

Oracle Hospitality OPERA Cloud Identity Management Identity Federation Overview



Release 24.2
G11507-01
August 2024

ORACLE®

Oracle Hospitality OPERA Cloud Identity Management Identity Federation Overview, Release 24.2

G11507-01

Copyright © 2023, 2024, Oracle and/or its affiliates.

Contents

1	Introduction	
	Terminologies	1-1
2	User Provisioning Options	
	Just-In-Time Provisioning (JIT)	2-1
	Microsoft Azure AD Synchronization	2-1
	SCIM API	2-1
3	OPERA Cloud Identity Management Seeded Groups	

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 explains the identity federation feature of OPERA Cloud. Identity federation can be used by customers to set up single sign on with OPERA Cloud using their identity provider.

Audience

This document is intended for OPERA Cloud Services application users.

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
August 2024	Initial Publication

1

Introduction

OPERA Cloud Identity Management provides the capability of identity federation by determining which customers can integrate their identity provider with OPERA Cloud to implement single sign on with OPERA Cloud. Leveraging OPERA Cloud Identity Management's identity federation feature, customers can use their corporate credentials to log on to OPERA Cloud, which eliminates the necessity to separately manage users and their access to OPERA Cloud.

OPERA Cloud Identity Management Identity Federation is based on the SAML 2.0 standard and can be integrated with any SAML 2.0 compliant identity provider.

Terminologies

The below terminologies are commonly used in OPERA Cloud Identity Management and are associated with Identity federation.

- **Identity Provider (IDP):** Identity provider is a service that provides identifying credentials and authentication for users. It is the system where actual user credentials are stored and is also the source of truth for users and their access.
- **Service Provider:** A service (such as an application, website, and so on) that calls upon an IdP to authenticate users. In this case, Oracle Hospitality OPERA Cloud is the SP.
- **Metadata File:** An IdP-provided XML-based document that provides the required information to an SP to federate with that IdP. Oracle Hospitality OPERA Cloud supports the SAML 2.0 protocol, which is an XML-based standard for sharing required information between the IdP and SP.
- **Federated Customer:** The OPERA Cloud customer who is using the identity federation feature in OPERA Cloud Identity Management to enable SSO for OPERA Cloud using their identity provider.
- **Federated User:** A user who logs in to Oracle Hospitality OPERA Cloud using a federated IdP login.
- **JIT:** Just-In-Time provisioning (JIT) is a feature in OPERA Cloud Identity Management Identity Federation which will create or update a federated user as soon as that user logs in to OPERA Cloud using IDP login.

2

User Provisioning Options

OPERA Cloud Identity Management provides the below three options for user provisioning for a federated customer.

- Just-In-Time provisioning (JIT)
- Microsoft Azure AD Synchronization
- SCIM APIs

Just-In-Time Provisioning (JIT)

Just-In-Time (JIT) Provisioning is a SAML protocol-based method that is used to create users the first time they log in to OPERA Cloud application through an identity provider. This eliminates the need to provision users or manually create user accounts.

Microsoft Azure AD Synchronization

An OPERA Cloud customer can use Microsoft Azure AD Synchronization if their identity provider is Microsoft Azure Active Directory. This option provides seamless synchronization of users, groups, and group memberships from Microsoft Azure AD (identity provider) to the OPERA Cloud Identity Management's customer OCI IAM Identity Domain (service provider).

SCIM API

System for Cross-domain Identity Management (SCIM) is an Internet Engineering Task Force (IETF) standard protocol that enables user provisioning across identity systems. OPERA Cloud Identity Management hosts a SCIM endpoint for provisioning federated users into OPERA Cloud Identity Management's OCI IAM Identity domain. This option can be utilized by customers if they have a SCIM compliant identity provider.

3

OPERA Cloud Identity Management Seeded Groups

OPERA Cloud Identity Management consists of two types of groups:

- Seeded Groups
- Custom Groups

Seeded Groups

Seeded groups are groups associated with chains and properties and are available by default and ready-to-use in OPERA Cloud Identity Management. Seeded groups are created in a customer's OCI IAM Identity Domains during chain or property provisioning in OPERA Cloud applications.

These groups cannot be deleted using the OPERA Cloud Identity Management Portal for a non-federated customer.

Custom Groups

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



Note:

When creating custom groups in identity provider, adhere to the naming convention for the custom group where custom groups must always have the prefix as Property or Chain code followed by '-' and the group name. For example, HOTEL1-FRONTDESK where HOTEL1 can be either chain code or property code and FRONTDESK is the group name. Ensure the custom group name is always in uppercase. If the custom group is not following the naming standard, then OPERA Cloud services will not recognise those custom groups.

Seeded Groups Created in Identity Provider by a Federated Customer

These are groups for various Hospitality Cloud Products in a customer's OCI IAM Identity Domains and are created during provisioning. These groups must be created in a customer's identity provider.

OPERA Cloud

<Property Code>-ADMIN

<Property Code>-OPERACASHIER

<Chain code>-ADMIN

<Chain code>-OPERACASHIER

Guest Experience

<Property Code>-GUESTEXPERIENCE

<Chain Code>-GUESTEXPERIENCE

OPI Cloud

<Property Code>-CCTTRANS

<Property Code>-CCCONF

<Property Code>-PPCONF

<Chain Code>-CCTTRANS

<Chain Code>-CCCONF

<Chain Code>-PPCONF

OHD (These roles are product specific only and are created only if the customer has purchased distribution.)

<Property Code>-HDP_ADMIN

<Property Code>-HDP_CHANNELMANAGEMENT

<Chain Code>-HDP_ADMIN

<Chain Code>-HDP_CHANNELMANAGEMENT

<Chain Code>-HDP_CLUSTERMGMT

OHIP

<Property Code>-DEVELOPERPORTALACCESS

<Chain Code>-DEVELOPERPORTALACCESS

R&A

OC_RNA-APPADMIN

OC_RNA-REPORTINGADMIN

OC_RNA-BIADMIN

OC_RNA-CHAINADMIN