

Oracle® Hospitality OPERA Cloud Identity Management

Managing Oracle Support Access Requests



Release 25.5
G47683-01
November 2025

ORACLE®

Oracle Hospitality OPERA Cloud Identity Management Managing Oracle Support Access Requests, Release 25.5

G47683-01

Copyright © 2024, 2025, Oracle and/or its affiliates.

Contents

1	Managing Oracle Support Access Requests	
	Navigating to Oracle Access Requests	1
	Oracle Access Requests Screen Overview	1
	Approving a Single Request	2
	Approving Multiple Requests	2
	Denying a Single Oracle Access Request	3
	Denying Multiple Requests	4
	Viewing your Oracle Access Requests	5
	Email Notifications Received for Oracle Access Requests	7

Notices

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 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" or "commercial computer software documentation" 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 and Java 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.

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 Oracle Support Access Requests 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
November 2025	Initial publication

1

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.

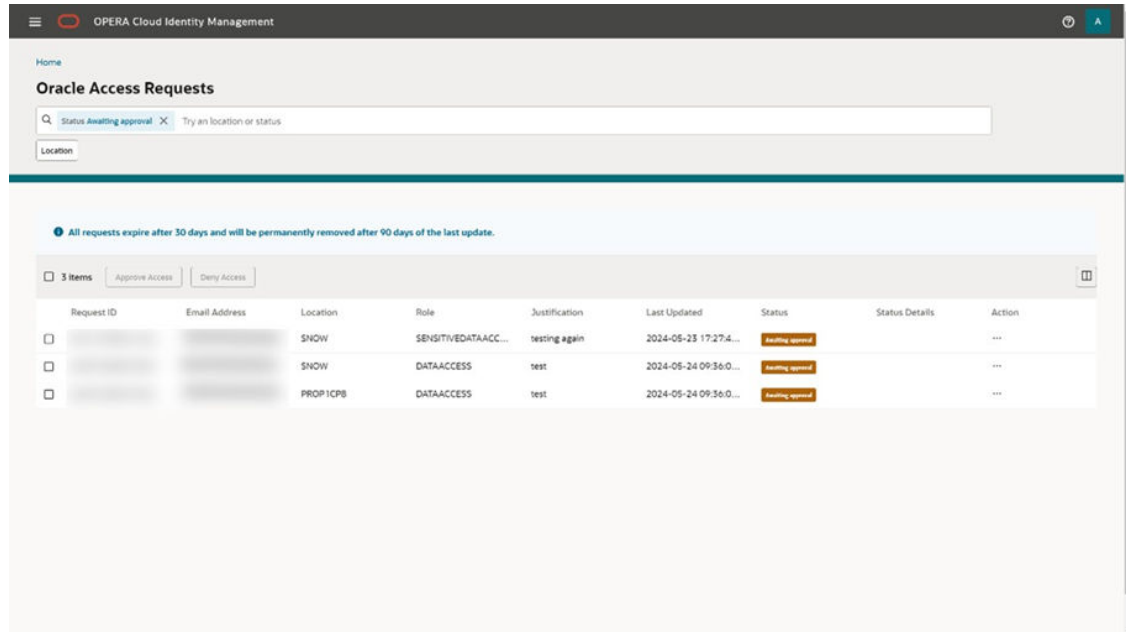
Note

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

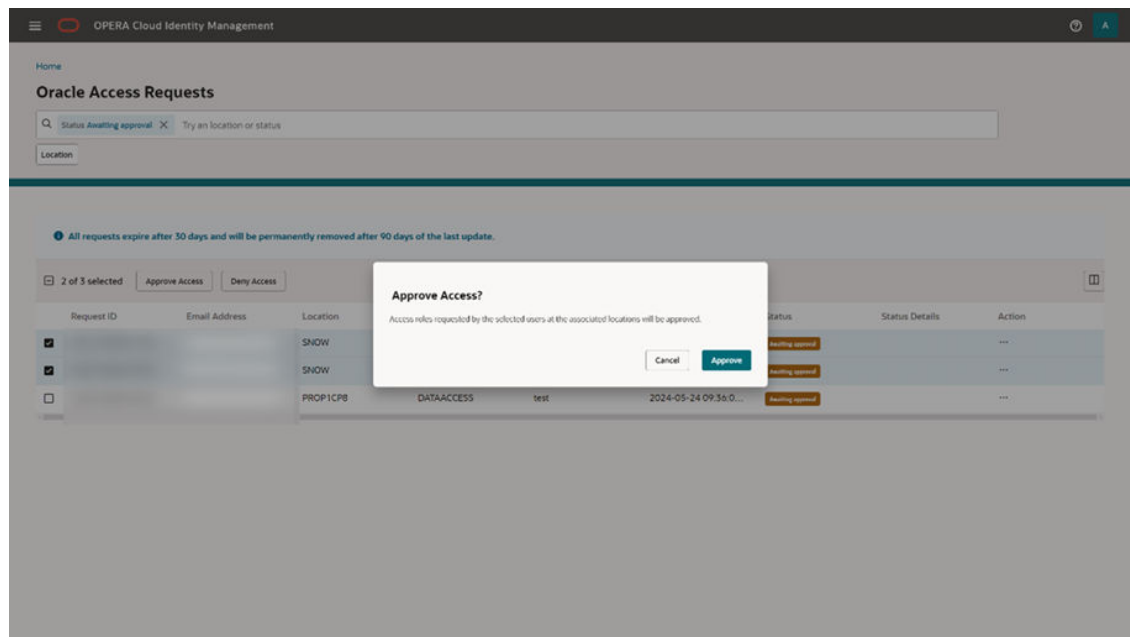
You can select up to a maximum of 20 requests at one time.

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

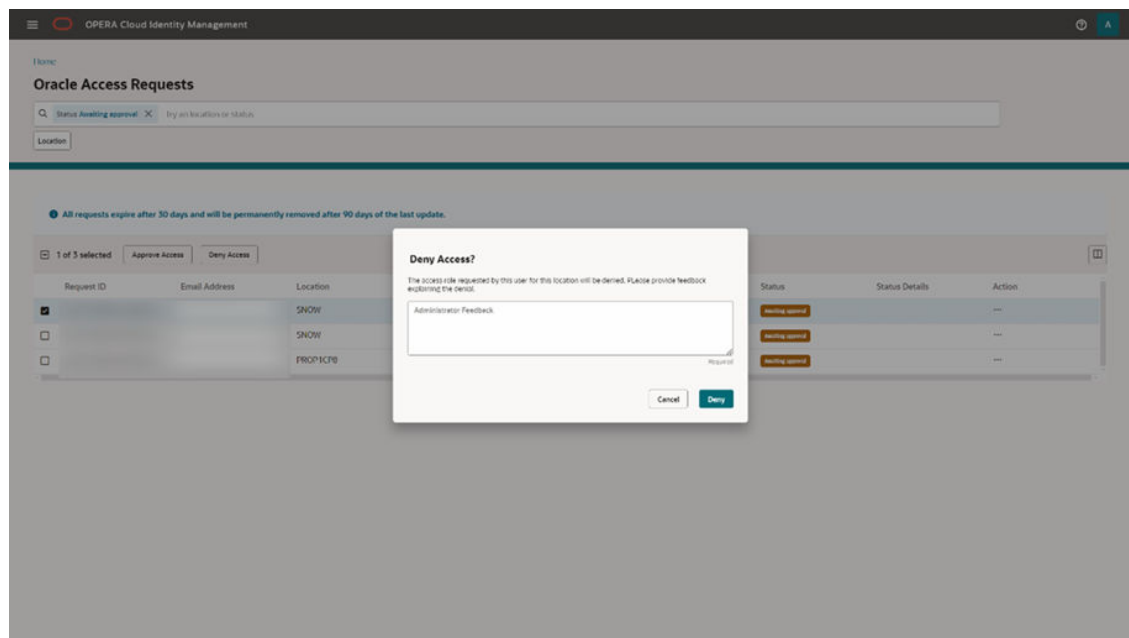
You can see the respective support access entry in the Oracle Support Access tile. This shows all the currently active Oracle support access for locations to which you have administrative access.



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

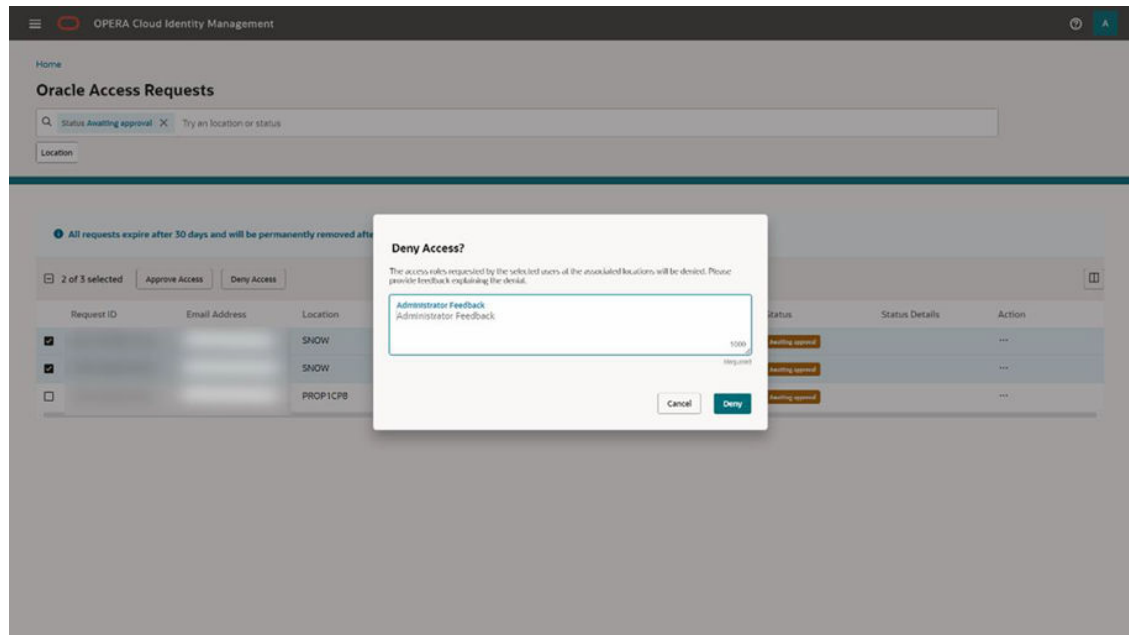
1. To deny one or multiple Oracle Access Requests with the page level action, first select the checkbox for all requests that you want to deny at the same time.

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

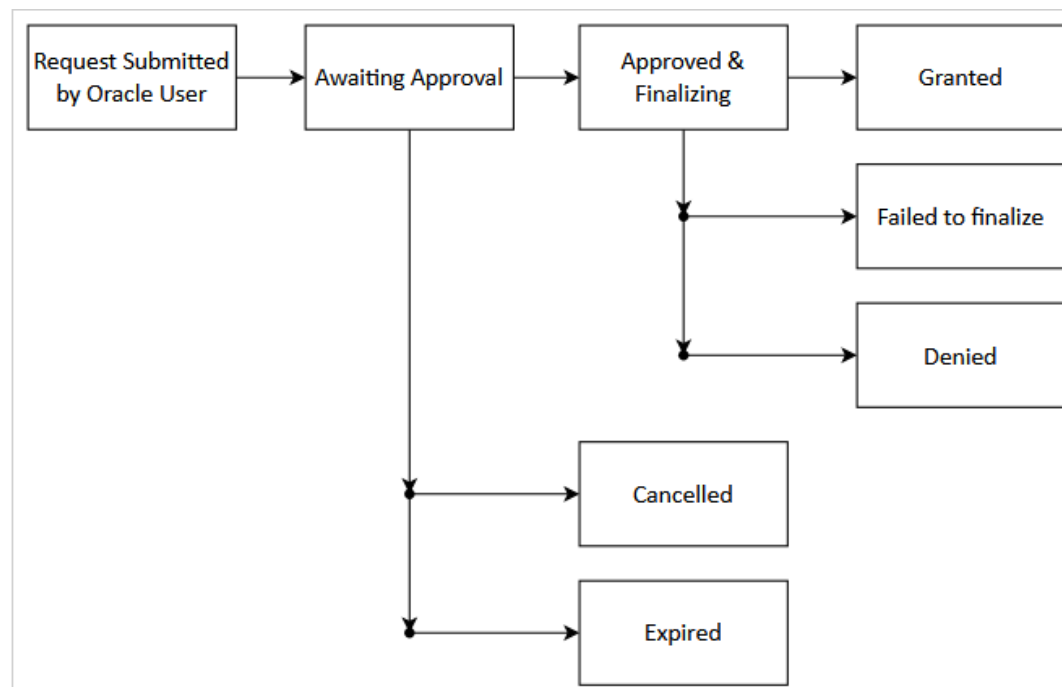
Only requests in “Awaiting Approval” status can be actioned by using the available row level actions or selecting the requests and using the available page level actions.

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

Figure 1-1 Oracle Access Requests Screen

Request ID	Email Address	Location	Role	Last Updated	Status	Status Details	Action
[Redacted]	[Redacted]	GKSOH1	SENSITIVEDATAACCESS	2024-05-02 18:19:34.6...	Awaiting Approval		...
[Redacted]	[Redacted]	GKSOH1	DATAACCESS	2024-05-02 18:19:34.6...	Awaiting Approval		...
[Redacted]	[Redacted]	GKSPR1	SENSITIVEDATAACCESS	2024-05-01 13:28:25.8...	Denied	denied testing 01 - new L...	...
[Redacted]	[Redacted]	GKSPR1	DATAACCESS	2024-05-01 13:28:01.2...	Granted		...
[Redacted]	[Redacted]	GKURPR01	SENSITIVEDATAACCESS	2024-05-01 12:59:22.7...	Cancelled		...
[Redacted]	[Redacted]	GKURPR01	DATAACCESS	2024-05-01 12:59:22.7...	Expired		...

Figure 1-2 Oracle Access Requests — Status Flows



Email Notifications Received for Oracle Access Requests

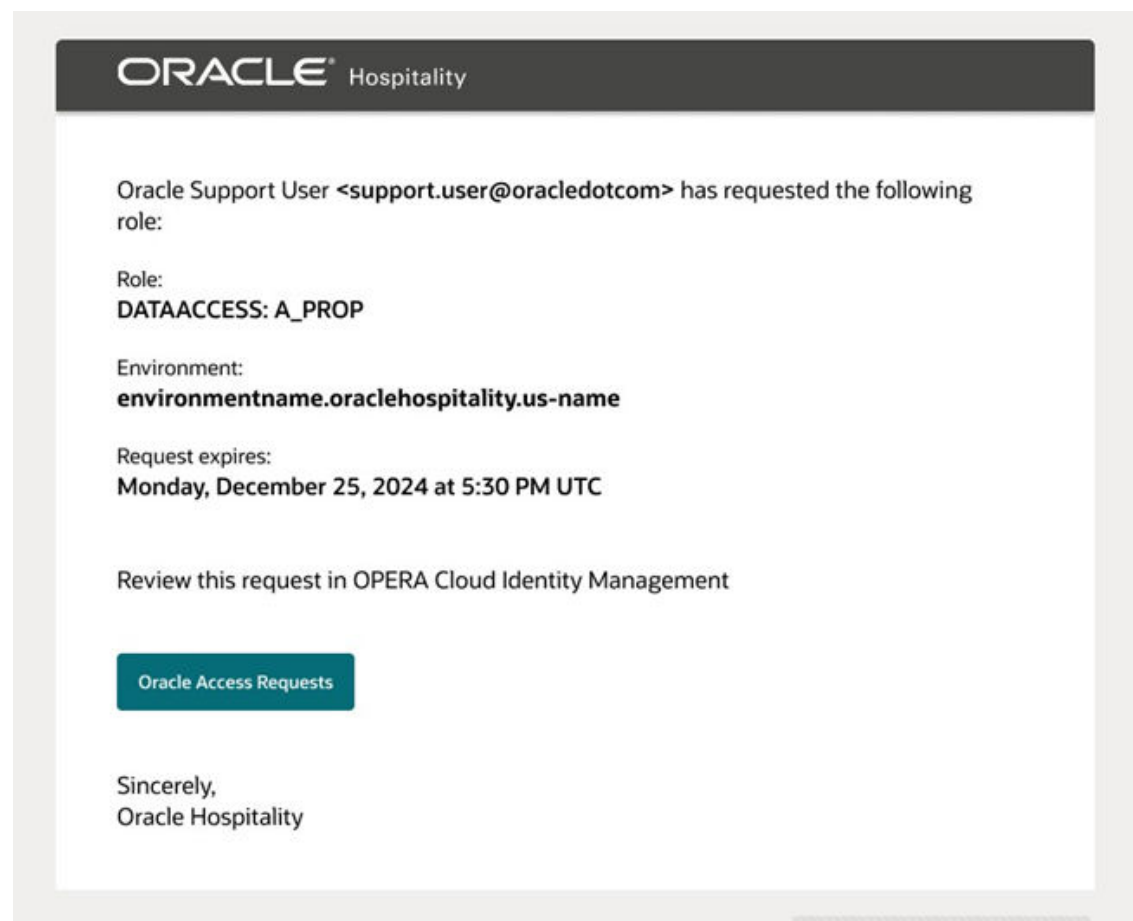
When an Oracle Support User creates a new access request, the respective customer administrator is notified by an email.

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.

