

Oracle FLEXCUBE Password Change
Oracle FLEXCUBE Investor Servicing

Release 14.7.5.0.0

[June] [2024]



Table of Contents

1.	ABOUT THIS MANUAL.....	1-1
1.1	INTRODUCTION	1-1
1.2	AUDIENCE	1-1
1.3	ORGANIZATION	1-1
1.4	RELATED DOCUMENTS	1-1
2.	ORACLE FLEXCUBE PASSWORD CHANGE.....	2-1
2.1	INTRODUCTION	2-1
3.	CHANGING PASSWORDS IN ORACLE WEBLOGIC	3-1
3.1	INTRODUCTION	3-1
3.2	CHANGING HOST SCHEMA PASSWORD	3-1
3.2.1	<i>Prerequisites</i>	3-1
3.2.2	<i>Changing Host Schema Password</i>	3-2
3.3	CHANGING SCHEDULER DATA SOURCE PASSWORD	3-5
3.3.1	<i>Prerequisites</i>	3-5
3.3.2	<i>Changing Scheduler Data Source Password</i>	3-6
3.4	CHANGING GATEWAY DATA SOURCE PASSWORD	3-8
3.4.1	<i>Prerequisites</i>	3-8
3.4.2	<i>Changing Gateway Data Source Password</i>	3-9

1. About this Manual

1.1 Introduction

This manual explains the method of changing the passwords in Oracle FLEXCUBE data sources and the servers associated with it.

1.2 Audience

This manual is intended for the following User/User Roles:

Role	Function
Implementers	Installation and implementation of Oracle FLEXCUBE
System Administrators	System administration

1.3 Organization

This manual is organized into the following chapters:

Chapter 1	<i>About this Manual</i> acquaints you quickly with the purpose, organization and the audience of the manual.
Chapter 2	<i>Oracle FLEXCUBE Password Change</i> gives an outline of the processes involved in changing the passwords of various data sources.
Chapter 3	<i>Changing Passwords in Oracle WebLogic</i> describes the method of changing data source passwords from Oracle WebLogic application server.

1.4 Related Documents

Oracle FLEXCUBE Installation Guide

2. Oracle FLEXCUBE Password Change

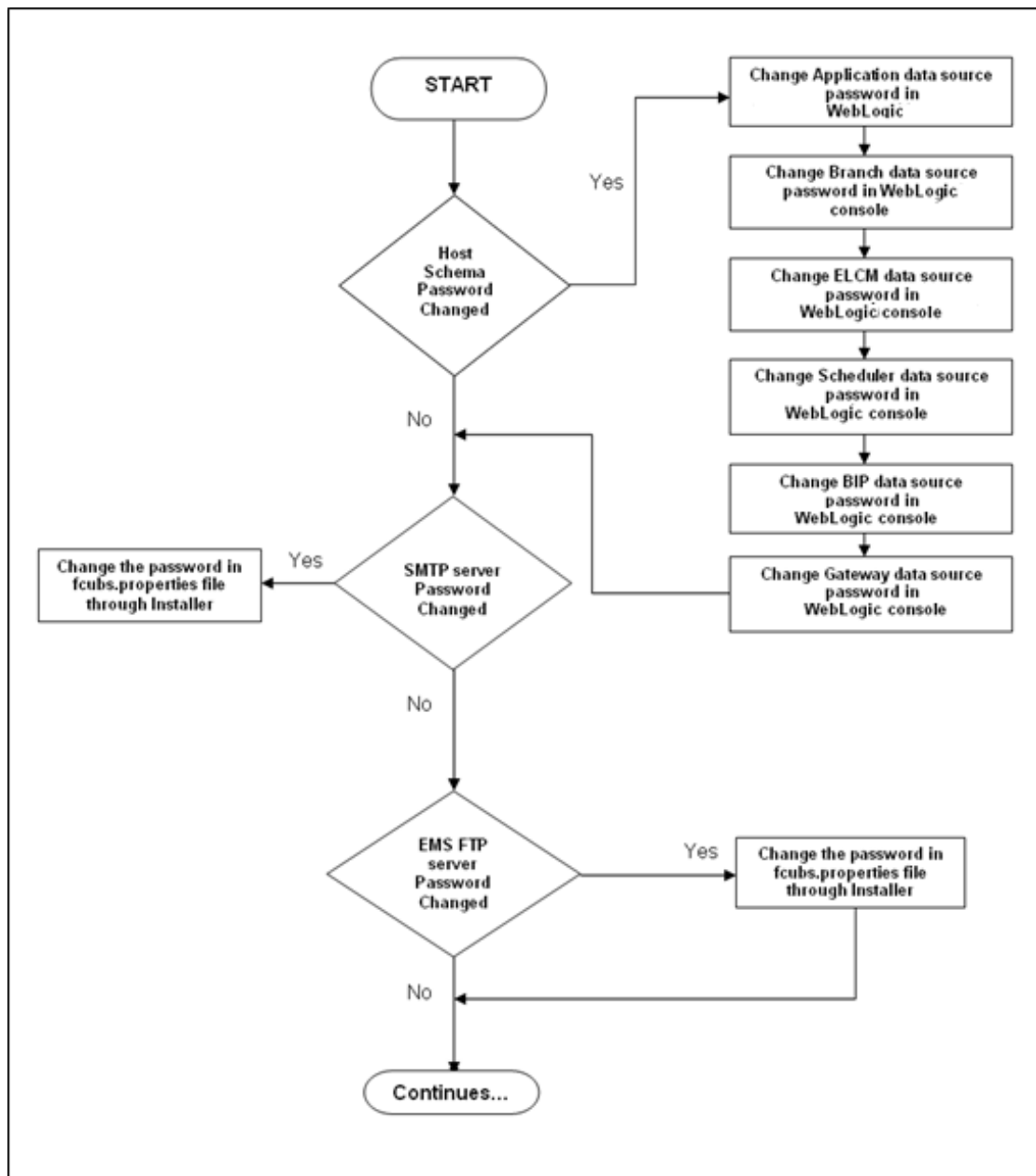
2.1 Introduction

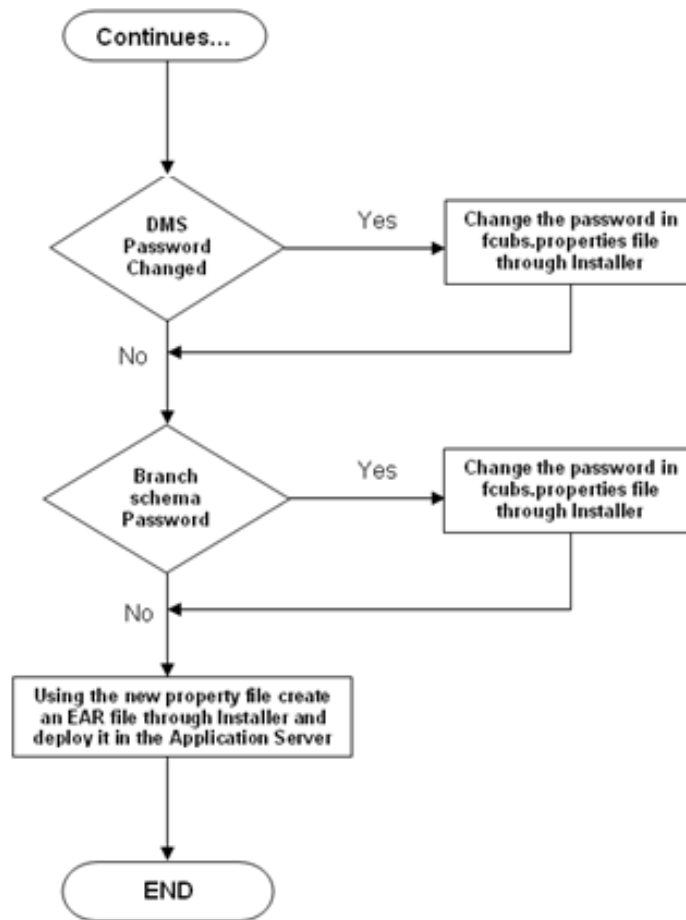
This chapter explains the process of changing the passwords of data sources associated with Oracle FLEXCUBE.

You will find the methods to change the passwords of the following components:

- Oracle FLEXCUBE Host Schema
- Scheduler Data Source
- ELCM Data Source
- Gateway Data Source
- Branch Data Source

The following diagram briefs the steps involved in changing the passwords of the above components.





3. Changing Passwords in Oracle WebLogic

3.1 Introduction

This chapter describes the method of changing data source passwords from Oracle WebLogic application server.

3.2 Changing Host Schema Password

This section explains the method to change the password of Oracle FLEXCUBE Host schema.

If you change the host schema password, you also need to change the passwords of the data sources pointing to the host schema.

3.2.1 Prerequisites

Before you change and test the passwords of the data sources, ensure that the following activities are completed:

1. Determine the downtime for the password change and test activities.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server, follow the steps below:
 - Login to Oracle WebLogic application server
 - Go to Home > Environments > Servers
 - Select and stop the server by clicking 'Stop' button.

This completes the prerequisites.

3.2.2 Changing Host Schema Password

You need to test whether the data source password change was successful. Follow the steps given below.

1. Login to Oracle WebLogic application server
2. Go to **Home > Services > Data Sources**. You will notice a table that contains the list of all data sources created in the application server.
3. Click the data source *jdbc/fcjdevDS*.
4. Select 'Connection Pool' tab.

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains a 'Domain Structure' tree with 'base_domain' expanded, showing 'Services' and 'Data Sources'. Below it is a 'How do I...' section with links to configure testing options, statement cache, and credential mapping. The 'System Status' section shows 'Health of Running Servers' with a list of servers and their status (Failed, Critical, Overloaded, Warning, OK). The main content area is titled 'Settings for FCUBDS' and has tabs for 'Configuration', 'Targets', 'Monitoring', 'Control', 'Security', and 'Notes'. The 'Configuration' tab is selected, and the 'Connection Pool' sub-tab is active. The 'URL' field is set to 'jdbc:oracle:thin:@10.184.74.142:1521:KERDEV3'. The 'Driver Class Name' is 'oracle.jdbc.OracleDriver'. The 'Properties' field is set to 'user=FCI131IUT'. The 'System Properties' field is empty. The 'Password' and 'Confirm Password' fields are both set to '*****' and are highlighted with a red box. The 'Password' field has a tooltip that says 'The password attribute passed to the JDBC driver when creating physical database connections. More Info...'. The 'Confirm Password' field has a tooltip that says 'The password attribute passed to the JDBC driver when creating physical database connections. More Info...'. The 'Save' button is at the top left of the configuration area.

5. Change the password. Use the following fields:

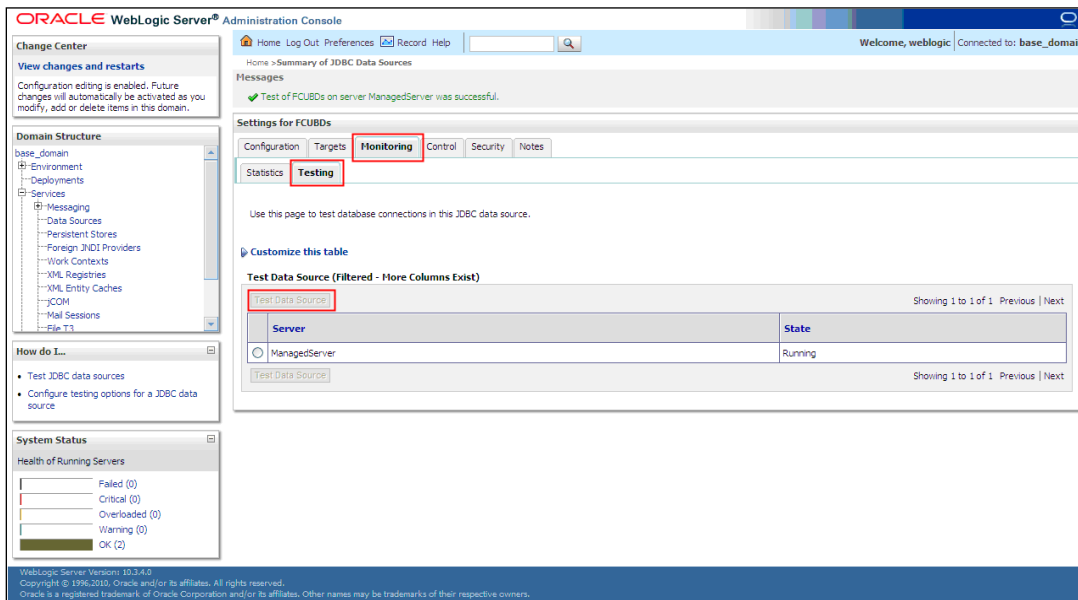
Password

Specify the new password.

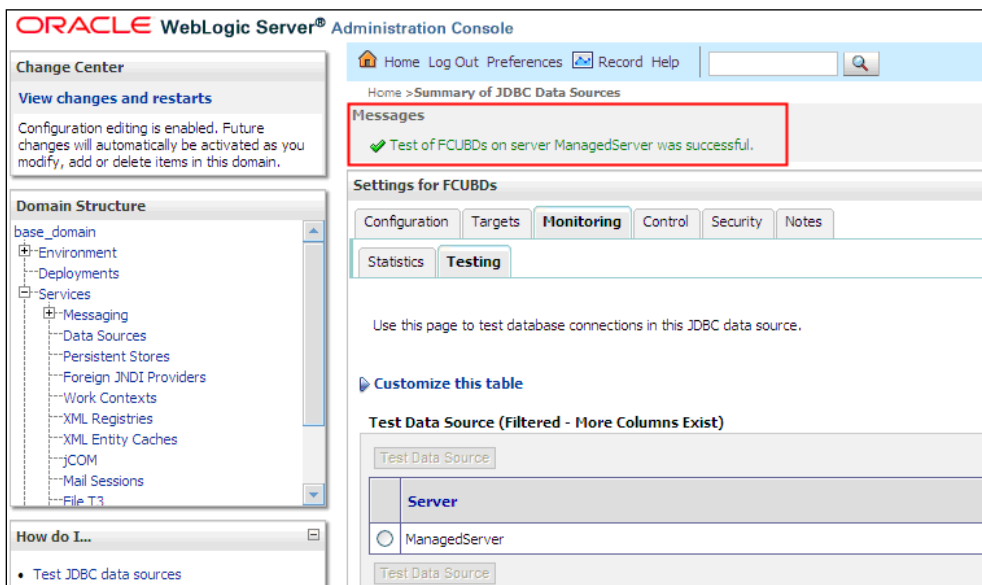
Confirm Password

Specify the new password again.

6. Click 'Save'.
7. To test the data source, select 'Monitoring' tab and select 'Testing' tab under it.



8. Select the target server and click 'Test Data Source'.
9. The screen displays a message confirming successful testing.



10. Once you get the message, restart the application server.
11. Start Oracle FLEXCUBE.
12. Log in to Oracle FLEXCUBE. Launch a summary screen or execute a simple transaction to test.



Try the above process in UAT or any other test environment before you change the password in a production environment.

Changing Password in Decentralized Setup

You need to change the branch schema password for a decentralized setup of Oracle FLEXCUBE. Follow the steps given below:

1. In Oracle FLEXCUBE Investor Servicing Installer, load the existing property file. Go to the step where you can define the branch properties.

Name	Value
Username	installer
Password
Connect String	testdb
IP Address	10.10.10.10
Port	1521

2. You need to modify the following field:

Password

Specify the new password for the branch schema

Refer to the Installation Guide for further information on the following topics:

- *Creating EAR file*
- *Loading and editing the property file*
- *Deploying EAR file*



Try the above process in UAT or any other test environment before you change the password in a production environment.

3.3 **Changing Scheduler Data Source Password**

After changing the host schema password, you need to change the password of scheduler data source.

3.3.1 **Prerequisites**

Before you change the password of scheduler data source, ensure that the following activities are completed:

1. Determine the down time for the password change activity.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server, follow the steps below:
 - Login to Oracle WebLogic application server
 - Go to **Home > Environments > Servers**
 - Select and stop the server by clicking 'Stop' button.

This completes the prerequisites.

3.3.2 Changing Scheduler Data Source Password

You need to change the password of scheduler data source. Follow the steps given below.

1. Login to Oracle WebLogic application server
2. Go to **Home > Services > Data Sources**. You will notice a table that contains the list of all data sources created in the application server.
3. Click the data scheduler source *jdbc/fcjschedulerDS*.
4. Select **Connection Pool** tab.

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains the 'Domain Structure' tree with 'base_domain' expanded, showing 'Services' and 'Data Sources'. The 'How do I...' section lists configuration tasks for JDBC data sources. The 'System Status' section shows the health of running servers. The main content area displays the 'Settings for FCUBS_SchedulerDS' with the 'Connection Pool' tab selected. The 'URL' field is 'jdbc:oracle:thin:@10.184.74.142:1521:KERDEV3'. The 'Driver Class Name' is 'oracle.jdbc.xa.client.OracleXADataSource'. The 'Properties' field contains 'user=FC1131IUT'. The 'System Properties' field is empty. The 'Password' and 'Confirm Password' fields are highlighted with a red box.

5. Change the password. Use the following fields:

Password

Specify the new password.

Confirm Password

Specify the new password again.

6. Click 'Save'.

7. To test the data source, select 'Monitoring' tab and select 'Testing' tab under it.

The screenshot shows the Oracle WebLogic Server Administration Console. On the left is the Domain Structure tree. The main area is titled 'Settings for FCUBS_SchedulerDS' with tabs for Configuration, Targets, Monitoring, Control, Security, and Notes. The Monitoring tab is active, and within it, the Testing sub-tab is selected. A message at the top states: 'Test of FCUBS_SchedulerDS on server ManagedServer was successful.' Below this, a table titled 'Test Data Source (Filtered - More Columns Exist)' shows a single row for 'ManagedServer' with a state of 'Running'.

8. Select the target server and click 'Test Data Source'.
9. The screen displays a message confirming successful testing.

This screenshot is similar to the previous one but highlights the success message with a red rectangle. The message reads: 'Test of FCUBS_SchedulerDS on server ManagedServer was successful.' The 'Testing' sub-tab remains selected in the Monitoring tab.

You need to change the branch schema password after the above steps. Refer to the section 'Changing Password in Decentralized Setup' for information on changing the branch schema password from Oracle FLEXCUBE Investor Servicing Installer.

STOP Try the above process in UAT or any other test environment before you change the password in a production environment.

3.4 **Changing Gateway Data Source Password**

If you change the host schema password, you also need to change the gateway password.

3.4.1 **Prerequisites**

Before you change the gateway password, ensure that the following activities are completed:

1. Determine the down time for the password change activity.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server, follow the steps below:
 - Login to Oracle WebLogic application server
 - Go to Home > Environments > Servers
 - Select and stop the server by clicking 'Stop' button.

This completes the prerequisites.

3.4.2 Changing Gateway Data Source Password

You need to change the password of Gateway data source. Follow the steps given below.

1. Login to Oracle WebLogic application server
2. Go to Home > Services > Data Sources. You will notice a table that contains the list of all data sources created in the application server.
3. Select Gateway data source (*FLEXTEST.WORLD*).
4. Select 'Connection Pool' tab.

The screenshot shows the Oracle WebLogic Administration Console interface. On the left, there is a 'Domain Structure' tree with 'Data Sources' expanded. Below it, a 'How to...' section lists tasks like 'Configure testing options for a JDBC data source'. The main area is titled 'Configuration' and has tabs for 'General', 'Connection Pool', 'Oracle', 'ONS', 'Transaction', 'Diagnostics', and 'Identity Options'. The 'Connection Pool' tab is active. It contains a 'Save' button and a description of the connection pool. Below this, there are several configuration fields: 'URL' (jdbc:oracle:thin:@10.10.10.10:1010:KERDEV3), 'Driver Class Name' (oracle.jdbc.xa.client:OracleXADataSource), 'Properties' (user=FC11S1IUT), 'System Properties', 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'Initial Capacity' (1), and 'Maximum Capacity' (15). The 'Password' and 'Confirm Password' fields are highlighted with a red rectangular box.

5. Change the password. Use the following fields:

Password

Specify the new password

Confirm Password

Specify the new password again

6. Click 'Save'.
7. To test the data source, select 'Monitoring' tab and select 'Testing tab' under it.
8. Select the target server and click 'Test Data Source'.
9. The screen displays a message confirming successful testing.

The screenshot shows the Oracle WebLogic Server Administration Console. The breadcrumb trail is: Home > Summary of JDBC Data Sources > FCUBS_SchedulerDS > Summary of JDBC Data Sources > FCUBS_ELCMDs > Summary of JDBC Data Sources > FLEXTTEST.WORLD > Summary of JDBC Data Sources > FLEXTTEST.WORLD. The 'Messages' section displays a green checkmark and the text: 'Test of FLEXTTEST.WORLD on server ManagedServer was successful.' The 'Settings for FLEXTTEST.WORLD' section has tabs for Configuration, Targets, Monitoring, Control, Security, and Notes. The 'Monitoring' tab is selected, and the 'Testing' sub-tab is active. Below the 'Testing' sub-tab, there is a section titled 'Test Data Source (Filtered - More Columns Exist)' with a table. The table has two columns: 'Server' and 'State'. The 'Server' column has a radio button next to 'ManagedServer'. The 'State' column shows 'Running'. There is a 'Test Data Source' button below the table.

10. Once you get the message, restart the application server.
11. Start Oracle FLEXCUBE. Log in to Oracle FLEXCUBE and test whether the change was successful.



Try the above process in UAT or any other test environment before you change the password in a production environment.



Oracle FLEXCUBE Password Change
[June] [2024]
Version 14.7.5.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
www.oracle.com/financialservices/

Copyright © [2007], [2024], Oracle and/or its affiliates.

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 failsafe, 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.

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.

This software or hardware and documentation may provide access to or information on 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. 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.

