Enterprise Risk and Finance- Platform Services

Data Security Management Guide

Release 23.09.01

F75076-02

October 2023

Enterprise Risk and Finance- Platform Services Data Security Management Guide, Release 23.09.01

F75076-02

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 Servrices 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 Enhancment 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 Enhancment Features

The Security Features helps you to make your environment secure. Some of these features are bundled with the Platform Services Subscription. You can also purchase any of the following features as add-on subscriptions.

- 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.

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.

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.
- Accessing Oracle Identity Cloud Service Console
- Creating a new Environment
- Creating New Vaults
- Creating New Keys

Prerequisites for Generating your own Vault and Key

Before proceed with the environment creation, ensure to add the following policies to the tenancy.

- **AFCS** - fsgbuerf-environment-family
- **PBSM** - fsgbupbsm-environment

Include the following code.

```
define tenancy SAAS as

ocid1.tenancy.oc1..aaaaaaaa6u6nllkls2lt7bht6rtkn6wr7ya7qaigactc7d5pmubpqdixsk
bqdefine dynamic-group SAASDB as

ocid1.dynamicgroup.oc1..aaaaaaaarbd43m3gpz2doxhdcol5kkslkdqvefhhccj4i3a4dqjid
7amzydqdefine dynamic-group SAASKA as

ocid1.dynamicgroup.oc1..aaaaaaaa6gqppen3vfojuyt6mfbgzcatvvkqiux5qx3cogluuajgy
tulat6qadmit dynamic-group SAASDB of tenancy SAAS to use keys in compartment
FSGBU_ERFadmit dynamic-group SAASKA of tenancy SAAS to read vaults in
compartment FSGBU_ERFadmit dynamic-group SAASKA of tenancy SAAS to read keys
in compartment
    FSGBU_ERF
```

Create and Activate your Cloud Account

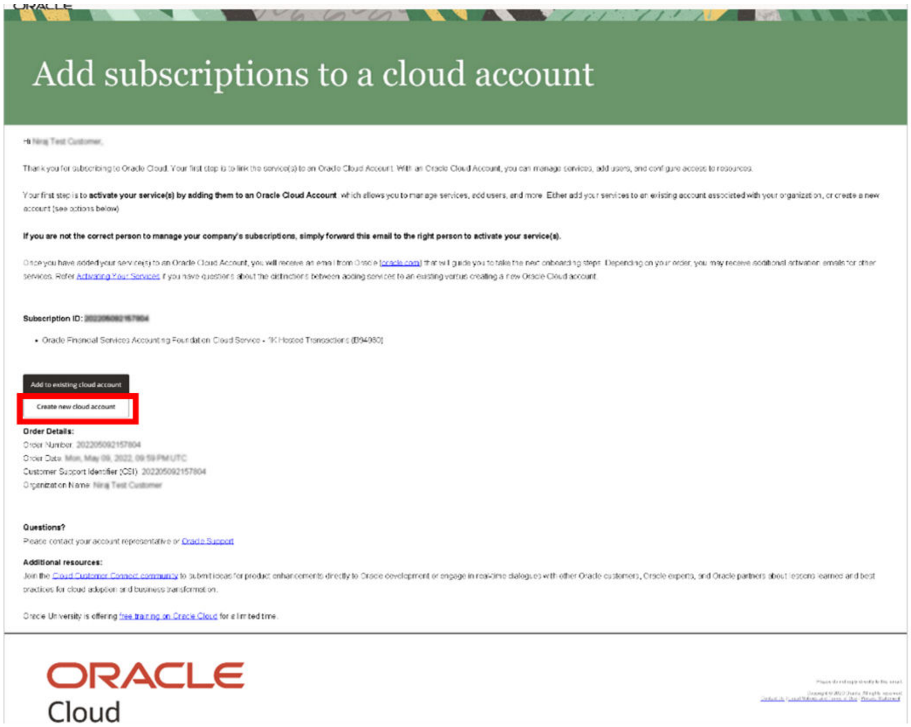
If you are a new Oracle Cloud Applications User, you will receive a Welcome to Oracle Cloud email that asks you to activate your Cloud Account. Follow the instructions in the email to create and activate your new Cloud Account.

You will then receive a follow-up email with the information you need to sign in and start using your Cloud Applications.

As an Administrator, to create and activate your new Cloud Account, perform the following steps:

1. Click **Create New Cloud Account** in the email.

Figure 2-1 Illustration of Welcome to Oracle Cloud - Setup Your Account Email



Add subscriptions to a cloud account

Hi [redacted]

Thank you for subscribing to Oracle Cloud. Your first step is to link the service(s) to an Oracle Cloud Account. With an Oracle Cloud Account, you can manage services, add users, and configure access to resources.

Your first step is to **activate your service(s) by adding them to an Oracle Cloud Account**, which allows you to manage services, add users, and more. Either add your services to an existing account associated with your organization, or create a new account (see options below)

If you are not the correct person to manage your company's subscriptions, simply forward this email to the right person to activate your service(s).

Once you have added your service(s) to an Oracle Cloud Account, you will receive an email from Oracle (oracle.com) that will guide you to take the next onboarding steps. Depending on your order, you may receive additional activation emails for other services. Refer Activating Your Services if you have questions about the distinctions between adding services to an existing versus creating a new Oracle Cloud account.

Subscription ID: [redacted]

- Oracle Financial Services Accounting Foundation Cloud Service - 1K Hosted Transactions (B94980)

Order Details:
Order Number: 202205092157804
Order Date: [redacted]
Customer Support Identifier (CSI): 202205092157804
Organization Name: [redacted]

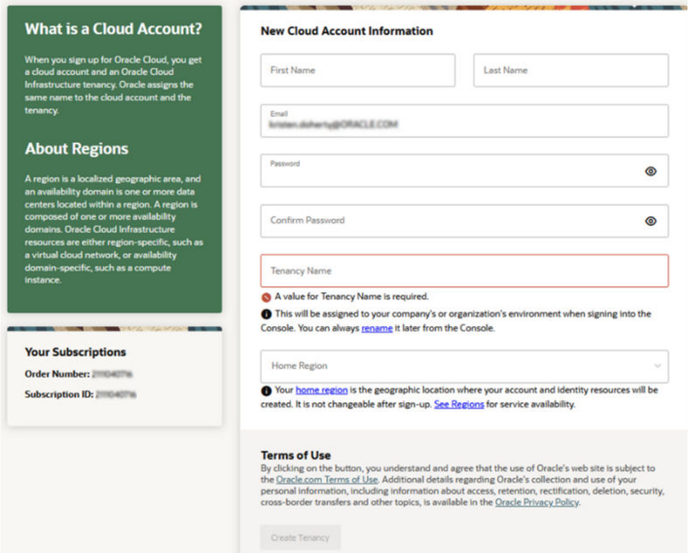
Questions?
Please contact your account representative or Oracle Support

Additional resources:
Join the Cloud Customer Connect community to submit ideas for product enhancements directly to Oracle development or engage in real-time dialogues with other Oracle customers, Oracle experts, and Oracle partners about lessons learned and best practices for cloud adoption and business transformation.

Oracle University is offering free training on Oracle Cloud for a limited time.

2. Complete the **New Cloud Account Information** Form to sign up.

Figure 2-2 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
[redacted]

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.

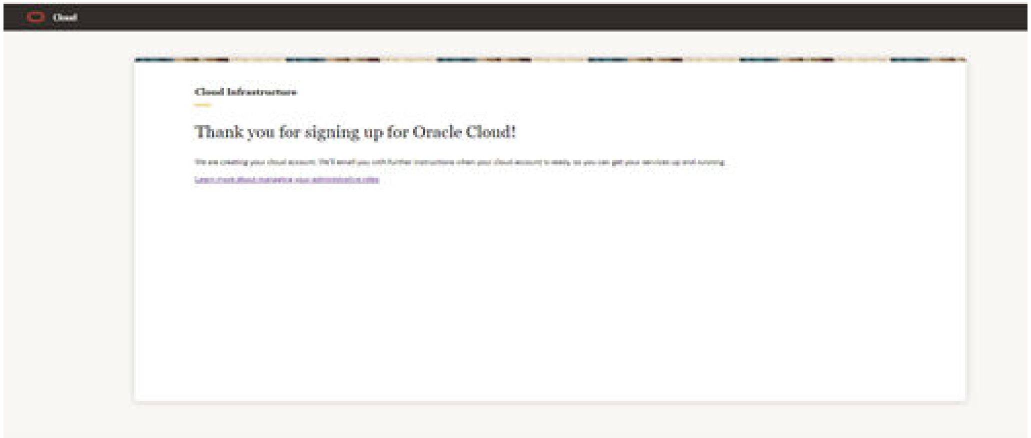
Terms of Use

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.

Enter the following details:

- **First Name** and the **Last Name**.
- **Email**: Provide the same email address which you had given to receive the Welcome email.
  Instructions to log into your new Oracle Cloud Account will be sent to this email address.
- **Password** to access the New Cloud Account.
- Re-enter the **Password** for confirmation.
  Make a note of the credentials. The same is required to log in after receiving the Activation email.
- **Tenancy Name**: New Tenancy name to be associated with the Cloud Account.
- **Home Region**: Select your Home Region, where the Identity Resources and Account are located. Check the service availability before selecting the Home Region.
- Click **Create Tenancy**.
  The New Cloud Creation Confirmation Screen is displayed.

Figure 2-3 Oracle Cloud Creation Confirmation Screen



Cloud Infrastructure

Thank you for signing up for Oracle Cloud!

We are creating your cloud account. We'll email you with further instructions when your cloud account is ready, so you can get your services up and running.

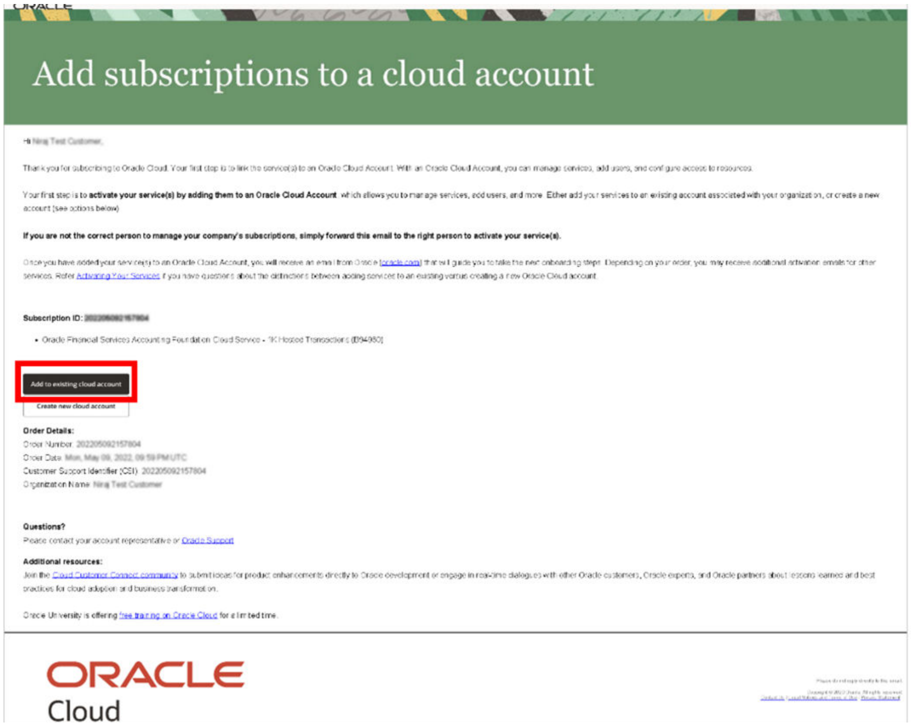
Learn more about managing your administration roles

After successful activation, you'll receive a Setup Complete Email.

Add to Existing Cloud Account

As an Administrator, if you already own a Cloud Account and need to use the Accounting Foundation Cloud Service (AFCS), perform the following steps:

1. In the Welcome email, click **Add to existing cloud** account option.



Add subscriptions to a cloud account

Hi [redacted],

Thank you for subscribing to Oracle Cloud. Your first step is to link the service(s) to an Oracle Cloud Account. With an Oracle Cloud Account, you can manage services, add users, and configure access to resources.

Your first step is to **activate your service(s) by adding them to an Oracle Cloud Account**, which allows you to manage services, add users, and more. Either add your services to an existing account associated with your organization, or create a new account (see options below)

If you are not the correct person to manage your company's subscriptions, simply forward this email to the right person to activate your service(s).

Once you have added your service(s) to an Oracle Cloud Account, you will receive an email from Oracle (oracle.com) that will guide you to take the next onboarding steps. Depending on your order, you may receive additional activation emails for other services. Refer Activating Your Services if you have questions about the distinctions between adding services to an existing versus creating a new Oracle Cloud account.

Subscription ID: [redacted]

- Oracle Financial Services Accounting Foundation Cloud Service - 1K Hosted Transactions (B94980)

Order Details:
Order Number: 202205092157804
Order Date: [redacted]
Customer Support Identifier (CSI): 202205092157804
Organization Name: [redacted]

Questions?
Please contact your account representative or Oracle Support

Additional resources:
Join the Cloud Customer Connect community to submit ideas for product enhancements directly to Oracle development or engage in real-time dialogues with other Oracle customers, Oracle experts, and Oracle partners about lessons learned and best practices for cloud adoption and business transformation.

Oracle University is offering free training on Oracle Cloud for a limited time.

Please do not reply directly to this email.
Copyright © 2022 Oracle. All rights reserved.
Contact Us | Legal Notices and Terms of Use | Privacy Statement

2. Perform the steps as mentioned in the Access the Oracle Identity Cloud Service Console section.

Access the Cloud Account

As an Administrator, to access the Cloud Account:

1. In the Setup Complete email, click Sign In.
2. Enter the Username and Password to access the **Oracle Cloud Console** URL.

   Use the same Username and Password that you provided during activation setup.
3. Reset the Password.
4. Relog in to **Oracle Cloud Infrastructure Classic Console** using the new Password.
5. Navigate to the **Oracle Cloud Infrastructure Classic Console**, the Application URLs are displayed.

Access the Oracle Identity Cloud Service Console

The Oracle Identity Cloud Service integrates directly with existing directories and Identity Management Systems and makes it easy for users to get access to applications. It provides the Security Platform for Oracle Cloud, which allows users to securely and easily access, develop, and deploy business applications such as Oracle Accounting Foundation Cloud Service (AFCS) and Profitability and Balance Sheet Management Cloud Service (PBSM).

Administrators and Application Users can use Oracle Identity Cloud Service 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.

Creating an Environment

This topic provides the procedure for creating Application specific environments.

After creating and activating your Cloud Account, you can login to your cloud account and access the Environments associated with that tenancy.

- Refer to the Prerequisites and add the required policies to the tenancy.
- The Vault and Key must be created in the same tenancy as the environment, before proceeding with the environment creation.

1. Select the **Compartment** from the drop-down list to view the Environments list.

   The environment list page is displayed.
2. Click **Create** to open the **Create Environment** page.
3. Select the **Region** from the drop-down list.
4. Enter an Unique **Name** for your environment.
5. Select one of the following **Instance Type** for the new environment.
   - **Production** - Set your environment to Production, if it is created for day-to-day usage, with authorized users having assigned roles and privileges.
   - **Non-Production** - Set your environment to non-production, if the setup is used for development, testing or trial purpose.
6. Provide the valid **Admin e-mail ID**, **Admin First Name** and **Admin Last Name** of the authorized Administrator of this environment.

7. Enter the **Last Name** of the Administrator.
8. Click **Show Advanced options**.

   The options to change the compartment, encryption keys and encryption tags is displayed.
9. Access the **Encryption** tab.
10. Select the option **Encrypt Using Customer Managed Keys**.

    When this option is selected, the authorized Oracle Support can access your database, after you approve their access request and provide the Encryption Key.
11. Select the **Vault ID** of the Vault to be associated with the environment, from the drop-down list.

    The vault should exist in the same tenancy. For more information, refer Creating New Vaults .
12. Click the Encryption tab.
13. Select the **Key ID** of the key to be associated with the environment, from the drop-down list .

    The key should exist in the same tenancy. For more information, refer Creating New Keys.
14. Click **Create**.

    A welcome email with sign-in instructions is sent to the Admin email address entered during environment creation, after successful creation of an environment.

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.

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.

For more information, refer:

- Approving/Rejecting Access Requests

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. To access the environment, they need to provide a Encryption Key given the customer.

You can enable data masking on Non-Production Environments. . For more information about Data Masking, refer About Data Masking.

To enable Data Masking, refer 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.