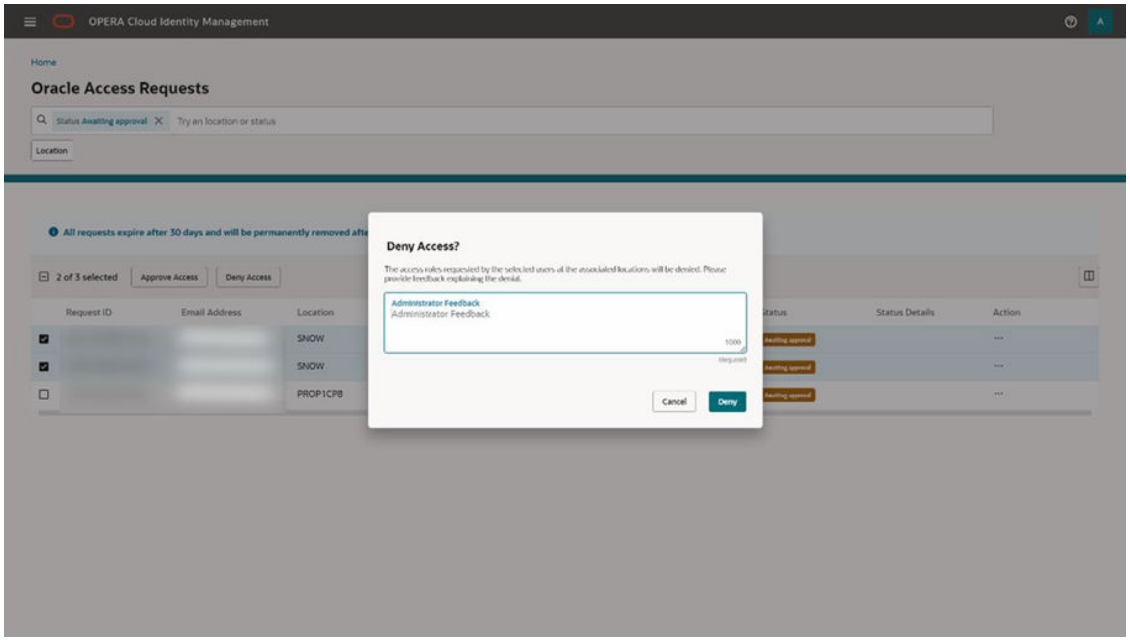
Denying Multiple Requests

1. To deny one or multiple Oracle Access Requests with the page level action, first select the checkbox for all requests that you want to deny at the same time.

> **Note:**
>
> You can select up to a maximum of 20 requests at one time.

2. Click the page level **Deny Access** button.
3. Provide a justification (required) to the requesting users explaining why the requests were denied and confirm by clicking the **Deny** button on the “Deny Access?” dialogue.

For the selected requests, you have successfully denied the requested support access to the selected Oracle user.



Viewing your Oracle Access Requests

1. On the Oracle Access Requests screen, you will see all access requests for the last 90 days assigned to you.
2. You can use the filter chips to filter by location and request status. By default, you will see the list filtered by request status “Awaiting Approval.”
3. Each access requests shows you the status of the request.
    a. **Awaiting Approval** – This status indicates the access request has been submitted by the Oracle user and awaiting approval from the respective hotel administrator(s).
    b. **Approved & Finalizing** – This status indicates the access request was approved or denied by the hotel administrator, and the backend system is finalizing the request approval or denial.
    c. **Granted** – This status indicates the access request was approved by the hotel administrator and granted in OPERA Cloud Identity Management.
    d. **Denied** – This status indicates the access request was denied by the hotel administrator. Note that all denied requests show the hotel administrator response in the “Status Details” column.
    e. **Expired** – This status indicates the access requests expired as it is not approved or denied by the hotelier administrator within 30 days. Expired requests are shown for information purposes only and cannot be actioned. You can create a new request with the same details if required.
    f. **Cancelled** – This status indicates the access request was cancelled by the Oracle user.
    g. **Failed to finalize** – This status indicates the access request was approved or denied by the hotelier administrator, but the request failed to be granted or denied due to a technical error. Requests with this status are no longer active. You can create a new request with the same details if required.

Note:

Only requests in “Awaiting Approval” status can be actioned by using the available row level actions or selecting the requests and using the available page level actions.

Requests that are in a status other than “Awaiting Approval” are not actionable and are shown for information only.

Figure 7-1 Oracle Access Requests Screen

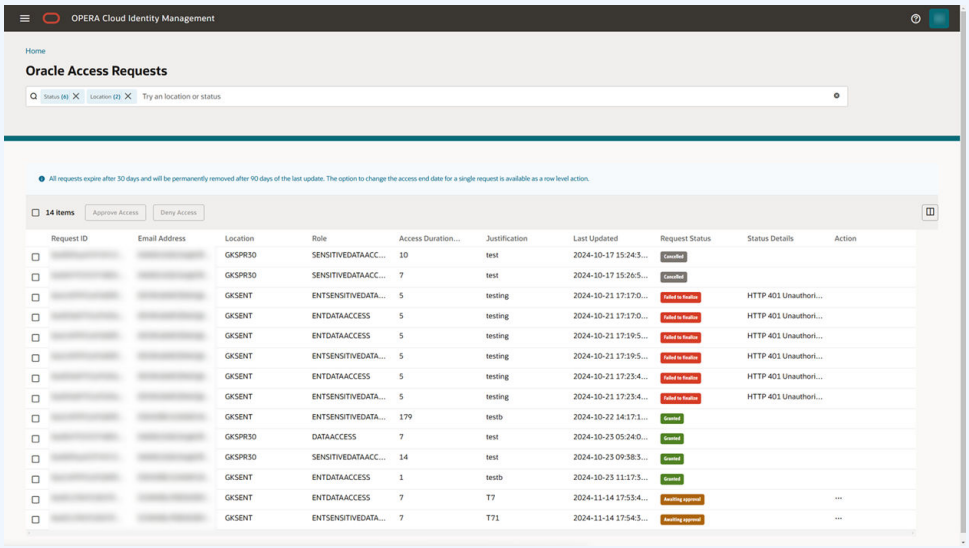
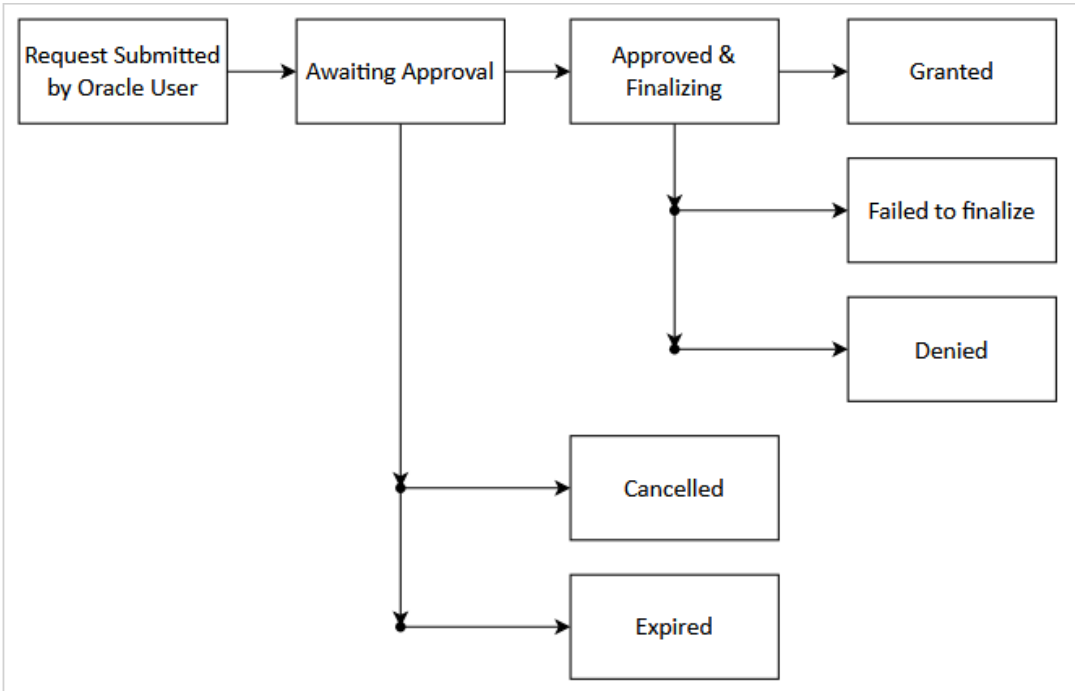


Figure 7-2 Oracle Access Requests — Status Flows



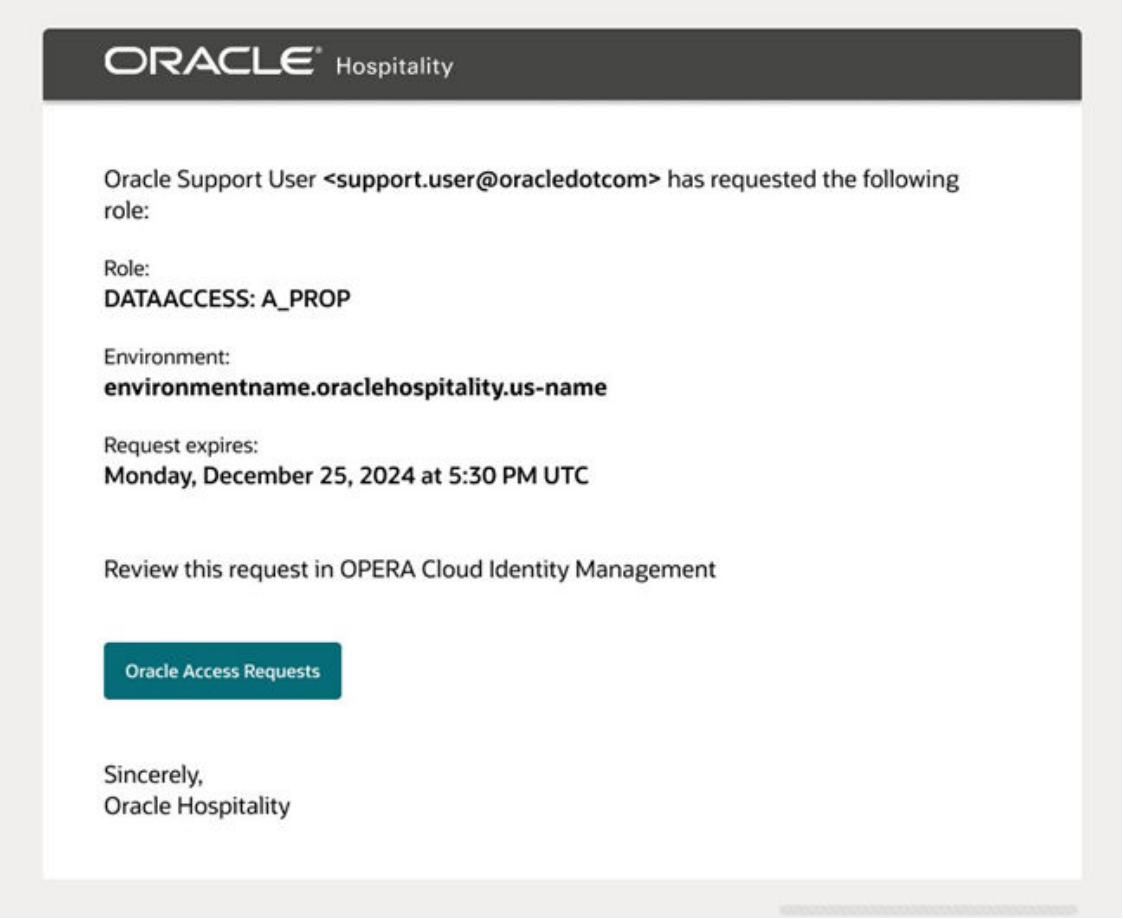
Email Notifications Received for Oracle Access Requests

When an Oracle Support User creates a new access request, the respective customer administrator is notified by an email.

> **Note:**
>
> An Oracle Support User can send a request for multiple roles at multiple locations at the same time. Because the multiple requests can each go to different Admins, the Admins will only receive one role request per email.

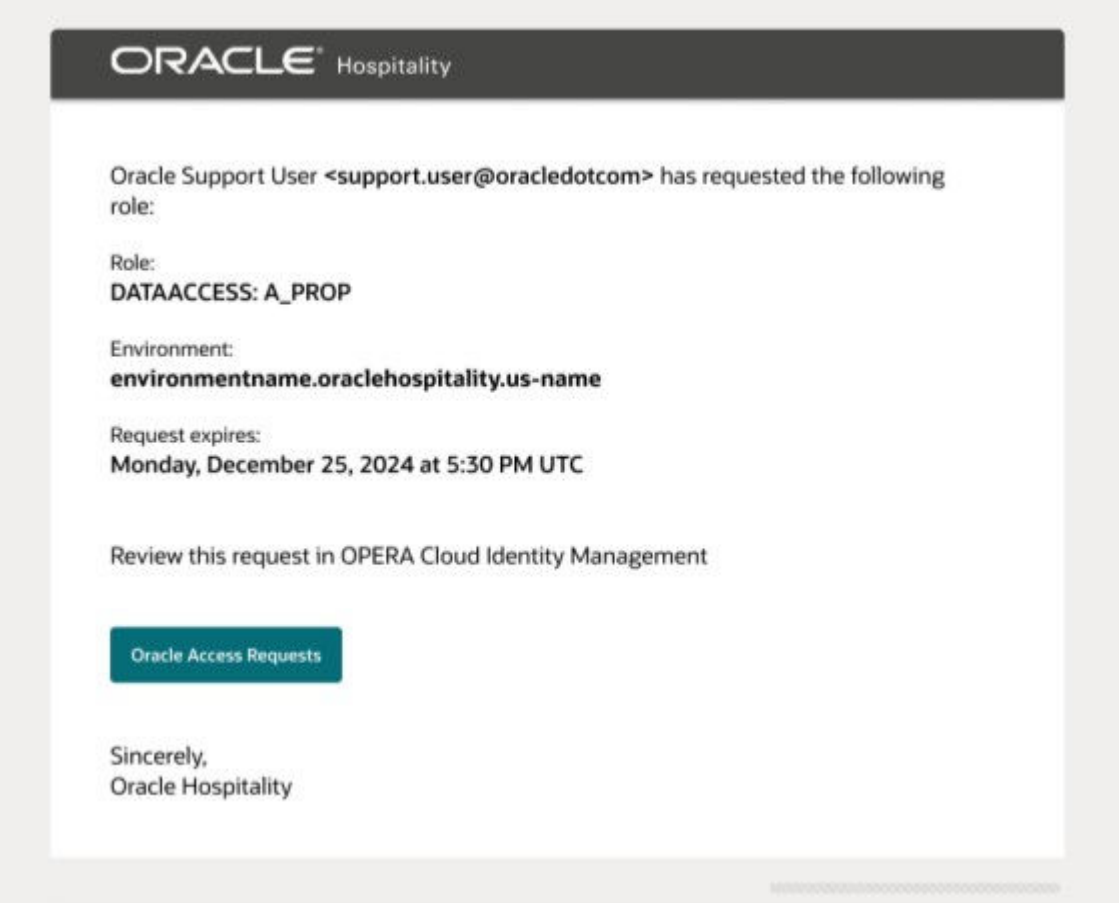
An access request email includes the following details:

- Oracle Support User email address
- The requested location / role
- The expiry date of the request
- A link to review the Oracle Access Requests in the OPERA Cloud Identity Management portal.



An Oracle user can send reminder emails for requests that are in awaiting approval status. A reminder email includes the following details:

- Oracle Support User email address
- The requested location / role
- The expiry date of the request
- A link to review the Oracle Access Requests in the OPERA Cloud Identity Management portal.



8
Identity Reports

Available Identity Reports

The following identity reports are available in the OPERA Cloud Identity Management portal.

1. **User Summary report**

   This report provides a comprehensive summary of customer users in their respective locations (chains or properties).

   This report allows the following filters:

   - Username
   - Display Name
   - First Name
   - Last Name
   - Email
   - Primary Work Location
   - User Status
   - Lock Status
   - Last Successful Login Date
   - Modified Date
   - Creation Date

   The following fields are available in this report:

   - Username
   - Display Name
   - First Name
   - Last Name
   - Email
   - Primary Work Location (required)
   - Department
   - Employee Number
   - User Type
   - Identity Status
     - Active (True)
     - Inactive (False)
   - Account Status
     - Locked (True)
     - Unlocked (False)

- Locked Date
- Locked Reason
  - 0 - Failed password login attempts
  - 1 - Admin lock
  - 2 - Failed reset password attempts
  - 3 - Failed MFA login attempts
  - 4 - Failed MFA login attempts for a federated user
  - 5 - Failed Database login attempts
- Last Successful Login Date
- Last Failed Login Date
- Modified Date
- Creation Date
- Password Expiry Flag
- Last Successful Password Set Date

2. **Group Summary Report**

   This report provides a comprehensive summary of groups in their respective locations (chains or properties).

   This report allows following filters:

   - Location (required)
   - Group Name
   - Description

   The following fields are available in this report:

   - Location
   - Group Name
   - Description

3. **Group Membership Report**

   This report provides a comprehensive summary of user group memberships in their respective locations (chains or properties).

   The report allows the following filters:

   - Group Name (required)
   - Username
   - First Name
   - Last Name
   - Email

   The following fields are available in this report:

   - Group Name
   - Username
   - First Name

- Last Name
- Email
- Employee Number

4. **Administrator Roles Membership Report**

   This report provides a comprehensive summary of OPERA Cloud Identity Management IAM administrator role memberships in their respective locations (chains or properties).

   This report allows the following filters:

   - Location (required)
   - Admin Role Name
   - Username
   - First Name
   - Last Name

   The following fields are available in this report:

   - Location
   - Admin Role Name
   - Username
   - First Name
   - Last Name
   - Employee Number
   - Membership Type
     - Direct — User assigned to application role.
     - Indirect — User assigned to administrator group.

5. **Oracle Support Access Grants Report**

   This report provides a summary of active Oracle Support Access Grants in their respective locations (enterprise, chains or properties).

   This report allows the following filters:

   - Location (required)
   - Role
   - Grantee Email
   - Grantor Username
   - Grant Start Date
   - Grant End Date

   The following fields are available in this report:

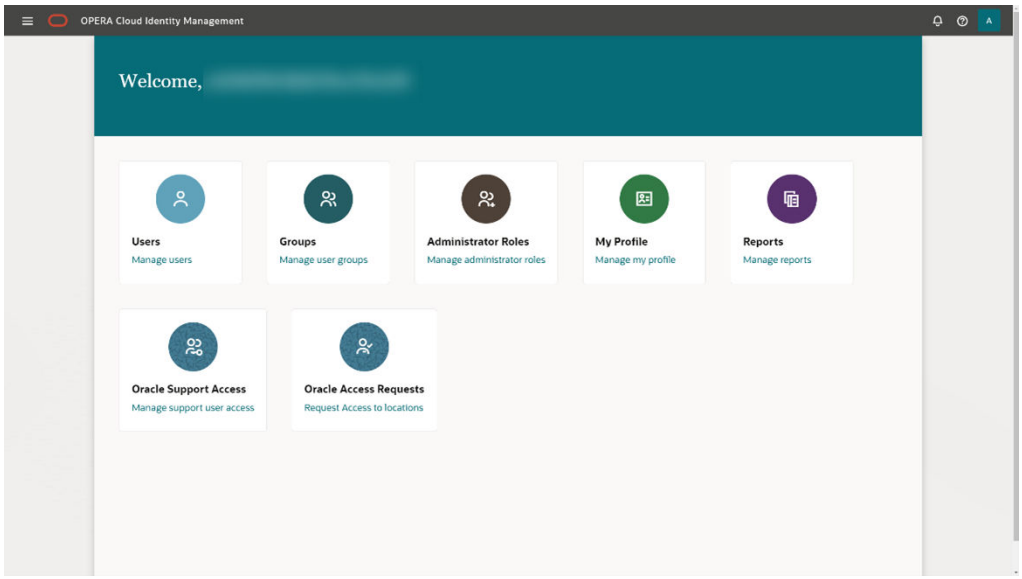
   - Enterprise Id
   - Location
   - Role Name
   - Grantor User Name
   - Grantee Email

- Grant Start Time
- Grant End Time
- Grant Revoke Time
- Extension Count

Managing Identity Reports

Navigate to Reports Management Page

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



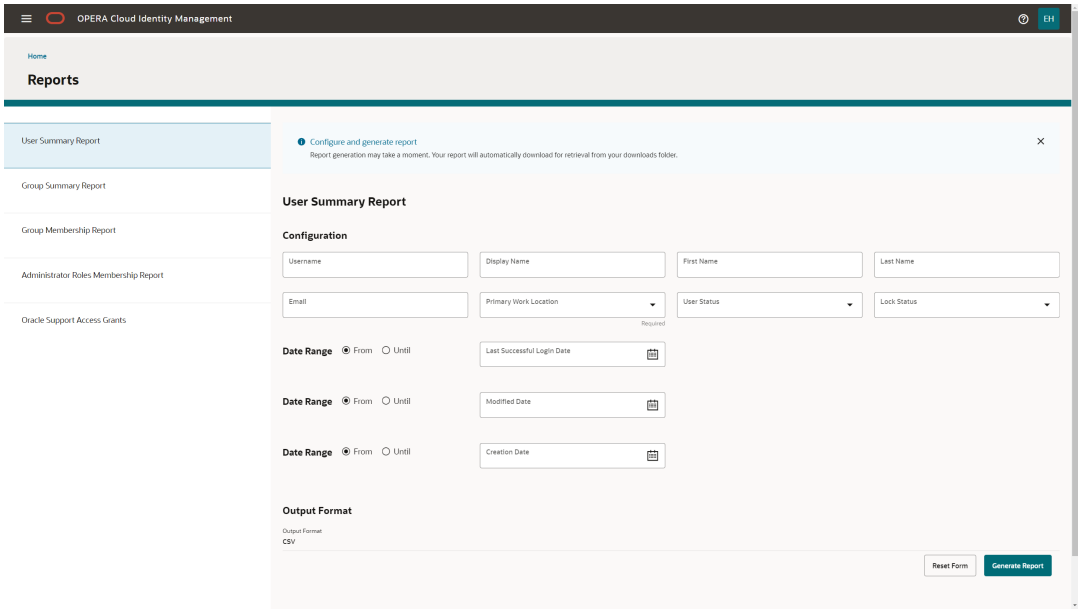
The Reports page consists of a list of available reports and a report generation page specific to each report.

Select a Report and Configure Report Filters

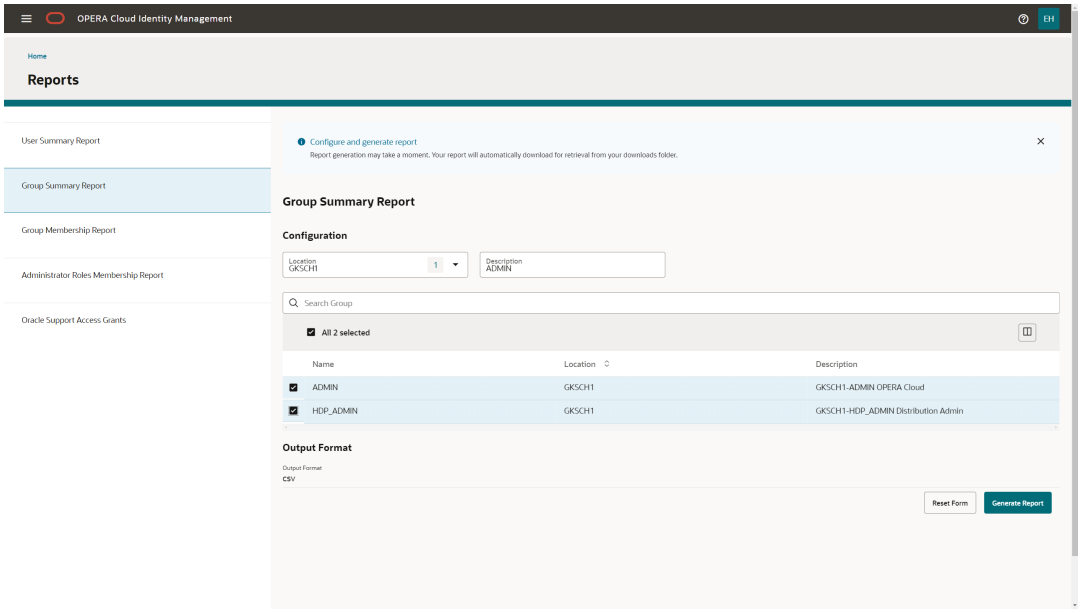
1. To see the filter configuration page for a report, select the respective report.

   On the right hand-side, you will see the available filter options for the selected report.
2. Add any required filter details. Optionally, you can also add additional filter criteria.

   Some filters (for example, group name filter) allow you to search for existing groups and select the groups that should be included in the report.



Some filters (for example, the Group Name filter) allow you to search for existing groups and select the groups that should be included in the report.



Generating and Saving Reports

1. After you have selected a report and added filter criteria, select **Generate Report** to create a report.
2. Once the report generation has completed, a toast message “Report Downloaded” appears as well as the following depending on your browser:
   a. A “Save As” dialogue that allows you to specify a download location for the report and save the report in that location.
   b. The report being added in the “downloads” area of your browser.

> **Note:**
>
> All report outputs are in CSV file format and report generation may take several minutes to download or several minutes before a toast message appears on the screen for “Save As.”

9 Tools

Copy Groups

In OPERA Cloud Identity Management, you can copy existing custom application groups from one location to multiple other locations. This is valuable when implementing new application groups across multiple chains or properties or for copying one or multiple existing application groups from existing chains or properties to newly provisioned ones. Enterprise and chain administrators have access to this feature in the OPERA Cloud Identity Management portal Tools page.

Copying Groups from one location to other locations

1. Log in to OPERA Cloud Identity Management Portal as an enterprise or chain administrator.
2. Click the **Tools** tile on the Homepage.

> **Note:**
>
> Only enterprise and chain-level administrators have access to the Tools tile.

The Tools page consists of a list of available tools including Copy Groups.

3. Select **Copy Groups To Additional Locations**.

   The details and options for copying groups from one location to another location(s) appear on the screen.

4. Configure the groups to copy.
   a. To start the process for copying groups, select the **source location** in the **Groups to Copy** section. You can select any chain or property location from the domain to which you have administrative access. Only one location selection is allowed.
   b. You have the option to exclude the group descriptions from the copy process. Deselect the **Copy group descriptions to all locations** option to exclude the group descriptions to be copied. By default, this option is selected and groups descriptions from the source location are copied to the destination locations.
5. Add the groups to be copied.
   a. After you select the source location for the groups, select one or multiple groups to be copied.

> **Note:**
>
> A maximum of 20 groups can be selected.

b. Click **Add Group** to add the selected groups to be copied.

6. Review and edit the selected groups.
   a. After you click **Add Groups**, the selected groups appear on the Copy Groups main page for inclusion in the copy process.
   b. Click **Edit Groups** to add/remove groups.
7. Select the destination locations.
   a. After you select and review the groups to be copied, you can select up to 5 destination locations.

> **Note:**
>
> You can only copy groups from one location type to the same location type (that is, copy chain groups to other chain locations and copy property groups to other property locations). The available destination locations only show the same type locations as selected in the source location.

8. Copy groups process.
   a. After you select the destination locations, you can click **Copy Groups** to copy the selected groups from the selected location to the destination locations.
   b. After the process completes, information banners show the successfully copied location/group combinations. This also shows any location/group combinations that could not be created in the destination location (that is, a group with the same name already existed in the destination location).
   c. The selected values from the copy group process appear after completion. This allows you to select other destination locations and repeat the process with the previously selected groups.
   d. You can reset the form by clicking **Reset Form**. This removes all selected details from the copy groups page.