

Oracle FLEXCUBE Password Change
Oracle FLEXCUBE Investor Servicing
Release 14.6.0.0.0
[May] [2022]



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 Prerequisites.....	3-1
3.2.2 Changing Host Schema Password.....	3-2
3.3 CHANGING SCHEDULER DATA SOURCE PASSWORD.....	3-5
3.3.1 Prerequisites.....	3-5
3.3.2 Changing Scheduler Data Source Password.....	3-6
3.4 CHANGING GATEWAY DATA SOURCE PASSWORD.....	3-8
3.4.1 Prerequisites.....	3-8
3.4.2 Changing Gateway Data Source Password.....	3-9
4. CHANGING PASSWORDS IN IBM WEBSHERE.....	4-1
4.1 INTRODUCTION.....	4-1
4.2 CHANGING HOST SCHEMA PASSWORD.....	4-1
4.2.1 Prerequisites.....	4-1
4.2.2 Changing Host Schema Password.....	4-2
4.2.3 Testing Host Schema Password Change.....	4-3
4.3 CHANGING SCHEDULER DATA SOURCE PASSWORD.....	4-4
4.3.1 Prerequisites.....	4-4
4.3.2 Changing Scheduler Data Source Password.....	4-5
4.3.3 Testing Scheduler Data Source Password Change.....	4-6
4.4 CHANGING GATEWAY PASSWORD.....	4-7
4.4.1 Prerequisites.....	4-7
4.4.2 Changing Gateway Data Source Password.....	4-8
4.4.3 Testing Gateway Data Source Password Change.....	4-9

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.
Chapter 4	<i>Changing Passwords in IBM Websphere</i> describes the method of changing data source passwords from IBM Websphere application server.
Chapter 5	<i>Server Password Change</i> explains the process of changing the passwords of the servers associated with Oracle FLEXCUBE.

1.4 Related Documents

Oracle FLEXCUBE Installation Guide

2. Oracle FLEXCUBE Password Change

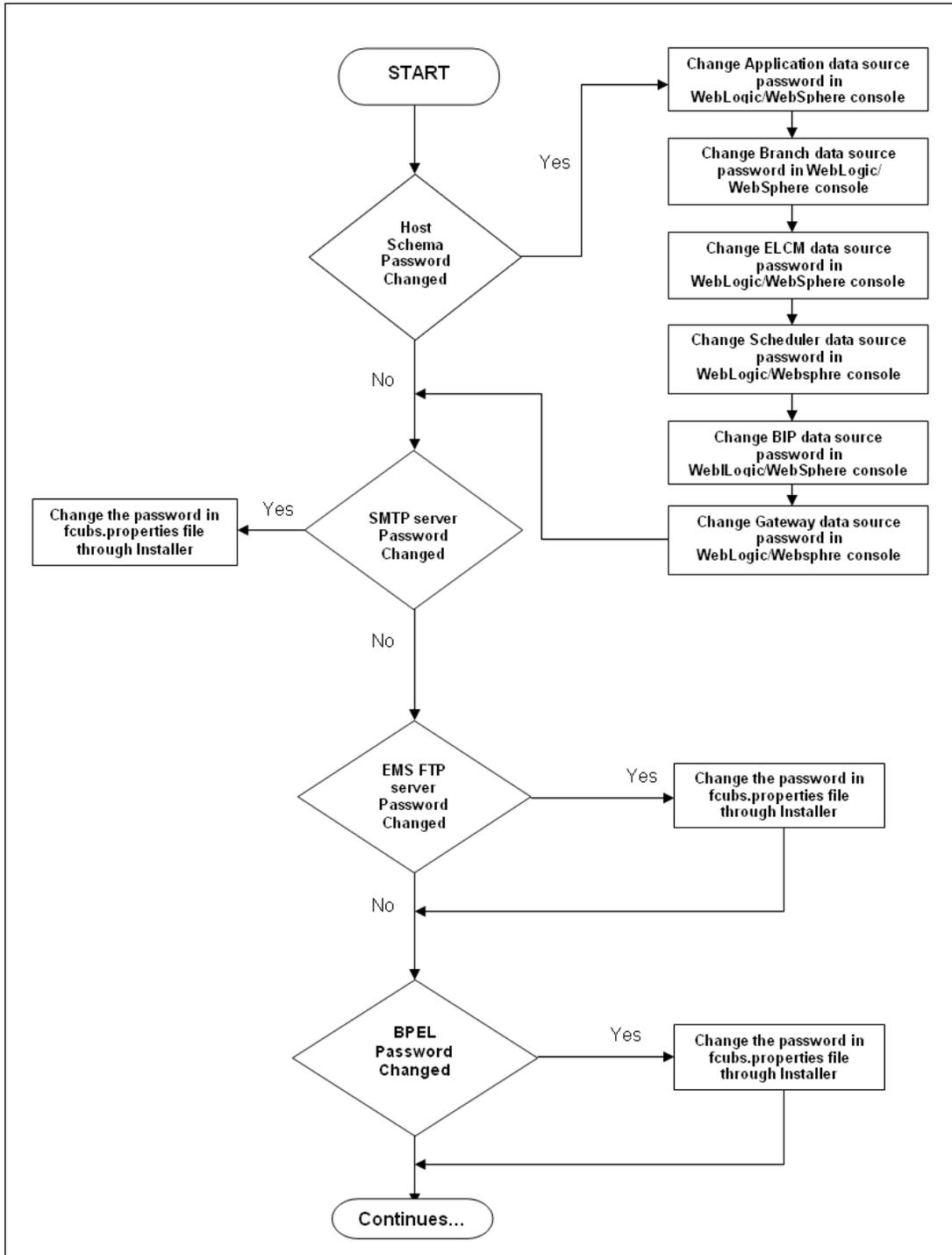
2.1 Introduction

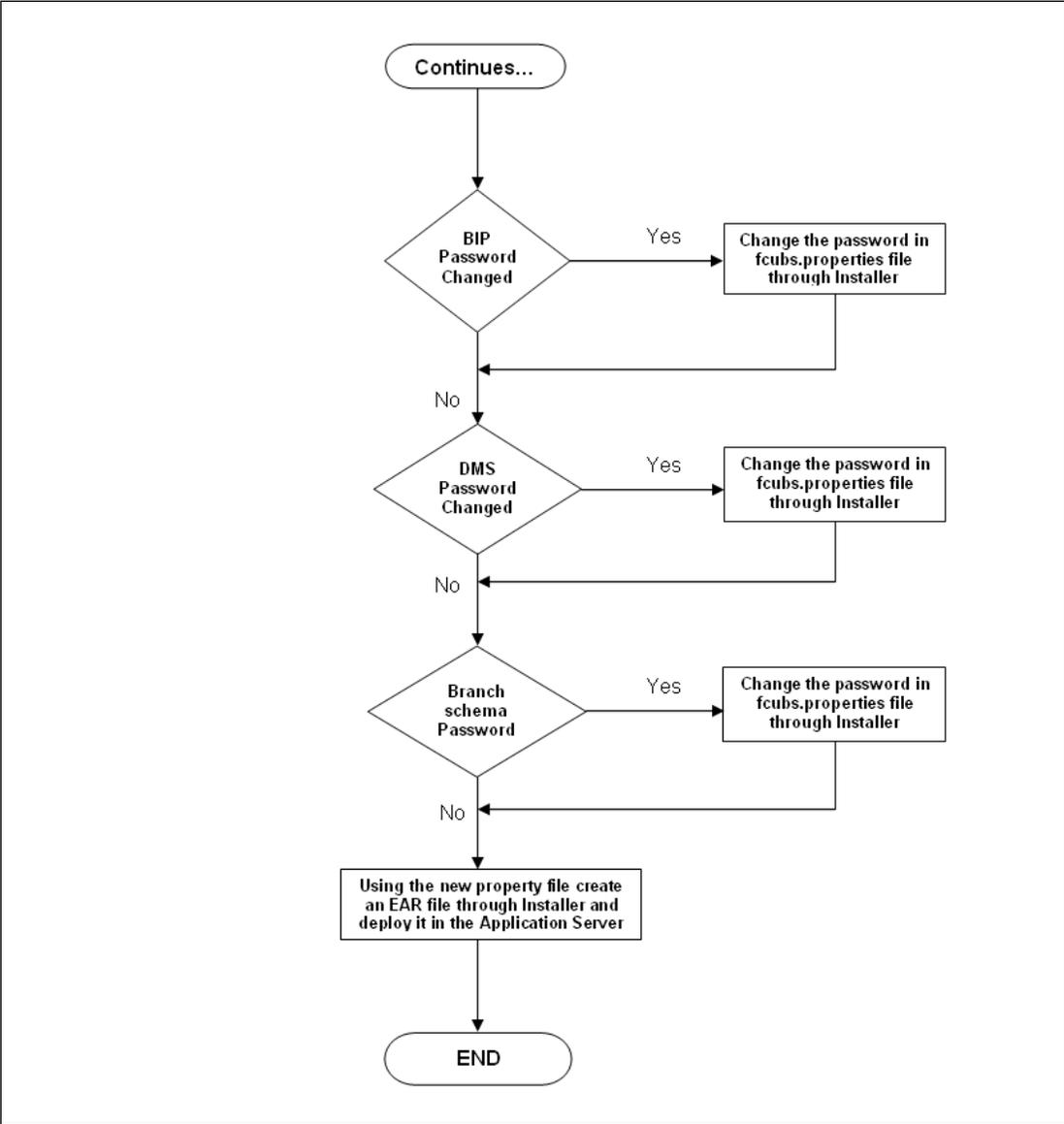
This chapter explains the process of changing the passwords of data sources associated with Oracle FLEXCUBE.

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:

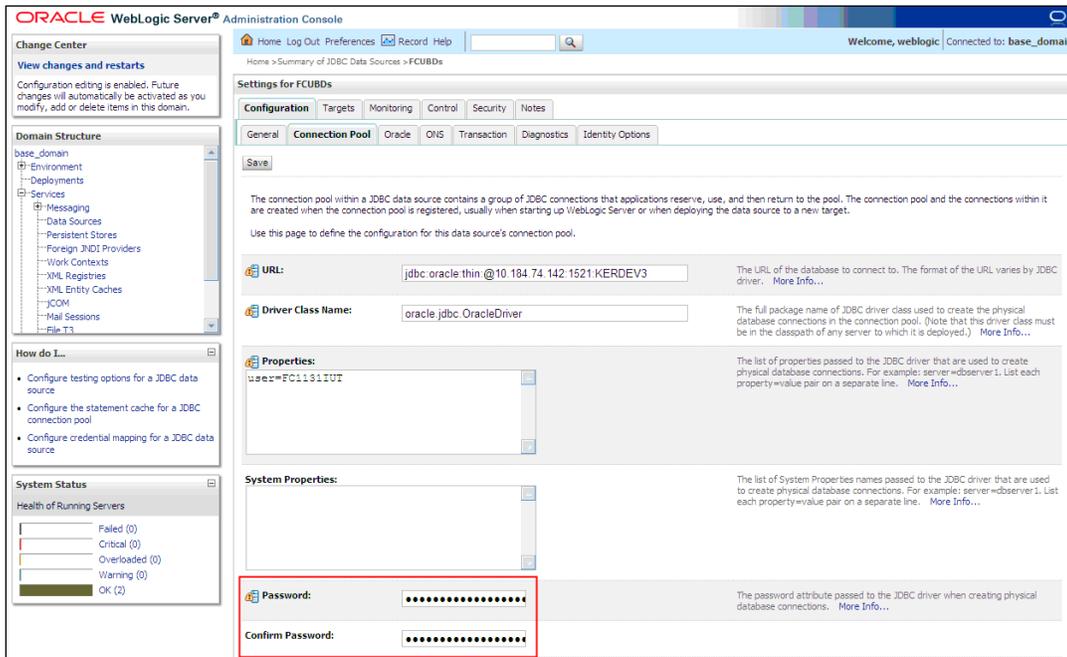
1. Determine the downtime for the password change and test activities.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server, 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.



5. Change the password. Use the following fields:

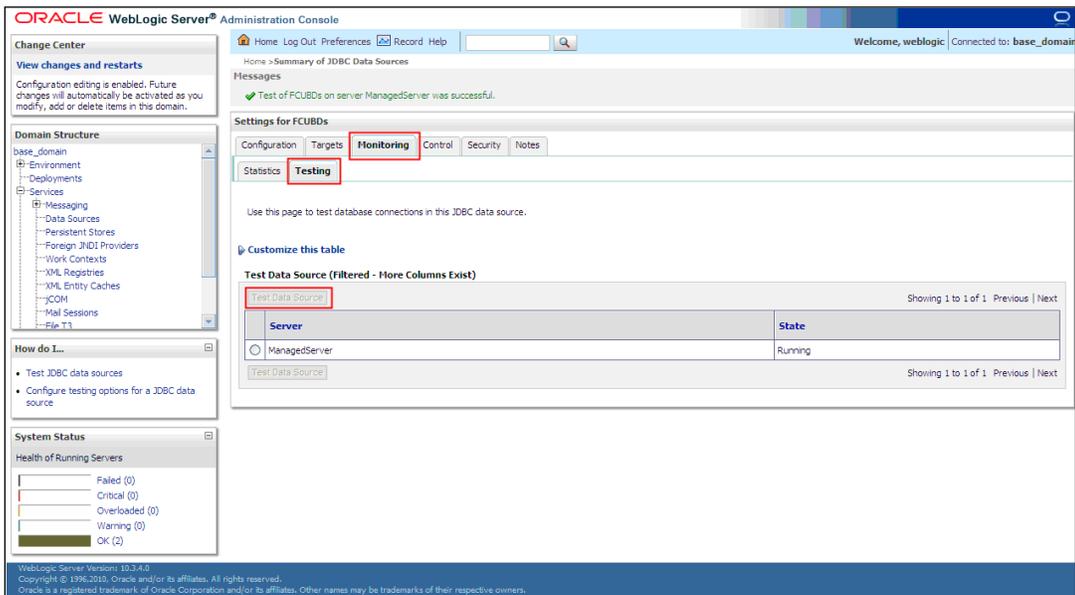
Password

Specify the new password.

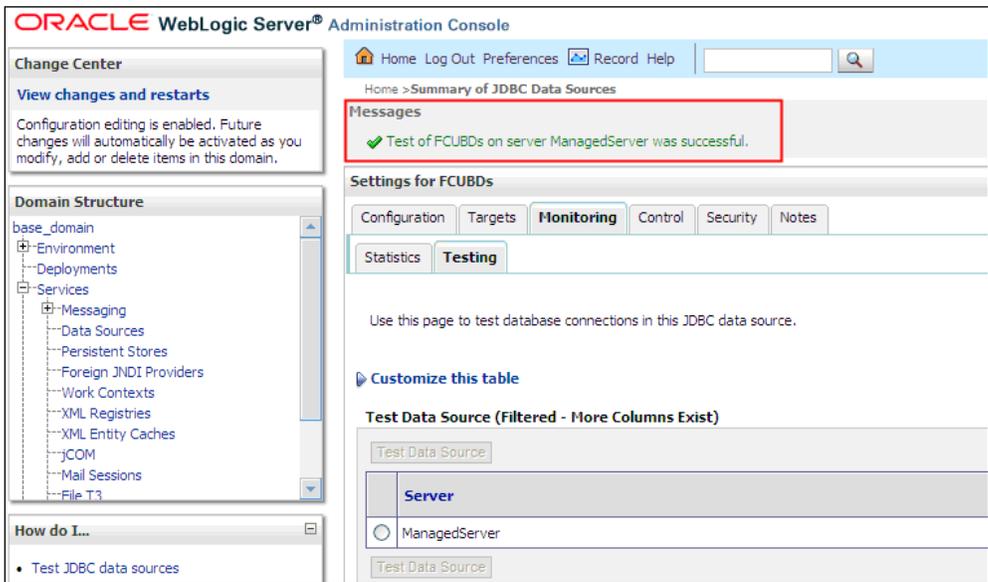
Confirm Password

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:

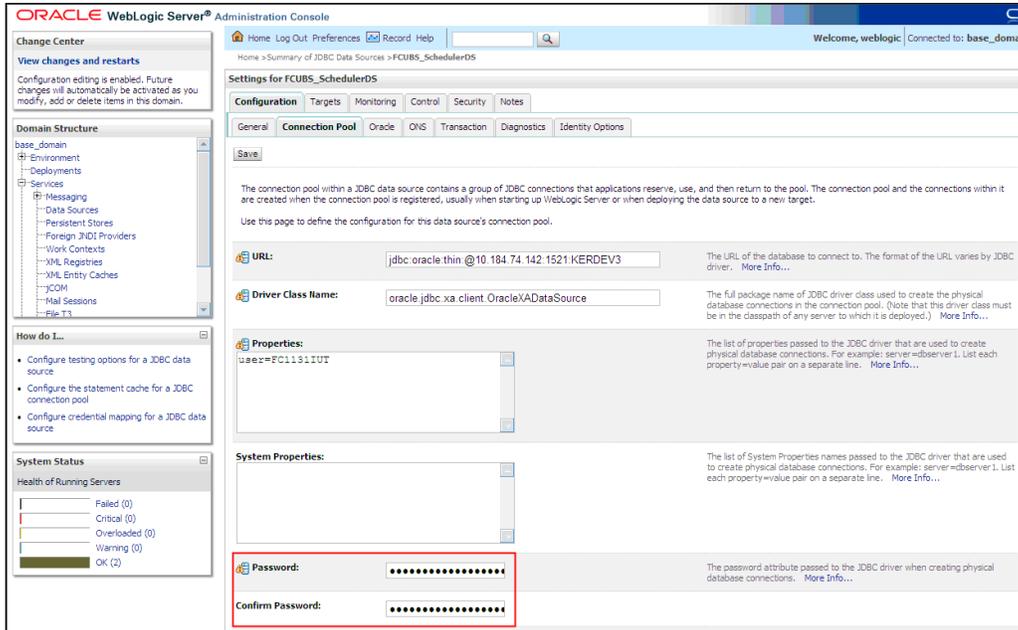
1. Determine the down time for the password change activity.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server, follow 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.



5. Change the password. Use the following fields:

Password

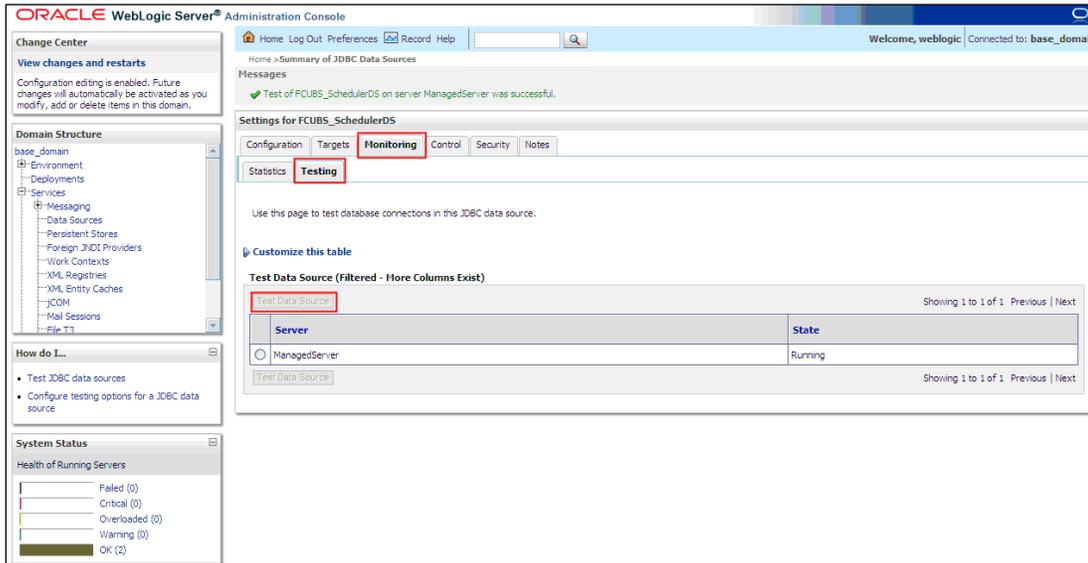
Specify the new password.

Confirm Password

Specify the new password again.

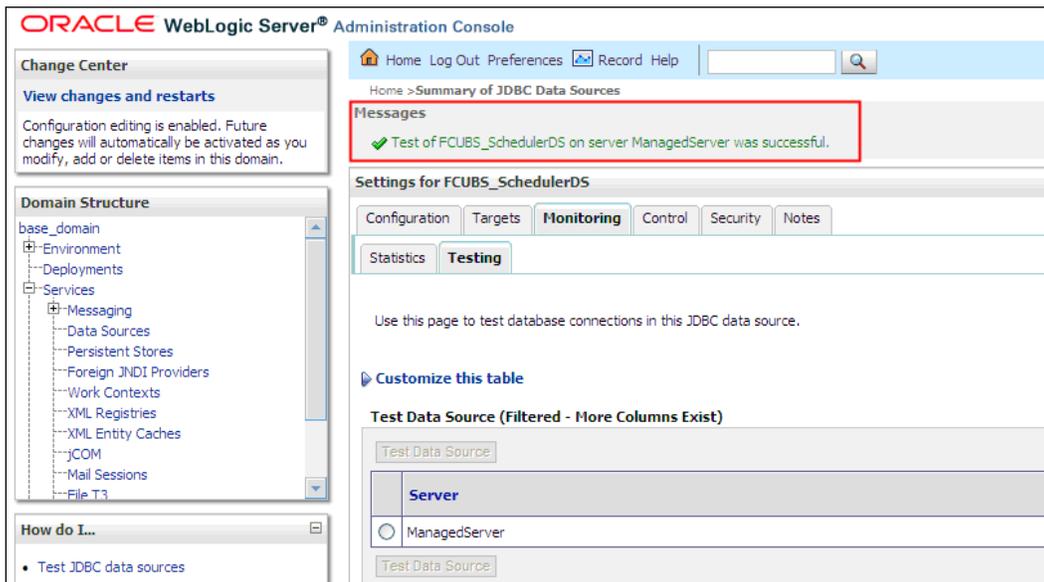
6. Click 'Save'.

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.



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:

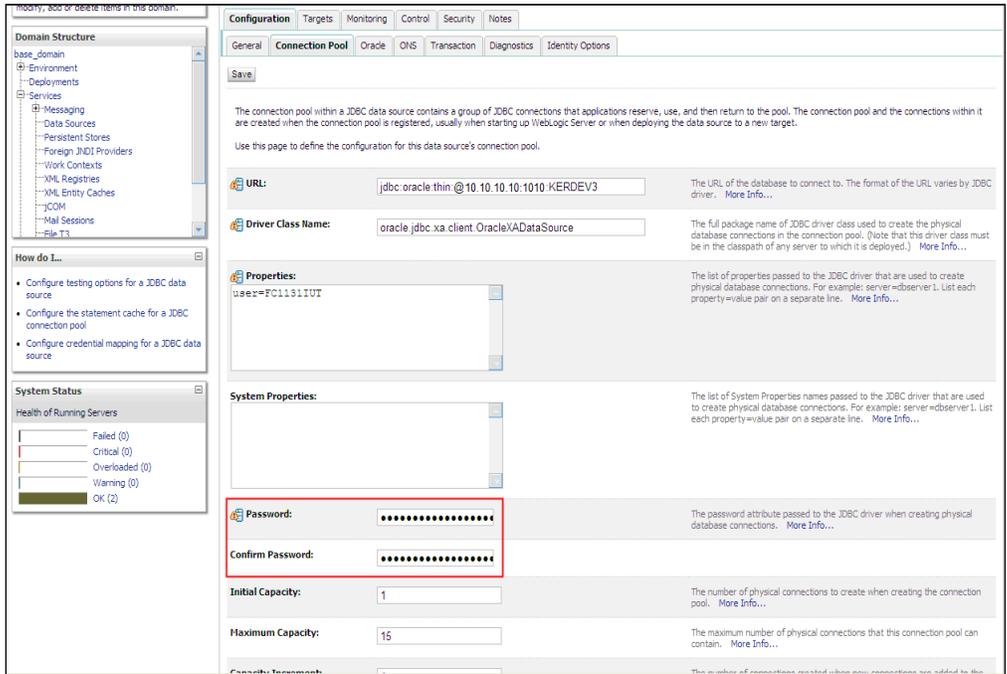
1. Determine the down time for the password change activity.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server, follow 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.



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 interface. The breadcrumb path is: Home > Summary of JDBC Data Sources > FCUBS_SchedulerDS > Summary of JDBC Data Sources > FCUBS_ELCMDs > Summary of JDBC Data Sources > Sources > FLEXTEST.WORLD > Summary of JDBC Data Sources > FLEXTEST.WORLD. A message box displays: "Test of FLEXTEST.WORLD on server ManagedServer was successful." The "Monitoring" tab is selected, and the "Testing" sub-tab is active. A table titled "Test Data Source (Filtered - More Columns Exist)" shows the following data:

Test Data Source	Server	State
Test Data Source	ManagedServer	Running

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.

4. Changing Passwords in IBM Websphere

4.1 Introduction

This chapter describes the methods of changing passwords of data sources from IBM Websphere application server.

4.2 Changing Host Schema Password

This section explains the method to change the password of Oracle FLEXCUBE Host schema in IBM Websphere application server. If you change the host schema password, you also need to change the passwords of the data sources pointing to the host schema.

4.2.1 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 the target server to which the data sources point.
5. Stop Oracle FLEXCUBE application

This completes the prerequisites.

4.2.2 Changing Host Schema Password

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

1. Login to IBM Websphere application server

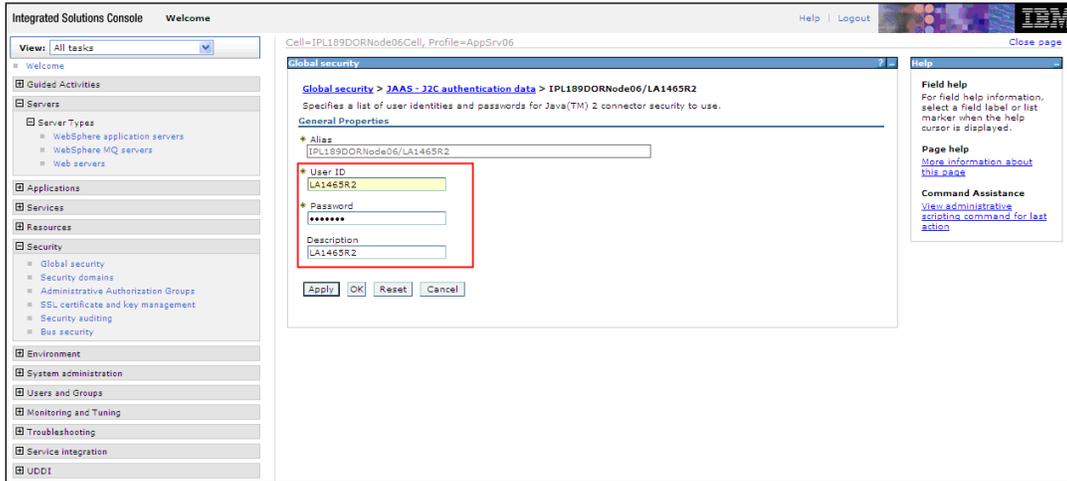
The screenshot shows the IBM Integrated Solutions Console interface. The left sidebar contains a navigation menu with 'Security' highlighted. The main content area displays the 'Global security' configuration page. The 'Java Authentication and Authorization Service' section is highlighted with a red box, showing options for 'Application logins', 'System logins', and 'J2C authentication data'. A tooltip is visible over the 'J2C authentication data' option, stating: 'Specifies realm of Java(TM) Authentication and Authorization Service (JAAS) login configurations that are used by system resources including the authentication mechanism, principal mapping, and credential mapping. You cannot remove the default login configurations because doing so might cause applications to fail.'

2. Go to Security > Global Security > Java Authentication and Authorization Schema > J2C Authentication Data.

The screenshot shows the IBM Integrated Solutions Console interface. The left sidebar contains a navigation menu with 'Security' highlighted. The main content area displays the 'Global security > JAAS - J2C authentication data' configuration page. The page shows a table of user identities and passwords for Java(TM) 2 connector security. The table has columns for 'Alias', 'User ID', and 'Description'. A red box highlights the table content.

Select	Alias	User ID	Description
<input type="checkbox"/>	IP1189DORNode06/LA1465R2	LA1465R2	LA1465R2
Total 1			

3. You will notice a table showing the list of JDBC sources. Choose the node used by host schema data source.



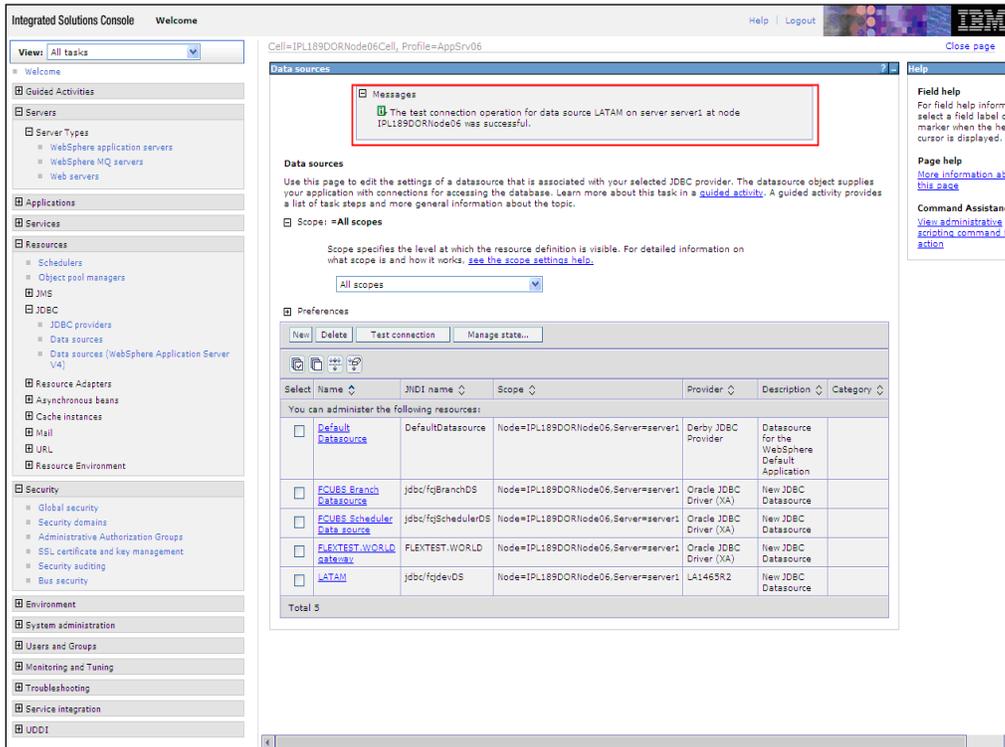
4. Specify the new password and click 'Apply' button. Click 'OK'.

4.2.3 Testing Host Schema Password Change

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

1. Login to IBM Websphere application server
2. Go to Home > Resources > JDBC >Data Sources. You will notice a table that contains the list of all data sources created in the application server.
3. Select the data source *jdbcfcjdevDS*.
4. Select 'Test Connection' tab.

5. The screen displays a message confirming successful testing.



6. Once you get the message, restart the application server.

7. Start Oracle FLEXCUBE. Log in 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.

4.3 Changing Scheduler Data Source Password

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

4.3.1 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.

This completes the prerequisites.

4.3.2 Changing Scheduler Data Source Password

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

1. Login to IBM Websphere application server

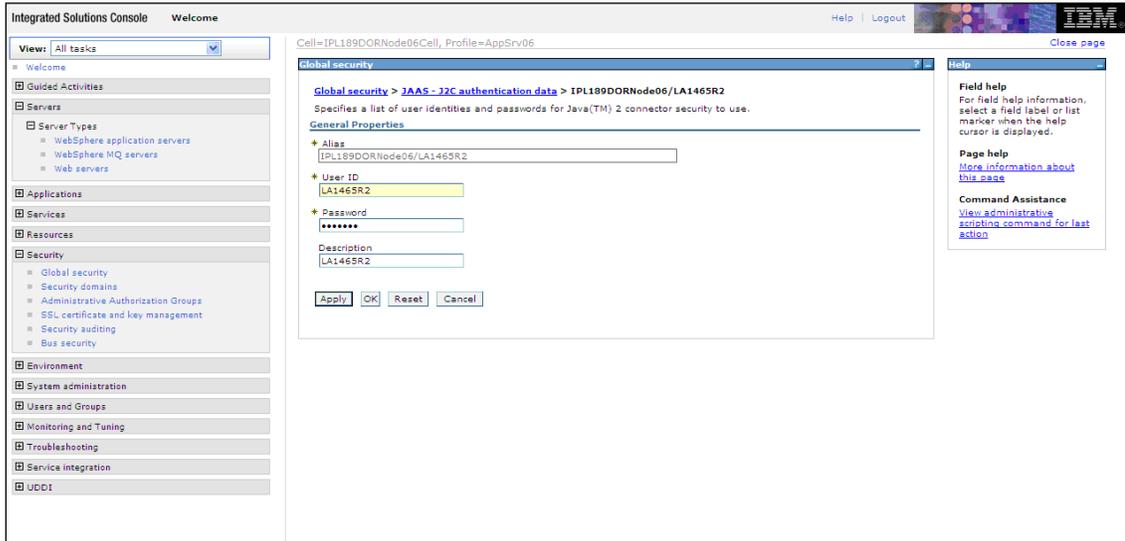
The screenshot shows the IBM Integrated Solutions Console interface. The left sidebar contains a navigation menu with 'Security' highlighted. The main content area is titled 'Global security' and contains several sections: 'Administrative security' with a checked 'Enable administrative security' option; 'Application security' with an unchecked 'Enable application security' option; 'Java 2 security' with an unchecked 'Use Java 2 security' option; and 'Java Authentication and Authorization Service' with a checked 'Use Java 2 security' option. The 'Java Authentication and Authorization Service' section is highlighted with a red box, showing options for 'Application logins', 'System logins', and 'J2C authentication data'. A tooltip is visible over the 'J2C authentication data' link, providing additional information about JAAS login configurations.

2. Go to Security > Global Security > Java Authentication and Authorization Schema > J2C Authentication Data.

The screenshot shows the IBM Integrated Solutions Console interface. The left sidebar contains a navigation menu with 'Security' highlighted. The main content area is titled 'Global security > JAAS - J2C authentication data'. The page shows a table of user identities and passwords for Java(TM) 2 connector security to use. The table has columns for 'Select', 'Alias', 'User ID', and 'Description'. One entry is visible: 'IPL189DORNode06/LA1465R2' with User ID 'LA1465R2' and Description 'LA1465R2'. The table is highlighted with a red box.

Select	Alias	User ID	Description
<input type="checkbox"/>	IPL189DORNode06/LA1465R2	LA1465R2	LA1465R2

3. You will notice a table showing list of JDBC sources choose the node which is used by Oracle FLEXCUBE application.



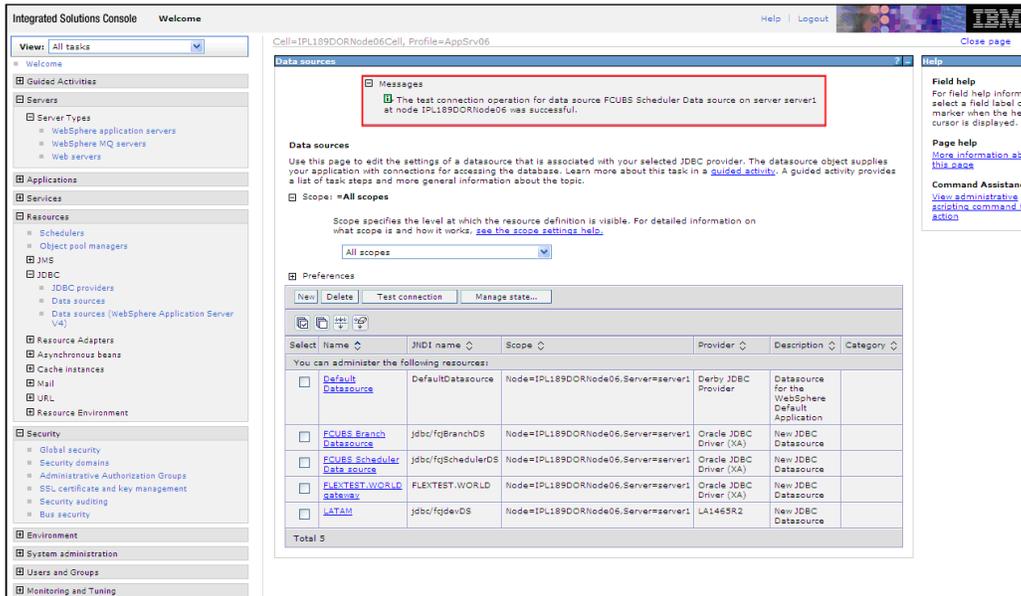
4. Specify the new password in the text field and click on Apply and then click on ok.

4.3.3 Testing Scheduler Data Source Password Change

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

1. Login to IBM Websphere application server
2. Go to Home > Resources > JDBC>Data Sources. You will notice a table that contains the list of all data sources created in the application server.
3. Select the data source *jdbcfcjSchedulerDS*.
4. Click 'Test connection' tab.

5. The screen displays a message confirming successful testing.



6. Once you get the message, restart the application server.

7. Start Oracle FLEXCUBE. Log in 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.

4.4 Changing Gateway Password

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

4.4.1 Prerequisites

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

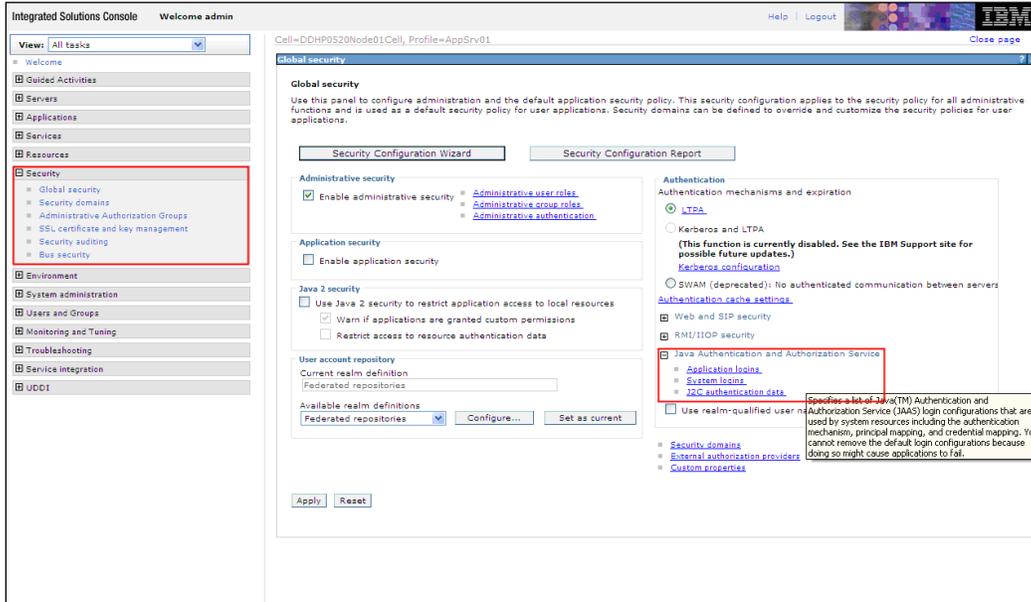
1. Determine the down time for the password change activity.
2. Inform all concerned users and groups.
3. Stop the target server to which the data sources point.
4. Ensure that all users have logged out of Oracle FLEXCUBE system
5. Stop Oracle FLEXCUBE application

This completes the prerequisites.

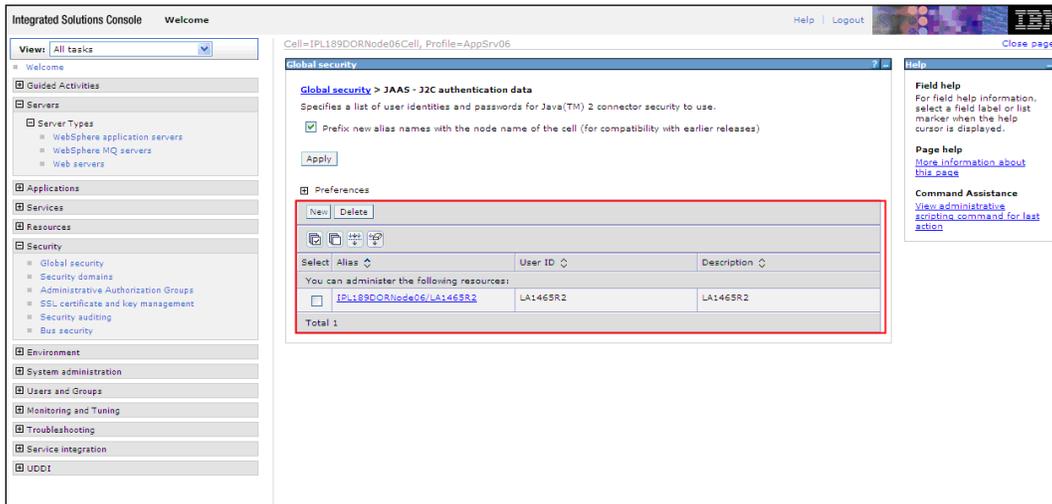
4.4.2 Changing Gateway Data Source Password

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

1. Log in to IBM Websphere application server.
2. Go to Security > Global Security > Java Authentication and Authorization Schema > J2C Authentication Data.



3. You will notice a table showing list of JDBC Sources choose the one which is been used by Gateway data source.



4. Specify the new password in the text field and click on Apply and then click on ok.

4.4.3 Testing Gateway Data Source Password Change

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

1. Log in to IBM Websphere application server.
2. Go to Home > Resources > JDBC > Data Sources. You will notice a table that contains the list of all data sources created in the application server.
3. Select the data source *FLEXTEST.WORLD*
4. Select 'Test Connection' tab.
5. The screen displays a message confirming successful testing.

The screenshot shows the 'Data sources' page in the Integrated Solutions Console. A message box at the top indicates a successful test connection for the 'FLEXTEST.WORLD' data source. Below the message, there is a table listing the data sources. The 'FLEXTEST.WORLD' data source is highlighted in the table.

Select	Name	JNDI name	Scope	Provider	Description	Category
<input type="checkbox"/>	Default Data source	DefaultData source	Node=IPL189DORNode06.Server=server1	Derby JDBC Provider	Data source for the WebSphere Default Application	
<input type="checkbox"/>	FLEXTEST.WORLD Data source	FLEXTEST.WORLD	Node=IPL189DORNode06.Server=server1	Oracle JDBC Driver (XA)	New JDBC Data source	
<input type="checkbox"/>	LATAM	jdbc/fqdevDS	Node=IPL189DORNode06.Server=server1	LA146SR2	New JDBC Data source	

6. Once you get the message, restart the application server.
7. 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
[May] [2022]
Version 14.6.0.0.0

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], [2022], 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.

