Oracle Hospitality OPERA Cloud Identity Management

Introduction

Release 23.1.1

F92553-01

March 2024

Oracle Hospitality OPERA Cloud Identity Management Introduction, Release 23.1.1

F92553-01

Contents

Preface

Purpose

This document provides an overview of OPERA Cloud Identity Management.

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 1 Revision History

Date	Description of Change
March 2024	Initial Publication

1 Introduction

Oracle Hospitality OPERA Cloud Identity Management is a cloud-ready identity and access management service for OPERA Cloud. OPERA Cloud Identity Management replaces Shared Security Domain (SSD) as the core identity and access management engine for OPERA Cloud.

Components

OPERA Cloud Identity Management consist of following components:

- **Customer OCI IAM Identity Domains**: The Oracle Cloud Infrastructure (OCI) Identity Domain is a container for managing users and roles, federating and provisioning users, securing application integration through Oracle Single Sign-On (SSO) configuration, and registering clients and resources through OAuth administration. It represents a user population in Oracle Cloud Infrastructure and its associated configurations and security settings (such as MFA).
  Every OPERA Cloud customer will be provisioned with two **dedicated** OCI IAM **Oracle Apps identity domains**: one for non-production environments and the other for production environments, which enables customers to use the OCI IAM Identity Domains service to manage their user access to their OPERA Cloud services. OCI IAM **Oracle Apps identity domain** should include almost every Identity and Access Management capability that an OPERA Cloud customer would need; however, if the customer requires additional features or higher limits, the customer can change to a different identity domain type. For more information, see IAM Identity Domain Types in the *Oracle Cloud Infrastructure Documentation*. Oracle Cloud Console (https://cloud.oracle.com) is the administration console for OCI IAM Identity Domain. Customers can refer to the Oracle Cloud Infrastructure Documentation to learn more about the OCI IAM Identity Domains.
- **Oracle Hospitality IAM**: The OCI IAM Identity domain is where Oracle users are stored and managed through the Oracle corporate identity management system. Customer users are never part of this identity domain and authorized Oracle users can access approved customer environments using Oracle Corporate Single Sign-On (SSO).
- **OPERA Cloud Identity Management Portal**: The OPERA Cloud Identity Management Portal is a user and group administration portal for OPERA Cloud Identity Management where OPERA Cloud customers can manage their user and group memberships (role memberships). The OPERA Cloud Identity Management Portal is a user interface which connects with the respective customer dedicated OCI IAM Identity Domain.

  > **Note:**
  >
  > The OPERA Cloud Identity Management Portal will be used by a federated customer only for managing custom groups and managing Oracle user access to sensitive data and data access roles in OPERA Cloud.

- **OPERA Cloud Identity Management SCIM API**: The System for Cross-domain Identity Management (SCIM) is an open specification that standardizes user and group management across applications and allows for the automation of user and group provisioning. Through the SCIM API available in the Oracle Hospitality Integration Platform (OHIP), OPERA Cloud customers can provision and synchronize data for their users and groups. The OPERA Cloud Identity Management SCIM API is an abstraction of the OCI IAM Identity Domain API with OPERA Cloud specific specifications.

Responsibilities

Security in OPERA Cloud is a shared reasonability where there are certain responsibilities for customers and certain responsibilities for Oracle. The below table lists the responsibilities for each.

Table 1-1 Responsibilities

Customer Responsibility	Oracle Responsibility
• User management and group management for users and groups stored in Customer OCI IAM Identity Domains (Customer users). • Security Configurations in Customer OCI IAM Identity Domains. For more information, refer to Securing IAM in the *Oracle Cloud Infrastructure Documentation*. • Identity Federation configurations in the customer’s OCI IAM Identity Domains and in the customer’s identity provider system. • Managing Customer OCI IAM Identity Domains Administrator Roles. For more information, refer to Understanding Administrator Roles in the *Oracle Cloud Infrastructure Documentation*.	• Customer OCI IAM Identity Domains – availability and performance monitoring.

Security Guidelines

Oracle Hospitality creates certain baseline security configurations in the customer OCI IAM Identity Domains during OPERA Cloud provisioning for a customer. Customers are advised to follow below guidelines when using OCI IAM with OPERA Cloud Identity Management.

- Customers are advised to follow the OCI IAM best practices when evaluating configuration changes in customer OCI IAM Identity Domains. For more information, refer to Securing IAM Security Recommendations in the *Oracle Cloud Infrastructure Documentation*.
- Non-Federated customers must manage OPERA Cloud services users and groups only in the OPERA Cloud Identity Management Portal and never directly in the Oracle Cloud Console.
- Federated customers must manage OPERA Cloud services users and groups only in their Identity provider system and never directly in the Oracle Cloud Console.

- Customers are advised to read the Understanding Administrator Roles topic in the *Oracle Cloud Infrastructure Documentation* to learn more about the administrator roles in the OCI IAM Identity domain. When any customer user requires access to the Oracle Cloud console, the customer's OCI IAM Identity domain administrator should assign the **OCICONSOLE_ACCESS** group membership and add users to the category of administrator based on the security levels. An identity domain administrator has super user privileges for a domain. For more information, refer to Adding Identity Domain Administrators in the *Oracle Cloud Infrastructure Documentation*.
- **Sign On Policies** are configured during OPERA Cloud provisioning in the customer OCI IAM Identity Domain to limit user access to the Oracle Cloud console and also to prompt multi-factor authentication (MFA) when accessing the Oracle Cloud console. Customers are advised not to deactivate or edit the "Security Policy for OCI Console" found in Sign-On Policies in their OCI IAM Identity Domains. Tampering sign-on policies in the customer identity domain will impact the MFA prompt while accessing the Oracle Cloud console. This can also allow enterprise admin, chain admin and property admin to access the Oracle Cloud console as these administrators inherit the user administrator role in the respective OCI IAM Identity Domain, which is a security risk.
- To keep their OCI IAM Identity Domains secure, customers are advised to periodically audit configurations, identities, their group memberships, and their administrator role memberships in the customer's OCI IAM identity domains.

2

Creating OCI IAM Identity Domain for a New OPERA Cloud Identity Management Customer

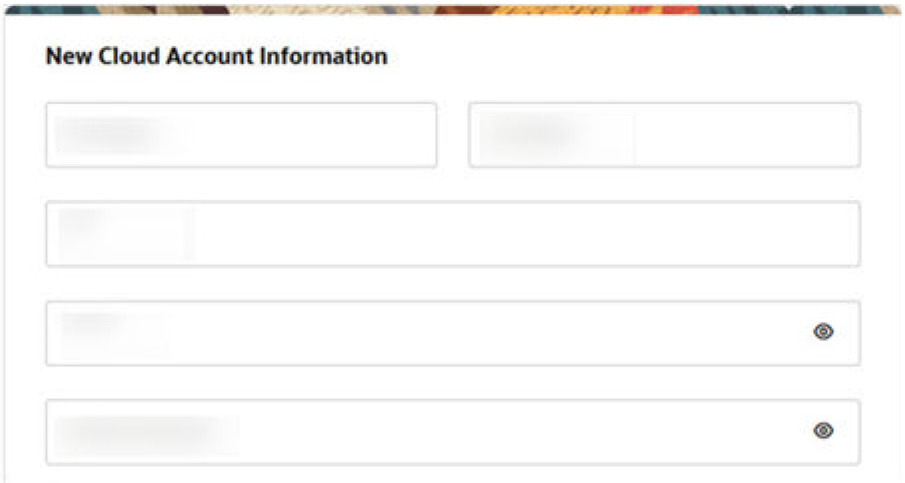
When signing up for an OPERA Cloud subscription, new OPERA Cloud customers receive an email to activate their OCI tenancy. The following sections explain the steps a customer must complete to create a customer-dedicated OCI IAM Identity domain. Customers are also required to note the following OCI IAM Identity Domain details:

- OCI IAM Identity Domain URL
- OCI IAM Identity Domain Region
- OCI Tenancy Name
- OCI Tenancy OCID

> **Note:**
>
> This is a prerequisite for provisioning in OPERA Cloud, and if OCI tenancy sign up is not completed by the customer, it could delay the OPERA Cloud onboarding.

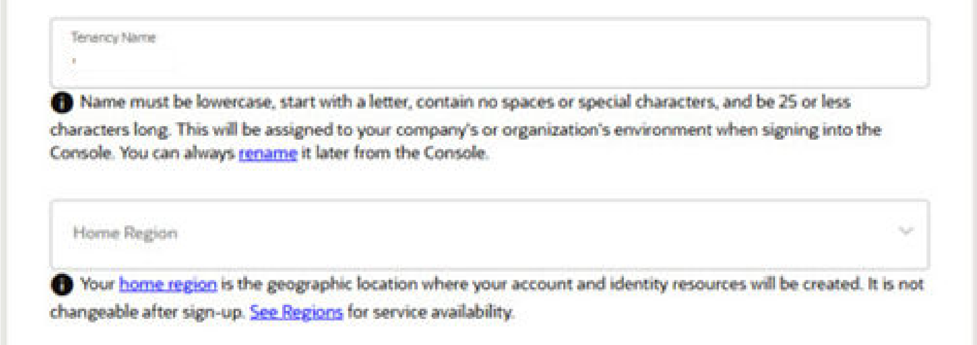
Creating a New Oracle Cloud Infrastructure (OCI) Tenancy

1. Click the **Create New Cloud Account** button in the Action required and add your service(s) to the Oracle Cloud Account email.
2. Enter the account administrator details: **First Name**, **Last Name**, and **Email Address**.
3. Enter and confirm a **Password**. You must specify and confirm a password that adheres to the password policy.



New Cloud Account Information

4. Enter the name of your organization into the **Tenancy Name** field.



Tenancy Name

Name must be lowercase, start with a letter, contain no spaces or special characters, and be 25 or less characters long. This will be assigned to your company's or organization's environment when signing into the Console. You can always rename it later from the Console.

Home Region

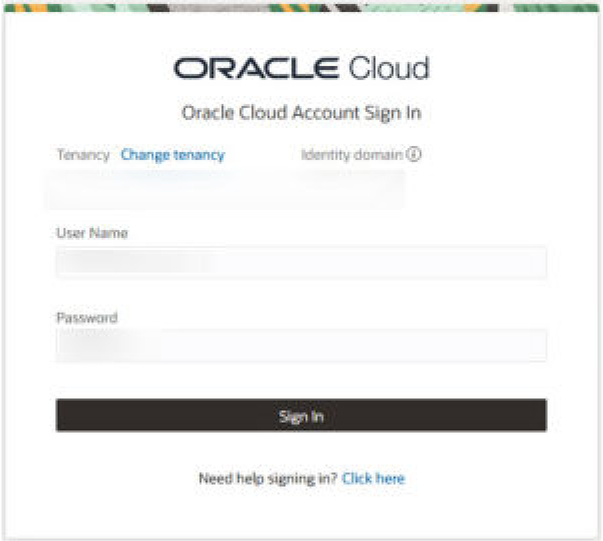
Your home region is the geographic location where your account and identity resources will be created. It is not changeable after sign-up. See Regions for service availability.

5. Select your **OCI Home Region**. Select this as the same OCI region where your OPERA Cloud is provisioned or planned to be provisioned. (Contact your Oracle project manager to find out this information.)
6. Click the **Create Tenancy** button to create your OCI tenancy, which also creates a default OCI IAM Identity Domain in that OCI tenancy.

Verifying the Newly Created Oracle Cloud Infrastructure (OCI) Tenancy

After the new cloud tenancy is created for the customer, the customer must log in and verify the newly created OCI cloud tenancy and verify the newly created OCI IAM Identity Domain. Customers must also note their default OCI IAM Identity Domain details in that OCI Cloud tenancy.

1. Log in to your OCI tenancy by accessing https://cloud.oracle.com and using your **Tenancy Name** and **Admin** user credentials created in the previous section.

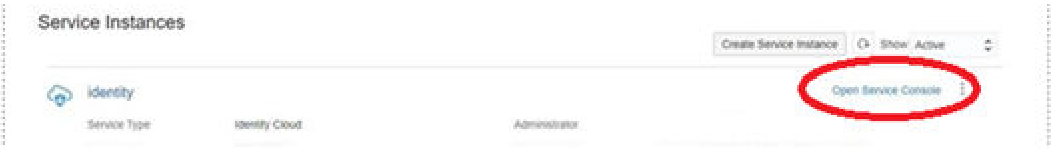


Tenancy: [redacted]

User Name: [redacted]

Password: [redacted]

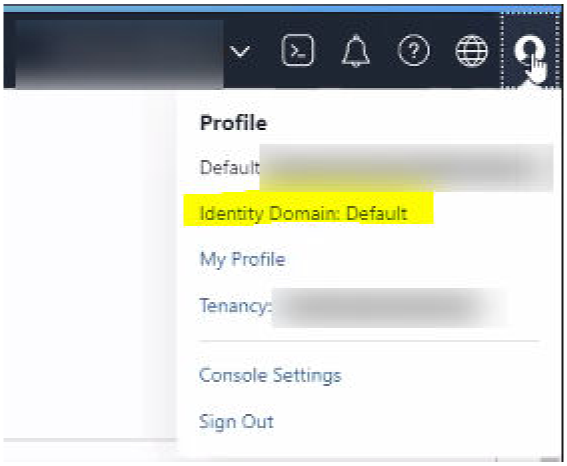
2. Click the **Identity Cloud** option under your Active Services section. If taken directly to the Service: Oracle Identity Cloud Service page, click the **Open Service Console** link at the bottom of the page.



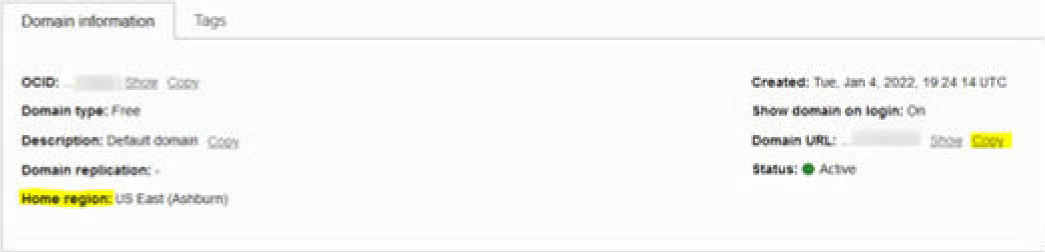
Service Type: Identity Cloud

Administrator

3. From the profile icon, select the **Identity Domain: Default** option.



4. Click the **Copy** link next to the Domain URL to copy the **OCI IAM Identity Domain URL**.



OCID: [redacted] Show Copy

Domain type: Free

Description: Default domain Copy

Domain replication: -

Home region: US East (Ashburn)

Created: Tue, Jan 4, 2022, 19:24:14 UTC

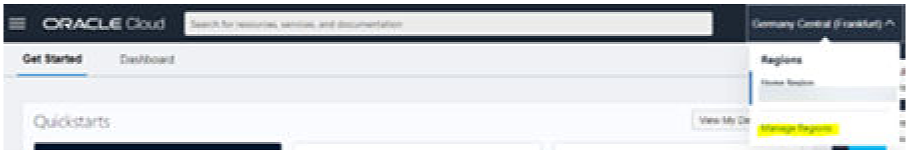
Show domain on login: On

Domain URL: [redacted] Show Copy

Status: ● Active

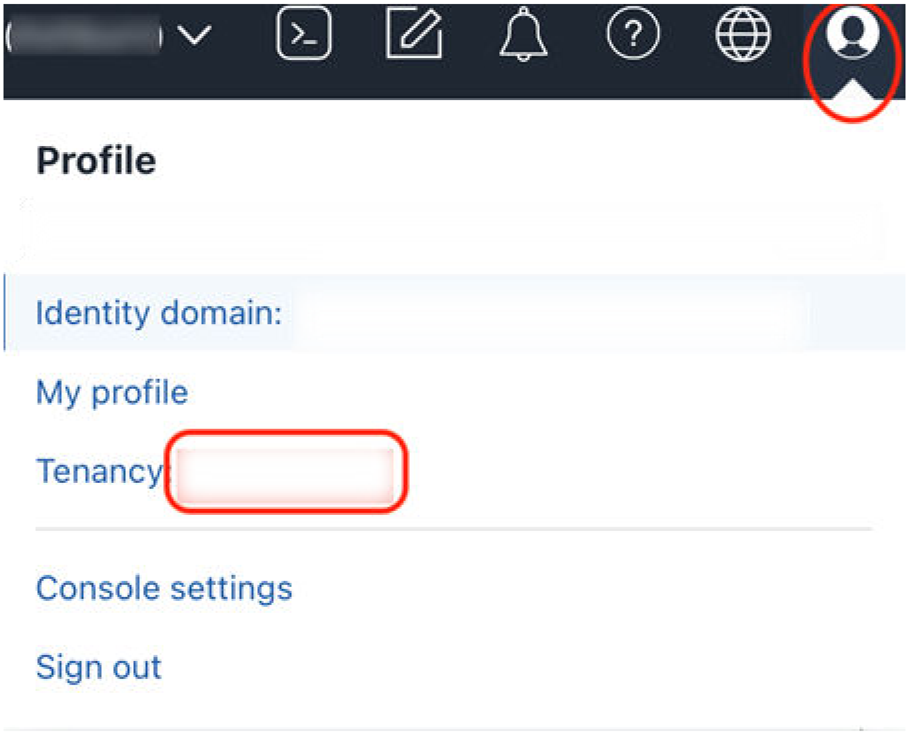
5. Share the copied **Domain URL** and **Home Region** value with your Oracle Sales/ Project Management contact through the email questionnaire. This helps Oracle to further provision the domain with OPERA Cloud Identity Management specific configurations for your property(s)/chain(s).

6. Click the drop-down on your current **Region** and select the **Manage Regions** option.

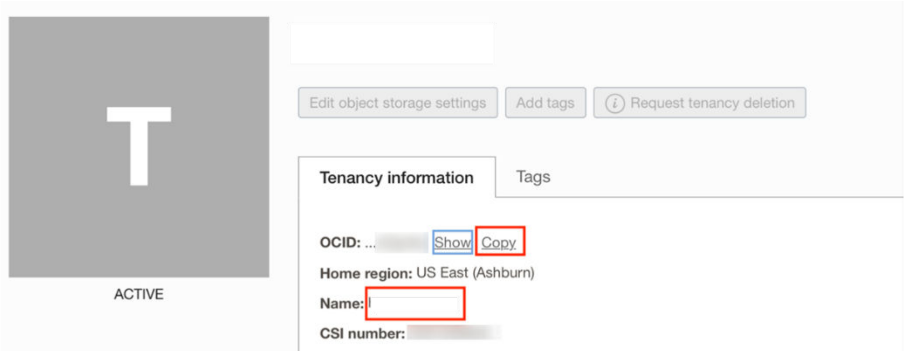


7. Share the **Region Identifier** value with your Oracle Sales/Project Management contact through the email questionnaire.

8. Open **Tenancy** by clicking the **profile icon** on the OCI console and then clicking the **tenancy names**.



9. On the Tenancy page, click **Copy** to copy the **OCID** and **Tenancy Name**.



OCID: ...

Home region: US East (Ashburn)

Name:

CSI number:

10. Share the copied **OCI OCID** and **OCI Tenancy Name** values with your Oracle Sales/Project Management contact through the email questionnaire.

Creating Additional OCI IAM Identity Domains for UAT or Non-Production Environments

1. Open the OCI Console using https://cloud.oracle.com.
2. Open the navigation menu and click **Identity & Security**.
3. Under **Identity**, click **Domains**.
4. Click **Create domain**.
5. On the Create domain page, enter the following information:
   a. **Display name**: Give the identity domain a name. Use only letters, numerals, hyphens, periods, or underscores. The name can contain up to 100 characters. It is highly recommended naming this domain as “UAT.”

   b. **Description:** Enter a description.

   c. **Domain type**: Choose **Free** from the available **Domain types**.

   d. **Domain administrator**: If you want to use your administrative user account for this identity domain, then deselect **Create an administrative user for this account**. Otherwise, enter the details of the user you want to administer this identity domain. Refer to Understanding Administrator Roles in the *Oracle Cloud Infrastructure Documentation* for more information about administrator roles.

   e. Optionally, choose a different compartment. For more information, see Managing Compartments in the *Oracle Cloud Infrastructure Documentation*.

   f. To add tagging, click **Show Advanced Options** and enter the tagging details.
6. Click **Create Domain**.
7. Ensure that the identity domain status is “**Creating**.”
8. Repeat the steps in Verifying the Newly Created Oracle Cloud Infrastructure (OCI) Tenancy to collect the details of the UAT domain.