Enterprise Risk and Finance- Platform Services

Data Security Management Guide

Release 25D
G48152-01
November 2025

ORACLE

Enterprise Risk and Finance- Platform Services Data Security Management Guide, Release 25D

G48152-01

Primary Author:

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 guide are the customers who are provisioning Financial Services SaaS Applications. In addition, customers having subscription for Break Glass and BYOK for data refreshes can use those services.

This prevents unnecessary and unplanned data access even by the authorized Oracle support team.

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 secure the databases utilized by SaaS applications.
- Data Redaction - Permanently hide the confidential, sensitive, and Personally Identifiable Information (PII) when performing data refreshes.

> **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..aaaaaaaa6u6nllkls2lt7bht6rtkn6wr7ya7qaigactc7d5pmubpqdixskb
q
define dynamic-group SAASDB as
ocid1.dynamicgroup.oc1..aaaaaaaarbd43m3gpz2doxhdcol5kkslkdqvefhhccj4i3a4dqjid7
amzydq
define dynamic-group SAASKA as
ocid1.dynamicgroup.oc1..aaaaaaaa6gqppen3vfojuyt6mfbgzcatvvkqiux5qx3cogluuajgyt
ulat6q
admit dynamic-group SAASDB of tenancy SAAS to read vaults in compartment
FSGBU_ERF
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.

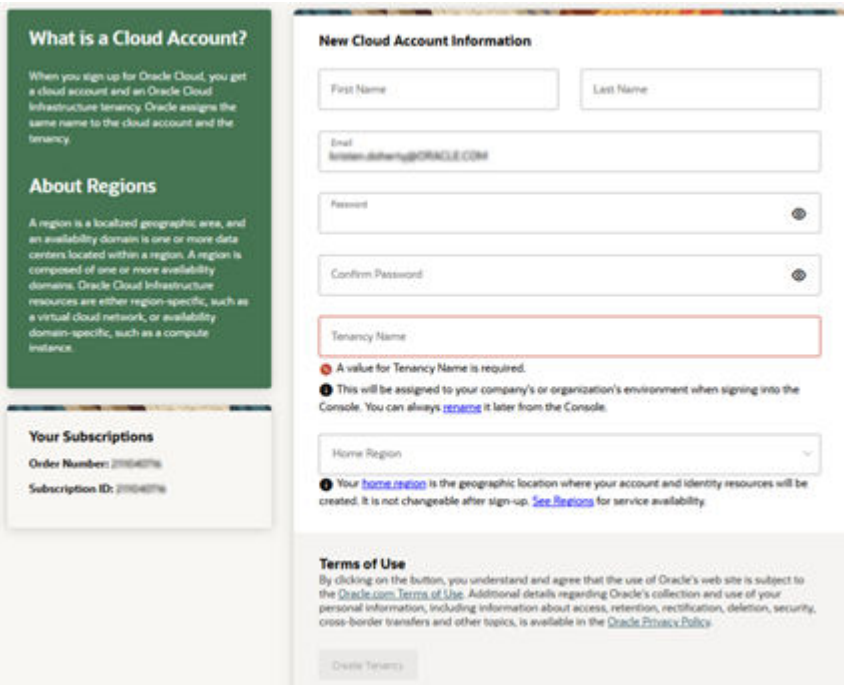
Create and Activate New Cloud Account

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



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 account is located. Check the service availability before selecting the home region.
  For assistance regarding home region selection, contact Oracle support. Existing customers have to ensure that the identity resources are located in 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 **Get Started Now with Oracle Cloud** email.

Add to an Existing Oracle Cloud Account

If you already have a cloud account associated with your administrator user name, you can add the newly subscribed cloud service to that account.

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 **Get Started Now with Oracle Cloud** email, to the email address provided while creating the account.

To access your Cloud account:

1. In the **Get Started Now with Oracle Cloud** email, click **Sign In**.
2. Enter the **Tenancy** name and click **Continue**.
3. Enter the **Username** and **Password** to log in to the **OCI Console** .

   Use the same **Username** and the **Password** that you provided during activation setup.
4. After successful login, proceed with the multi-factor authentication. Select the configured authentication mode and enter the OTP generated using the Oracle Mobile Authenticator application.

   Once the MFA is successfully completed, you can access the **Environment Page**.

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 environment/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. From **My Applications**, click the application in which you want to create an environment. Example: Oracle Financial Services Crime and Compliance Management Anti Money Laundering.
3. On the **Overview** page, click **Environments**.
4. From the **Compartments** drop-down list, select the compartment in which you want to create an environment.
5. Click **Create**, to access the list of cloud services to which the customer has subscribed and the region from where these services are operated.
6. (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.

7. 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. Log in 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. Ensure that the displayed identity domain matches the expected value.

> **Note**
>
> Cloud environments are created under the **Default** identity domain. If you need to assign your environment to a different identity domain, raise a Service Request.

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 protect data in SaaS databases from unauthorized access.

Keys are created in these vaults and shared during / after environment creation as master encryption keys on the database.

- 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.

(Optional). You can add a key (Key ID) to an environment, while you create an environment. You can create vaults using OCI Console or OCI APIs and SDK.

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

- Best practices for setting up and managing vaults and keys
- Managing keys

3

Managing Access Requests (Break Glass)

When the Oracle Support wants to access your Data for resolving technical issues, they will raise an access request.

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

Authorized Oracle support members can create access requests for temporary access to cloud resources. Access requests are valid for a specific time period. Approvers 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 creates a temporary access request to access your database, approvers can approve/reject the request within the time period.

The approver is identified based on the assigned approval templates.

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 log in to the OCI Console.

   Make sure to log in with required roles and privileges required for request approval.
2. Click **Managed Access**, 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:
   a. **Approve** - Approve the access request with proper validation.
   b. **Reject** - Decline the access request with reason.

4

Redaction Framework

OFSAAI is enhanced to enable masking of sensitive data and Personal Identification Information (PII) to adhere to Regulations and Privacy Policies.

Oracle Data Redaction provides selective, on-the-fly redaction of sensitive data in database query results prior to display by applications so that unauthorized users cannot view the sensitive data.

The stored data remains unaltered, while displayed data is transformed to a pattern that does not contain any identifiable information.

> **Note**
>
> Redaction is supported only on Oracle database.

Redaction Functions

Use functions to define the type of redaction to be applied.

To define a redaction function:

1. Click **Data Management Tools** > **Redaction Framework** and select **Redaction Functions**. The **Redaction Functions Summary** screen appears.
2. Click **Add** and provide the following details:
3. **Redact Function Name**: Specify a name for the function. Example: Email_ID.
4. **Description**: Provide a description for the function. Example: Function to redact email IDs.
5. **Redact Type**: Select the redaction type to be applied.
   - **Full**: You can redact all of the contents of the column data. The redacted value returned to the querying application user depends on the data type of the column. For example, columns of the NUMBER data type are redacted with a zero (0), and character data types are redacted with a single space.
   - **Partial Trailing**: You can hide or obscure a part of the data at the end of a column value. For example, you can redact a Social Security number with asterisks (*), except for the initial 4 digits.

     > **Note**
     >
     > Only VARCHAR and VARCHAR2 are supported.

   - **Partial Leading**: You can hide or obscure a part of the data at the beginning of a column value. For example, you can redact a Social Security number with asterisks (*), except for the last 4 digits.

> **Note**
>
> Only VARCHAR and VARCHAR2 are supported.

- **No of characters**: (Available only if partial redaction is applied). Specify the number of characters to be redacted.

> **Note**
>
> You can't apply partial redaction to date type columns. Only full redaction is applicable to date type columns.

6. Click **Apply**.

Redaction Policies

You can use policies to map redaction functions to classification codes.

A classification code is a logical abstraction for a table column. Example: Social Security Number. These codes are pre-seeded.

By mapping classification codes to redaction functions, you can redact the underlying table column.

View redaction policies

You can view the defined redaction policies using the Redaction Policies Summary screen.

To view the redaction policies:

1. Click **Data Management Tools** > **Redaction Framework** and select **Redaction Policies**.

   The **Redaction Policies Summary** screen appears.

2. Enter the text of the second step here.

   See the table below for fields and their description.

Table 4-1 Redaction Policies Summary

Field	Description
Classification Name	Pre-seeded classification code name.
Redact Functions	Redact function name
Version	The latest version of the classification.
Request Type	Types of request: • Refresh: Map redaction as per latest addition of table columns. • Unmap: Remove redaction. • Map: Apply redaction
Status	Policy status
Policy Applied On	Date on which the policy was applied.
Created By	The user who created the policy.

Table 4-1 (Cont.) Redaction Policies Summary

Field	Description
Created Date	Date of creation of the policy.
Actions	You can perform the following actions: a. Edit b. Drop c. Refresh d. View

3. Click the **Actions** menu corresponding to the policy you want to view and select **View**.

The Redaction Policies Preview screen appears containing details of the policy.

Create redaction policies

Perform the following steps to create a redaction policy:

1. Click **Data Management Tools** > **Redaction Framework** and select **Redaction Policies**.

   The **Redaction Policies Summary** screen appears.
2. Click **Add**.
3. Select the classification from the **Classification Name** drop-down list.
4. Select the function to be mapped to the classification name, from the **Redact Function Name** drop-down list.
5. Click **Map**.

   The affected table and columns are displayed as a result of this mapping.
6. Click **Submit for Approval** or click **Reject** to cancel the mapping.

Modify a redaction policy

Perform the following steps to modify a redaction policy.

1. Click **Data Management Tools** > **Redaction Framework** and select **Redaction Policies**.

   The **Redaction Policies Summary** screen appears.
2. Click the **Actions** menu corresponding to the policy you want to modify and select **Edit**.
3. Select the required function from the **Redact Function Name** drop-down list.
4. Click **Update Map**.

   The screen displays the affected table and columns as a result of this modification.
5. Verify the details and click **Submit for Approval**.

Drop a redaction policy

Perform the following steps to drop a redaction policy.

1. Click **Data Management Tools** > **Redaction Framework** and select **Redaction Policies**.

The **Redaction Policies Summary** screen appears.

2. Click the **Actions** menu corresponding to the policy you want to drop and select **Drop**.

   The screen displays the affected table and columns as a result of this drop action.

3. Verify the details and click **Submit for Approval**.

Refresh a redaction policy

Use the Refresh feature to extend redaction to newly added columns within an existing policy, preserving previous redactions.

To refresh a redaction policy:

1. Click **Data Management Tools** > **Redaction Framework** and select **Redaction Policies**.

   The **Redaction Policies Summary** screen appears.

2. Click the **Actions** menu corresponding to the policy you want to refresh and select **Refresh**.

   The **Refresh Dialog** appears.

3. Click **Run Refresh**.

Redaction Approval

You can approve or reject the redaction policies, using the Redaction Policies Authorization screen.

You must have the REDACT_AUTH role to approve/reject the policies.

Perform the following steps:

1. Click **Data Management Tools** > **Redaction Framework** and select **Redaction Approval**. The **Redaction Policies Authorization Summary** screen appears listing the policies awaiting approval/rejection.
2. Click the **Actions** menu corresponding to the policy you want to approve/reject. The screen displays the affected tables and columns as a result of approving/rejecting this policy.
3. Verify the details and click **Approve & Execute** to approve the policy. Or, click **Reject** to cancel the policy.
4. Depending on the selection, provide the Approver Comments/Rejected Comments and click the **Approve & Execute**/**Reject** button once again to complete the action.