Enterprise Risk and Finance- Platform Services

Data Security Management Guide

Release 24.03.01
F75076-07
April 2024

Enterprise Risk and Finance- Platform Services Data Security Management Guide, Release 24.03.01

F75076-07

Primary Author:

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Contents

1

About Data Security Management Guide

Data Security Management Guide helps a customer to enable and access the enhanced security features in the Platform Serrvices of Enterprise Risk Platform.

With these enhanced security features, the customer can now restrict the access to Database and also provide their own Encryption key to access their database during an emergency.

For more information about new Security Features, refer Security Enhancement Features .

Target Audience

The Target Audience for this Data Security Management Guide are those customers who want to enable Data Masking. In case of technical issues, they can generate their own Encryption Keys and provide them to Oracle Support, to access their data.

This prevents unnecessary and unplanned data access even by the authorized Oracle Support Personnel.

Security Enhancement Features

The Security features helps to enhance the security of your environments.

The supported security features are:

- Break Glass Support for Environments - Provide access to authorized Oracle Support to access your resources , for troubleshooting any technical issues. This access is valid for a specific time period and also can be given only to specific users with assigned roles and privileges
- Customer-Managed Keys for Oracle Break Glass - Provide your own Encryption Key to authorized Oracle Support, to access their database.
- Data Masking - Hide the confidential, sensitive and Personally Identifiable Information (PII) even from authorized users who have access to a specific environment, permanently.

> **Note:**
>
> These features are enabled based on subscription. To subscribe to these features, contact Oracle Sales team.

2

Creating Your Own Vaults and Keys (Bring Your Own Key)

The customer-managed vaults and keys helps you to restrict the access to your data even by authorized support. You can provide the vault and key and approve access to your data, only when you have to resolve a technical issue.

> **Note:**
>
> This feature is enabled based on subscription. To subscribe to this feature, contact Oracle Sales team.

The process flow for creating customer managed vaults and keys is as follows.

- Checking the prerequisites
- Creating and activating a New Cloud account or accessing an existing Cloud account.
- Creating a new Environment
- Accessing Oracle Identity Cloud Service Console
- Creating New Vaults
- Creating New Keys

Prerequisites for Generating Your Own Vault and Key

Before proceed with the environment creation, ensure to add the required policy to the tenancy.

Add the following policy to the tenancy.

```
define tenancy SAAS as
ocid1.tenancy.oc1..aaaaaaaa6u6nllkls2lt7bht6rtkn6wr7ya7qaigactc7d5pmubpqdixsk
bq
define dynamic-group SAASDB as
ocid1.dynamicgroup.oc1..aaaaaaaarbd43m3gpz2doxhdcol5kkslkdqvefhhccj4i3a4dqjid
7amzydq
define dynamic-group SAASKA as
ocid1.dynamicgroup.oc1..aaaaaaaa6gqppen3vfojuyt6mfbgzcatvvkqiux5qx3cogluuajgy
tulat6q
admit dynamic-group SAASDB of tenancy SAAS to use keys in compartment
FSGBU_ERF
admit dynamic-group SAASKA of tenancy SAAS to read vaults in compartment
FSGBU_ERF
```

```
admit dynamic-group SAASKA of tenancy SAAS to read keys in compartment
FSGBU_ERF
```

For more information about policies, refer to creating a policy using IAM console.

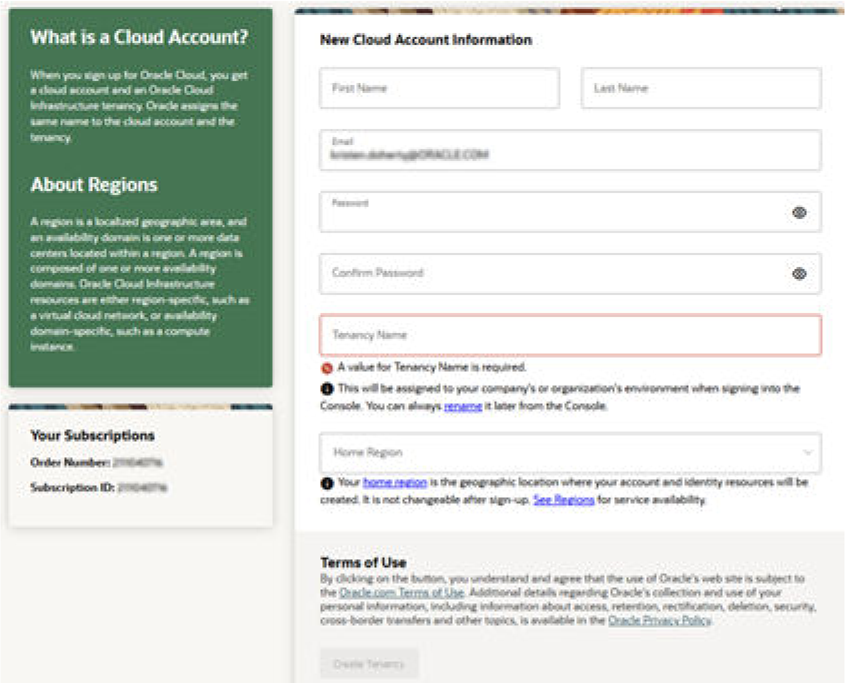
Create and Activate New Cloud Account

After you subscribe to the cloud service, you will receive a **Welcome to Oracle Cloud** email with details to create and activate your cloud account.

To create and activate a new cloud account:

1. Click **Create New Cloud Account** in the email.
2. Complete the **New Cloud Account Information** to sign up.

Figure 2-1 New Cloud Account Information page



What is a Cloud Account?

When you sign up for Oracle Cloud, you get a cloud account and an Oracle Cloud Infrastructure tenancy. Oracle assigns the same name to the cloud account and the tenancy.

About Regions

A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network, or availability domain-specific, such as a compute instance.

Your Subscriptions

Order Number: [redacted]

Subscription ID: [redacted]

New Cloud Account Information

First Name

Last Name

Email
kristen.doherty@ORACLE.COM

Password

Confirm Password

Tenancy Name

A value for Tenancy Name is required.

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.

Terms of Use

By clicking on the button, you understand and agree that the use of Oracle's web site is subject to the Oracle.com Terms of Use. Additional details regarding Oracle's collection and use of your personal information, including information about access, retention, rectification, deletion, security, cross-border transfers and other topics, is available in the Oracle Privacy Policy.

3. Enter the following details:
   - **First Name** and the **Last Name** of the person who will be the cloud administrator.
   - **Email** address of the person who will be the cloud administrator. Instructions to log into the new Oracle Cloud Account will be sent to this email address.
   - **Password** to access the new cloud account.
   - **Tenancy Name**: New **Tenancy Name** to be associated with the cloud account.

> **Note:**
>
> You cannot modify the tenancy name after it is created. Hence, ensure to provide a valid tenancy name, based on your organization's requirements and naming conventions.

- **Home Region**: Select the **Home Region**, where the Identity Resources and Account are located. Check the service availability before selecting the Home Region.

> **Note:**
>
> You can subscribe to additional regions but you cannot modify the home region, after provisioning your tenancy.

4. Click **Create Tenancy** to access the **New Cloud Creation Confirmation** page.

   After successful activation, the cloud account administrator will receive a **Setup Complete** email.

Add to an Existing Oracle Cloud Account

If you already have a Cloud Account associated with your Administrator user name, you can always add another Cloud Service, if required.

To add an existing Cloud account:

1. In the Welcome email, click **Add** to add an existing cloud account.
2. Perform the steps as mentioned in the Access the Oracle Cloud Infrastructure Identity and Access Management (IAM) console.

Accessing the Cloud Account

An Administrator can access the Cloud Account activated and associated with their email address.

After your new cloud account is created and activated, you will receive a **Setup Complete** email, to the email address provided while creating the account.

To access your Cloud account:

- In the **Setup Complete** email, click **Sign In** and enter the **Username** and **Password** to access the **OCI Console** , to log in to the Console. Use the same **Username** and the **Password** that you provided during activation setup.

Create an Environment

After logging into the Oracle Cloud Infrastructure Console, an Administrator can create one or multiple environments/instances for different user groups.

To create an instance:

1. Log in to **Oracle Cloud Infrastructure Console** (OCI).

You can view the list of all the environments (instances) provisioned for the one or multiple cloud applications, with the following details:

- **Name**: The cloud application's instance name.
- **Type**: The instance type.
- **Life cycle status**: The instance status.
- **Region**: The region from where the specific instance is active.
- **Application URL**: The URL to access the instance.

2. Click **Create environment**, to access the list of cloud services to which the customer has subscribed and the region from where these services are operated.
3. (Optional). Select the **Region** to host the OCI environment/instance, from the drop-down list.

   If you are not sure about the region, contact My Oracle Support (MoS).

   > **Note:**
   >
   > You can select the region only for the first environment/subscription and for the additionally added instances, the region cannot be modified.

4. Enter the following **Environment Details**, and click **Create**.
   - **Name**: The name of the new environment or instance.

     > **Note:**
     >
     > You cannot modify the environment name after the environment is created. Hence, ensure to provide a valid environment name, based on your organization's requirements and naming conventions.

   - **Instance type**: Select one of the following instances:
     - **Production**: If the environment is used for Production activities.
     - **Non-production**: If the environment is used for testing and development purposes. For example, a sandbox environment.
   - **Admin email**: The administrator email ID used to log in to the Cloud Console. You can also enter a different email ID that needs to be part of the cloud tenancy. For more details, see Managing Users.
   - **Admin first name** and **Admin last name**: The first and last names of the Administrator.

   The environment details are added to the Oracle Cloud Infrastructure Classic Console under the **Environments** tab (LHS menu). It may take a few hours for the status to change to Active. If there are any issues, you can raise a service ticket with My Oracle Support (MoS).

After the environment is set to **Active**, click the environment name to view the **Environment details**. Click the Service console URL under **Environment Information** to create users and groups.

Access Oracle Identity and Access Management

Oracle Cloud Infrastructure Identity and Access Management (IAM) provides identity and access management features such as authentication, single sign-on (SSO), and identity life cycle management for Oracle Cloud as well as Oracle and non-Oracle applications, whether SaaS, cloud-hosted, or on-premises. Employees, business partners, and customers can access applications at any time, from anywhere, and on any device in a secure manner.

IAM integrates with existing identity stores, external identity providers, and applications across cloud and on-premises to facilitate easy access for end users. It provides the security platform for Oracle Cloud, which allows users to securely and easily access, develop, and deploy business applications such as Oracle Human Capital Management (HCM) and Oracle Sales Cloud, and platform services such as Oracle Java Cloud Service, Oracle Business Intelligence (BI) Cloud Service, and others.
Administrators and users can use IAM to help them effectively and securely create, manage, and use a cloud-based identity management environment without worrying about setting up any infrastructure or platform details.

To add users to your Cloud Services, navigate to the **Oracle Identity and Access Management (IAM)** Console.

To access the **IAM** Console:

1. Browse to Cloud.Oracle.com, to view all the details pertaining to your cloud order.

   Access the service link from the console to start using your subscriber cloud service.
2. Enter the **Cloud Account Name** and click **Next** to access the **IAM Console**.
3. Click **Change tenancy** option if you want to use a different tenancy.
4. Select the **Identity domain** from the drop-down list and click **Next**, to access the **IAM Login** page.
5. Log in with your **Username** and **Password**.

As an Administrator, you can create and manage users with different access rights to the Cloud Service.
For example, the IAM Administrator has superuser privileges for an Oracle Identity and Access Management Domain. This administrator can create users, groups, group memberships, and so on.

Creating New Vaults

Vaults help to restrict unauthorized users from accessing sensitive data, and also prevent unauthorized database changes.

A vault (Vault ID) is added to an environment, while you create an environment. The linked vault and the environment must be in the same tenancy. You can create vaults using OCI Console. For more information, refer to the following topics.

- Best Practices for Setting Up and Managing Vaults and Keys
- Managing Vaults
- Creating New Vaults

Creating New Keys

Oracle Key Vault securely stores the Encryption Keys, Wallets and other Secure Data.

A Key (Key ID) is added to an environment, while you create an environment. The associated key and the new environment must be in the same tenancy. You can create vaults using OCI Console.

> **Note:**
>
> You can apply a new key to an environment only once in 15 days.

For more information, refer to the following topics.

- Best Practices for Setting Up and Managing Vaults and Keys
- Managing Keys

3 Managing Access Requests (Break Glass)

Access requests are raised by the Oracle Support team, to access the customer Database when the customer faces technical issues.

> **Note:**
>
> This feature is enabled based on subscription. To subscribe to this feature, contact Oracle Sales team.

Access requests are valid for a specific time period. You can approve or reject the access requests, based on the assigned Roles and Privileges, within the given time.

Approving/Rejecting Access Requests

When the Oracle Support team requests to access your database, complete the following steps to approve a reqest.

When the Oracle Support wants to access your Data for resolving technical issues, they will raise a request. After proper approval by the Oracle support team, will receive a email from Oracle Support (Managed Access), with the Service Request (SR) number, access level, access duration and the Expiration time. To approve the request:

1. Click the link in the e-mail to login to the OCI Console.

   Make sure to login with required roles and privileges required for request approval.
2. Click **Managed Acces**s, to view the list of **Access requests**.
3. Click the **Request name** to view the Access request details.
4. Click One of the following options to approve/reject the request.
   a. **Approve -** Approve the access request with proper validation.
   b. **Reject -** Decline the access request with reason.

4

Introduction to Data Masking

Data Masking permanently hides the confidential, sensitive and Personally Identifiable Information (PII) even from authorized users who have access to a specific environment.

> **Note:**
>
> This feature is enabled based on subscription. To subscribe to this feature, contact Oracle Sales team.

You can enable data masking on non-production environments as part of the data refresh process from other environments. For more information about data masking, refer About Data Masking and Enabling Data Masking.

Enabling Data Masking

You can raise a request to enable Data Masking using My Oracle Support page.

Before initiating the process of enabling Data Masking, provision the Source and Target Environments.

> **Note:**
>
> The Source Environment is generally a production environment and the Target Environment must always be an Non-Production Environment.

Login to My Oracle Support Page and raise a service request with the following details to enable Data Masking.

- Subscription ID
- Source Environment OCID - The Source Environment is usually a Production Environment.
- Target Environment OCID - Ensure that the target environment is always a Non-Production Environment.