

Oracle FLEXCUBE Password Change
Oracle FLEXCUBE Universal Banking
Release 14.5.3.0.0
Part No. F50379-01
[November] [2021]



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	3-1
3.2.3 Changing Password in Decentralized Setup	3-4
3.3 CHANGING SCHEDULER DATA SOURCE PASSWORD	3-4
3.3.1 Prerequisites	3-4
3.3.2 Changing Scheduler Data Source Password	3-5
3.4 CHANGING ELCM DATA SOURCE PASSWORD	3-7
3.4.1 Prerequisites	3-7
3.4.2 Changing ELCM Data Source Password	3-7
3.5 CHANGING BI PUBLISHER DATA SOURCE PASSWORD	3-9
3.5.1 Prerequisites	3-9
3.5.2 Changing BI Publisher Data Source Password	3-9
3.6 CHANGING ORACLE BUSINESS INTELLIGENCE ENTERPRISE EDITION SCHEMA PASSWORD	3-10
3.6.1 Prerequisites	3-10
3.6.2 Changing BI Publisher Data Source Password	3-11
3.7 CHANGING GATEWAY DATA SOURCE PASSWORD	3-12
3.7.1 Prerequisites	3-12
3.7.2 Changing Gateway Data Source Password	3-12
3.8 CHANGING BRANCH SCHEMA PASSWORD	3-14
3.8.1 Prerequisites	3-14
3.8.2 Changing Branch Data Source Password	3-14
4. CHANGING PASSWORDS IN IBM WEBSPHERE.....	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	4-1
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 ELCM DATA SOURCE PASSWORD	4-7
4.4.1 Prerequisites	4-7
4.4.2 Changing ELCM Data Source Password	4-7
4.4.3 Testing ELCM Schema Password Change	4-9
4.5 CHANGING GATEWAY PASSWORD	4-10
4.5.1 Prerequisites	4-10
4.5.2 Changing Gateway Data Source Password	4-10
4.5.3 Testing Gateway Data Source Password Change	4-11

4.6	CHANGING BRANCH SCHEMA PASSWORD	4-12
4.6.1	<i>Prerequisites</i>	4-12
4.6.2	<i>Changing Branch Data Source Password</i>	4-13
4.6.3	<i>Testing Branch Schema Password Change</i>	4-14
5.	SERVER PASSWORD CHANGE	5-1
5.1	INTRODUCTION	5-1
5.2	CHANGING SMTP SERVER PASSWORD.....	5-1
5.2.1	<i>Prerequisites</i>	5-2
5.2.2	<i>Changing SMTP Server Password</i>	5-2
5.3	CHANGING EMS FTP SERVER PASSWORD	5-3
5.3.1	<i>Prerequisites</i>	5-4
5.3.2	<i>Changing FTP Server Password</i>	5-4
5.4	CHANGING BPEL ADMINISTRATIVE CONSOLE PASSWORD	5-5
5.4.1	<i>Prerequisites</i>	5-6
5.4.2	<i>Changing BPEL Server Password</i>	5-6
5.5	CHANGING BIP ADMINISTRATIVE CONSOLE PASSWORD.....	5-7
5.5.1	<i>Prerequisites</i>	5-8
5.5.2	<i>Changing BIP Server Password</i>	5-8
5.6	CHANGING DMS SERVER PASSWORD	5-9
5.6.1	<i>Prerequisites</i>	5-10
5.6.2	<i>Changing BIP Server Password</i>	5-10

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	About this Manual acquaints you quickly with the purpose, organization and the audience of the manual.
Chapter 2	Oracle FLEXCUBE Password Change gives an outline of the processes involved in changing the passwords of various data sources.
Chapter 3	Changing Passwords in Oracle WebLogic describes the method of changing data source passwords from Oracle WebLogic application server.
Chapter 4	Changing Passwords in IBM Websphere describes the method of changing data source passwords from IBM Websphere application server.
Chapter 5	Server Password Change 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

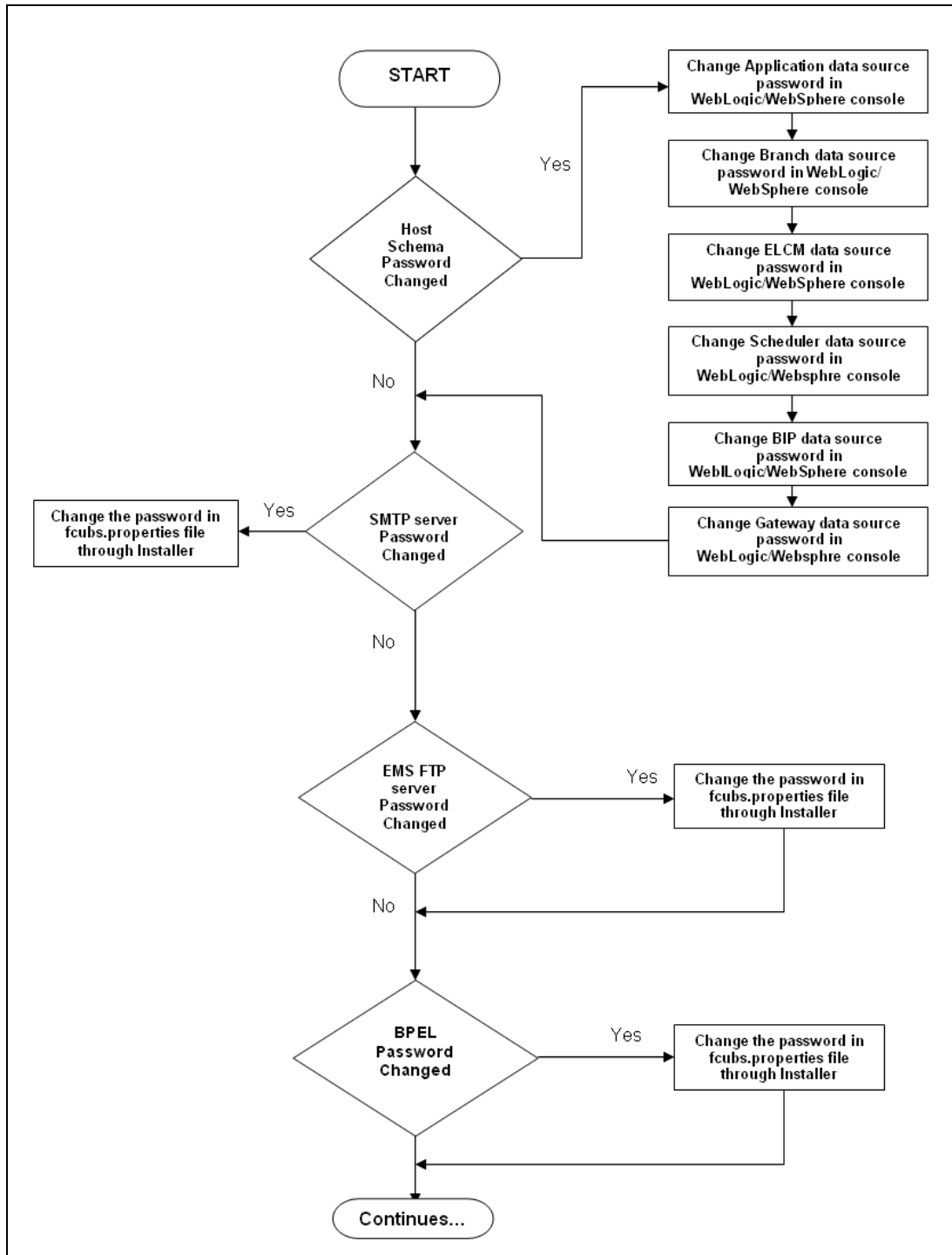
2.1 Introduction

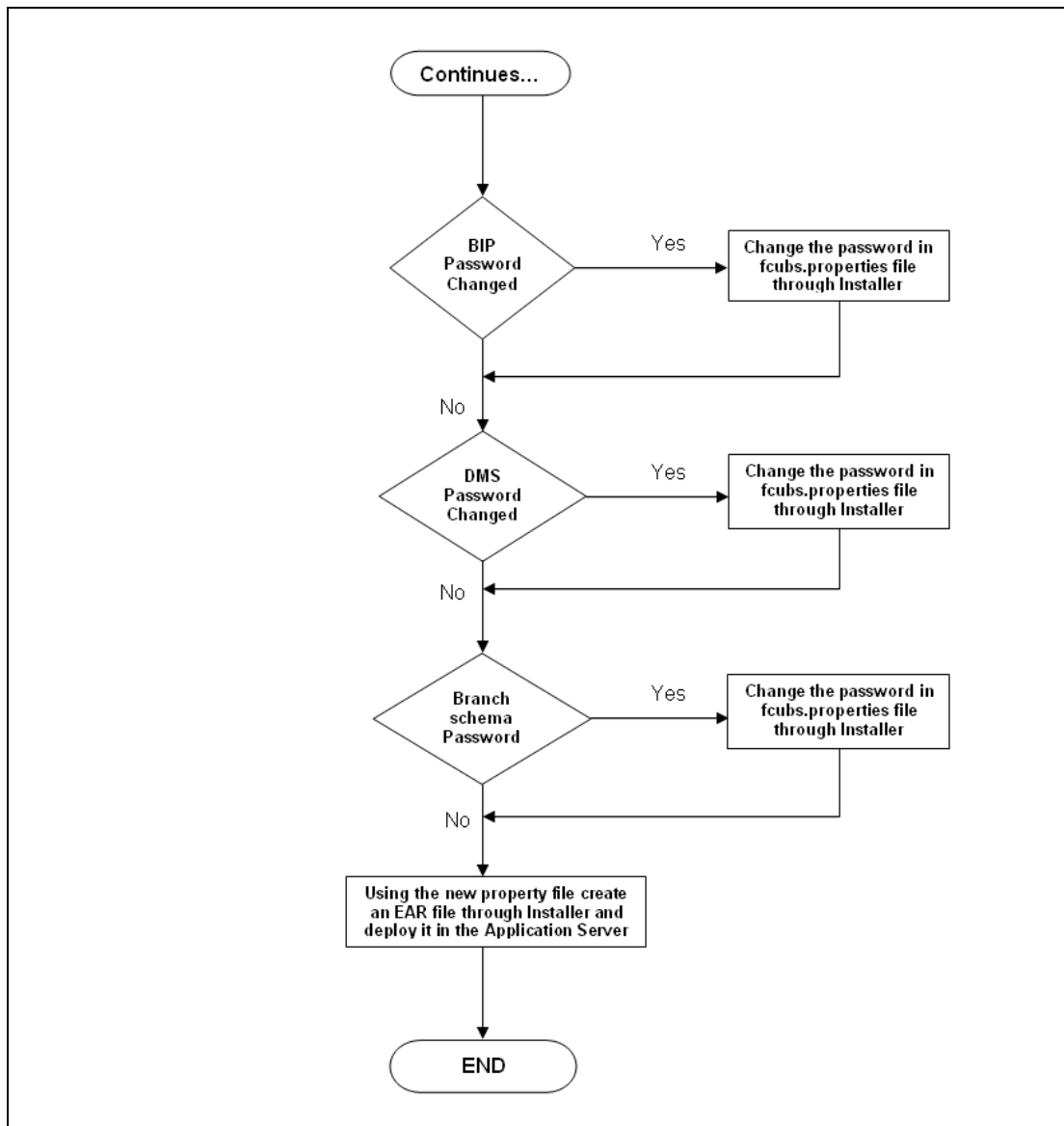
This chapter explains the process of changing the passwords of data sources associated with Oracle FLEXCUBE.

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

- Oracle FLEXCUBE Host Schema
- Scheduler Data Source
- ELCM Data Source
- BI Publisher 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:

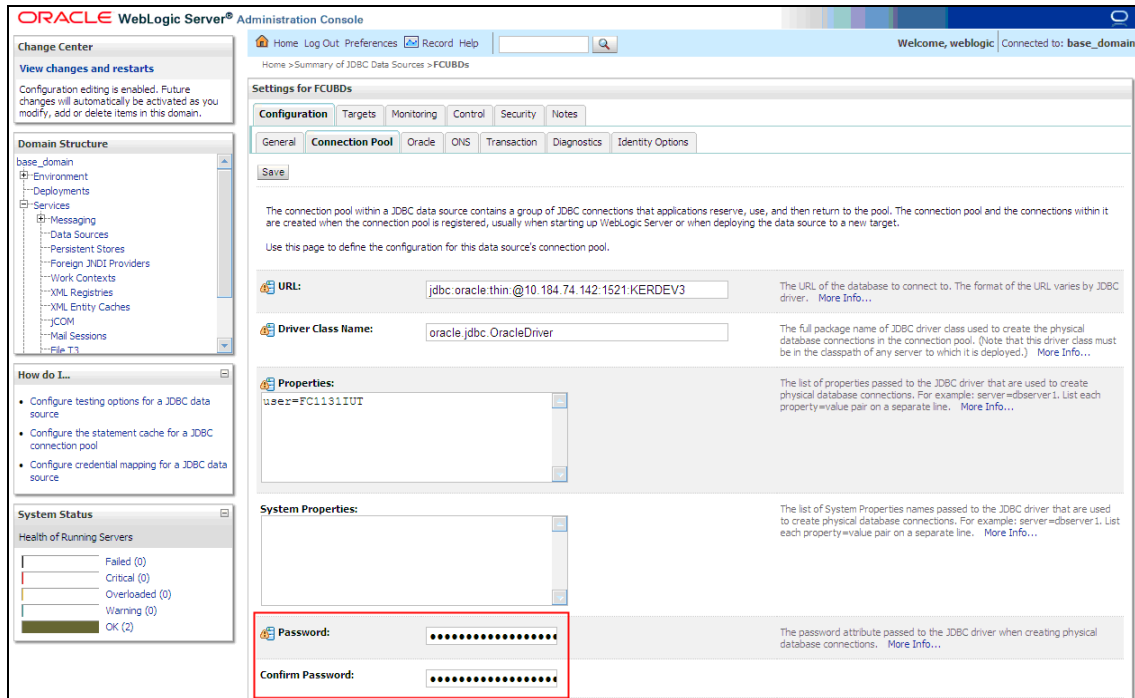
1. Determine the downtime for the password change and test activities.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server,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

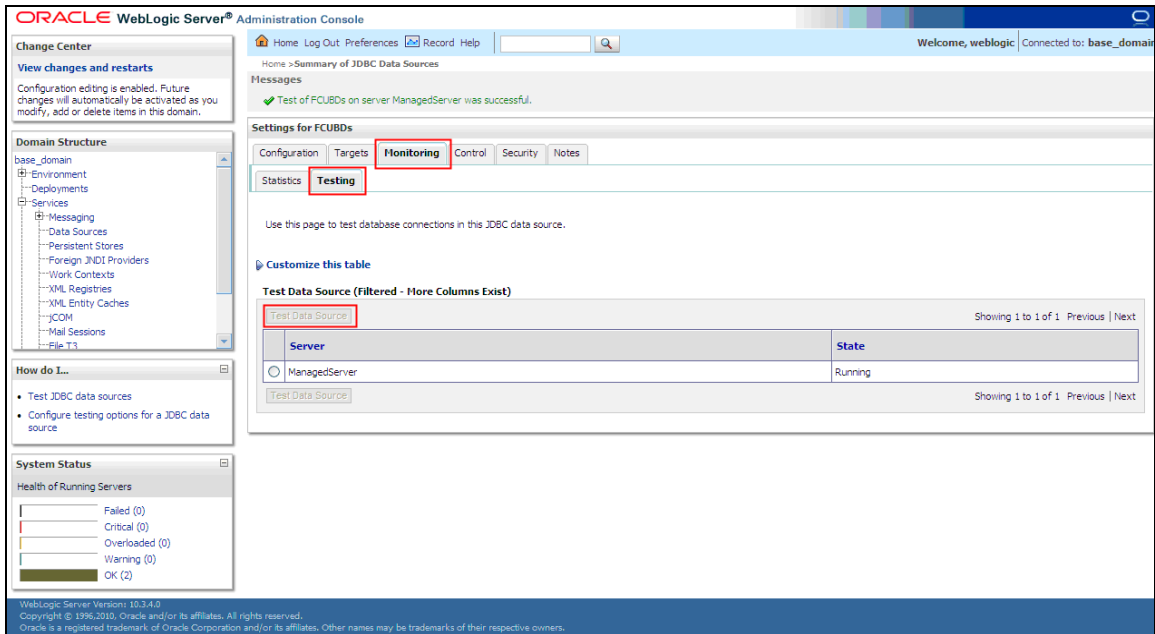
Specify the new password.

Confirm Password

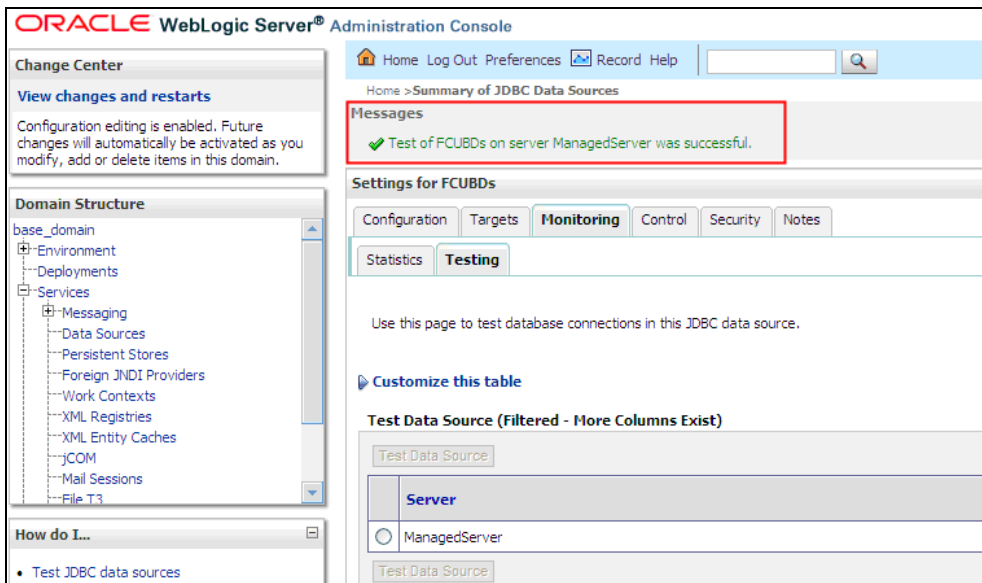
Specify the new password again.

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.

3.2.3 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 Universal Banking Solution 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 'Change Center' and 'Domain Structure' panels. The main content area displays the 'Settings for FCUBS_SchedulerDS' page. The 'Connection Pool' tab is 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=FC11S1IUT'. 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. The left sidebar contains the 'Change Center' and 'Domain Structure' tree. The main area displays the 'Settings for FCUBS_SchedulerDS' with the 'Monitoring' tab selected. Below the tabs, the 'Testing' sub-tab is active. A message box 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 the test results. The table has two columns: 'Server' and 'State'. The 'ManagedServer' is listed with a 'Running' state.

Server	State
ManagedServer	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, showing the 'Monitoring' tab for 'FCUBS_SchedulerDS'. A red box highlights the message: 'Test of FCUBS_SchedulerDS on server ManagedServer was successful.' The 'Testing' sub-tab is still selected, and the table below it shows the 'ManagedServer' in a 'Running' state.

Server	State
ManagedServer	Running

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 Universal Banking Solution Installer.



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

3.4 Changing ELCM Data Source Password

You need to change the password of ELCM data source.

3.4.1 Prerequisites

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

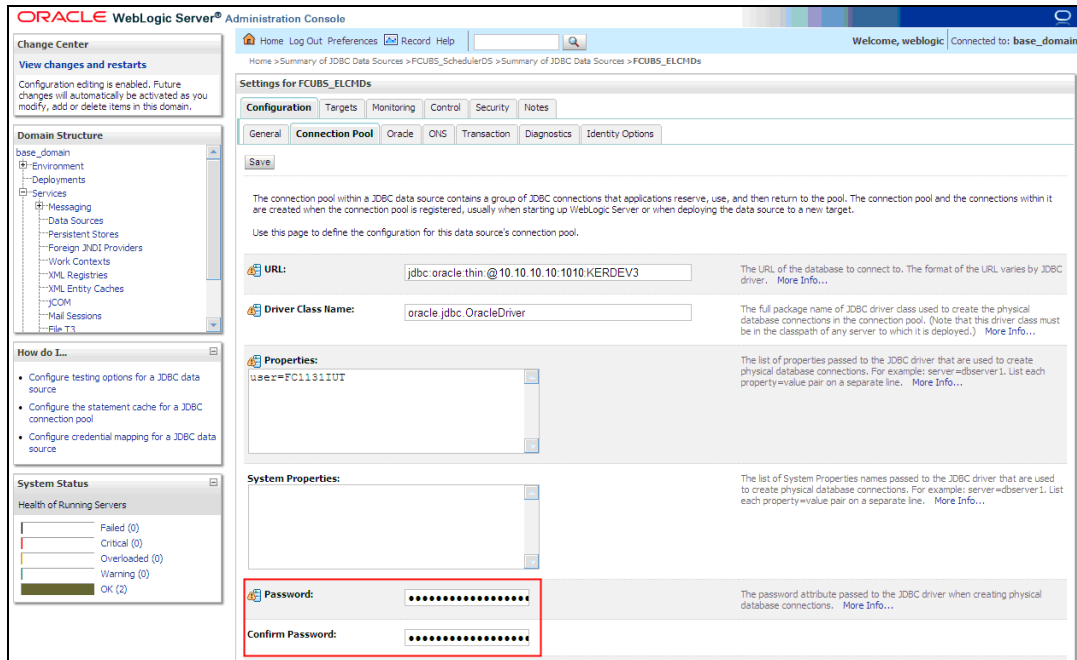
1. Determine the down time for the password change activity.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server, follow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

3.4.2 Changing ELCM Data Source Password

You need to change the password of ELCM 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 ELCM data source.
4. Select **Connection Pool** tab.



5. Change the password. Use the following fields:

Password

Specify the new password.

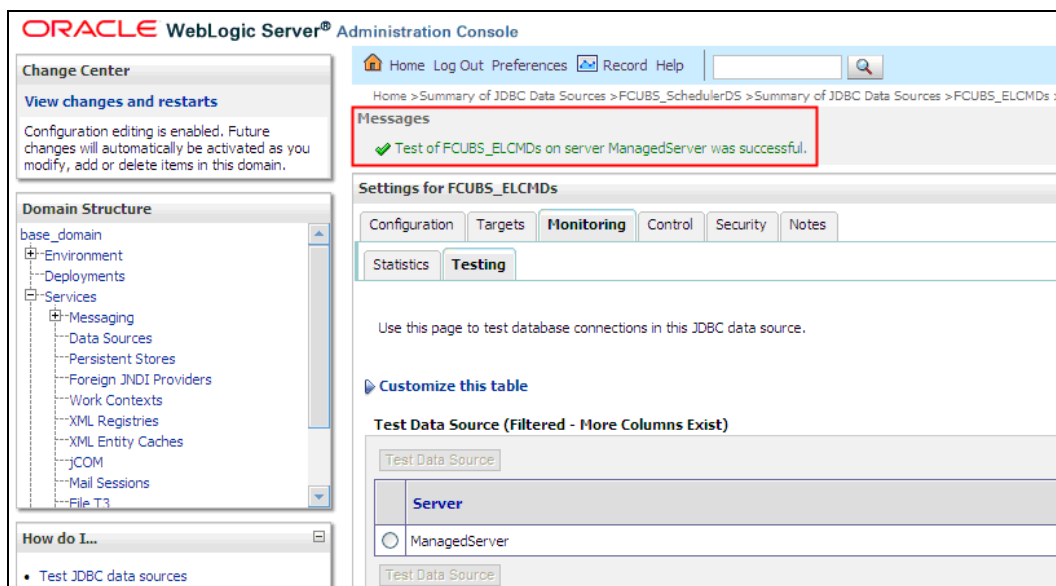
Confirm Password

6. Specify the new password again. 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 Universal Banking Solution Installer.



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

3.5 Changing BI Publisher Data Source Password

You need to change the password of the BI Publisher data source.

3.5.1 Prerequisites

Before you change the password of BI Publisher 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:
6. Login to Oracle WebLogic application server
7. Go to **Home > Environments > Servers**
8. Select and stop the server and clicking 'Stop' button.
9. This completes the prerequisites.

3.5.2 Changing BI Publisher Data Source Password

To change the BI Publisher data source password, follow the steps given below:

1. Log in to BI Publisher server.
2. Go to Admin > JDBC > Update Data Source.

ORACLE BI Publisher Enterprise

Welcome, administrator Preferences Sign Out Help

Reports Schedules Admin

Admin > JDBC > Update Data Source: Oracle BI EE

Update Data Source: Oracle BI EE

Cancel Apply

General

TIP Please make sure to install the required JDBC driver classes.

Data Source Name: Oracle BI EE

* Driver Type: Oracle BI Server

* Database Driver Class: oracle.bi.jdbc.AnaJdbcDriver

* Connection String: jdbc:oraclebi://HOST:PORT/

* Username: Administrator

Password:

Pre Process Function

Post Process Function

☒ Use Proxy Authentication

Test Connection

Security

Available Roles

Allowed Roles

Move Move All Remove Remove All

3. Choose the data source whose password needs to be modified.
4. Modify the following field:

Password

Specify the new password.

5. Click 'Apply' button.
6. Restart the application server.
7. Start Oracle FLEXCUBE.
8. Log in to Oracle FLEXCUBE. Generate a sample report to test.



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

3.6 Changing Oracle Business Intelligence Enterprise Edition Schema Password

You need to change the password of the Oracle Business Intelligence Enterprise Edition (OBIEE) data sources.

3.6.1 Prerequisites

Before you change the password of BI Publisher 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.

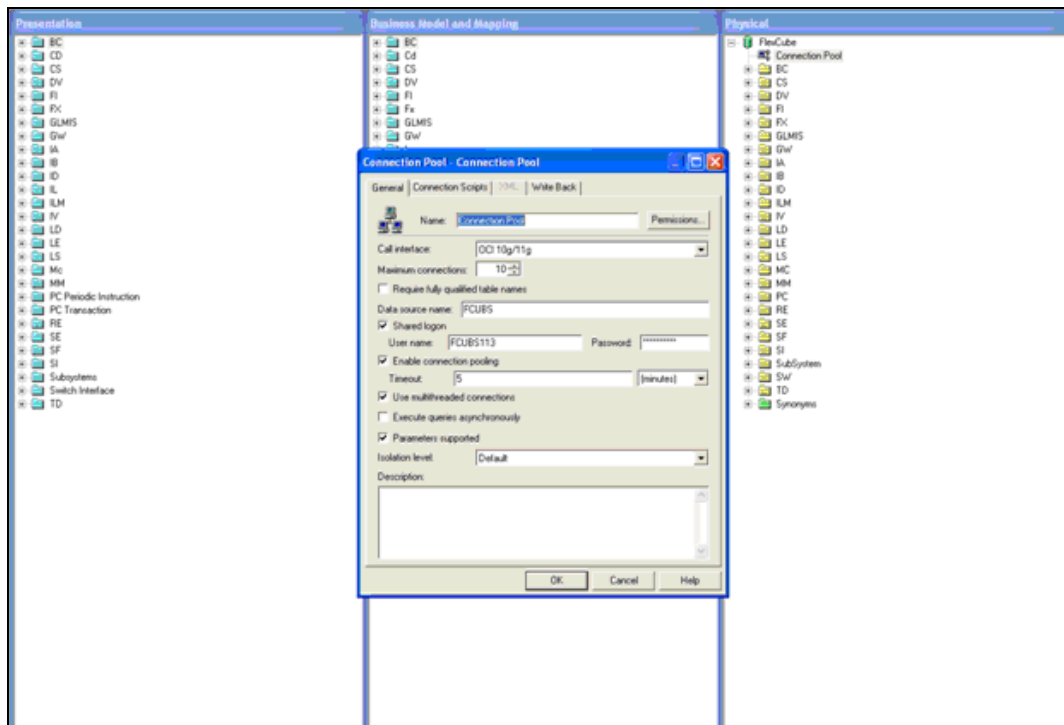
3. Ensure that all users have logged out of Oracle FLEXCUBE system.
4. Stop Oracle FLEXCUBE application.
5. Stop the target server to which the data sources point. To stop the target server, follow the steps below:
 - Login to Oracle WebLogic application server
 - Go to **Home > Environments > Servers**
 - Select and stop the server by clicking 'Stop' button.

This completes the prerequisites.


3.6.2 Changing BI Publisher Data Source Password

To change the OBIEE data source password, follow the steps given below:

1. Login in to OBIEE Administrative console.
2. Go to Database created > Connection Pool. You will get 'Connection Pool' window.



3. Change the password. You will be prompted to re-enter the password. Click 'OK'.
4. Restart the application server.
5. Start Oracle FLEXCUBE.
6. Log in to Oracle FLEXCUBE. Generate a sample report to test.

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

3.7 **Changing Gateway Data Source Password**

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

3.7.1 **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.

3.7.2 **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.

Modify, add or delete items in this domain.

Domain Structure

- base_domain
 - Environment
 - Deployments
 - Services
 - Messaging
 - Data Sources
 - Persistent Stores
 - Foreign JNDI Providers
 - Work Contexts
 - XML Registries
 - XML Entity Caches
 - JCOM
 - Mail Sessions
 - File T3

How do I...

- Configure testing options for a JDBC data source
- Configure the statement cache for a JDBC connection pool
- Configure credential mapping for a JDBC data source

System Status

Health of Running Servers

Failed (0)	OK (2)
------------	--------

Configuration | Targets | Monitoring | Control | Security | Notes

General | **Connection Pool** | Oracle | ONS | Transaction | Diagnostics | Identity Options

Save

The connection pool within a JDBC data source contains a group of JDBC connections that applications reserve, use, and then return to the pool. The connection pool and the connections within it are created when the connection pool is registered, usually when starting up WebLogic Server or when deploying the data source to a new target.

Use this page to define the configuration for this data source's connection pool.

URL: jdbc:oracle:thin:@10.10.10.10:1010:KERDEV3
The URL of the database to connect to. The format of the URL varies by JDBC driver. [More Info...](#)

Driver Class Name: oracle.jdbc.xa.client.OracleXADataSource
The full package name of JDBC driver class used to create the physical database connections in the connection pool. (Note that this driver class must be in the classpath of any server to which it is deployed.) [More Info...](#)

Properties:
user=FC1131IUT
The list of properties passed to the JDBC driver that are used to create physical database connections. For example: server=dbserver1. List each property=value pair on a separate line. [More Info...](#)

System Properties:
The list of System Properties names passed to the JDBC driver that are used to create physical database connections. For example: server=dbserver1. List each property=value pair on a separate line. [More Info...](#)

Password:
The password attribute passed to the JDBC driver when creating physical database connections. [More Info...](#)

Confirm Password:
The password attribute passed to the JDBC driver when creating physical database connections. [More Info...](#)

Initial Capacity: 1
The number of physical connections to create when creating the connection pool. [More Info...](#)

Maximum Capacity: 15
The maximum number of physical connections that this connection pool can contain. [More Info...](#)

Capacity Threshold:
The number of connections reached when new connections are added to the pool. [More Info...](#)

5. Change the password. Use the following fields:

Password

Specify the new password

Confirm Password

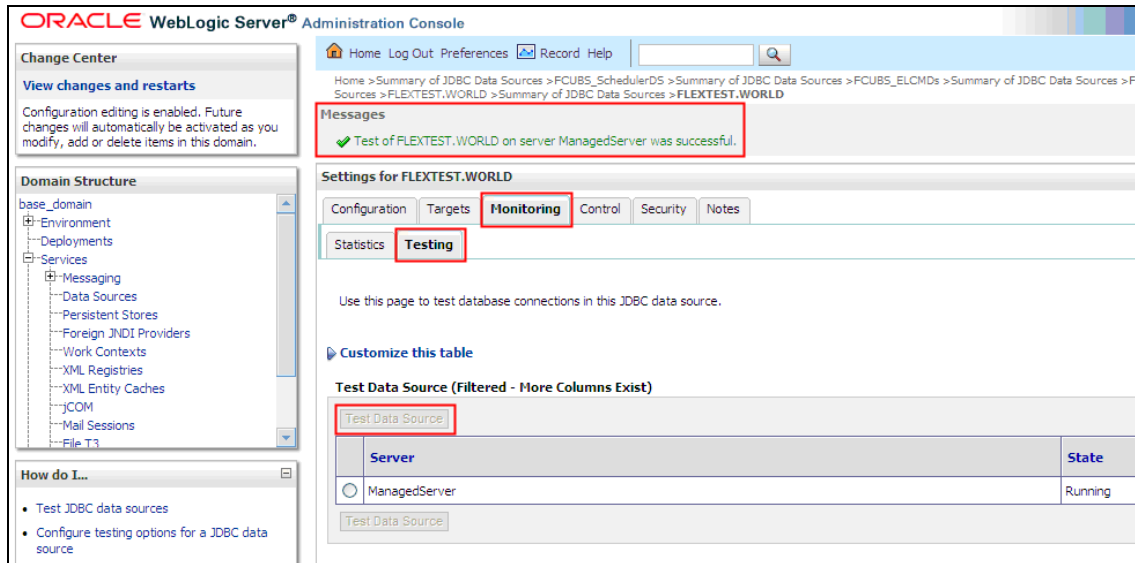
Specify the new password again

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. Log in to Oracle FLEXCUBE and test whether the change was successful.

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

3.8 Changing Branch Schema Password

This section describes the steps involved in changing branch schema password.

3.8.1 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. Stop Oracle FLEXCUBE application.
4. 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.
5. Ensure that all users have logged out of Oracle FLEXCUBE system.

This completes the prerequisites.

3.8.2 Changing Branch 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 (jdbc/fcjddevDSBranch).
4. Select 'Connection Pool' tab.

ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: base_domain

Home > Summary of JDBC Data Sources > FCUBSBranch

Settings for FCUBSBranch

Configuration Targets Monitoring Control Security Notes

General **Connection Pool** Oracle ONS Transaction Diagnostics Identity Options

Save

The connection pool within a JDBC data source contains a group of JDBC connections that applications reserve, use, and then return to the pool. The connection pool and the connections within it are created when the connection pool is registered, usually when starting up WebLogic Server or when deploying the data source to a new target.

Use this page to define the configuration for this data source's connection pool.

URL: jdbc:oracle:thin:@10.10.10.10:1010:KERDEV3 The URL of the database to connect to. The format of the URL varies by JDBC driver. [More Info...](#)

Driver Class Name: oracle.jdbc.xa.client.OracleXADataSource The full package name of JDBC driver class used to create the physical database connections in the connection pool. (Note that this driver class must be in the classpath of any server to which it is deployed.) [More Info...](#)

Properties: user=FC1131IUT The list of properties passed to the JDBC driver that are used to create physical database connections. For example: server=dbserver1. List each property=value pair on a separate line. [More Info...](#)

System Properties: The list of System Properties names passed to the JDBC driver that are used to create physical database connections. For example: server=dbserver1. List each property=value pair on a separate line. [More Info...](#)

Password: The password attribute passed to the JDBC driver when creating physical database connections. [More Info...](#)

Confirm Password:

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.

ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: base_domain

Home > Summary of Servers > Summary of JDBC Data Sources > FCUBSBranch

Messages

Test of FCUBSBranch on server ManagedServer was successful.

Settings for FCUBSBranch

Configuration Targets **Monitoring** Control Security Notes

Statistics **Testing**

Use this page to test database connections in this JDBC data source.

Customize this table

Test Data Source (Filtered - More Columns Exist)

Test Data Source Showing 1 to 1 of 1 Previous Next

Server	State
ManagedServer	Running

Test Data Source Showing 1 to 1 of 1 Previous Next

How do I...

- Test JDBC data sources
- Configure testing options for a JDBC data source

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.

STOP 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

Integrated Solutions Console Welcome admin

Cell=DDHP0520Node01Cell, Profile=AppSrvV01

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard | Security Configuration Report

Administrative security

☒ Enable administrative security

Application security

☐ Enable application security

Java 2 security

☐ Use Java 2 security to restrict application access to local resources

☒ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

User account repository

Current realm definition

Federated repositories

Available realm definitions

Federated repositories

Configure... Set as current

Apply Reset

Authentication

Authentication mechanisms and expiration

☒ LTPA

☐ Kerberos and LTPA

(This function is currently disabled. See the IBM Support site for possible future updates.)

☐ SWAM (deprecated): No authenticated communication between servers

Java Authentication and Authorization Service

☒ Application logins

☒ System logins

☒ J2C authentication data

☐ Use realm-qualified user names

Specifies a list 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.

Integrated Solutions Console Welcome

Cell=IPL189DORNode06Cell, Profile=AppSrvV06

Global security > J2C authentication data

Specifies a list of user identities and passwords for Java(TM) 2 connector security to use.

☒ Prefix new alias names with the node name of the cell (for compatibility with earlier releases)

Apply

Preferences

New Delete

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

Total 1

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

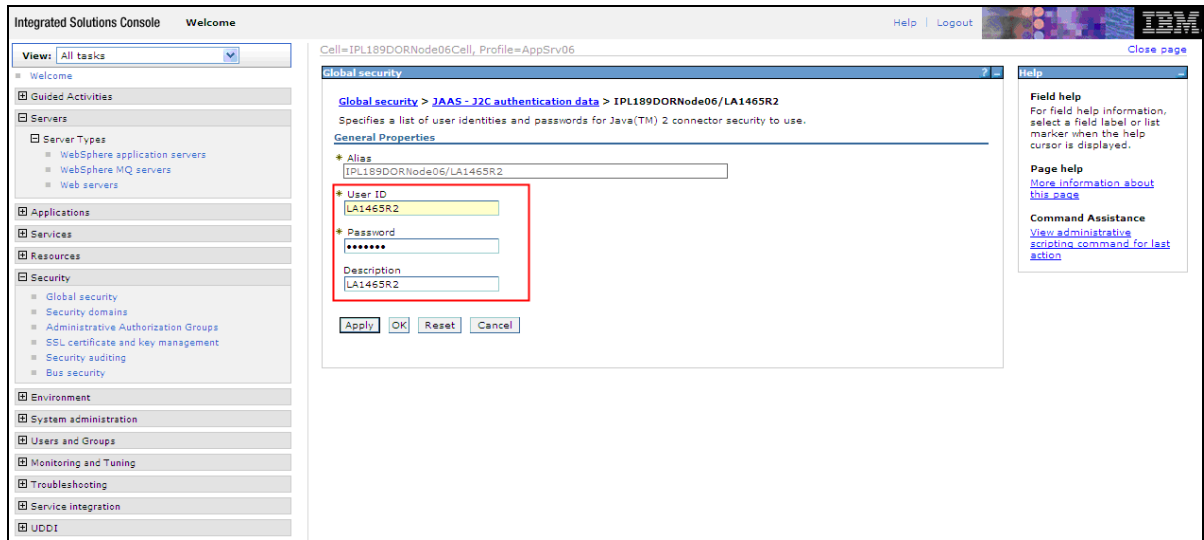
Page help

More information about this page

Command Assistance

View administrative actions command for last action

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

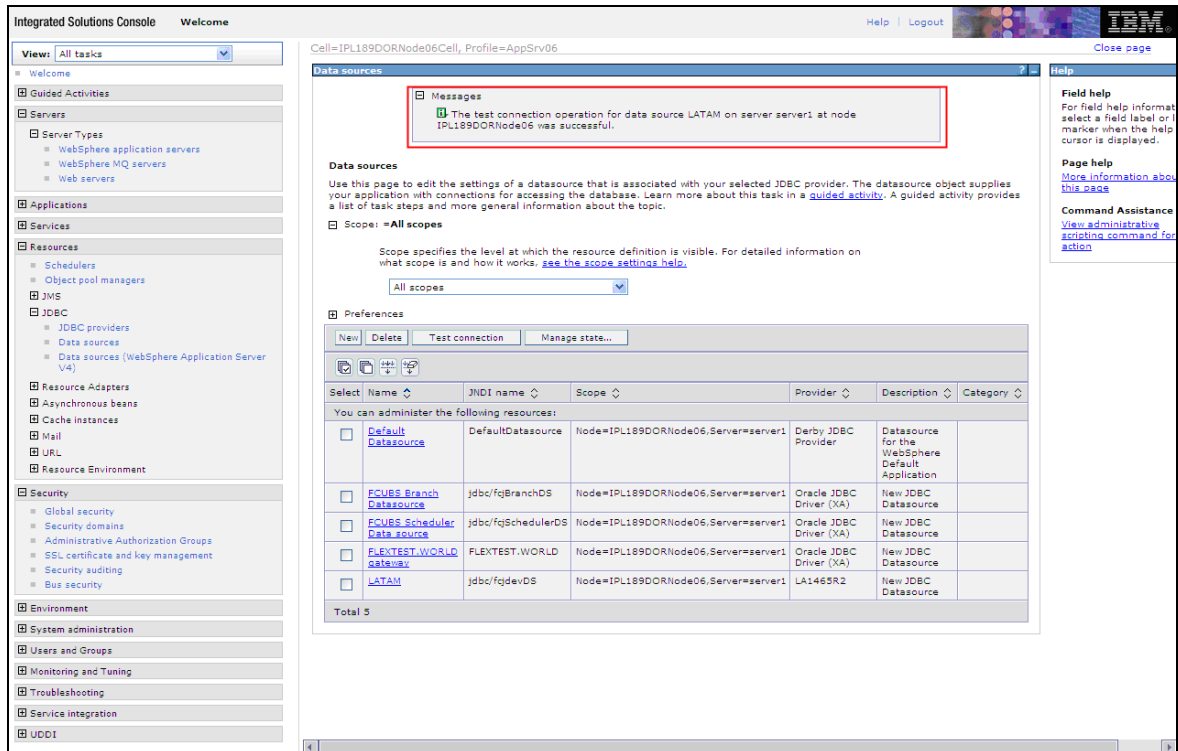


4. Specify the new password and click 'Apply' button. Click 'OK'.

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 *jdbcfc/devDS*.
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

Integrated Solutions Console Welcome admin

Cell=DDHP0520Node01Cell, Profile=AppSrv01

Global security

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard Security Configuration Report

Administrative security

☒ Enable administrative security

Application security

☐ Enable application security

Java 2 security

☐ Use Java 2 security to restrict application access to local resources

User account repository

Current realm definition

Federated repositories

Available realm definitions

Federated repositories

Configure... Set as current

Apply Reset

Authentication

Authentication mechanisms and expiration

☒ LTPA

☐ Kerberos and LTPA

(This function is currently disabled. See the IBM Support site for possible future updates.)

Kerberos configuration

SWAM (deprecated): No authenticated communication between servers

Authentication cache settings

Web and SIP security

RM/IIOP security

Java Authentication and Authorization Service

☒ Application logins

☒ System logins

☒ J2C authentication data

Use realm-qualified user names

Specify a list 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.

Security domains

External authorization providers

Custom properties

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

Integrated Solutions Console Welcome

Cell=JPL189DORNode06Cell, Profile=AppSrv06

Global security

Global security > JAAS - J2C authentication data

Specifies a list of user identities and passwords for Java(TM) 2 connector security to use.

☒ Prefix new alias names with the node name of the cell (for compatibility with earlier releases)

Apply

Preferences

New Delete

Select Alias User ID Description

You can administer the following resources:

<input type="checkbox"/>	J2C189DORNode06/LA1465R2	LA1465R2	LA1465R2
--------------------------	--------------------------	----------	----------

Total 1

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

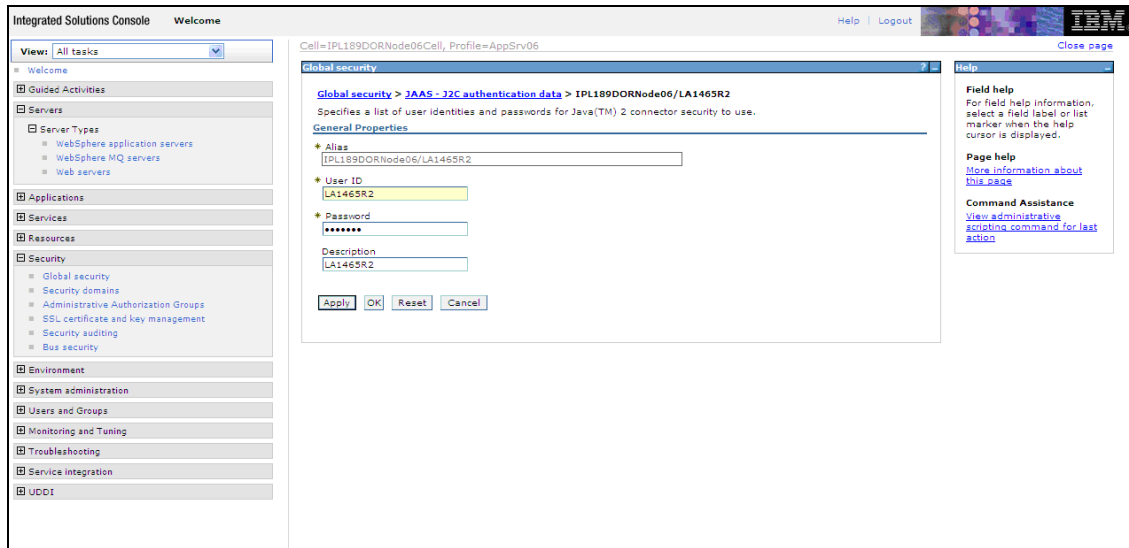
Page help

More information about this page

Command Assistance

View administrative scripting commands for J2C actions

3. You will notice a table listing 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 *jdbc/fcjSchedulerDS*.
4. Click 'Test connection' tab.
5. The screen displays a message confirming successful testing.

The screenshot shows the Integrated Solutions Console interface. On the left is a navigation tree with categories like Servers, Applications, Services, Resources, Security, and Environment. The main panel displays a message box stating: "The test connection operation for data source FCUBS Scheduler Data source on server server1 at node IPL189DORNode06 was successful." Below this, there's a section for "Data sources" with a table listing various data sources. The table has columns for Name, JNDI name, Scope, Provider, Description, and Category. The listed data sources include DefaultDataSource, FCUBS Branch Data source, FCUBS Scheduler Data source, FLEXTTEST.WORLD, and LATAM.

Select	Name	JNDI name	Scope	Provider	Description	Category
<input type="checkbox"/>	DefaultDataSource	DefaultDataSource	Node=IPL189DORNode06,Server=server1	Derby JDBC Provider	DataSource for the WebSphere Default Application	
<input type="checkbox"/>	FCUBS Branch Data source	jdbc/fqBranchDS	Node=IPL189DORNode06,Server=server1	Oracle JDBC Driver (XA)	New JDBC DataSource	
<input type="checkbox"/>	FCUBS Scheduler Data source	jdbc/fqSchedulerDS	Node=IPL189DORNode06,Server=server1	Oracle JDBC Driver (XA)	New JDBC DataSource	
<input type="checkbox"/>	FLEXTTEST.WORLD	FLEXTTEST.WORLD	Node=IPL189DORNode06,Server=server1	Oracle JDBC Driver (XA)	New JDBC DataSource	
<input type="checkbox"/>	LATAM	jdbc/fqdevDS	Node=IPL189DORNode06,Server=server1	LA1465R2	New JDBC DataSource	

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 ELCM Data Source Password

4.4.1 Prerequisites

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

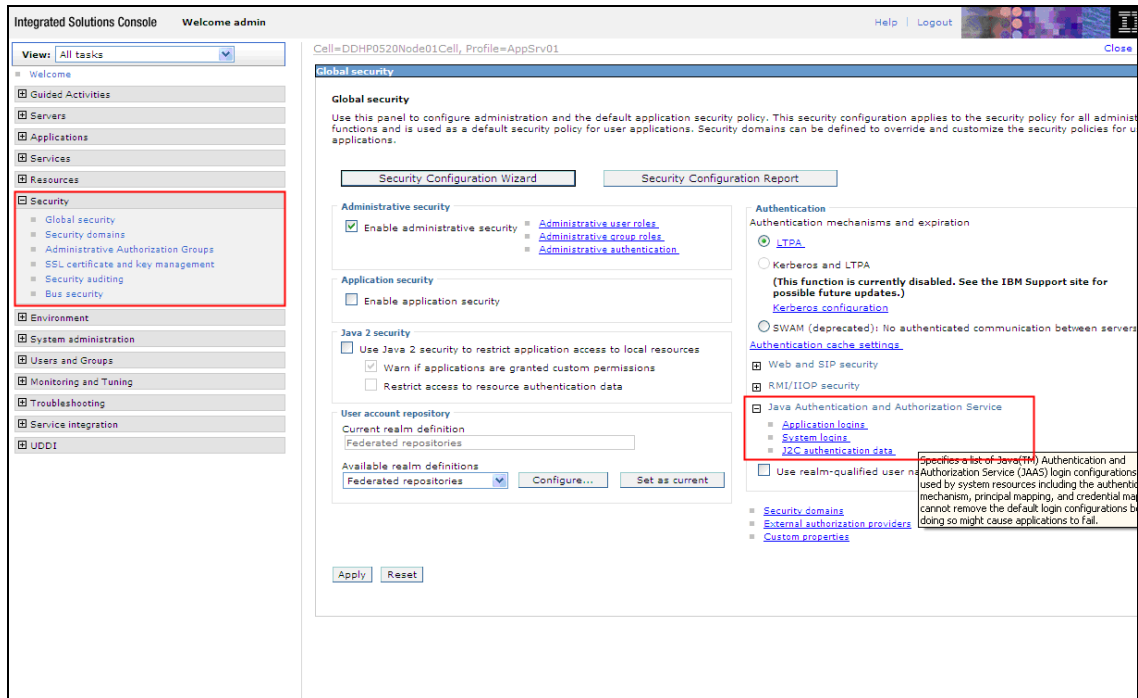
1. Determine the down time for the password change activity.
2. Inform all concerned users and groups.
3. Ensure that all users have logged out of Oracle FLEXCUBE system
4. Stop Oracle FLEXCUBE application
5. Stop the target server to which the data sources point.

This completes the prerequisites.

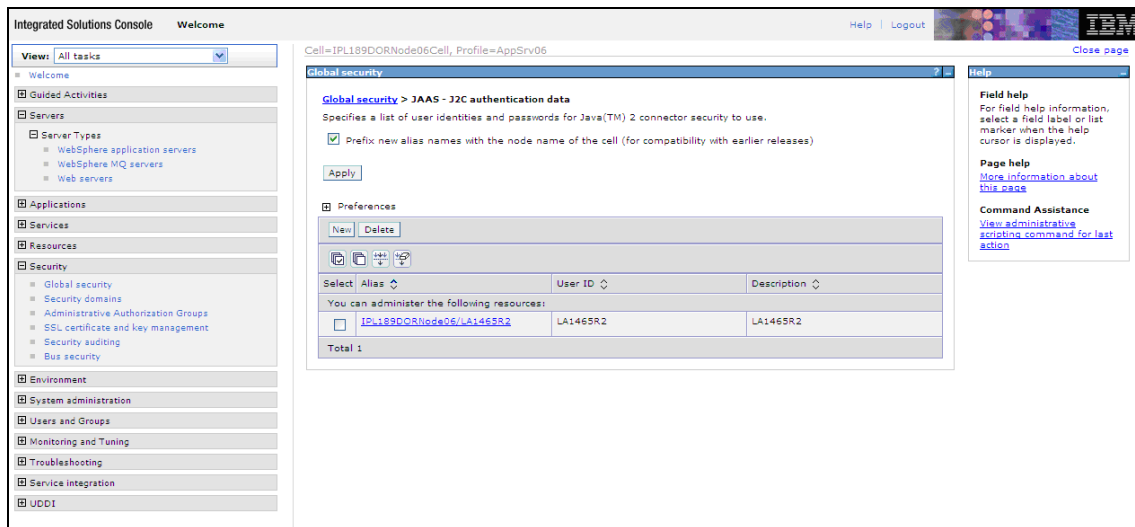
4.4.2 Changing ELCM Data Source Password

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

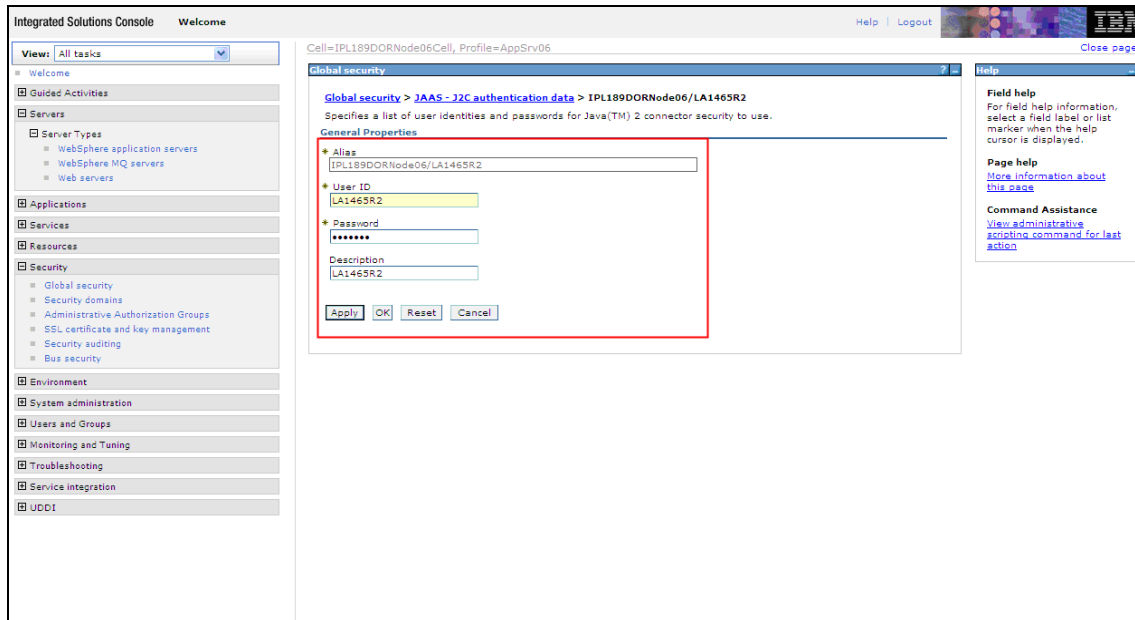
1. Log in to IBM Websphere application server.



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 node which is been used by ELCM data source.



4. Specify the new password in the text field and click 'Apply'. Click 'OK'.

4.4.3 **Testing ELCM Schema 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 *jdbc/fcjddevDS*.
4. Select 'Test connection' tab.
5. The screen displays a message confirming successful testing.

The screenshot shows the Integrated Solutions Console interface. On the left is a navigation tree with categories like Servers, Applications, Services, Resources, and Security. The main panel displays the 'Data sources' configuration page for the cell 'IPL189DORNode06Cell, Profile=AppSrv06'. A red box highlights a message: 'The test connection operation for data source LATAM on server server1 at node IPL189DORNode06 was successful.' Below this, the 'Data sources' section provides instructions and a table of existing data sources.

Select	Name	JNDI name	Scope	Provider	Description	Category
<input type="checkbox"/>	Default Datasource	DefaultDatasource	Node=IPL189DORNode06,Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application	
<input type="checkbox"/>	FLEXCUBE Branch Datasource	jdbc/fqBranchDS	Node=IPL189DORNode06,Server=server1	Oracle JDBC Driver (XA)	New JDBC Datasource	
<input type="checkbox"/>	FLEXCUBE Scheduler Datasource	jdbc/fqSchedulerDS	Node=IPL189DORNode06,Server=server1	Oracle JDBC Driver (XA)	New JDBC Datasource	
<input type="checkbox"/>	FLEXTEST.WORLD datasource	FLEXTEST.WORLD	Node=IPL189DORNode06,Server=server1	Oracle JDBC Driver (XA)	New JDBC Datasource	
<input type="checkbox"/>	LATAM	jdbc/fqdevDS	Node=IPL189DORNode06,Server=server1	LA1465R2	New JDBC Datasource	

Total 5

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

4.5 Changing Gateway Password

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

4.5.1 Prerequisites

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

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

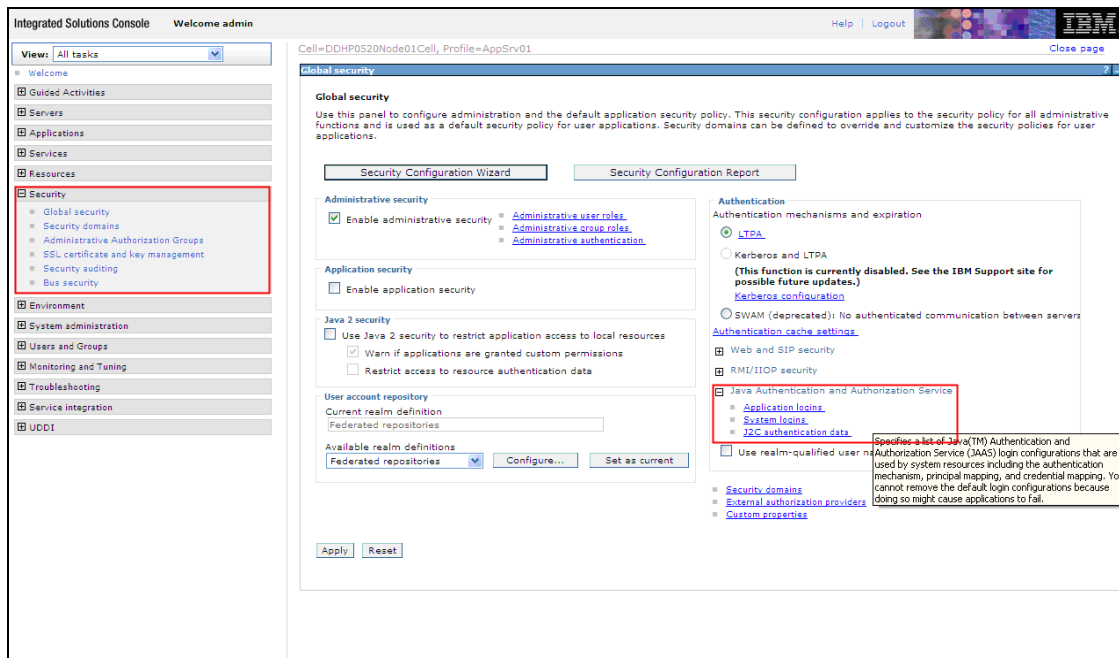
This completes the prerequisites.

4.5.2 Changing Gateway Data Source Password

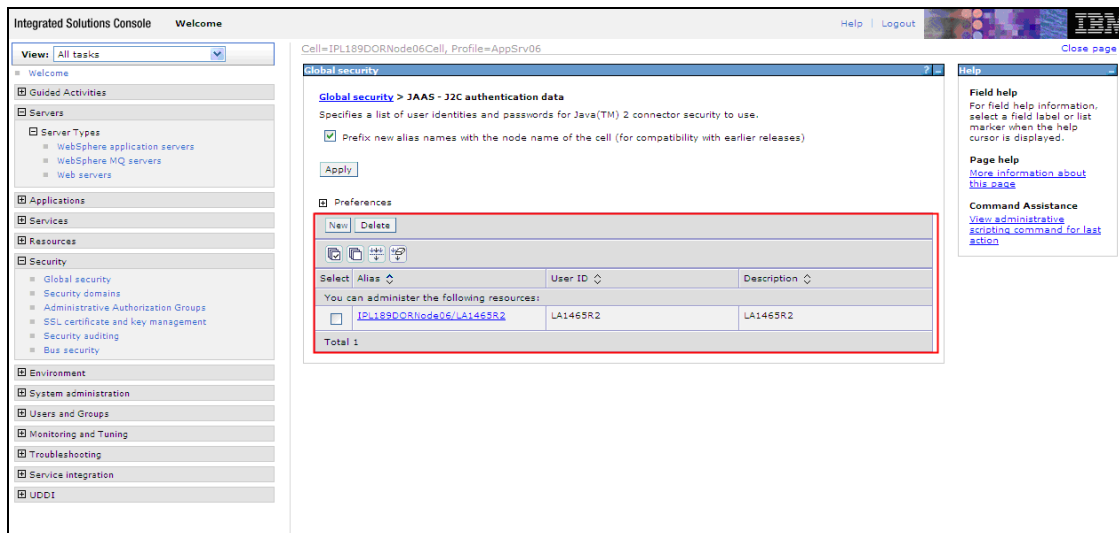
You need to change the password of Host Schema data source. Follow the steps given below.

- 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.



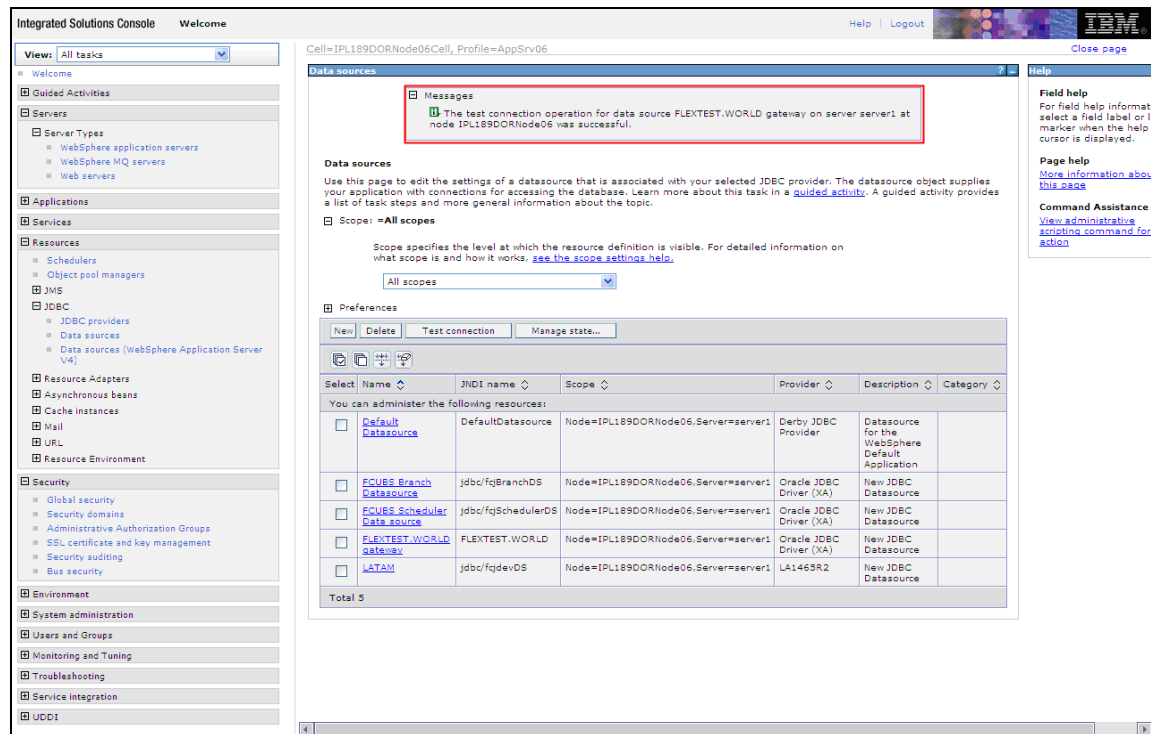
4. Specify the new password in the text field and click on Apply and then click on ok.

4.5.3 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.



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.

4.6 Changing Branch Schema Password

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

4.6.1 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.

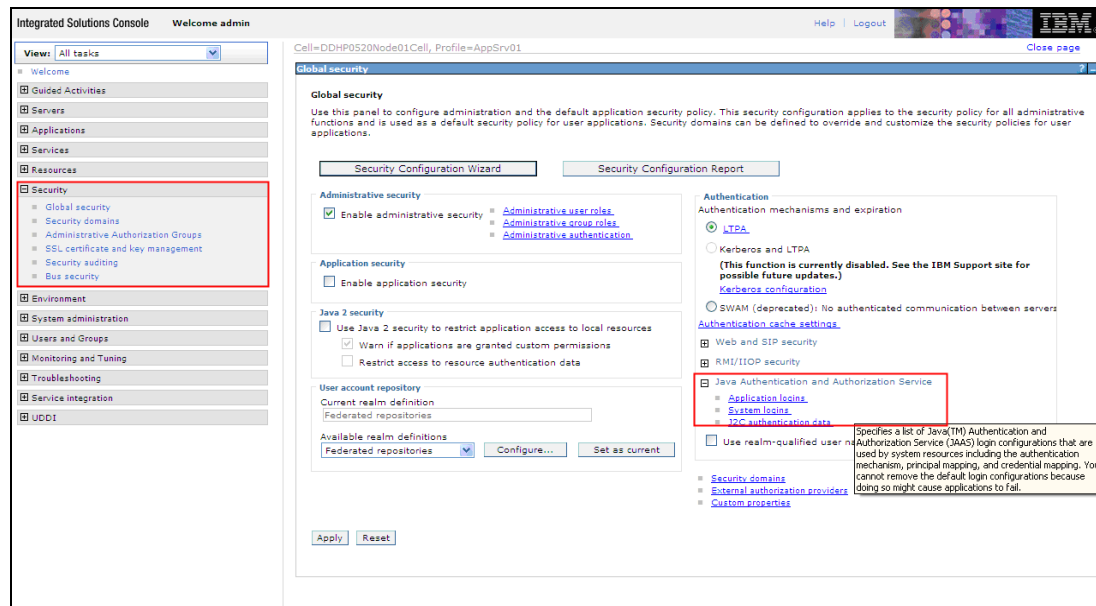
4. Ensure that all users have logged out of Oracle FLEXCUBE system.
5. Stop Oracle FLEXCUBE application.

This completes the prerequisites.

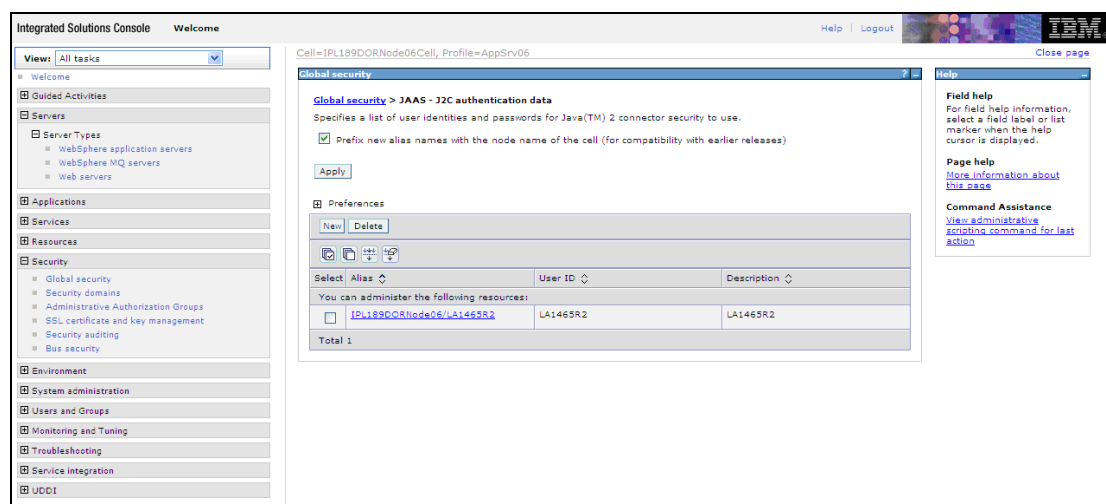
4.6.2 Changing Branch Data Source Password

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 Branch data source.



4. Specify the new password in the text field and click 'Apply'. Click 'OK'.

4.6.3 Testing Branch 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 *jdbc/fcjBranchDs*.
4. Select 'Test Connection' tab.
5. The screen displays a message confirming successful testing.

Integrated Solutions Console Welcome

Cell=IPL189DORNode06Cell_Profile=AppSrv06

Help Logout

Close page

Views: All tasks

Guided Activities

Servers

- Server Types
 - WebSphere application servers
 - WebSphere MQ servers
 - Web servers

Applications

Services

Resources

- Schedulers
- Object pool managers
- JMS
- JDBC
 - JDBC providers
 - Data sources
 - Data sources (WebSphere Application Server V4)

Resource Adapters

- Asynchronous beans
- Cache instances
- Mail
- URL
- Resource Environment

Security

- Global security
- Security domains
- Administrative Authorization Groups
- SSL certificate and key management
- Security auditing
- Bus security

Environment

- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration

Data sources

Messages

The test connection operation for data source FCUBS Branch Datasource on server server1 at node IPL189DORNode06 was successful.

Data sources

Use this page to edit the settings of a datasource that is associated with your selected JDBC provider. The datasource object supplies your application with connections for accessing the database. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

Scope: All scopes

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

All scopes

Preferences

New Delete Test connection Manage state...

Select	Name	JNDI name	Scope	Provider	Description	Category
<input type="checkbox"/>	Default Datasource	DefaultDatasource	Node=IPL189DORNode06.Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application	
<input type="checkbox"/>	FCUBS Branch Datasource	jdbc/fcjBranchDS	Node=IPL189DORNode06.Server=server1	Oracle JDBC Driver (XA)	New JDBC Datasource	
<input type="checkbox"/>	FCUBS Scheduler Data source	jdbc/fcjSchedulerDS	Node=IPL189DORNode06.Server=server1	Oracle JDBC Driver (XA)	New JDBC Datasource	
<input type="checkbox"/>	FLEXTTEST_WORLD Datasource	FLEXTTEST.WORLD	Node=IPL189DORNode06.Server=server1	Oracle JDBC Driver (XA)	New JDBC Datasource	
<input type="checkbox"/>	LATAM	jdbc/fcjdevDS	Node=IPL189DORNode06.Server=server1	LA146SR2	New JDBC Datasource	

Total 5

Field help

For field help information, select a field label or the marker when the help cursor is displayed.

Page help

[View information about this page](#)

Command Assistance

[View administrative scripting command for action](#)

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.

5. Server Password Change

5.1 Introduction

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

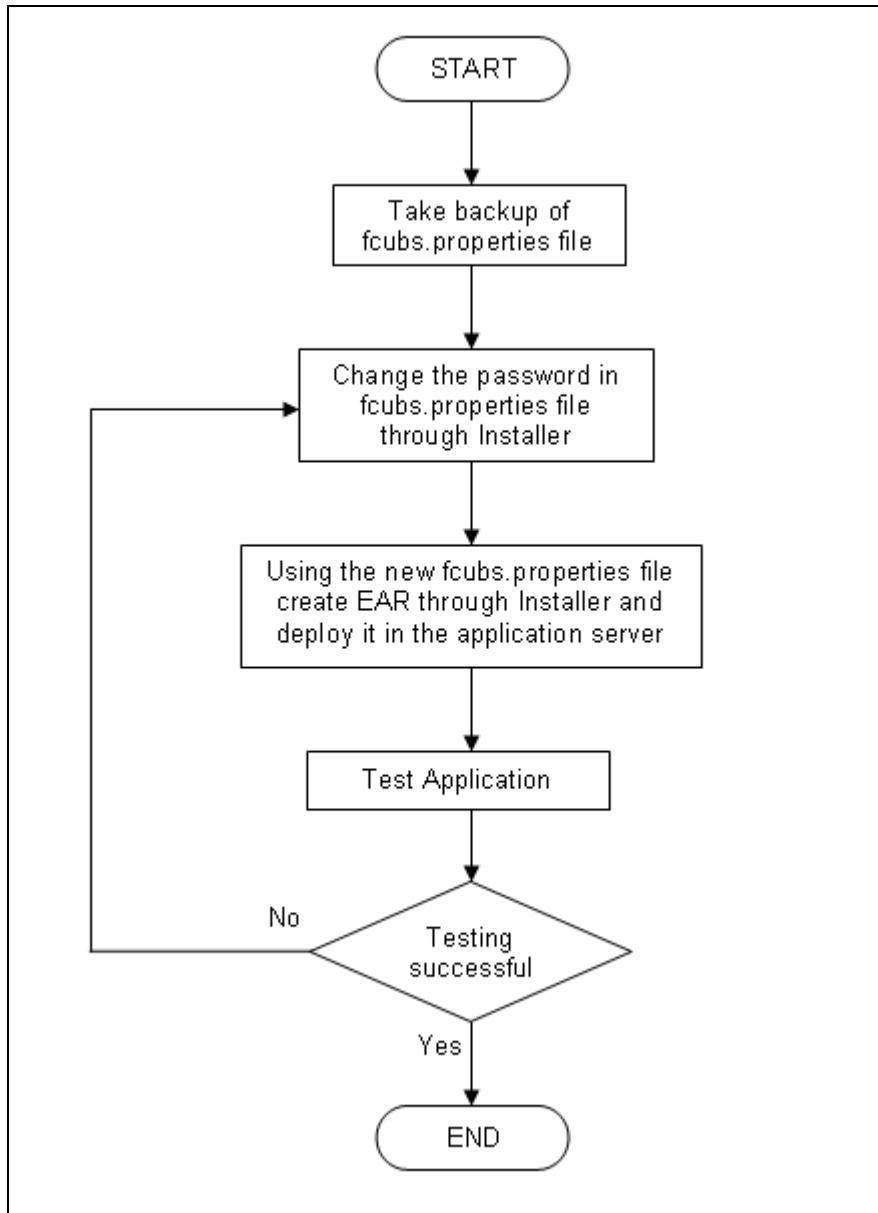
You will find the methods to change the passwords of the following servers:

- SMTP Server
- EMS FTP Server
- BPEL Server
- BIP Server
- DMS Server

5.2 Changing SMTP Server Password

This section describes the process of changing the SMTP server password.

The following diagram briefs the steps involved in changing the passwords of the SMTP server.



5.2.1 Prerequisites

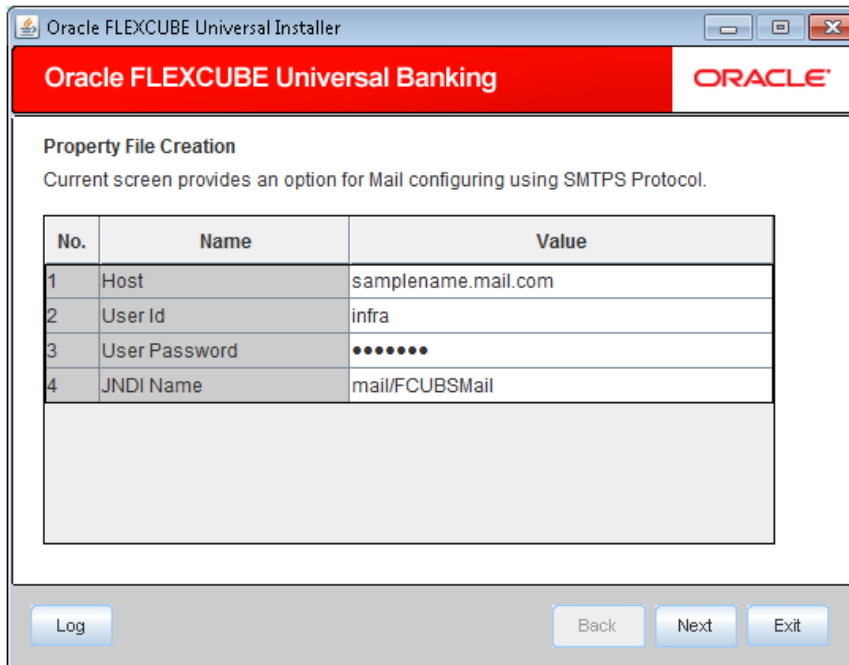
Before you change the password of the SMTP server, ensure that the following activity is completed:

- Take a backup of *fcubs.properties* file from the current EAR file.

5.2.2 Changing SMTP Server Password

To change the password of SMTP server, follow the steps given below:

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



2. You need to modify the following field:

User Password

Specify the new password

3. Once you have deployed the EAR file, inform the concerned users and groups about the password change.
4. Test whether the password change was successful. In case the test is not successful, repeat the above steps and test again.

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

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

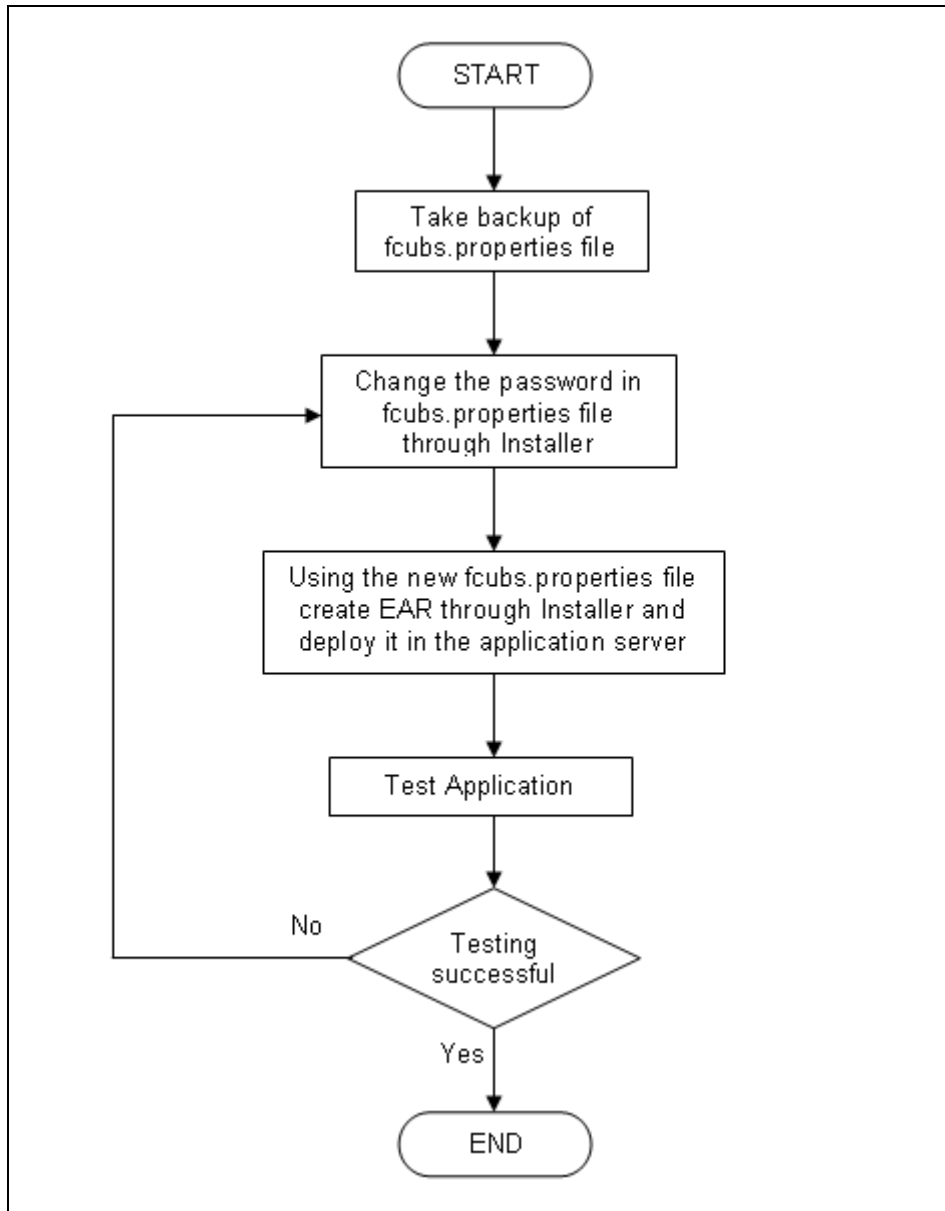


Try the above process in UAT or any other test environment before you change the password in a production environment.

5.3 Changing EMS FTP Server Password

This section describes the process of changing the EMS FTP server password.

The following diagram briefs the steps involved in changing the passwords of the EMS FTP server.



5.3.1 **Prerequisites**

Before you change the password of the EMS FTP server, ensure that the following activity is completed:

Take a backup of *fcubs.properties* file from the current EAR file.

5.3.2 **Changing FTP Server Password**

To change the password of EMS FTP server, follow the steps given below:

1. In Oracle FLEXCUBE Universal Banking Solution Installer, load the existing property file. Go to the step where you can define the branch properties.
2. Change the password of the FTP server.

3. Once you have deployed the EAR file, inform the concerned users and groups about the password change.
4. Test whether the password change was successful. In case the test is not successful, repeat the above steps and test again.

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

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

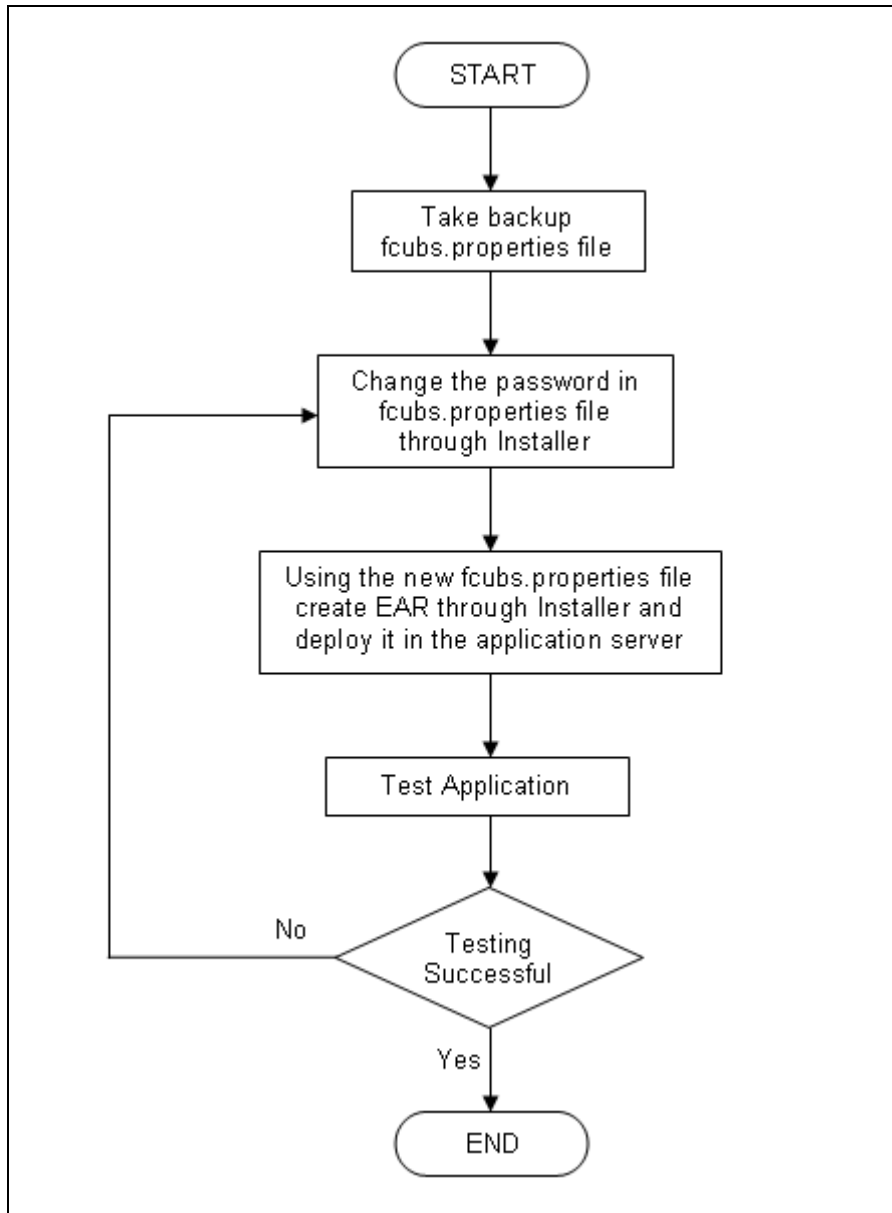


Try the above process in UAT or any other test environment before you change the password in a production environment.

5.4 Changing BPEL Administrative Console Password

This section describes the process of changing the BPEL server password.

The following diagram briefs the steps involved in changing the passwords of the BPEL server.



5.4.1 **Prerequisites**

Before you change the password of the BPEL server, ensure that the following activity is completed:

Take a backup of *fcubs.properties* file from the current EAR file.

5.4.2 **Changing BPEL Server Password**

To change the password of BPEL server, follow the steps given below:

1. In Oracle FLEXCUBE Universal Banking Solution Installer, load the existing property file. Go to the step where you can define the branch properties.
2. You need to modify the following field:

- BI_PASSWORD: Specify the new password
- 3. Once you have deployed the EAR file, inform the concerned users and groups about the password change.
- 4. Test whether the password change was successful. In case the test is not successful, repeat the above steps and test again.

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

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

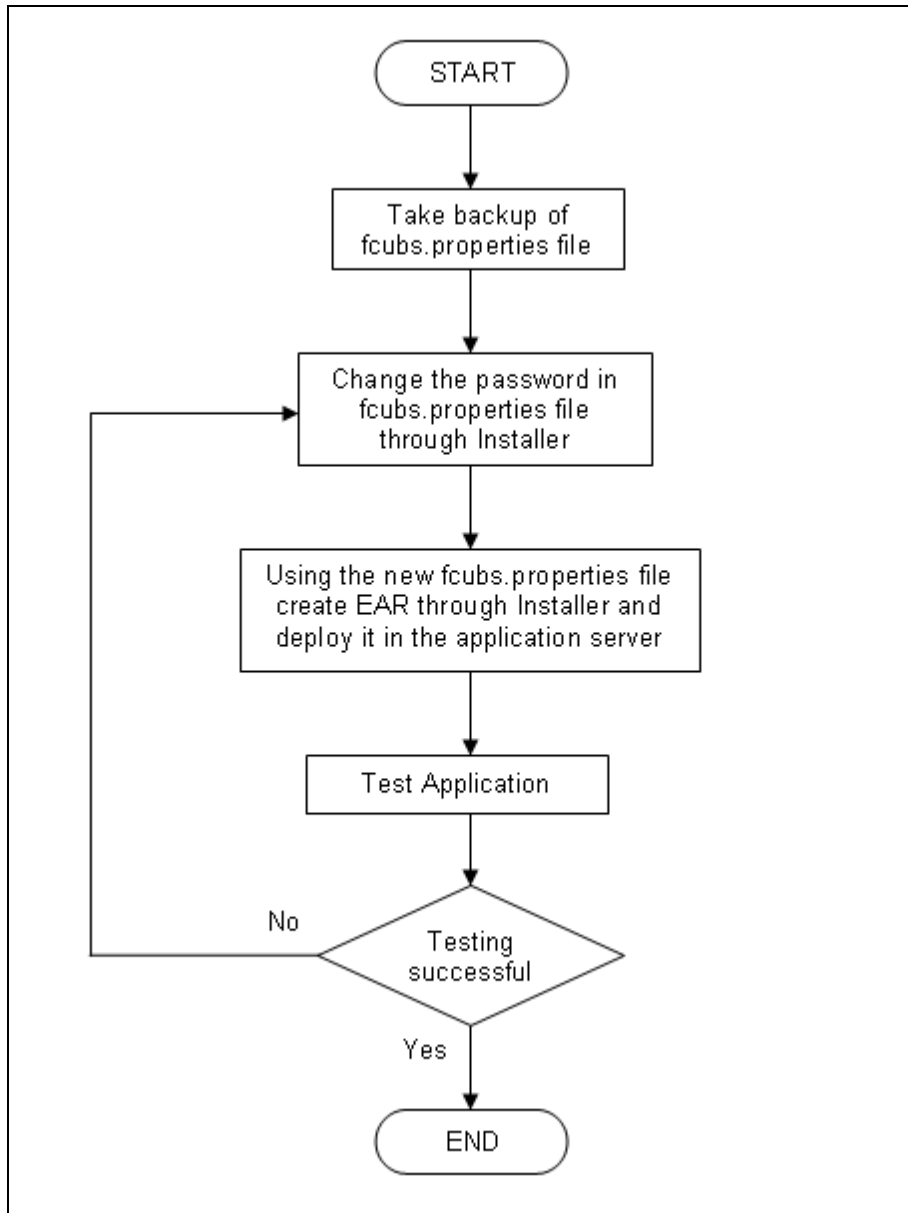


Try the above process in UAT or any other test environment before you change the password in a production environment.

5.5 Changing BIP Administrative Console Password

This section describes the process of changing the BI Publisher server password.

The following diagram briefs the steps involved in changing the passwords of the BIP server.



5.5.1 **Prerequisites**

Before you change the password of the BIP server, ensure that the following activity is completed:

Take a backup of *fcubs.properties* file from the current EAR file.

5.5.2 **Changing BIP Server Password**

To change the password of BIP server, follow the steps given below:

1. In Oracle FLEXCUBE Universal Banking Solution Installer, load the existing property file. Go to the step where you can define the branch properties.
2. You need to modify the following field:

BIP Password

Specify the new password

3. Once you have deployed the EAR file, inform the concerned users and groups about the password change.
4. Test whether the password change was successful. In case the test is not successful, repeat the above steps and test again.

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

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

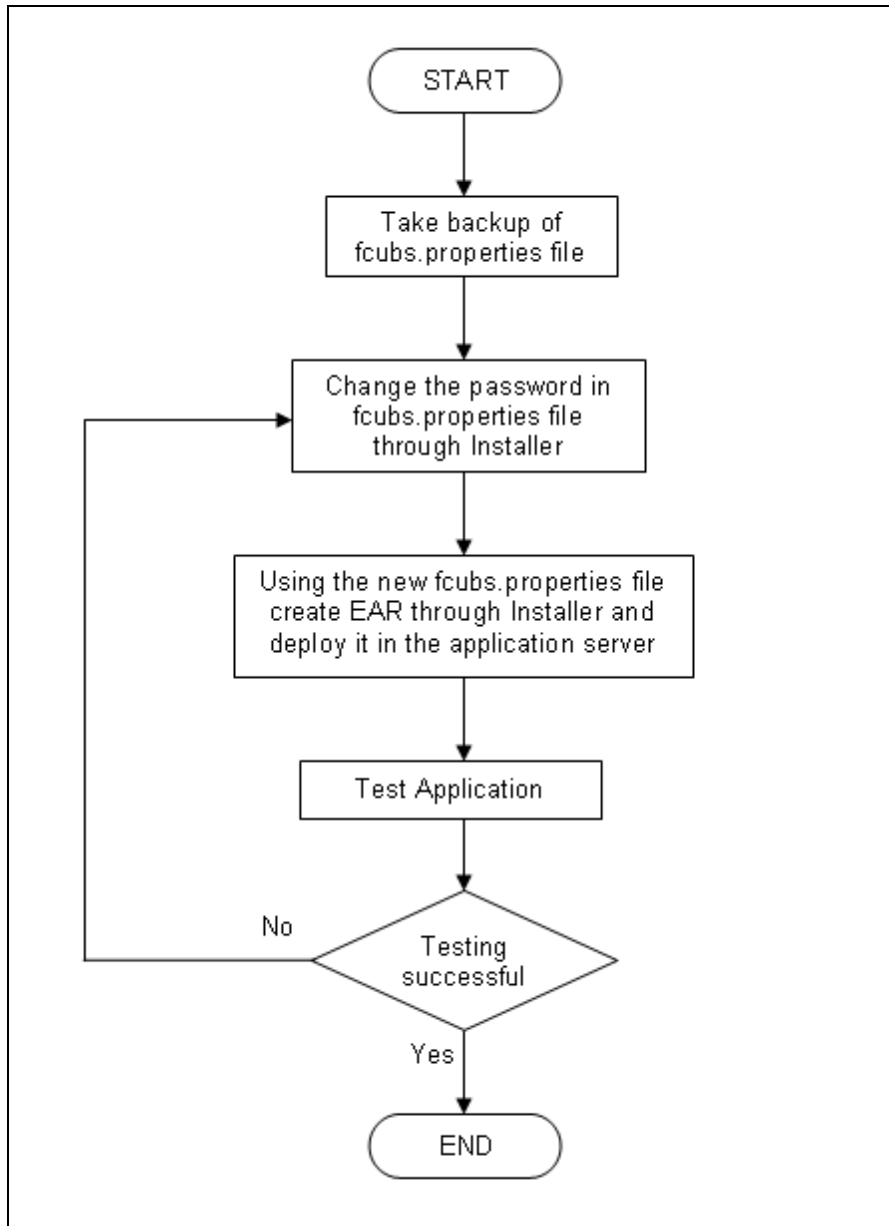


Try the above process in UAT or any other test environment before you change the password in a production environment.

5.6 Changing DMS Server Password

This section describes the process of changing the DMS server password.

The following diagram briefs the steps involved in changing the passwords of the DMS server.



5.6.1 Prerequisites

Before you change the password of the DMS server, ensure that the following activity is completed:

Take a backup of *fcubs.properties* file from the current EAR file.

5.6.2 Changing BIP Server Password

To change the password of DMS server, follow the steps given below:

1. In Oracle FLEXCUBE Universal Banking Solution Installer, load the existing property file. Go to the step where you can define the branch properties.
2. Change the password.

3. Once you have deployed the EAR file, inform the concerned users and groups about the password change.
4. Test whether the password change was successful. In case the test is not successful, repeat the above steps and test again.

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.



Oracle FLEXCUBE Password Change
[November] [2021]
Version 14.5.3.0.0

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
<https://www.oracle.com/industries/financial-services/index.html>

Copyright © [2007], [2021], Oracle and/or its affiliates. All rights reserved.

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.