Oracle Hospitality OPERA Cloud Identity Management

Introduction

Release 25.2
G35085-02
July 2025

Oracle Hospitality OPERA Cloud Identity Management Introduction, Release 25.2

G35085-02

Contents

Preface

1 Introduction

Components 1-1

Responsibilities 1-3

Security Guidelines 1-3

Determining if OPERA Cloud Environment is Using SSD or OPERA Cloud Identity Management 1-4

Primary Work Location 1-5

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

Creating a New Oracle Cloud Infrastructure (OCI) Tenancy 2-1

Verifying the Newly Created Oracle Cloud Infrastructure (OCI) Tenancy 2-2

OCI IAM Identity Domain Replication 2-5

Creating Additional OCI IAM Identity Domains for UAT or Non-Production Environments 2-7

3 Configuring OCI IAM Identity Domain to Allow User Creation without Mandatory Email Requirement

Preface

Purpose

This document provides an overview of OPERA Cloud Identity Management.

Audience

This document is intended for OPERA Cloud Identity Management 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
June 2025	Initial Publication
July 2025	Minor updates to the 'OCI IAM Identity Domain Replication' topic.

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 Multi-Factor Authentication).

  Each OPERA Cloud customer is provided with an Oracle Cloud Infrastructure (OCI) tenancy under the Hospitality Identity Cloud Service (HGBUHIM SKU - CPQ SKU: B94442). The customer is entitled to two dedicated OCI IAM Oracle Apps identity domains within this OCI tenancy: one for non-production environments and one for production environments. This setup allows customers to manage user access to their OPERA Cloud environments through OCI IAM Identity Domains.

  The OCI IAM Oracle Apps identity domain includes the essential Identity and Access Management (IAM) capabilities needed to manage users and their access to OPERA Cloud services. If additional features or higher limits are required, the customer may choose a different identity domain type, which incurs usage-based charges. For details on available identity domain types, refer to the IAM Identity Domain Types page.

> **Note:**
>
> Breaching the limits of the OCI IAM APPS Identity Domain type can negatively impact the performance of OPERA Cloud services. Customers are strongly advised to adhere to the prescribed limits for this domain type; refer to the IAM Identity Domain Types page for detailed information on these limits. The OCI IAM APPS Identity Domain provided for the customer's usage is restricted to the following features only:
>
> - Storing users and groups specific to OPERA Cloud services.
> - Managing user passwords (for non-federated users).
> - Configuring identity providers to establish single sign-on with the customer’s identity system for OPERA Cloud service portals.
> - Enabling multi-factor authentication and setting network perimeters for OPERA Cloud service portals.
> - Using OAuth 2.0 features for OHIP API authentication and authorisation.
> - Utilizing auditing and reporting functions to monitor access to OPERA Cloud services.

- **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 is used by a federated customer only for managing Admin Roles, managing custom groups, copying custom groups across multiple chains or properties, 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.

> **Note:**
>
> **SCIM API Usage**: The SCIM APIs for OPERA Cloud services should only be accessed through OHIP as OHIP publishes the OPERA Cloud Identity Management SCIM APIs. OCI IAM Identity Domain APIs are not to be used for SCIM API access.

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*.

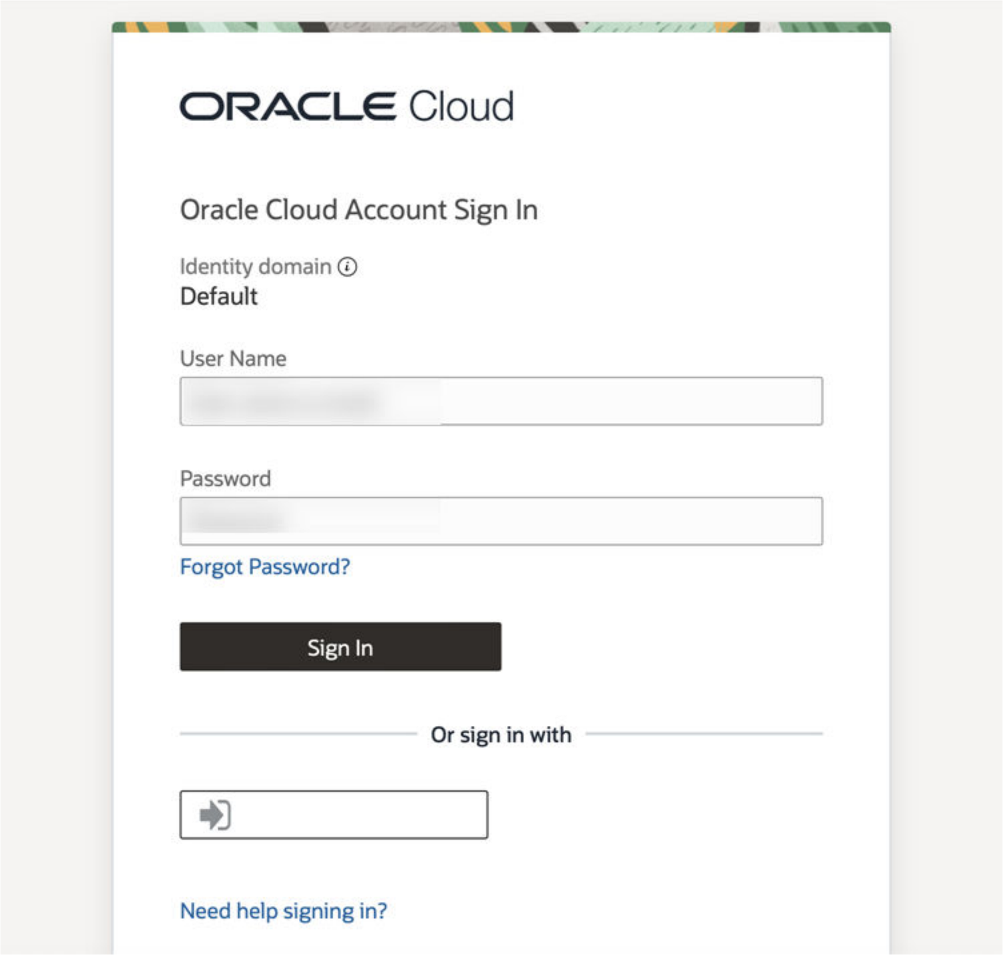
> **Note:**
>
> To avoid losing access to the Oracle cloud console when the only domain administrator leaves the company, it is highly recommended to add multiple administrators under the domain administrator.

- **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.

Determining if OPERA Cloud Environment is Using SSD or OPERA Cloud Identity Management

Shared Security Domain (SSD) is the Identity and Access Management service of OPERA Cloud. OPERA Cloud Identity Management is replacing SSD.

If an OPERA Cloud environment is using OPERA Cloud Identity Management, then the login page has the look and feel of the below screen, and it also has the Identity Domain name on the login page.



ORACLE Cloud

Oracle Cloud Account Sign In

Identity domain ⓘ
Default

User Name

Password

Forgot Password?

Note:

Customers on OCIM have the following OPERA Cloud URL format where <enterprise Id> is the customer's enterprise ID:

https://<hostname>/<enterprise Id>/operacloud

Customers on SSD have the following OPERA Cloud URL format (basically there is no enterprise id):

https://<hostname>/OPERA9/opera/operacloud

Primary Work Location

Every user in OPERA Cloud Identity Management has a Primary Work Location field denoted as “oc_primaryworklocation” in the customer's OCI IAM Identity Domain. The primary work location for a user determines which administrator can manage the user in the OPERA Cloud Identity Management Portal and in OPERA Cloud Role Manager. The primary work location’s value is either an Enterprise ID, a chain code, or a property code and that work location's administrator can manage the user in OPERA Cloud Identity Management. Further, the primary work location can only have a single value (for example, an Enterprise ID, a chain code, or a property code) and can never be assigned with multiple values.

> **Note:**
>
> If the primary work location for a user is set as Enterprise ID, then only an enterprise administrator can manage this user in OPERA Cloud Role Manager. An enterprise administrator is a user with group membership for the group <Enterprise ID>-ADMIN. If this group does not exist in OCI IAM Identity Domain, manually create this group and assign the administrator user as the group member.

2

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

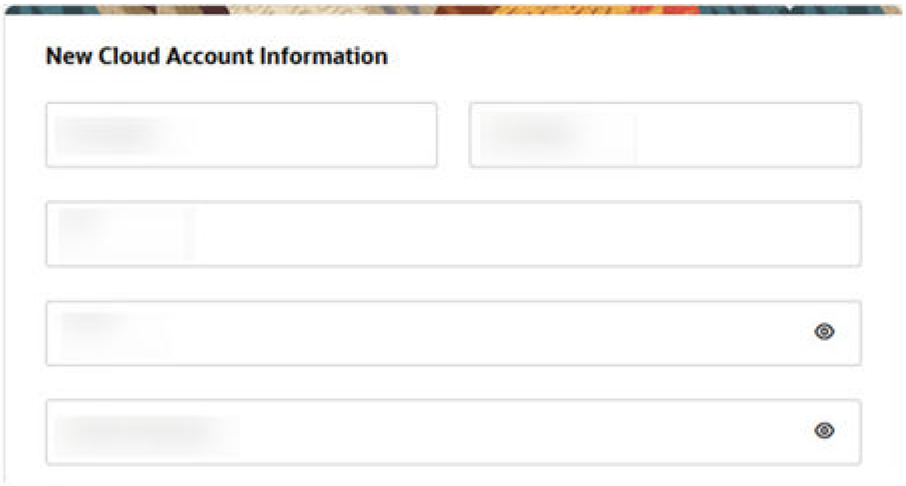
When signing up for an OPERA Cloud subscription, new OPERA Cloud customers receive an email to activate their OCI tenancy. The following sections explain the steps a customer must complete to create a customer-dedicated OCI IAM Identity domain. Customers are also required to note the following OCI IAM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

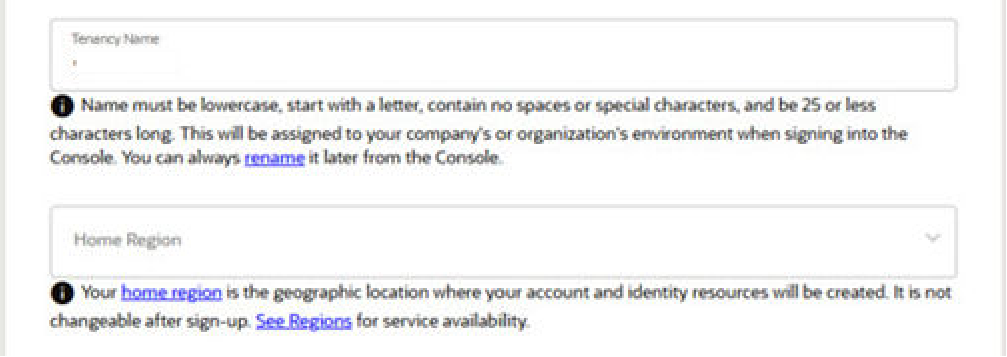
Creating a New Oracle Cloud Infrastructure (OCI) Tenancy

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.)

   It is highly recommended to use any of the below regions as the home region when signing up for an OCI Cloud account so that the OCI IAM Identity Domains are created in that region. Selecting any other region can lead to issues during OPERA Cloud services provisioning.

   Table 2-1 Regions

Region Name	Region Identifier	Region Location
US East (Ashburn)	us-ashburn-1	Ashburn, VA
Germany Central (Frankfurt)	eu-frankfurt-1	Frankfurt, Germany
Saudi Arabia West (Jeddah)	me-jeddah-1	Jeddah, Saudi Arabia
India West (Mumbai)	ap-mumbai-1	Mumbai, India
India South (Hyderabad)	ap-hyderabad-1	Hyderabad, India
Singapore (Singapore)	ap-singapore-1	Singapore,Singapore
Australia Southeast (Melbourne)	ap-melbourne-1	Melbourne, Australia
Australia East (Sydney)	ap-sydney-1	Sydney, Australia

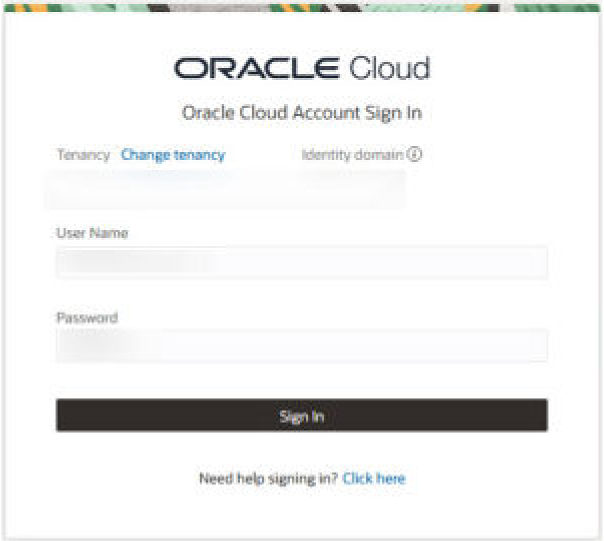
6. Click the **Create Tenancy** button to create your OCI tenancy, which also creates a default OCI IAM Identity Domain in that OCI tenancy.

Verifying the Newly Created Oracle Cloud Infrastructure (OCI) Tenancy

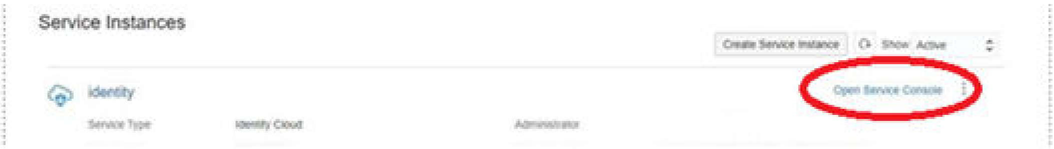
After the new cloud tenancy is created for the customer, the customer must log in and verify the newly created OCI cloud tenancy and verify the newly created OCI IAM Identity Domain. Customers must also note their default OCI IAM Identity Domain details in that OCI Cloud tenancy.

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.

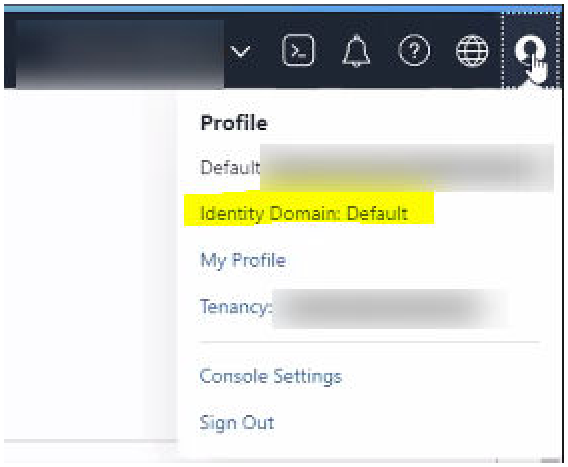
> **Note:**
>
> When signing in for the first time, follow the instructions for Signing In for the First Time in the Oracle Cloud Infrastructure documentation to setup MFA.



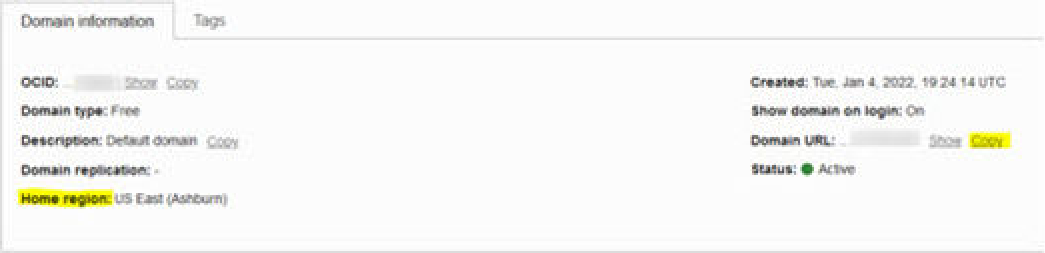
2. Click the **Identity Cloud** option under your Active Services section. If taken directly to the Service: Oracle Identity Cloud Service page, click the **Open Service Console** link at the bottom of the page.



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**.



Domain information | Tags

OCID: [redacted] Show Copy

Domain type: Free

Description: Default domain Copy

Domain replication: -

Home region: US East (Ashburn)

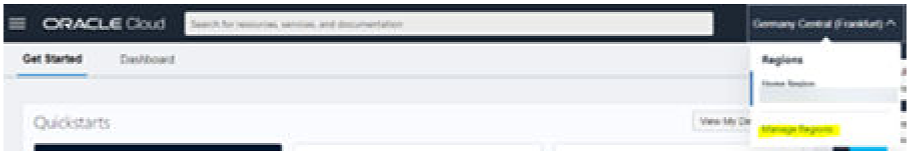
Created: Tue, Jan 4, 2022, 19:24:14 UTC

Show domain on login: On

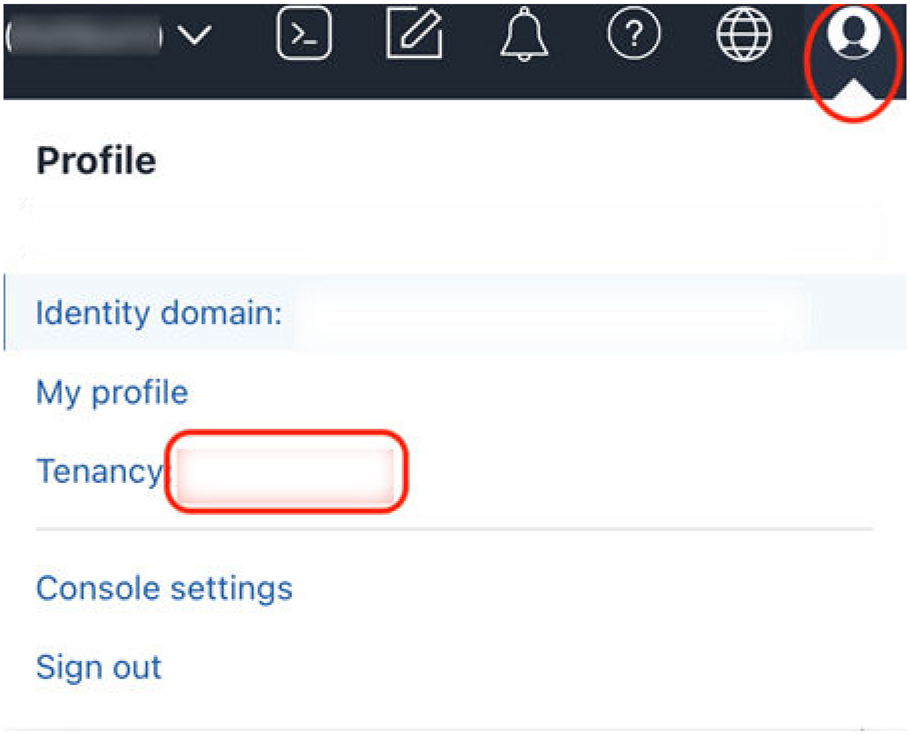
Domain URL: [redacted] Show Copy

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**.



Profile

Identity domain: [redacted]

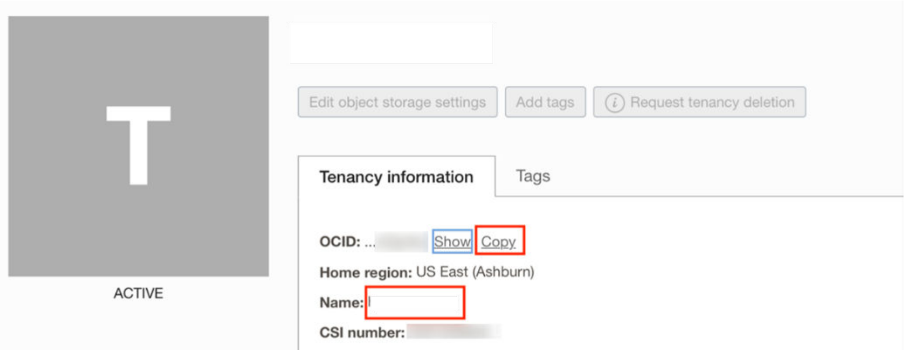
My profile

Tenancy: [redacted]

Console settings

Sign out

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



OCID: ... [redacted]

Home region: US East (Ashburn)

Name:

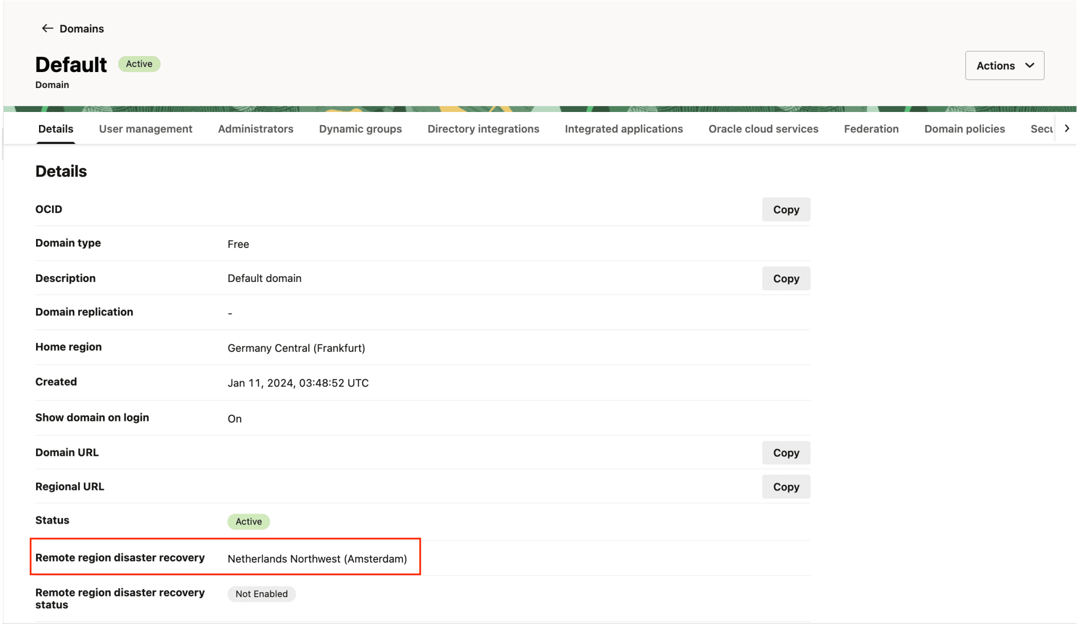
CSI number: [redacted]

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

OCI IAM Identity Domain Replication

Subscribing to Additional Infrastructure Regions

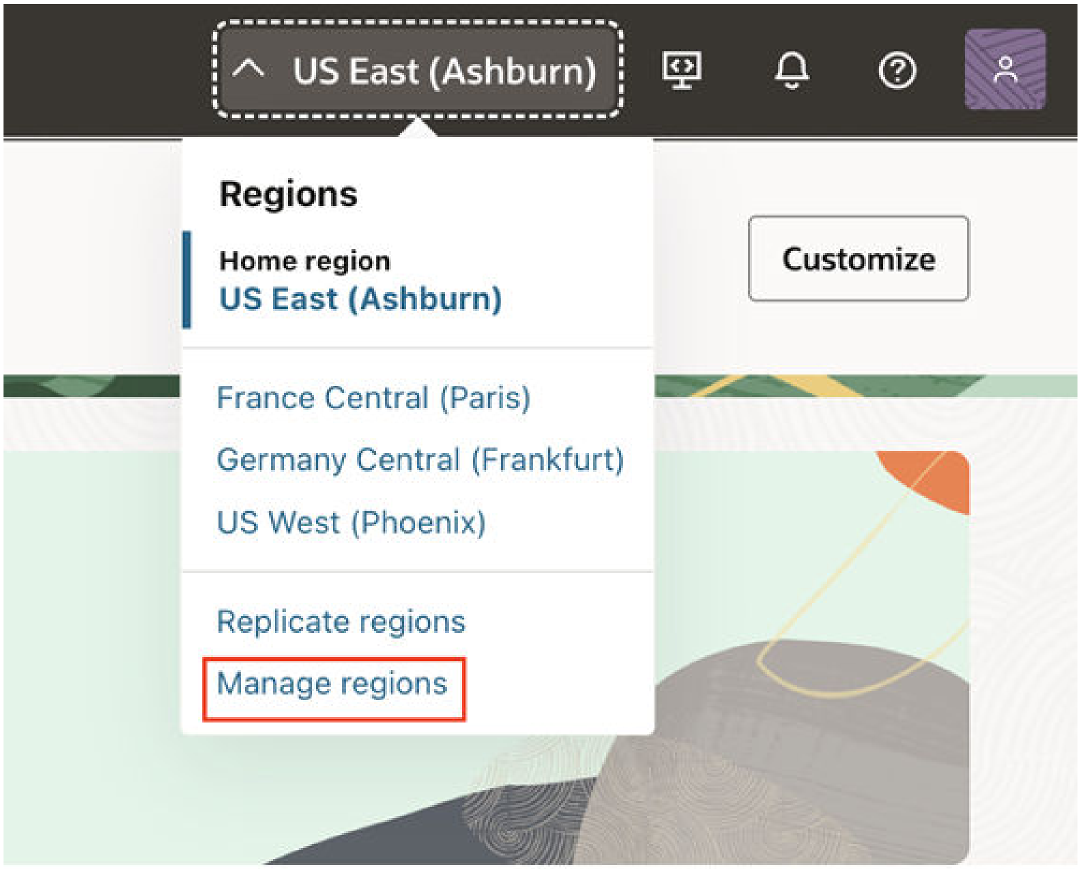
1. Open the OCI Console using https://cloud.oracle.com.
2. Open the navigation menu and select **Identity & Security**. Under Identity, select **Domains**. A table with a list of the identity domains appears.
3. Select the **Default** domain. From the Default domain overview page, note the **Remote Region Disaster Recovery** region.



Details

OCID	
Domain type	Free
Description	Default domain
Domain replication	-
Home region	Germany Central (Frankfurt)
Created	Jan 11, 2024, 03:48:52 UTC
Show domain on login	On
Domain URL	
Regional URL	
Status	Active
Remote region disaster recovery	Netherlands Northwest (Amsterdam)
Remote region disaster recovery status	Not Enabled

4. Click your current **Region name** on the top right corner and then select **Manage regions**. A table shows the list of Oracle Cloud Infrastructure regions to which you are subscribed or unsubscribed.



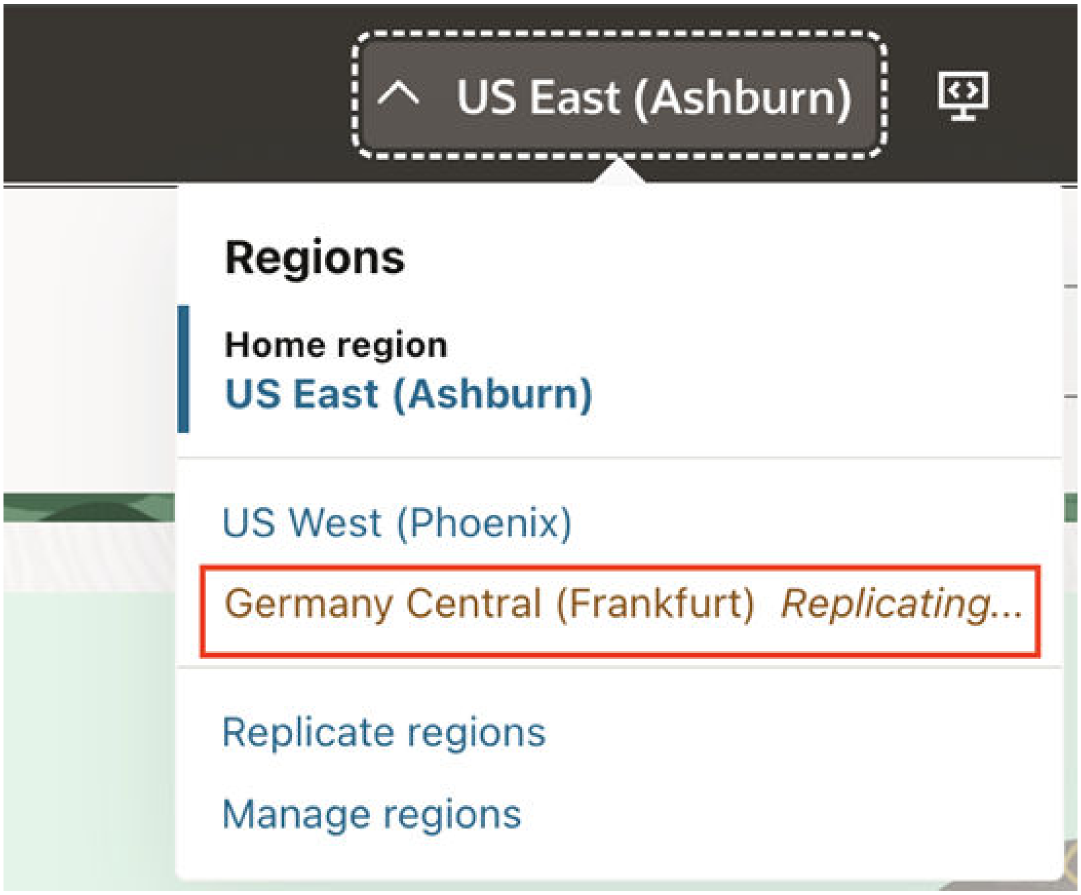
5. Search for the Remote Region Disaster Recovery region noted earlier and Subscribe to the region. To subscribe to a region, Select the Actions menu next to the region and then select **Subscribe**. You can refer to OCI paired Disaster Recovery region to find the Remote region disaster recovery region for your Home Region.

> **Note:**
>
> It could take several minutes to subscribe to a new region.

Verifying Default Identity Domain Replication

Identity domain replication is always enabled for the Default Identity Domain, and the Default Identity Domain automatically replicates to all regions to which the tenant is subscribed.

1. Click your current **Region name** on the top right corner to see the list of regions subscribed in the OCI tenancy. When you subscribe to a new region, the default identity domain automatically replicates to that region and you will see the "Replicating" status from the Region menu as shown below.



Note:

Allow the default domain replication to complete before enabling replication for additional domains.

Verify the "Replicating" status no longer appears on the Region menu. If it no longer appears, this indicates the default domain replication to the newly subscribed region has completed.

You cannot replicate an additional domain to a subscribed region without first completing the default domain replication to that subscribed region.

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 **Add tag** and enter the tagging details.

6. Click **Next**.

7. Under Remote region disaster recovery, select **Enable remote region disaster recovery**. You must be subscribed to the paired region to enable remote region disaster recovery. For example, if your home region is US East (Ashburn), then you must be subscribed to US West (Phoenix).

8. Click **Next** and then click **Create**.

9. Ensure that the additional domain is created and the **Remote region disaster recovery** is in the "**Enabling**" status.

10. Repeat the steps in Verifying the Newly Created Oracle Cloud Infrastructure (OCI) Tenancy to collect the details of the UAT domain.

11. Customers are advised to read the Understanding Administrator Roles topic 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.

> **Note:**
>
> To avoid losing access to the Oracle cloud console when the only domain administrator leaves the company, it is highly recommended to add multiple administrators under the domain administrator.

3 Configuring OCI IAM Identity Domain to Allow User Creation without Mandatory Email Requirement

In OPERA Cloud Identity Management, you can configure the domain to allow user creation without an email requirement. This configuration is valuable for environments where users do not have an email account, and it allows these users to be managed through OPERA Cloud Identity Management.

> **Note:**
>
> For users without an email address, the administrator must create a temporary password for the user. Once the temporary password is created, the administrator must provide the user with the Login URL, the username, and the temporary password. The new user can log in with these credentials and will be prompted to create a password for future login to the user account.

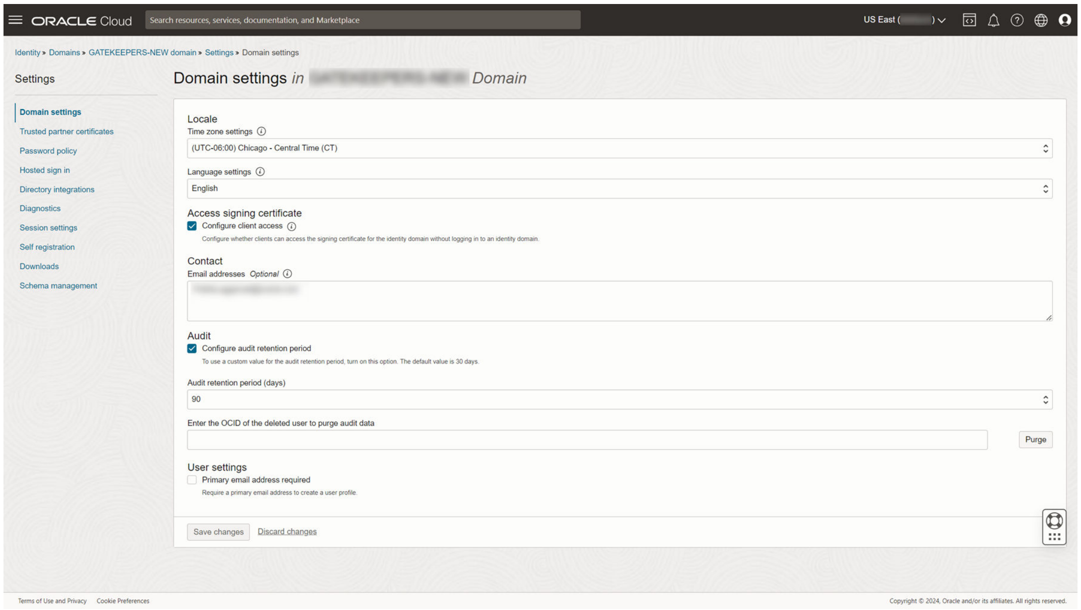
For environments without an email, communication related to user account activation and the forgot password process must be managed with manual communication (that is, by text, in writing, verbal, and so on) between the OPERA Cloud Identity Management Administrator and the user since these users lack an email address that can be used for communication.

> **Note:**
>
> Once an environment is configured with non-mandatory email for users and any user exists without email, you should not reactivate the mandatory email requirement unless all users have been given an email address.

For federated environments, you must configure the respective customer Identity Provider for both user creation without an email address and temporary password generation.

Configure the OCI IAM Identity Domain to change the mandatory requirement for user email during user creation:

1. Log in to the OCI console for your domain with a domain administrator user.
2. Under ‘User settings,’ deselect **Primary email address required**.
3. Click **Save changes**.



Domain settings *in* [redacted] *Domain*

Locale

Time zone settings: (UTC-06:00) Chicago - Central Time (CT)

Language settings: English

Access signing certificate

☑ Configure client access

Configure whether clients can access the signing certificate for the identity domain without logging in to an identity domain.

Contact

Email addresses *Optional*: [redacted]

Audit

☑ Configure audit retention period

To use a custom value for the audit retention period, turn on this option. The default value is 30 days.

Audit retention period (days): 90

Enter the OCID of the deleted user to purge audit data

User settings

☐ Primary email address required

Require a primary email address to create a user profile.

After this change, an email address will no longer be required to create a user.