Oracle Hospitality OPERA Cloud Identity Management

Administrator Guide for Managing Oracle Users

Release 23.1.1
F85289-01
March 2024

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Managing Oracle Users, Release 23.1.1

F85289-01

Copyright © 2023, Oracle and/or its affiliates.

Contents

1 Introduction

Process Overview 1-1

2 OPERA Cloud Identity Management – Manage Oracle Support User Access

Navigating to Oracle Support Access 2-1
Granting, Extending, and Revoking Access to Oracle Support Users 2-1
Searching for Existing Oracle Support User Access 2-2
Granting Access to Users 2-2
Extending Access for Users 2-3
- Extending Access for an Individual User 2-3
- Extending Access for Multiple Users 2-4

Revoking Access for Users 2-5
- Revoking Access for an Individual User 2-5
- Revoking Access for Multiple Users 2-5

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

Purpose

This guide describes the steps for customer administrators to grant the DATA ACCESS & DATA SENSITIVE ACCESS role to Oracle users, so users can access a customer's OPERA Cloud environment.

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
- Screen shots 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/

Revision History

Table Revision History

Date	Description of Change
March 2024	Initial Publication

1 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.

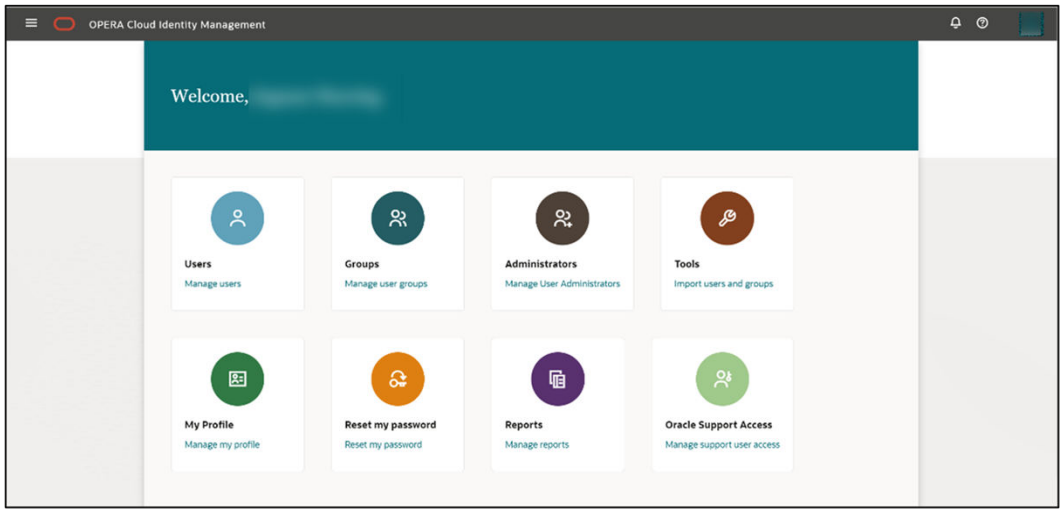
2

OPERA Cloud Identity Management – Manage 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.



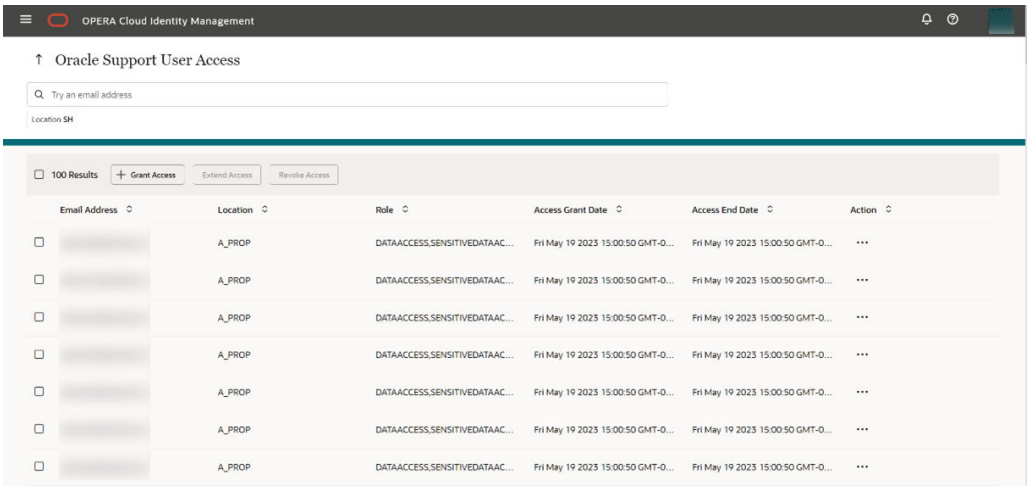
Granting, Extending, and Revoking Access to Oracle Support Users

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.

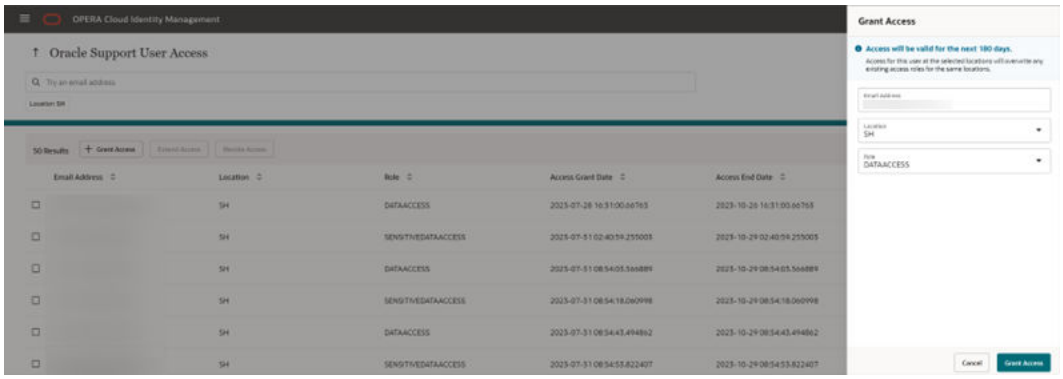
The search result table will refresh and show the users that are matching the search criteria.

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

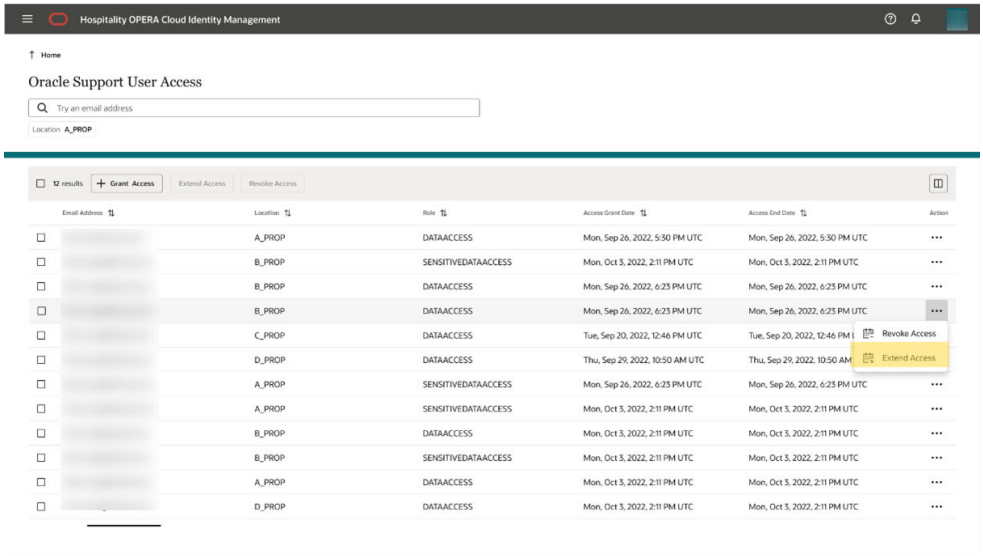
Extending Access for an Individual User

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.

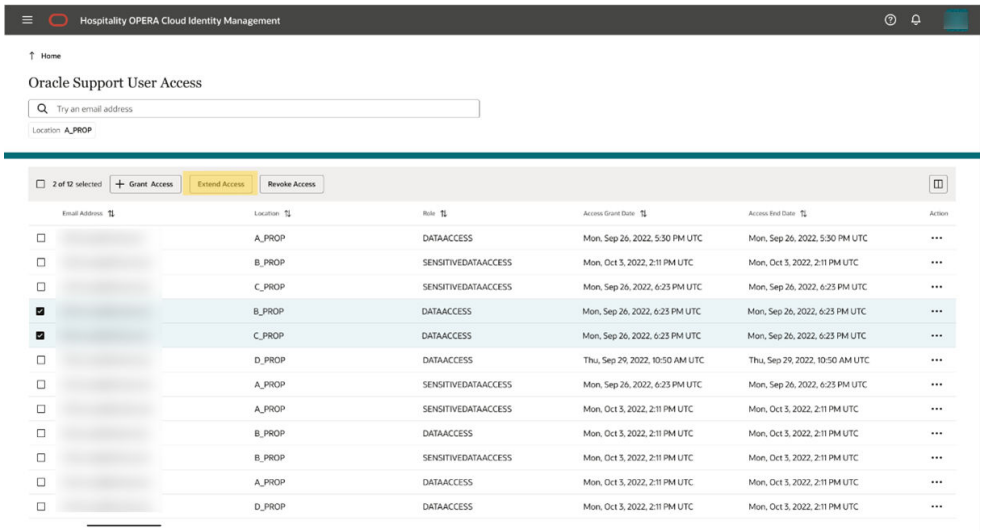


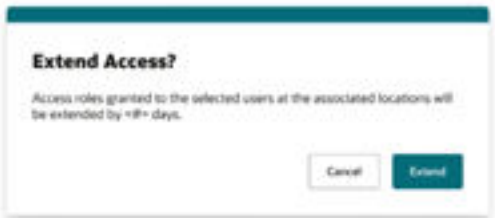
Extending Access for Multiple Users

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.



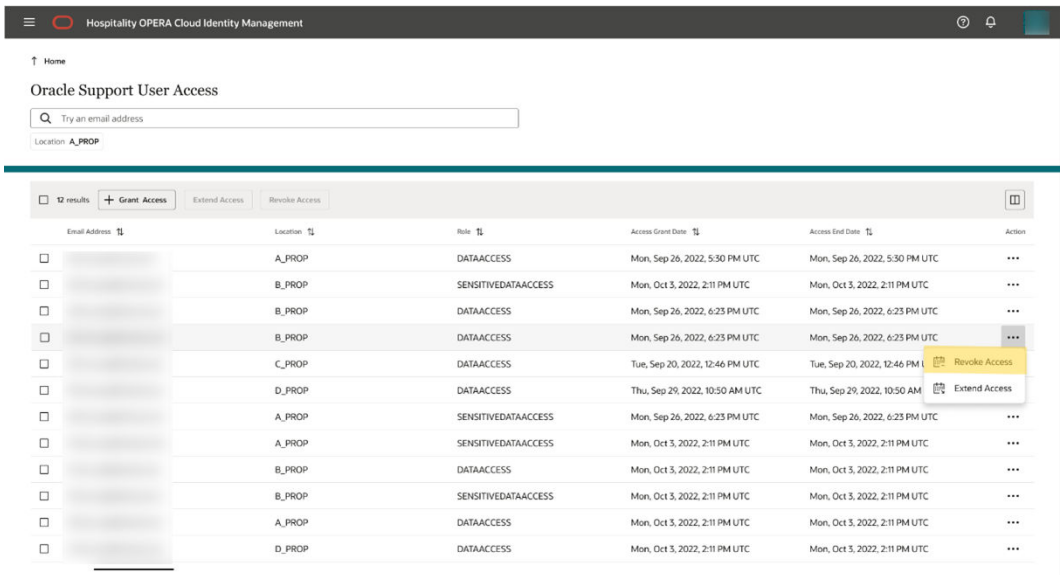


Revoking Access for Users

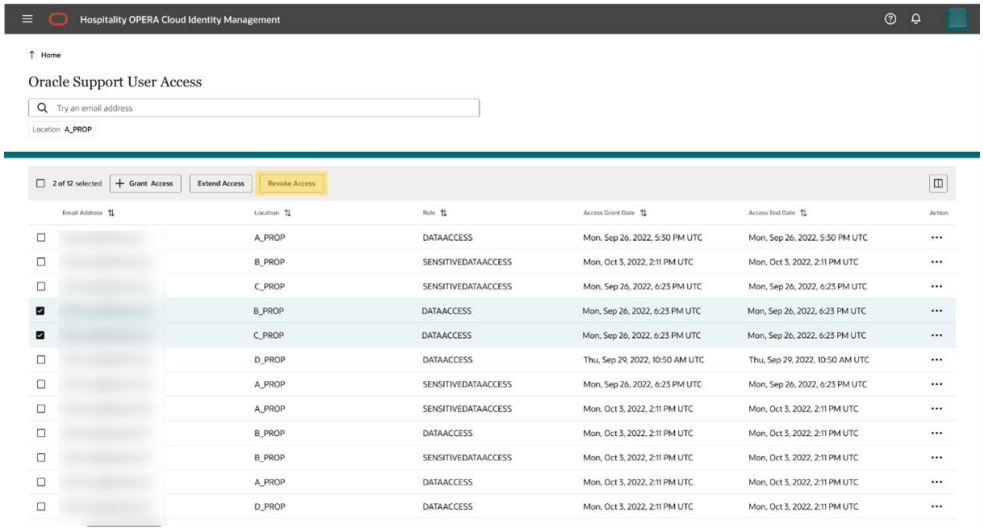
1. You can revoke an existing Oracle support user access from the Oracle Support User Access page for any user with active support access.
2. Revoking access for one or multiple users will IMMEDIATELY revoke the existing access.
3. You have two options to revoke a user's grant:
   - Revoking access for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