Oracle® Hospitality OPERA Cloud Identity Management

Administrator Guide

Release 24.2
G13421-01
August 2024

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide, Release 24.2

G13421-01

Contents

5 Managing Oracle Support Access Requests

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
August 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

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 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.

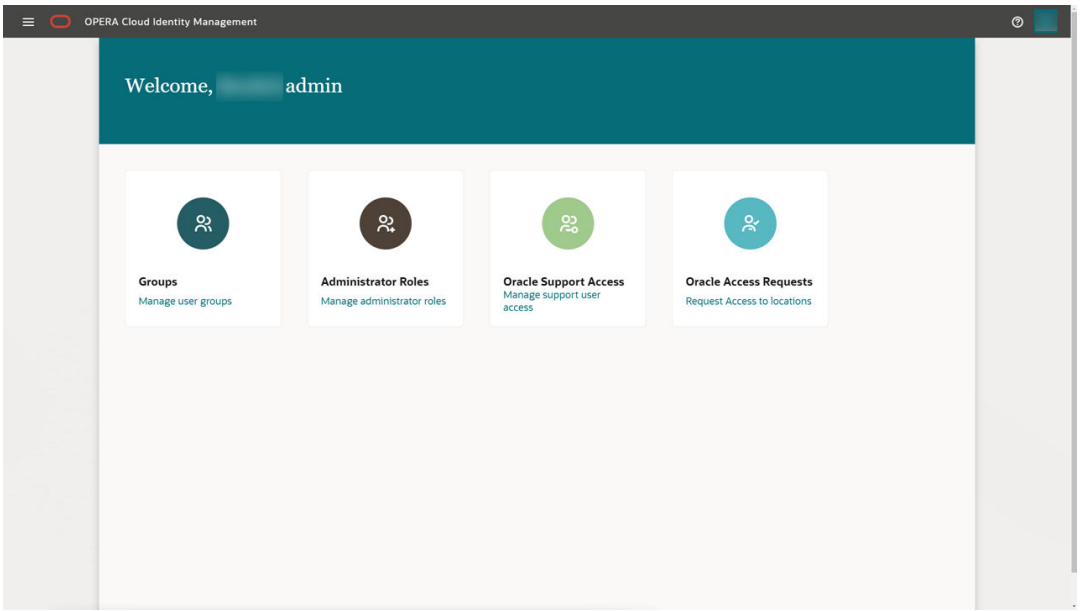
Navigating to Administrator Roles

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

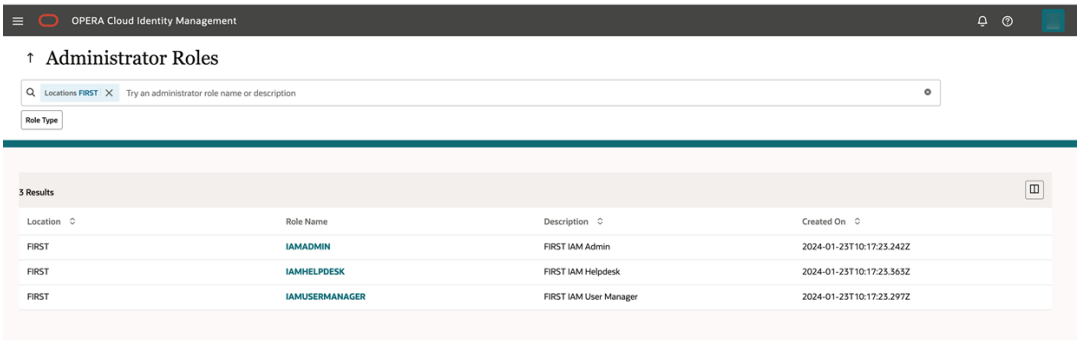
   > **Note:**
   >
   > During provisioning of OPERA Cloud, the Enterprise administrator along with the Chain administrator and Property administrator are created in the customer's OCI IAM Identity Domain, and those users automatically get assigned the IAMADMIN role in OPERA Cloud Identity Management.

   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.

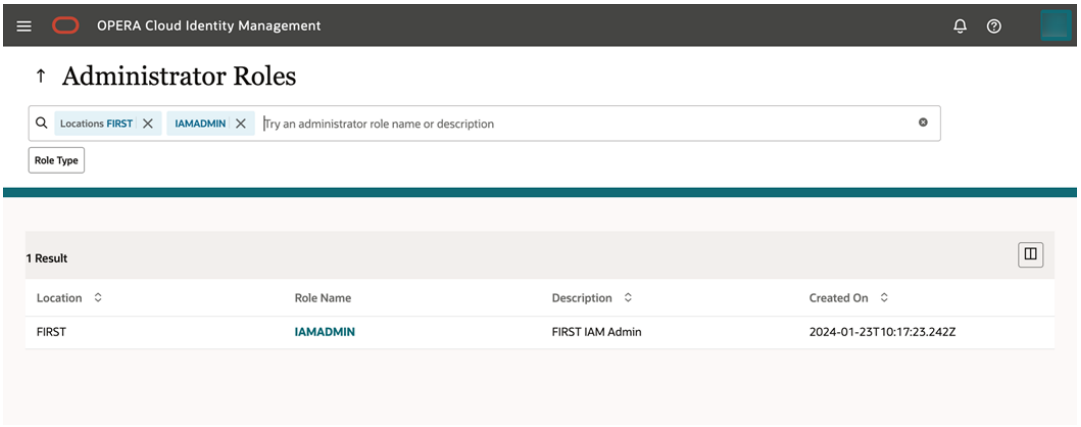


- The Administrator Roles page consist of a search bar and displays the Administrator Roles for your location.
- The search bar can be used to filter administrator roles based on locations and role name.



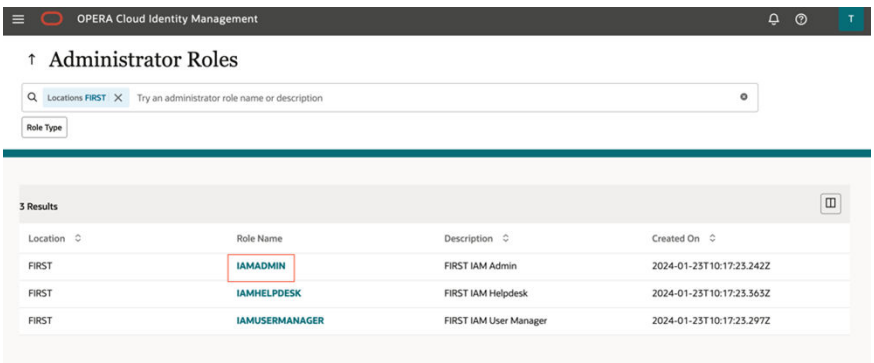
Searching for Existing Administrator Roles

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.



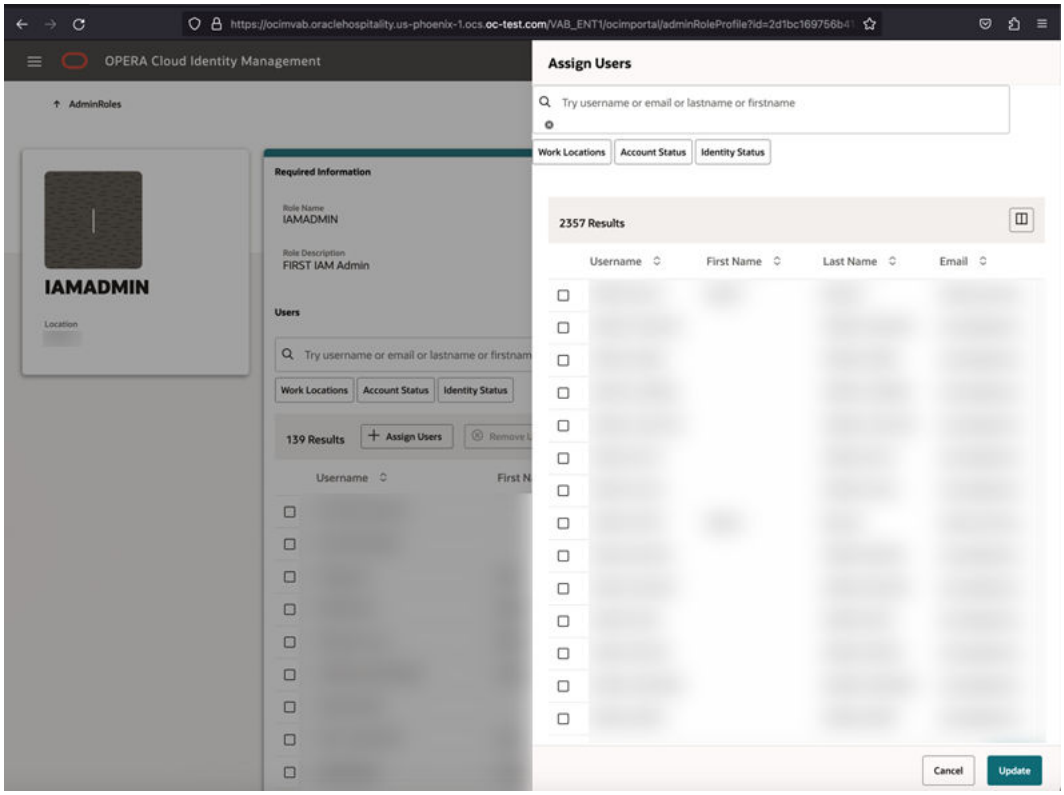
Managing Administrator Role Memberships

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

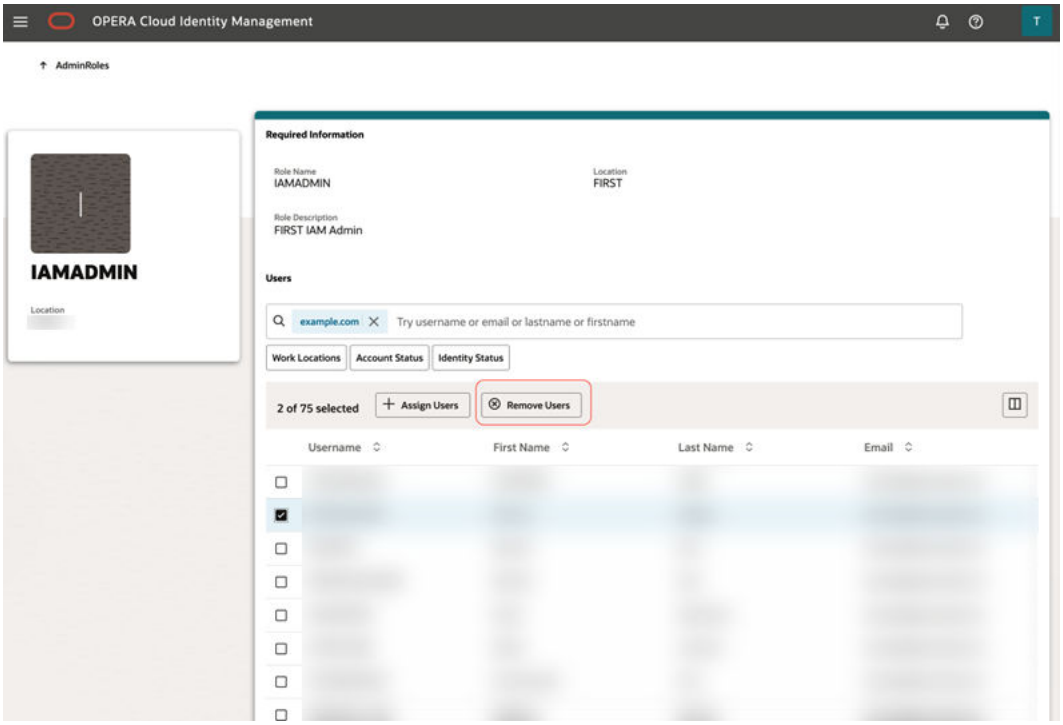


- On clicking the administrator role name, the respective administrator role profile page opens.
- Administrator Roles Profile page consist of a search bar and a table listing members of that role which also supports filtering.
- Administrator Roles Profile also consist of buttons to Assign Users and 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

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

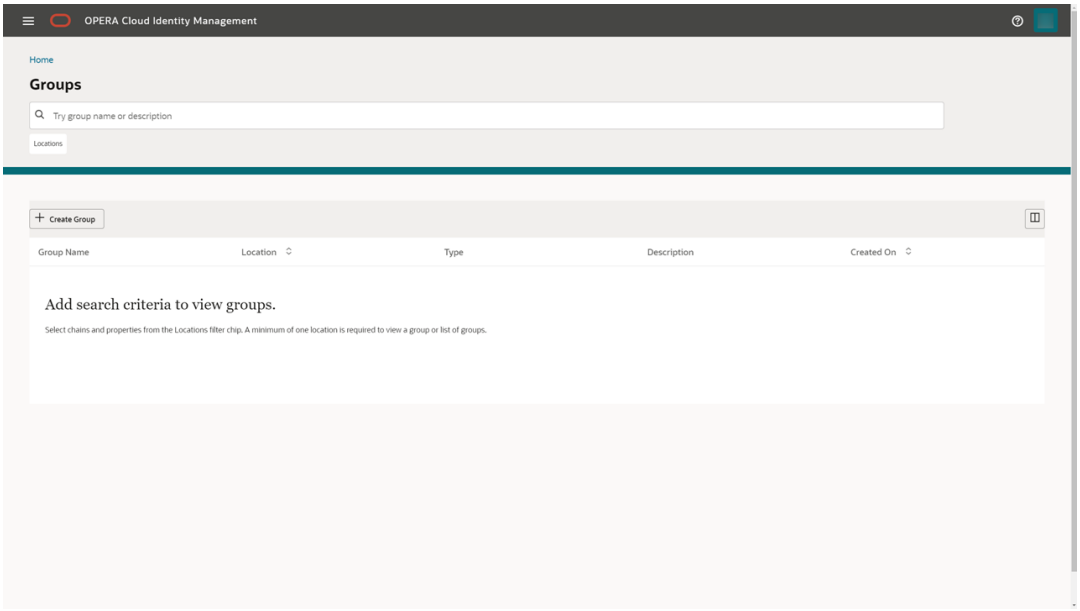
   > **Note:**
   >
   > OC_RNA groups are only visible in Reporting and Analytics in the location "OC_RNA."

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.

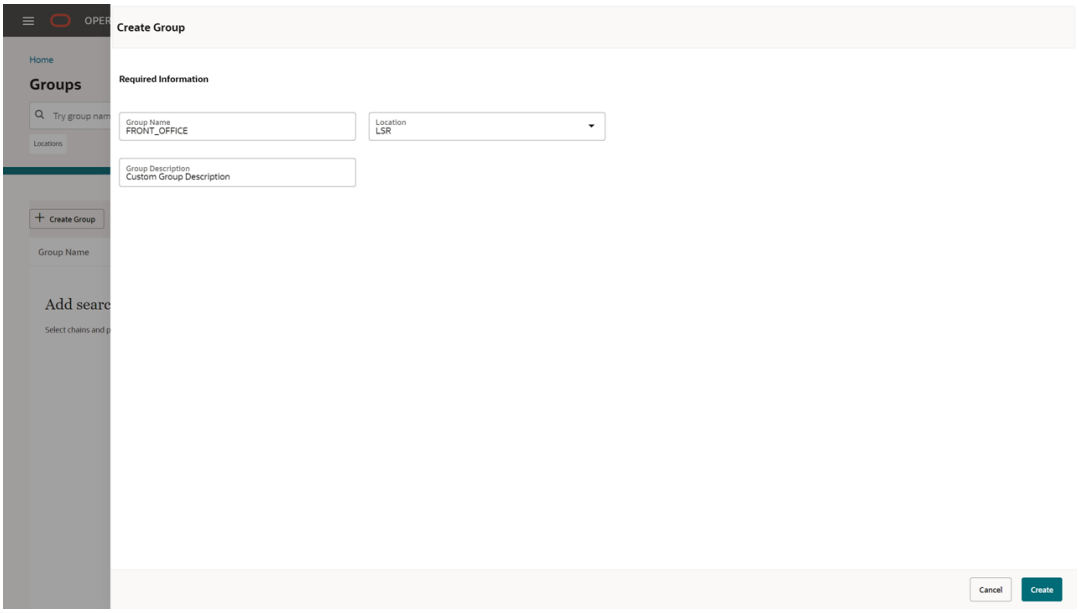


Creating a Custom Group

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.

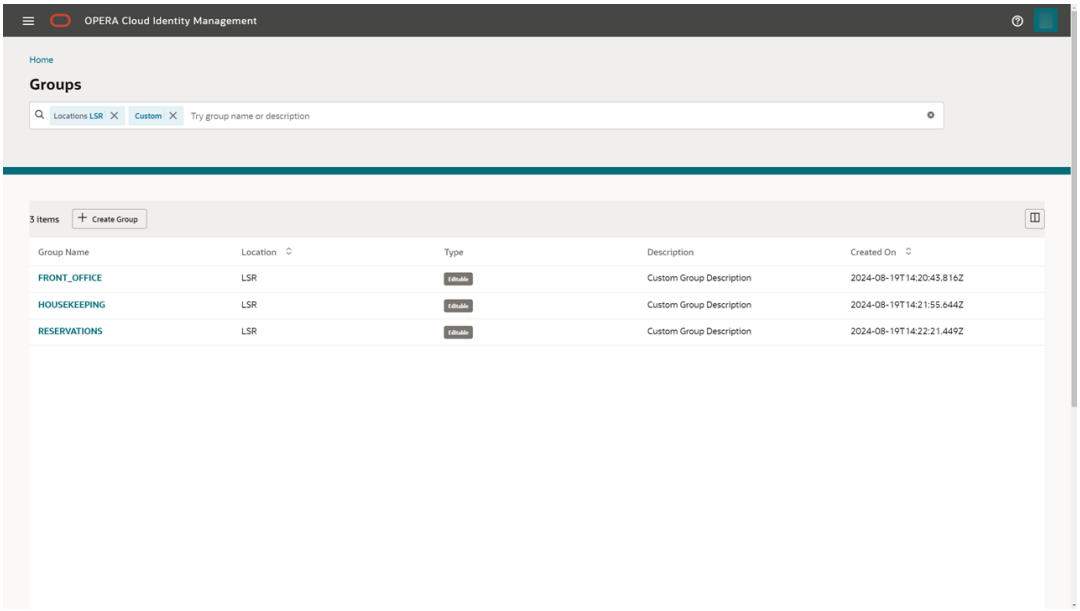
3. Select a location from the location list of values.
4. Optionally, you can also select users for assigning group membership.
5. Click **Submit** to create the custom group.



Searching for Groups

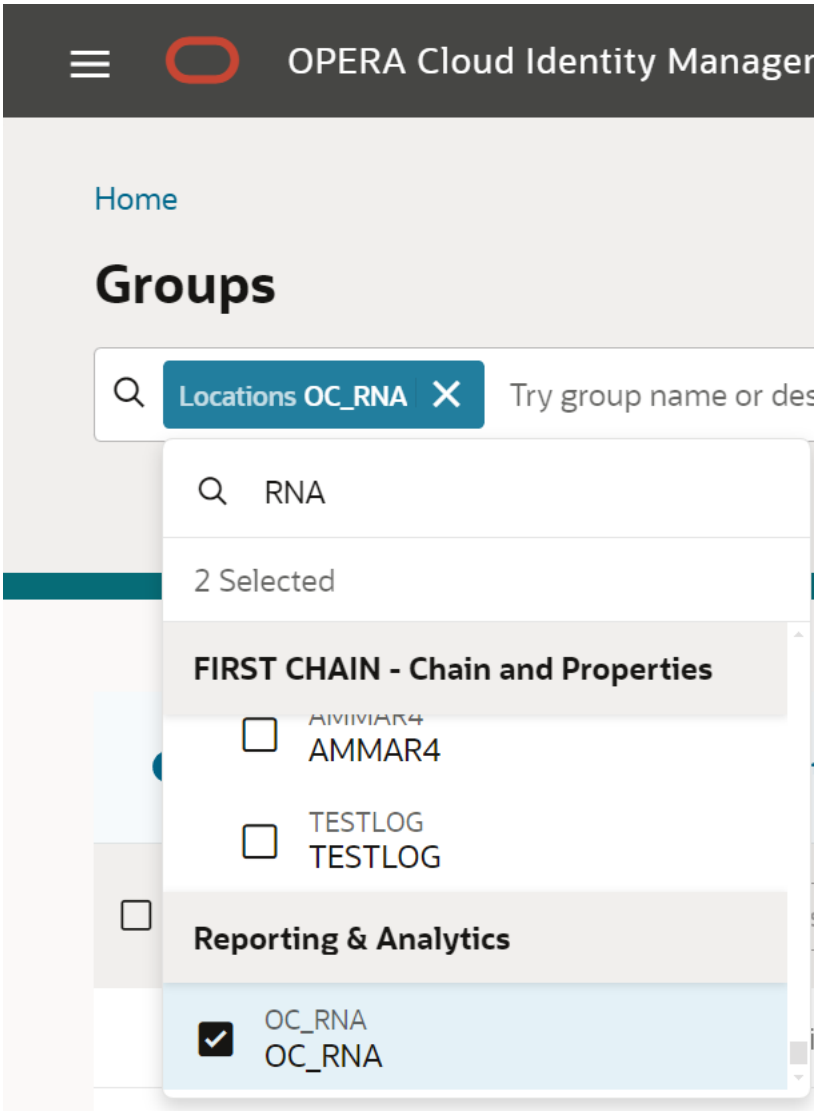
1. Click **Locations** and select the location to search the associated groups for that location.

   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**.


OPERA Cloud Identity Manager
Home
Groups
Locations OC_RNA
Try group name or des
RNA
2 Selected
FIRST CHAIN - Chain and Properties
AMMAR4
TESTLOG
TESTLOG
Reporting & Analytics
OC_RNA
OC_RNA

4

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 DATA ACCESS & SENSITIVE DATA ACCESS role 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.

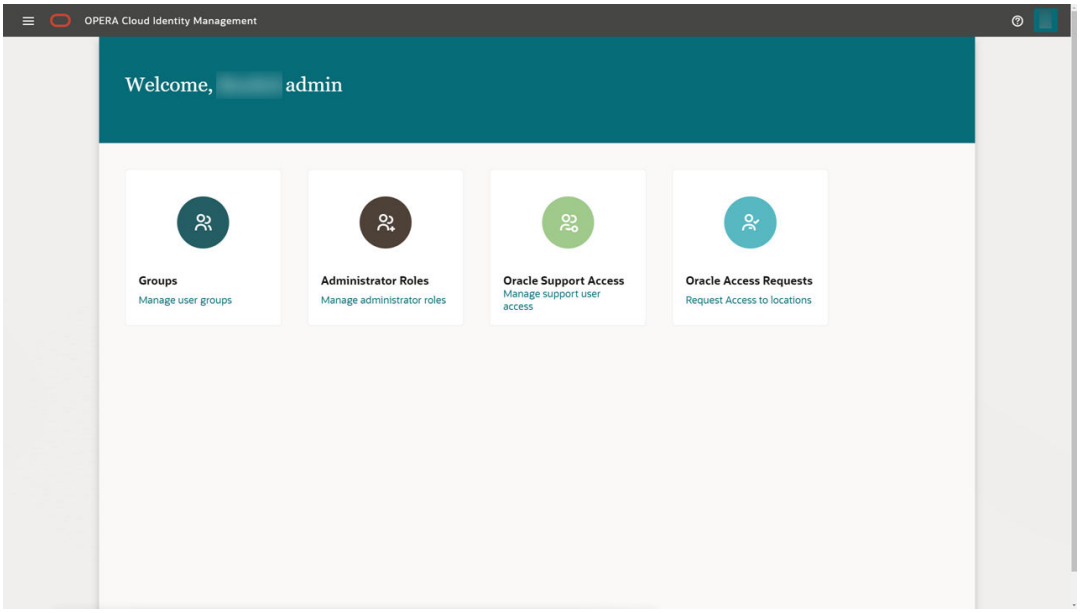
- Customers can assign data sensitive access and the data access role membership to an Oracle user.
- Oracle users must manually communicate to customers through email or through an Oracle support SR to assign data sensitive access or the data access role in the relevant property/chain in that customer OPERA Cloud environment. Oracle users will receive a notification when a customer assigns data access or data sensitive access to them through the OPERA Cloud Identity Management portal.

Managing Oracle Support User Access

The below section describes the steps required for granting data access and sensitive data access 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.

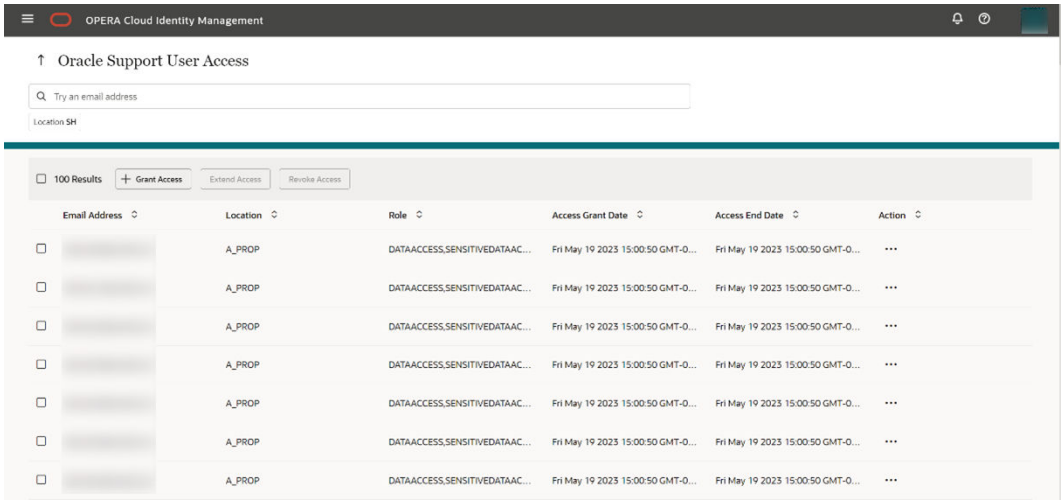


Granting, Extending, and Revoking Access to Oracle Support Users

After selecting the **Oracle Support Access** tile, the Oracle Support User Access page will open. 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 Users access
- Grant access to users
- Extend and revoke the access for users



Searching for Existing Oracle Support User Access

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

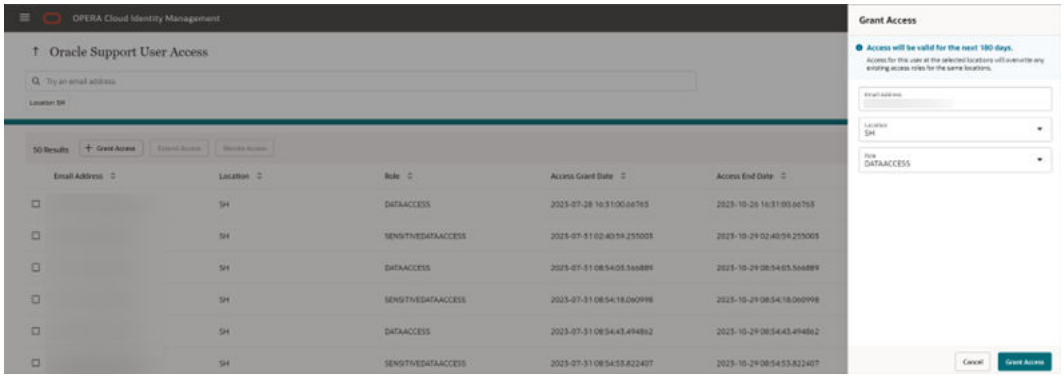
The search result table will refresh and show the users that are matching the search criteria.

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.
   You will see a grant access drawer that enables you to enter the required details for the new Oracle Support User Access grant.
2. Enter the following details:
   - **Email Address** (must end with @oracle.com)
   - **Location** (that is, SH (chain), 879 (property), and so on)
   - **Role** (DATAACCESS, SENSITIVEDATAACCESS)
3. 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.



Extending Access for Users

You can extend existing Oracle support user access from the Oracle Support User Access page for any user with an active support access.

Extending access for one or multiple users will extend the existing access to 90 days from the point of time the access was extended. You have two options to extend a user's grant:

- Extending access for an individual user
- Extending access for multiple users

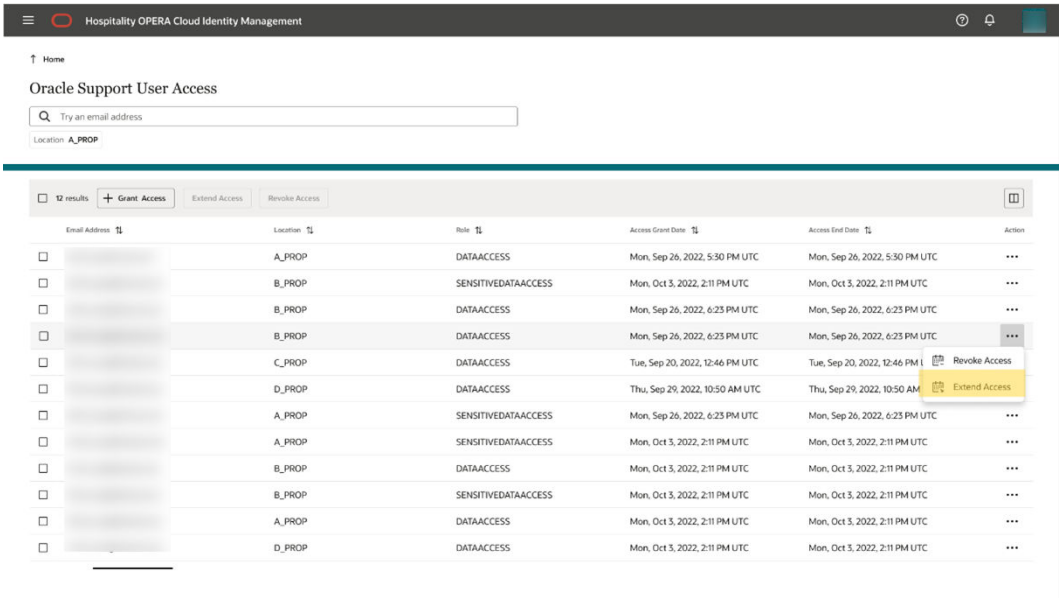
Extending Access for an Individual User

You can extend an existing Oracle Support User Access from the Oracle Support User Access page for any user with active support access.

Extending one or multiple user access will extend the existing access to 90 days from the point of time the access was extended.

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

1. Click the icon in the **Action** column and select **Extend Access**.
2. Confirm the pop-up message to extend the user access to 180 days from the point of time you confirm or cancel the grant process.

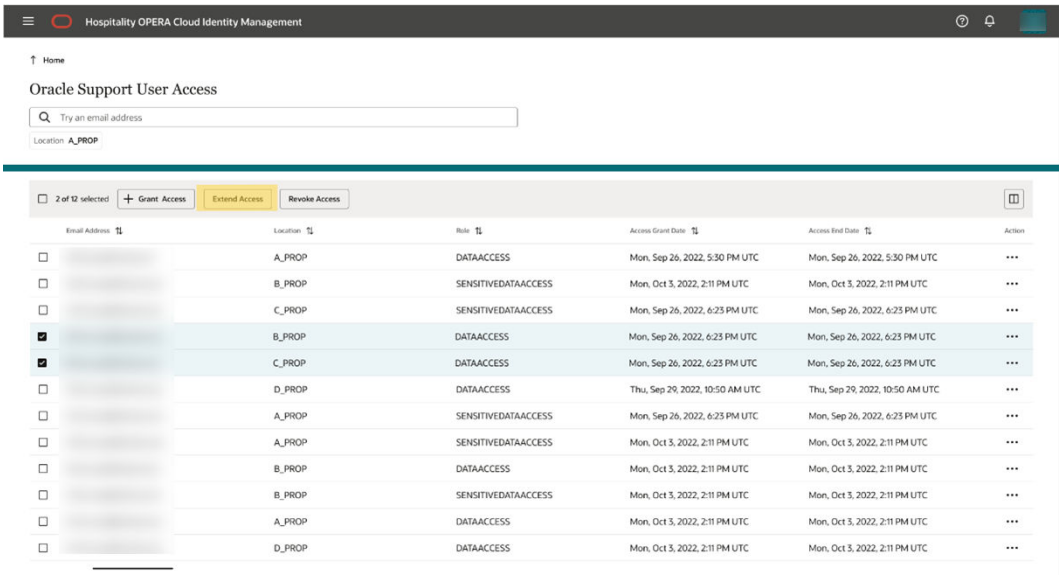


Extending Access for Multiple Users

You can select multiple users on the Oracle Support User Access table to extend 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 "Extend Access" is enabled.

1. Click the **Extend Access** button.
2. Confirm the pop-up message to extend the user access for all selected users to 180 days from the point of time you confirm or cancel the grant process.



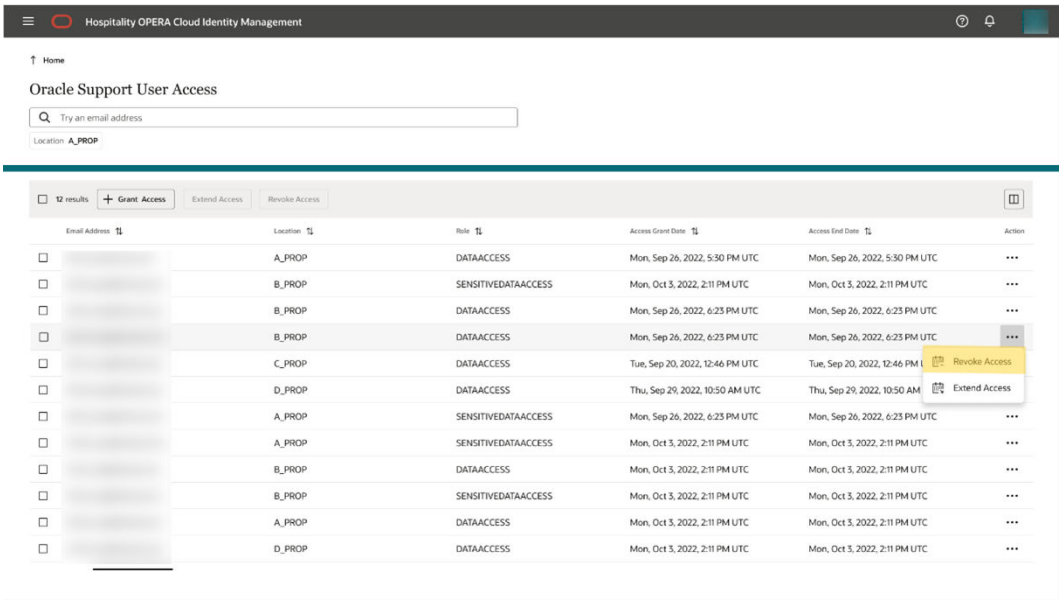
Revoking Access for Users

> **Note:**
>
> In OPERA Cloud Identity Management version 24.2 and earlier versions, a hotel administrator must manually revoke Oracle Support Access. Oracle Support Access will not be revoked automatically.

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

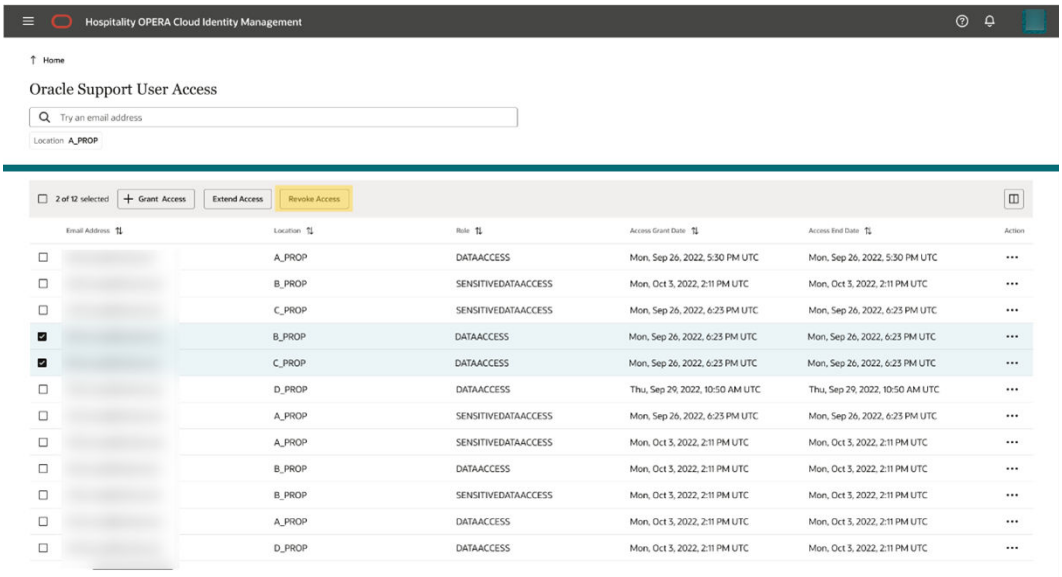
Revoking Access for an Individual User

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.




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

5

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 DATA ACCESS and SENSITIVE DATA ACCESS, and respective customer administrators can approve/deny this request based on their discretion.

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

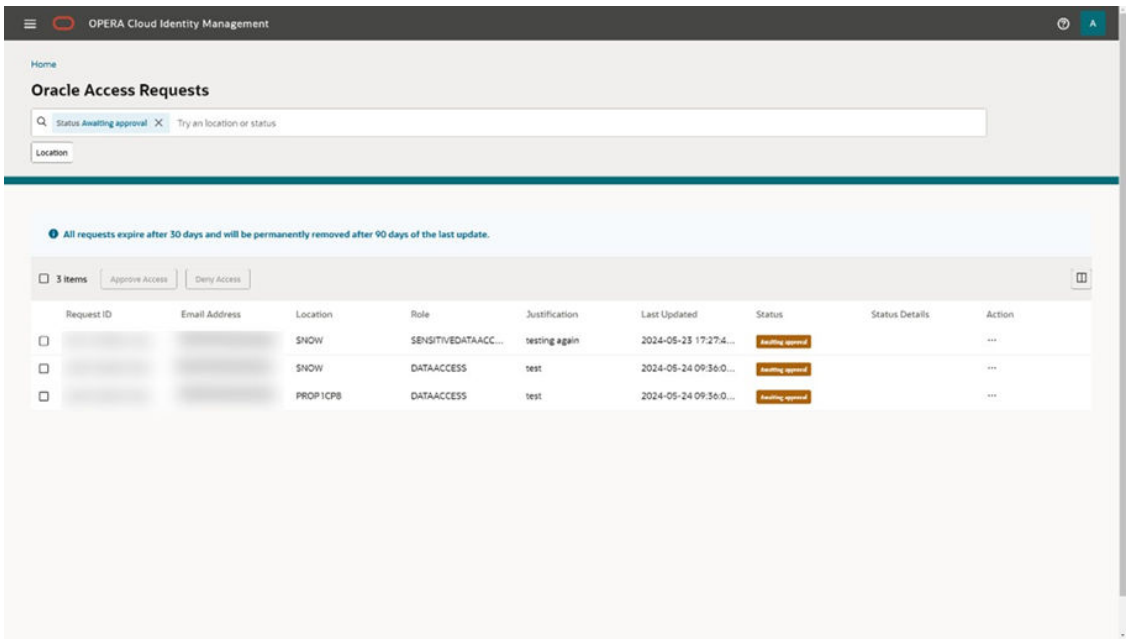
The Oracle Access Requests screen:

- 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**.
3. Confirm by clicking **Approve** in the “Approve Access?” dialogue.

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

> **Note:**
>
> You can see the respective support access entry 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

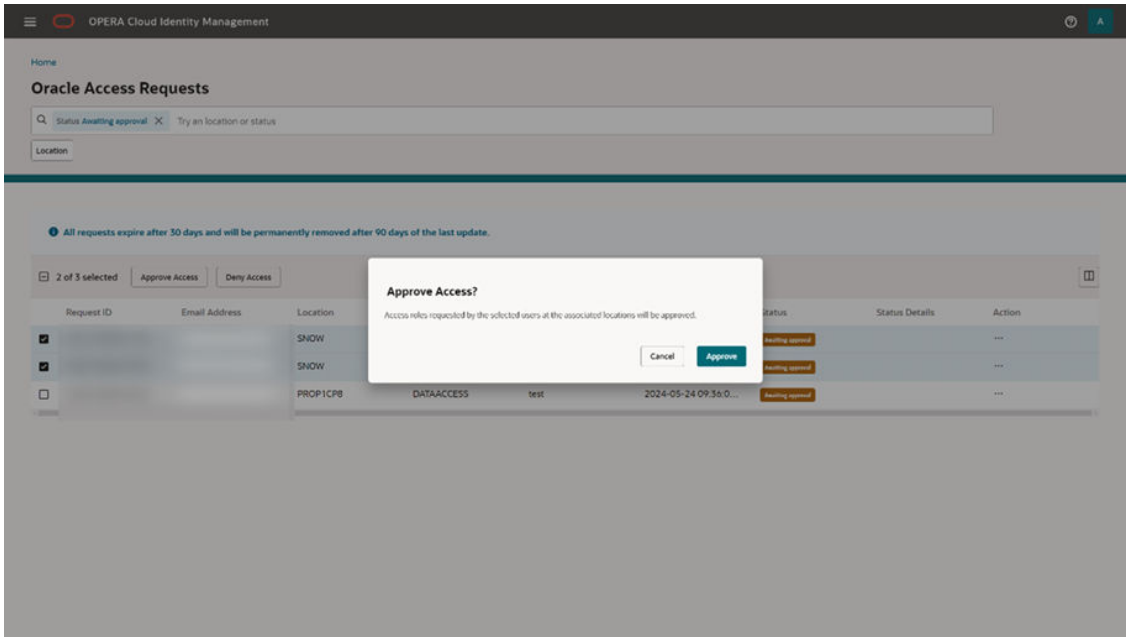
1. To approve one or multiple Oracle Access Requests with the page level action, first select the checkbox for all requests that you want to approve at the same time.

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

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.

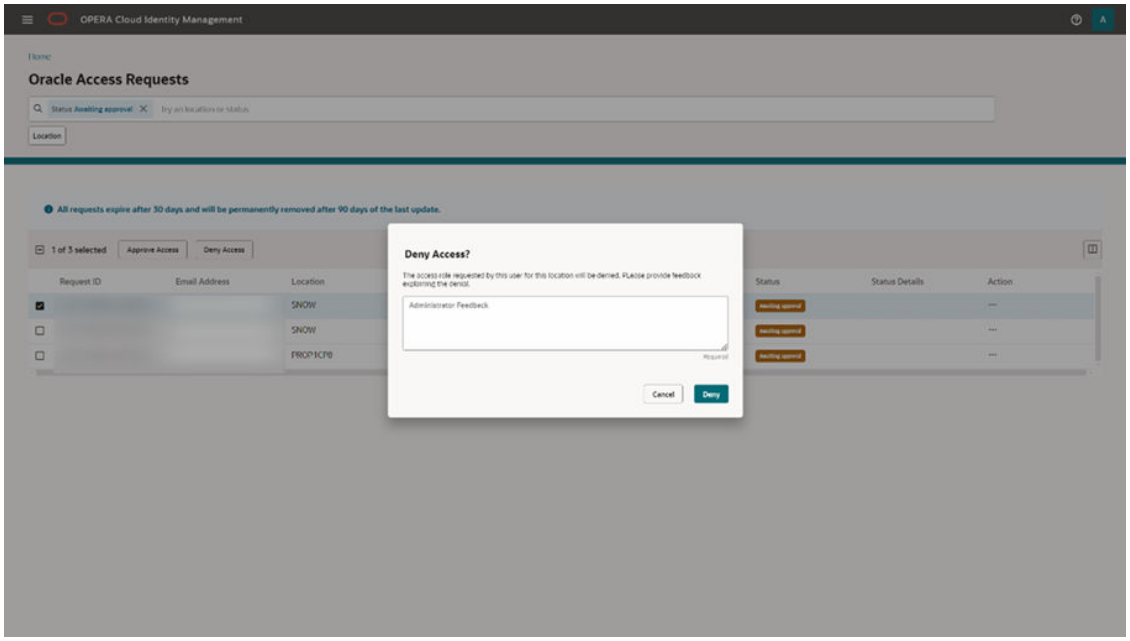
> **Note:**
>
> You can see the respective support access entry in the Oracle Support Access tile. This shows all the currently active Oracle support access for locations to which you have administrative access.



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.



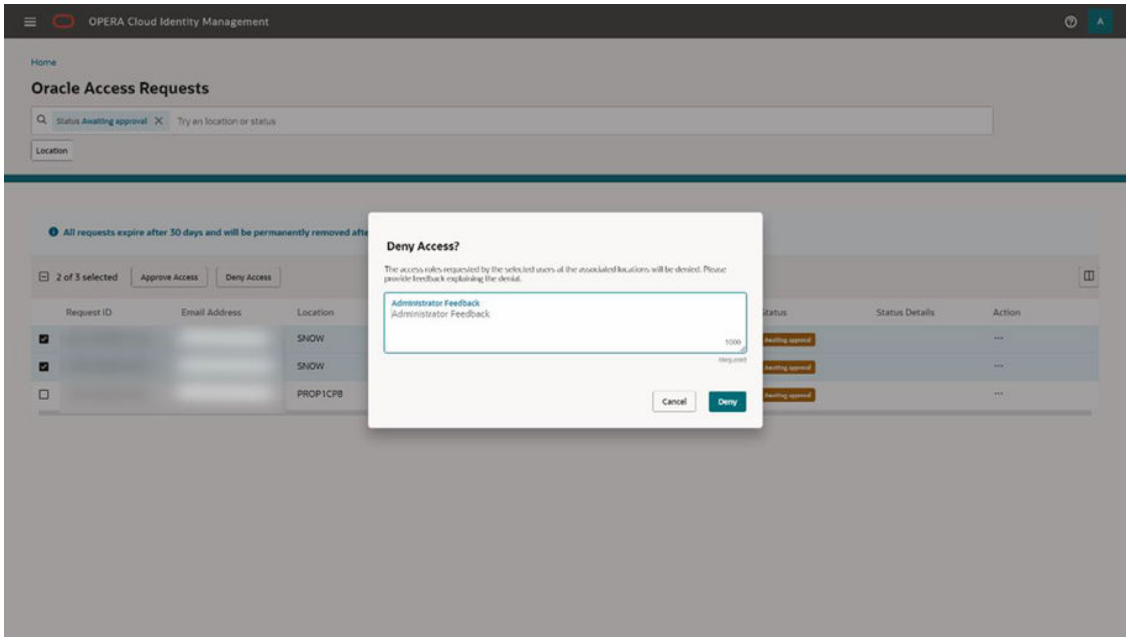
Denying Multiple Requests

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 5-1 Oracle Access Requests Screen

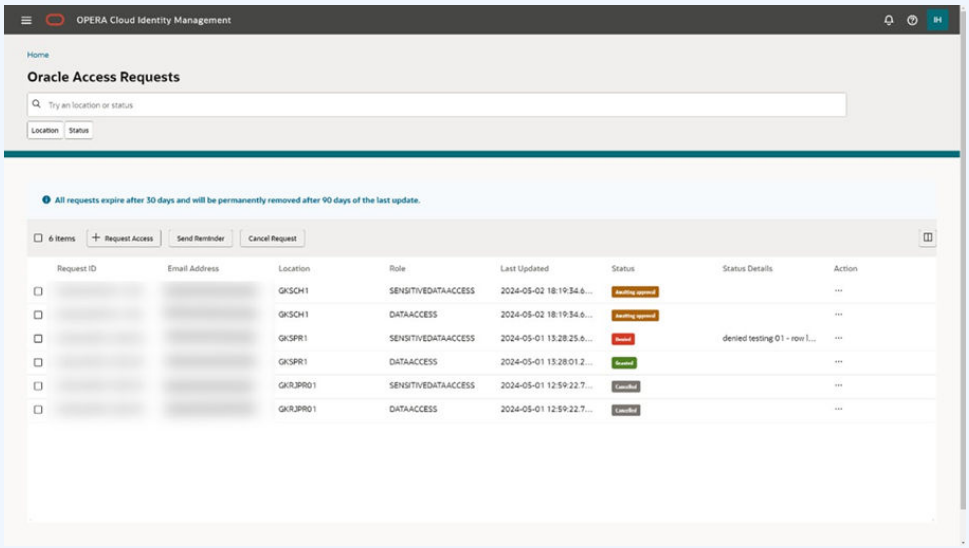
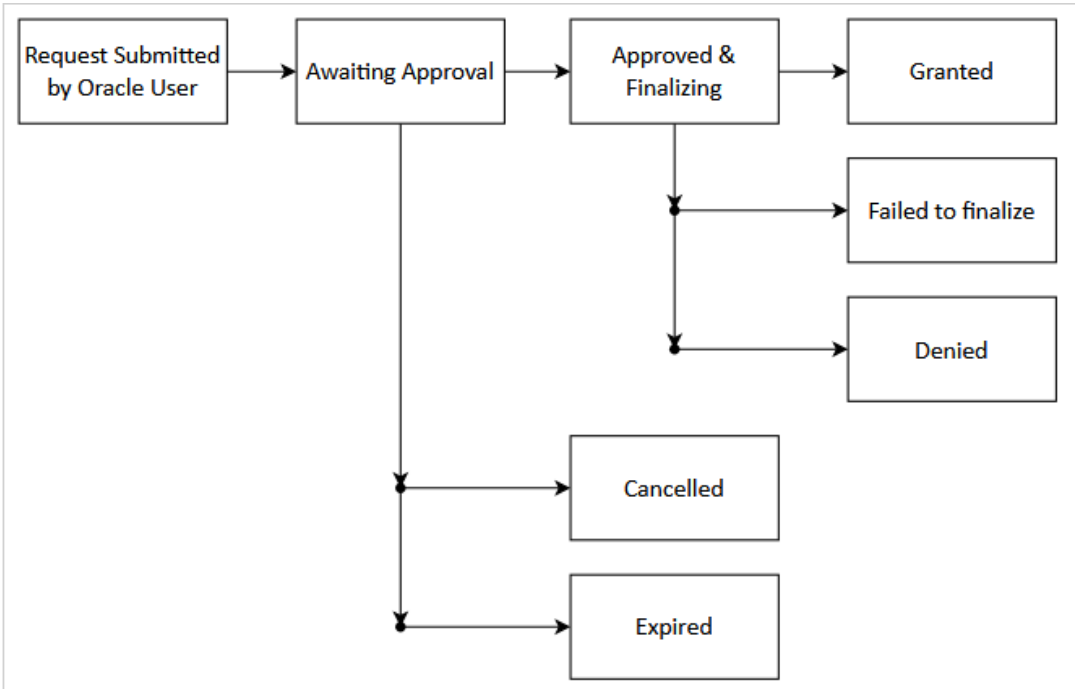


Figure 5-2 Oracle Access Requests — Status Flows



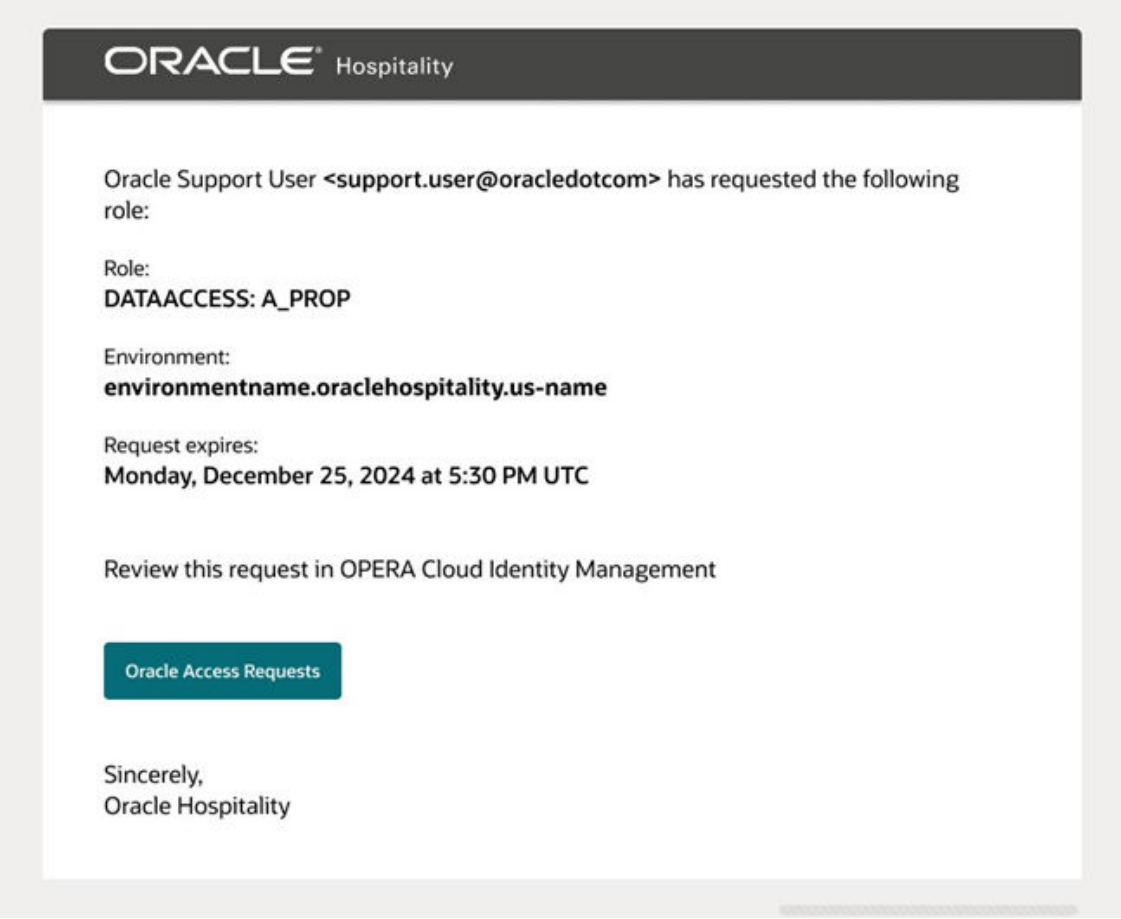
Email Notifications Received for Oracle Access Requests

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.