Enterprise Risk and Finance- Platform Services

Data Security Management Guide



Release 23.09.01 F75076-02 October 2023

ORACLE

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

F75076-02

Copyright © 2022, 2022, Oracle and/or its affiliates.

Primary Author:

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1	About Data Security Management Guide			
	Target Audience Security Enhancment Features	1-1 1-1		
2	Creating Your Own Vaults and Keys (Bring Your Own Key)			
	Prerequisites for Generating your own Vault and Key	2-1		
	Create and Activate your Cloud Account	2-2		
	Add to Existing Cloud Account	2-4		
	Access the Cloud Account	2-5		
	Access the Oracle Identity Cloud Service Console	2-5		
	Creating an Environment	2-5		
	Creating New Vaults	2-6		
	Creating New Keys	2-6		
3	Managing Access Requests (Break Glass)			
	Approving/Rejecting Access Requests	3-1		
4	Introduction to Data Masking			
	Enabling Data Masking	4-1		



1 About Data Security Management Guide

Data Security Management Guide helps a customer to enable and access the enhanced security features in the Platform Services 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.



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

ocidl.dynamicgroup.ocl..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



2

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

CHALLE
Add subscriptions to a cloud account
That subscriptions to a croad account
4 Neg Test Custower,
Thank you for subscribing to Orade Coult. Your fail, this to b think the convergible on Orade Cloud Account, Will an Crosic Could Account, you can manage converse, add users, and over gave access to resources.
Your first stol is to activate your service(b) by adding them to an Oracle Good Account, which clows you to manage services, and more. Either add your reinities to an existing account associated with your organization, or owner a new account (see actions 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(d).
Decrystichel ander jour sev registe an Oracle Casis Account, you will encour an email from Disce Journal, and if fir will guide you to take the oraboard to their Disce Journal of the oraboard to their services. Relet Activity Account, you inservices advantation of the oraboard activity account of the oraboard account.
Subscription D: and the second s
Oracle Financial Sonietra Accounting Foundation Cloud Service - 1K Hoston Transactions (094960)
Add to existing cloud account
Casada mere cloud account
Order Ordalitis: Chron further: 2022050021159104
Order Date Man May 100, 2022, 00 59 PM UTC
Cestorer Support Merciler (CSI) 2022/00021978/04 C spinztator Niane Teat Customer
Questions?
Deate (ontail your account representative or <u>Crade Support</u>
Additional resources:
Join the Courd Duration Connect commung to submit costs for product onhancements directly to Croce execlapment or congage in reactine dialogues with other Oracle custement, Croce expense, and Oracle pathers about externo evalues and text sections for courd adaption and boxeness bandometron.
Oracle University is offering the analogion Draces Direct for a limited time.
and the function of the second se
Cloud

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



Figure 2-2 New Cloud Account Information Page

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.



Geed Infrastructure
Thank you for signing up for Oracle Cloud!
We are centricly our chose accure, We'll annual you, with Authon instructions along your chose account is week, so you can per you services up and sources Learn chose discovers a new administration chose

Figure 2-3 Oracle Cloud Creation Confirmation Screen

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.

between the server between the twee types that the type is the twee twee types the add between types in a cost of types t	Add subscriptions to a cloud account			
The table is to address your service) by adding them to an Oracle Good Account, which diewy you to marge service, address, and now. Either address restricts as societad with your organization, or or when an address your services is a dress to an existing account associetad with your organization, or or when an address your services is a dress to an organization or organization, and when the analytic presents and when a present address your services is an address your services. Address and the correct present to manage your company's subscriptions, simply forward the whall to be fight presents address your services. Address and the correct presents address is a dress address address your services and the services address your services. Address and the correct presents address is a dress address or organization or organization. Address address address your services is a dress address or organization. dress address add	Hilling Test Customer,			
<pre>count jees counts been fyces an not the correct period to manage your company's subscriptions, simply forward the small to the sight persons to address your service(d). therepise the correct period to manage your company's subscriptions, simply forward the small to the sight persons to address your service(d). therepise the correct period to manage your company's subscriptions, simply forward the small to the sight persons to address your service(d). therepise the correct period to manage your company's subscriptions, simply forward the small to the sight persons to the state your service(d). therepise the correct period to manage your company's subscriptions, simply forward the small to the sight persons to the state your service(d). therepise the correct period to the state correct is the shade to the state your service(d). therepise the state of the state</pre>	Thank you for subscribing to Grade Cloud. Your first step is to link the service(s) to an Grade Cloud Account. With an Cresce Cloud Account, you can manage convices, add	users, and configure access to resources.		
A strain when doed your avvirege to all out the Close Acoust you will reveal as a new it from 0 the places and if will get you to the the new doed sign on your acces, you my encesses and the doed out the encesses will be accesses. Automatic Strains Strains O words: Provide Strains Acoust your approximation of the strains accesses out the doed out the encesses out the encesses out the doed out the encesses out the doed out the encesses out the doed out the encesses out the encesse	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 se account (see actions below)	mices to an existing account associated with your organization, or create a ne		
everos Refer Autoring Your Songle Types have autoring in with the attendence to between acting variance covaling a new Orace David account.	fyou are not the correct person to manage your company's subscriptions, simply forward this email to the right person to activate your service(s).			
Oracle Phonoid Sensors Account is Pear Advan Dowd Server - 10:10000 Tomosober (004000) Advanced Sensors	Diseyas here nodedysar very rozen to a Oracle Closis Activity, you will receive an email from 0 sice <u>Equippine</u> from all galaxies to talk the ner onbrand by their t nervos. Rifer <u>Albump Zou Structur</u> you have quarters inform the activitient's between acception to the exampliance realing a new Oracle Courd account.	Sepanding on your order, you may receive additional activation emails for othe		
The Cost Net Net Net Net Net Net Net Net Net Ne	Noteen plan ID: an annual Senters Accounting Fean dation Cloud Service - 11: Hosted Transactions (ID94960)			
Inter Statis Inter Statis Inter Statis Inter Statis Inter Statis Inter Statis Inter Statis Inter Statis Inter Statis Inter Statis Inter				
tion Yanza 202060219584 Was Deal Selling Mergin Status desement Support Second Mercille (SSE) 2022/2002195800 Systematic Status Fing Time Container Support Second Mergins Container Support Second Mergins Container (Second Second Second Second Mergins Container) is submittable on product onhair contents directly to Cacce development or engage in rescince delegates with effer Oracle custement, Croce expense, and Oracle partners should estate or engage in rescince delegates with effer Oracle custement, Croce expense, and Oracle partners should estate or engage in rescince delegates with effer Oracle custement, Croce expense, and Oracle partners should estate or engage in rescince delegates with effer Oracle custement, Croce expense, and Oracle partners should estate or engage in rescince delegates with effer Oracle custement, Croce expense, and Oracle partners should estate or engage in rescince delegates with effer Oracle custement, Croce expense, and Oracle partners should estate or engage in rescince delegates and and and estate or engage in the custement of the Oracle custement, Croce expense, and Oracle partners should estate or engage in rescince delegates and and and estate or engage in the custement of the oracle custement, Croce expense, and Oracle partners should estate or engage in the custement of the oracle custement, Croce expense, and Oracle partners should estate or engage in the custement of the oracle custement, Croce expense, and Oracle partners should estate or engage in the custement or engage in the custement of the oracle custement of the				
Succes Excess Landler COD, 2022/2020/21575/004 Sprace contains from Counter For Counter Substant Substant Resources In the Count Counter Count Counter or Count Success In the Count Counter Counter Counter Counter or product onbar connects directly to Cloce development or engage in reactine delegues with other Oracle counteres, Choice opens, and Oracle partners sheet essents and bee reactions for doub adapters and former to a soften on one reaction. For doub adapters and choice counteres, Choice opens, and Oracle partners sheet essents and bee reaction. For doub adapters and choice counteres, Choice opens, and Oracle partners sheet essents and bee reaction. For doub adapters and advector opens, and Oracle partners sheet essents and bee reaction. For doub adapters and shore the opens, and Oracle partners sheet essents and be reaction. For doub adapters and shore the opens, and Oracle partners sheet essents and be reaction. For doub adapters and advector opens. The open opens and the open open open open opens and the reaction. For double address and advector open open open open open open open open	2rder Namber, 202205092157804			
ispanzen kom Fang Tead Culturer Instituter Maler Contact your accept representative or <u>Calco Support</u> different resource: In the <u>Caulo Culturer</u> Contact culturers, Crace expense, and Oracle pathens affect expenses and brance malers. For source and patheness are demoted on.				
Yeas creat your acoust representing or <u>Cable Succes</u> defined resource: the <u>Devind Cable Constant</u> (to submit coaching product onher consts; directly to Cable coveragement or engage in residine delegates with other Oracle custement, Cracle expents, and Oracle partners about escence and bese reactions for data adapters and bearward and direct. Cloud for a Insteadment inter University is direct <u>Deat Backing on Cracle Cloud</u> for a Insteadment.	Spontation Subject Western (201) and another for the			
ddfanal resource: we be <u>Could fortener Check communit</u> to submit local for product onhancements directly to Disco coveragment or ongage in residine datage over the offer Oracle custement, Crisce expens, and Oracle pathents street estons earned and be reacted for cloud adapters and discuss zer domation.	Zunstions?			
on the <u>Cost Submer Connectonments</u> to submitted for product enterts dready to Sace condigment or engage to reacine delega conditioned or submers, Crace expense, and Grade partners alors: excens earlied and be reactive for closed adaptors and the submitted or a submitted or and the submitted adaptors adaptor adaptor adaptor adaptor adaptor adaptor adaptor adaptor				
		usterners, Criscle expens, and Oracle partners about lescens learnes and bes		
ORACLE	ince University is offering <u>the than ing on Grace Cloud</u> for a limited time.			
	URALLE	Phases do not apply should Unable (V 2010) The Art of t		
	Cloud			

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.
- 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 dropdown 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

S 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 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 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.