

Oracle Banking Digital Experience

Web Service Username Token Configuration Guide

Release 18.2.0.0.0

Part No. E97823-01

June 2018

ORACLE®

June 2018

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 © 2018, 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.

Table of Contents

1. Preface.....	4
1.1 Intended Audience	4
1.2 Documentation Accessibility	4
1.3 Access to OFSS Support	4
1.4 Structure.....	4
1.5 Related Information Sources.....	4
2. Anonymous User Configuration	5
3. Logged-In User Configuration	9

1. Preface

1.1 Intended Audience

This document is intended for the following audience:

- Customers
- Partners

1.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

1.3 Access to OFSS Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

1.4 Structure

This manual is organized into the following categories:

Preface gives information on the intended audience. It also describes the overall structure of the User Manual.

The subsequent chapters describes following details:

- Prerequisite
- UI Deployment
- Configuration / Installation

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 18.2.0.0.0, refer to the following documents:

- Oracle Banking Digital Experience Licensing Guide
- Oracle Banking Digital Experience Security Guide

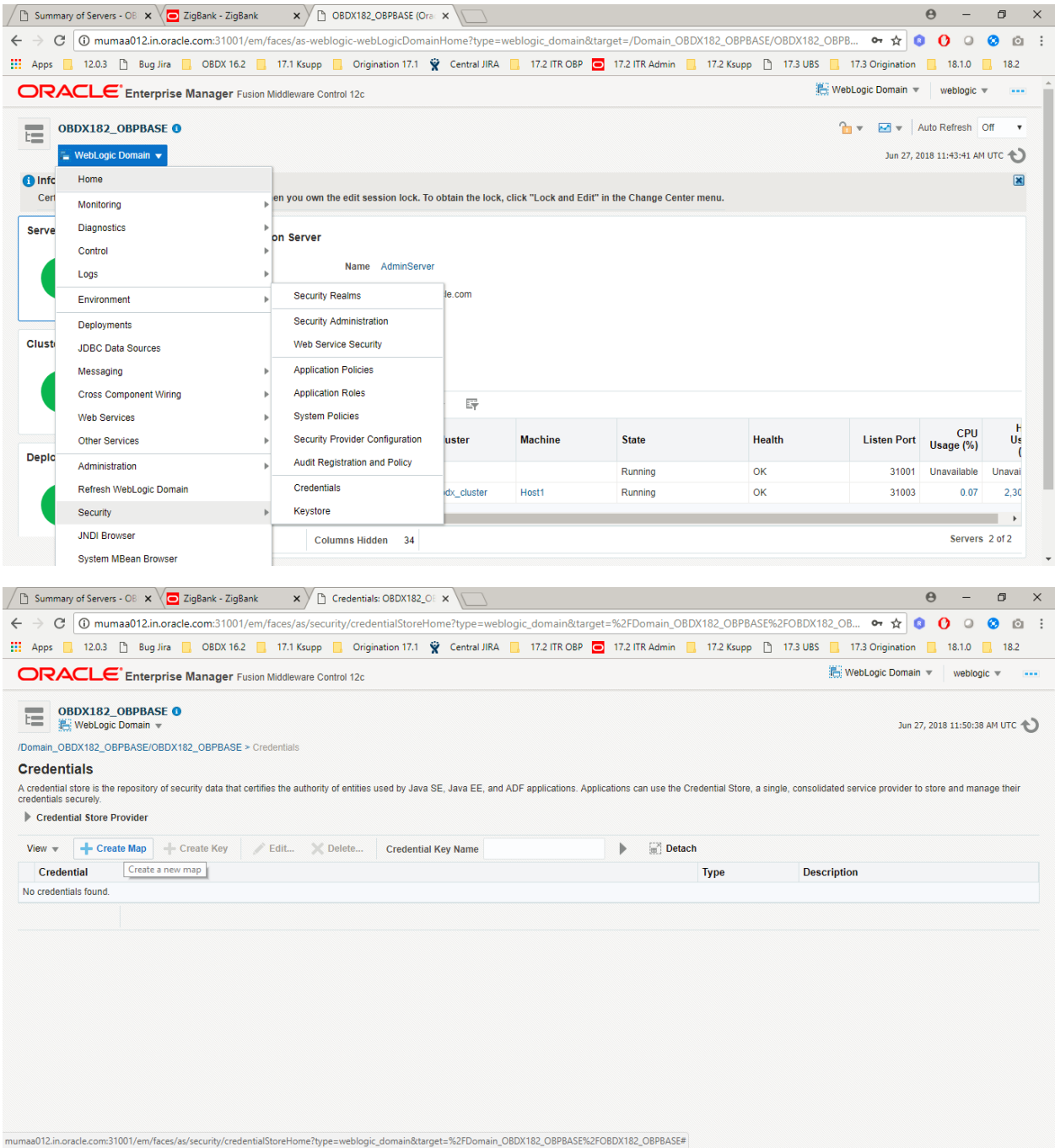
2. Anonymous User Configuration

- Insert/Update security policy to be used in the field in **Anonymous Security Policy** at Day1 (defaulted to “oracle/wss_username_token_client_policy”)

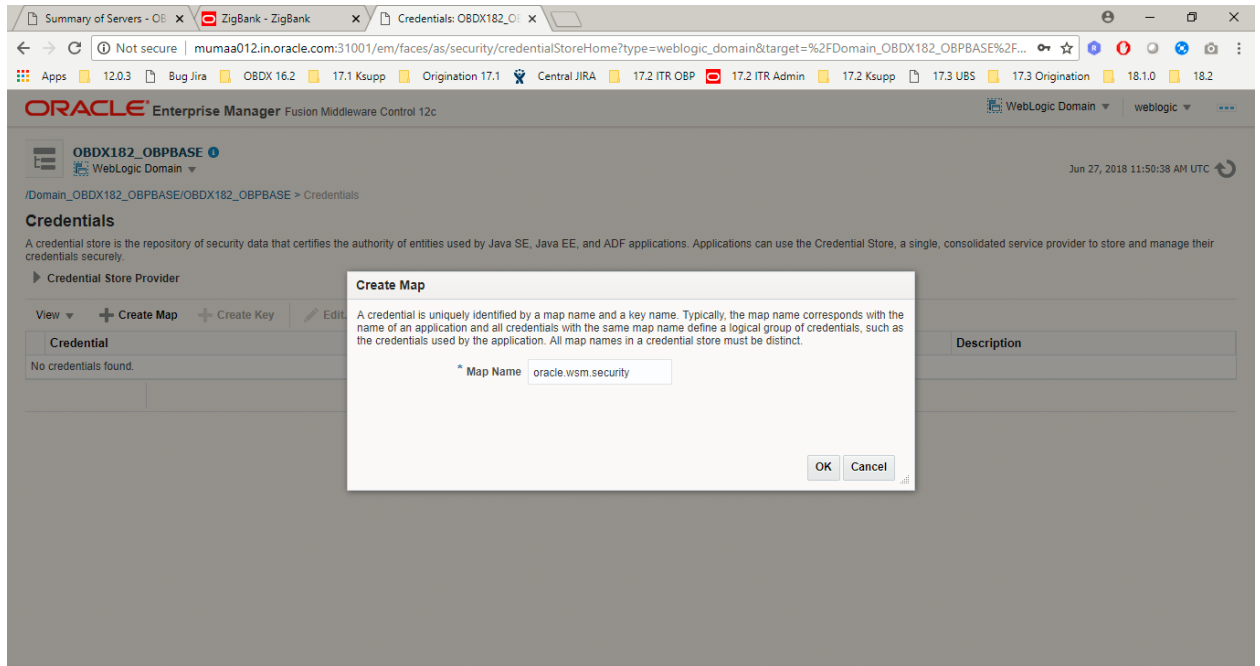
The screenshot shows the ZigBank system configuration page. The left sidebar contains a navigation menu with options: Dynamic Module, Brand, OTHERMODULE, Origination, and Common. The main content area displays a configuration form for the 'Anonymous Security Key' and 'Anonymous Security Policy' fields. The 'Anonymous Security Key' field is highlighted with a red box and contains the value 'origination_owsm_key'. The 'Anonymous Security Policy' field is also highlighted with a red box and contains the value 'oracle/wss_username_token_client_policy'. Other configuration fields include Application Server Port (9003), IDCS Host Port (443), IDCS Host IP, Application Server Host (mum00chq.in.oracle.com), IPM Host IP address, Retail User Supported Auth (OTP~SOFT_TOKEN~SEC_QUE), Type, Port (8011), Host IP (10.180.86.15), Region (INDIA), Bank Code (10), Channel (IB), and Application Server Port (9003).

- Insert/Update security policy key to be used in the field in **Anonymous Security Key** at Day1 (defaulted to “origination_owsm_key”)
- Name should match with credential key stored inside the credential store repository.
- Create a map named “**oracle.wsm.security**” in credential store provider.

Anonymous User Configuration

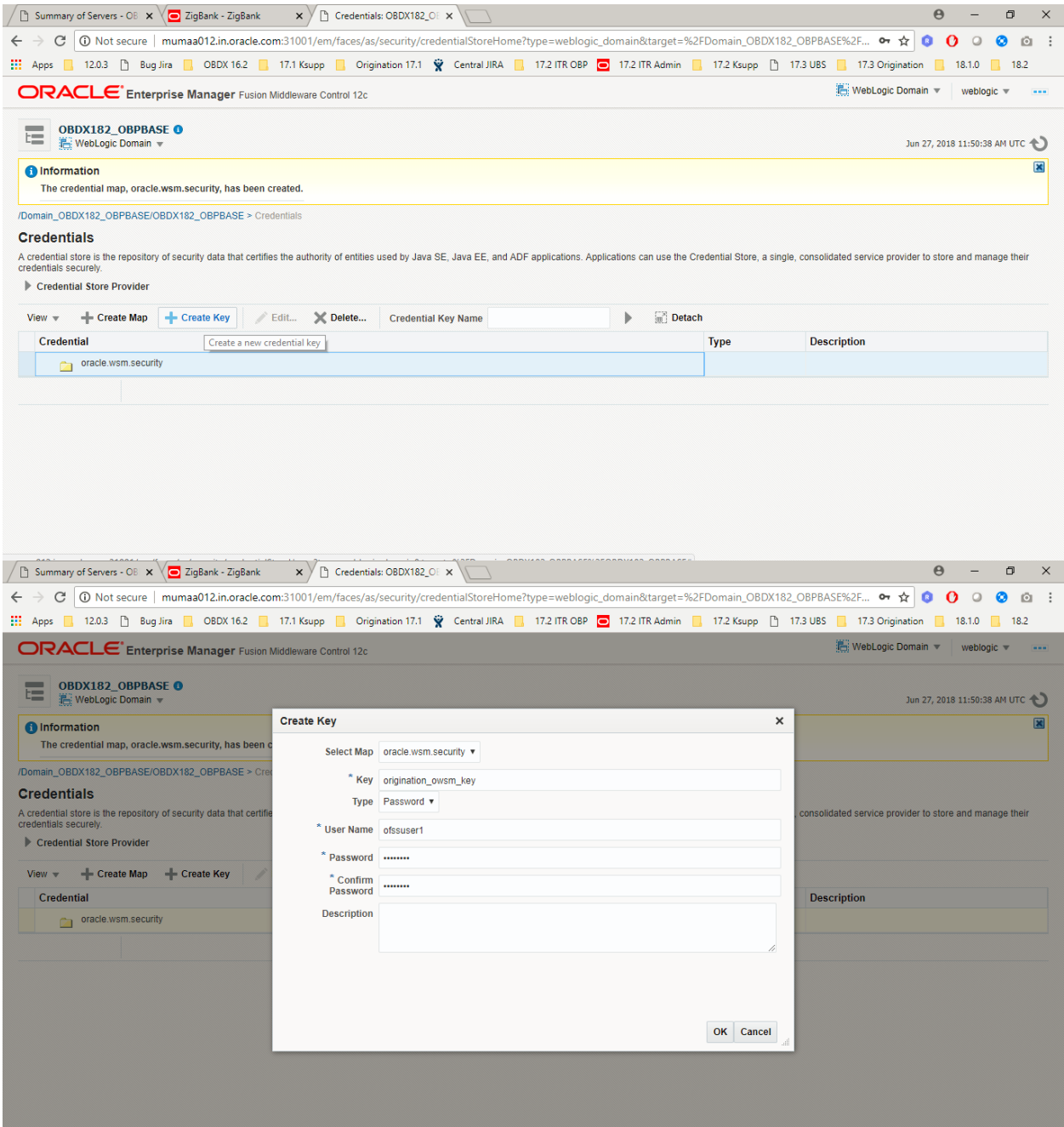


Anonymous User Configuration



- Create credential key and provide username & password which will be used for authentication and authorization at OBP.

Anonymous User Configuration



[Home](#)

3. Logged-In User Configuration

- Insert a credentials entry for the connector.

```
Insert into DIGX_FW_CONFIG_ALL_B ( PROP_ID, CATEGORY_ID, PROP_VALUE,
FACTORY_SHIPPED_FLAG, PROP_COMMENTS,SUMMARY_TEXT, CREATED_BY,
CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS,
OBJECT_VERSION_NUMBER, EDITABLE,CATEGORY_DESCRIPTION ) values (
'OBP_RA_JNDIKEY', 'CredentialConnector', 'ra/DIGXConnectorOBP', 'N', 'RA Connector for
OBP', 'RA Connector for OBP', 'ofssuser', sysdate, 'ofssuser', sysdate, 'Y', 1, 'N', '1');
```

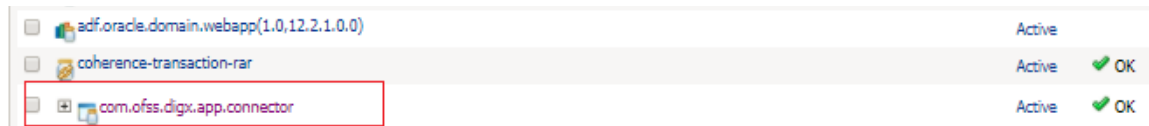
- Update the connector name for the logged-in user.

```
update DIGX_FW_CONFIG_OUT_WS_CFG_B set
HTTP_BASIC_AUTH_CONNECTOR='OBP' where
SECURITY_POLICY='oracle/wss10_saml_token_client_policy';
```

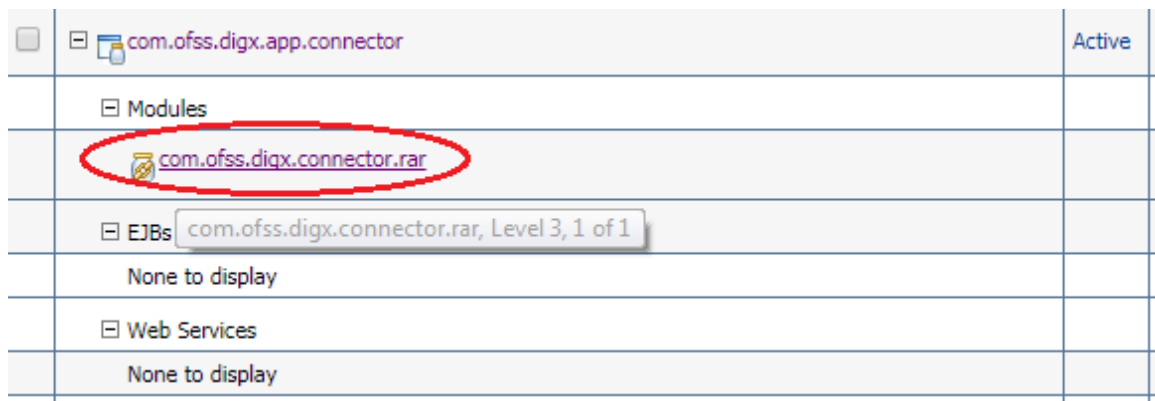
- Update security policy of logged-in user from saml token to user token policy

```
update DIGX_FW_CONFIG_OUT_WS_CFG_B set
SECURITY_POLICY='oracle/wss_username_token_client_policy' where
SECURITY_POLICY='oracle/wss10_saml_token_client_policy';
```

- Create a new “Outbound Credentials Mapping” in the connector (com.ofss.digx.app.connector.ear) ear and create a default user (use user id and credentials as provided by OBP team) for the mapping in the security tab. Managed server restart is required after these changes.
- Login into Weblogic console.
- Click on **Deployments**.
- Expand by clicking ‘+’ icon present in front of **com.ofss.digx.app.connector** application as shown below.



- Click **com.ofss.digx.connector.rar** as shown below.



- Click On “configuration” tab as shown in figure.

Anonymous User Configuration

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains the 'Change Center' and 'Domain Structure' panels. The main content area is titled 'Settings for com.oracle.digx.connector.rar' and has tabs for 'Overview', 'Configuration', 'Security', 'Control', 'Testing', and 'Monitoring'. The 'Configuration' tab is active, showing the 'Outbound Connection Pools' section. A table titled 'Outbound Connection Pool Configuration Table' lists one entry: 'javax.resource.cdi.ConnectionFactory'. The 'New' button is located at the bottom left of the table.

- Click on “New” button and select connection factory. Refer Screenshot.

The screenshot shows the 'Create a New Outbound Connection' wizard in the Oracle WebLogic Server Administration Console. The 'Outbound Connection Group' step is active, showing a list of groups with 'javax.resource.cdi.ConnectionFactory' selected. The 'Next' button is visible at the bottom of the wizard.

- Provide JINDI name as inserted in previous scripts. In this case name will be “ra/DIGXConnectorOBP”. After providing the name and Click on “Next”.

Anonymous User Configuration

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains the 'Change Center' with 'View changes and restarts' and 'Release Configuration' buttons, and the 'Domain Structure' tree. The main area displays the 'Create a New Outbound Connection' wizard. The 'JNDI name for Outbound Connection Instance' step is active, showing a text field with the value 'ra/DIGXConnectorOBP2.5.0'. The wizard includes 'Back', 'Next', 'Finish', and 'Cancel' buttons.

- Click on “Ok” to confirm.

The screenshot shows the 'Save Deployment Plan Assistant' dialog box. It has 'OK' and 'Cancel' buttons at the top. The 'Save Deployment Plan' section contains instructions: 'You have made configuration changes that need to be stored in a new deployment plan. Select or enter the path of a deployment plan file. The path must end with ".xml". It is highly recommended that this file be named "Plan.xml". Each plan should be located in its own directory, otherwise applications can inadvertently share deployment plan files. The plan file will be overwritten if it already exists. Other files in the plan directory may be overwritten as well.' Below this, there is a 'Path:' field with the value '/home/devops/domain/OBDX182_OBPBASE/servers/AdminServer/upload/com.ofss.digx.app.connector/Plan.xml', a 'Recently Used Paths:' field with '(none)', and a 'Current Location:' field with the path 'mumaa012.in.oracle.com / home / devops / domain / OBDX182_OBPBASE / servers / AdminServer / upload / com.ofss.digx.app.connector'. At the bottom, there is an 'app' folder icon and 'OK' and 'Cancel' buttons.

- Click on Activate changes.

Anonymous User Configuration

The first screenshot shows the 'Settings for com.ofss.digx.connector.rar' page in the Oracle WebLogic Server Administration Console. The 'Overview' tab is selected, displaying basic information about the resource adapter. The 'Name' is 'com.ofss.digx.connector.rar' and the 'Source Path' is 'servers/AdminServer/upload/com.ofss.digx.app.connector/app/com.ofss.digx.app.connector.ear'. The 'Messages' section shows two green checkmarks: 'A new deployment plan has been successfully created in /home/devops/domain/OBDX182_OBPBASE/servers/AdminServer/upload/com.ofss.digx.app.connector/Plan.xml.' and 'Your deployment configuration has been updated to include the new plan.'

The second screenshot shows the same page after changes have been activated. The 'Messages' section now shows a green checkmark: 'All changes have been activated. No restarts are necessary.' The 'Change Center' on the left indicates that changes have been activated and no restarts are necessary.

- Click on Security tab of connector, click on “Outbound credentials mapping”, click on “New” and select the newly created provider “ra/DIGXConnectorOBP” and click on “Next”.

Anonymous User Configuration

Oracle WebLogic Server Administration Console 12c

Home > Summary of Security Realms > myrealm > Providers > Summary of Environment > Summary of Servers > Summary of Deployments > com.ofss.digx.connector.rar > Roles > com.ofss.digx.connector.rar

Create a New Security Credential Mapping

Back Next Finish Cancel

Which Outbound Connection Pool would you like the credential map to be associated with? Selecting Resource Adapter Default will configure the credential mapping for all Outbound Connection Pools in this resource adapter. Each Outbound Connection Pool can then configure themselves to override these credentials.

Customize this table

Create a New Security Credential Map Entry for:

Outbound Connection Pool
<input checked="" type="checkbox"/> ra/DIGXConnectorOBP2.5.0.2.0
<input type="checkbox"/> Resource Adapter Default

Showing 11 to 12 of 12 Previous Next

Back Next Finish Cancel

- Select the default user and Click on “Next”.

Oracle WebLogic Server Administration Console 12c

Home > Summary of Security Realms > myrealm > Providers > Summary of Environment > Summary of Servers > Summary of Deployments > com.ofss.digx.connector.rar > Roles > com.ofss.digx.connector.rar

Create a New Security Credential Mapping

Back Next Finish Cancel

WebLogic Server User

Select the WebLogic Server user that you would like to map an EIS user to. Selecting 'User for creating initial connections' will configure the user that will be used for creating the initial connections when the resource adapter is first started. Selecting 'Default User' will configure the user that will be used as the default for any authenticated WebLogic Server user that does not have a credential mapping specifically for them. Selecting 'User for unauthenticated user' will configure the user that will be used for an unauthenticated WebLogic Server user. If you select 'Configured User' you must type in the WebLogic Server user that you are configuring. This user must be a configured WebLogic Server user.

☐ User for creating initial connections

☒ Default User

☐ Unauthenticated WLS User

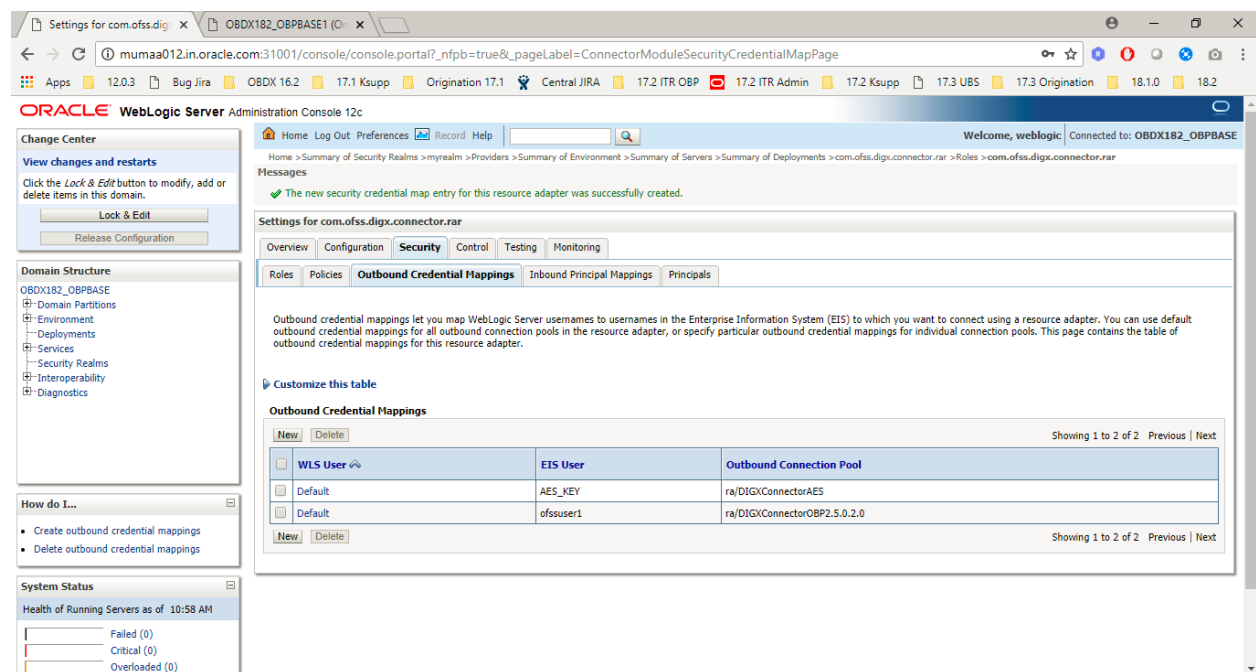
☐ Configured User Name

WebLogic Server User Name:

Back Next Finish Cancel

- Provide the user details as provided by OBP Team and Click on Finish.

Anonymous User Configuration



- Restart managed server to take effects.