

Oracle Banking Digital Experience

Web Service Username Token Configuration Guide
Release 19.2.0.0.0

Part No. F25153-01

December 2019

ORACLE®

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 © 2019, 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 19.2.0.0.0, 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 table with the following data:

Application Server Port	9003	IDCS Host Port	443
Anonymous Security Key	origination_owsm_key	Limits Effective from Same Day (Y/N)	Y
Name			
IDCS Host IP		Application Server Host	mum00chq.in.oracle.com
IPM Host IP address		Retail User Supported Auth Type	OTP~SOFT_TOKEN~SEC_QUE
Port	8011	Host IP	10.180.86.15
Host IP	10.180.86.15	Region	INDIA
Bank Code	10	Port	8011
Channel	IB	Anonymous Security Policy	oracle/wss_username_token_client_policy
Port	8011	Application Server Port	9003

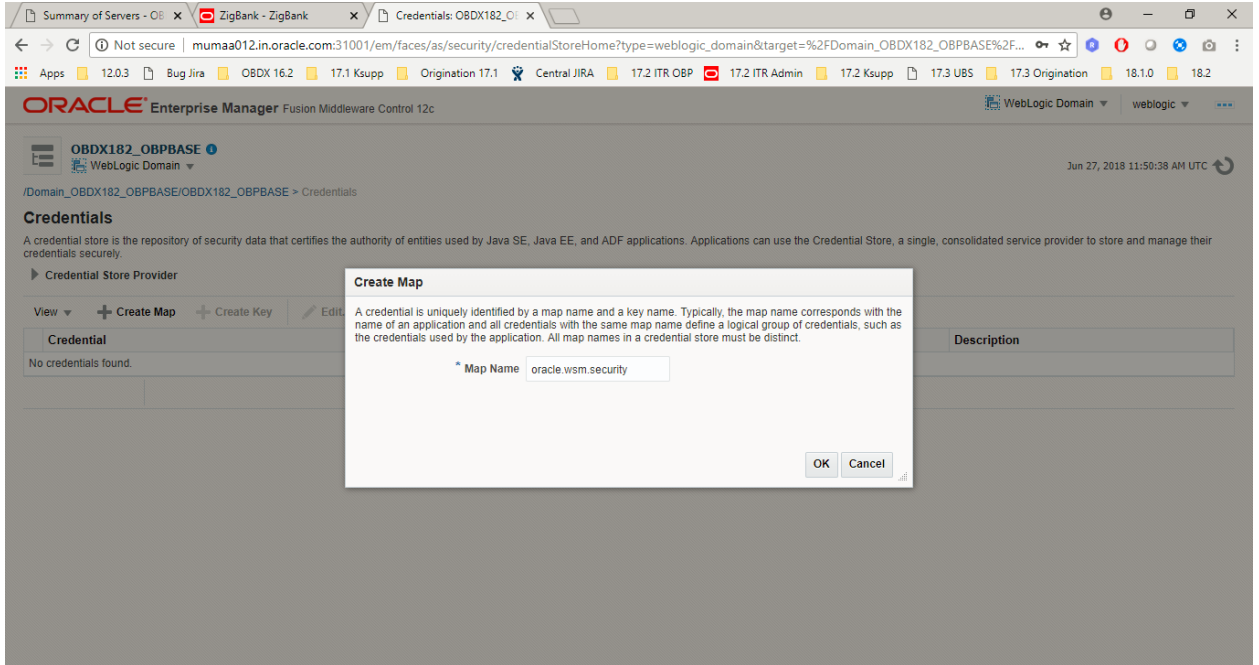
- Insert/Update security policy key to be used in the field in **Anonymous Security Key** at Day1 (defaulted to “origination_owsm_key”)
- Name should match with credential key stored inside the credential store repository.
- Create a map named “**oracle.wsm.security**” in credential store provider.

Anonymous User Configuration

The screenshot shows the Oracle Enterprise Manager interface for 'OBDX182_OBPBASE'. The left-hand navigation menu is expanded to the 'Security' section. The 'Security' menu item is highlighted, and a sub-menu is displayed with the following options: Security Realms, Security Administration, Web Service Security, Application Policies, Application Roles, System Policies, Security Provider Configuration, Audit Registration and Policy, Credentials, and Keystore. The main content area shows a table with columns for 'Cluster', 'Machine', 'State', 'Health', 'Listen Port', 'CPU Usage (%)', and 'Host Us...'. The table contains two rows of data: one for 'dx_cluster' on 'Host1' with state 'Running' and health 'OK', and another for 'Host1' with state 'Running' and health 'OK'. The bottom right of the table indicates 'Servers 2 of 2'.

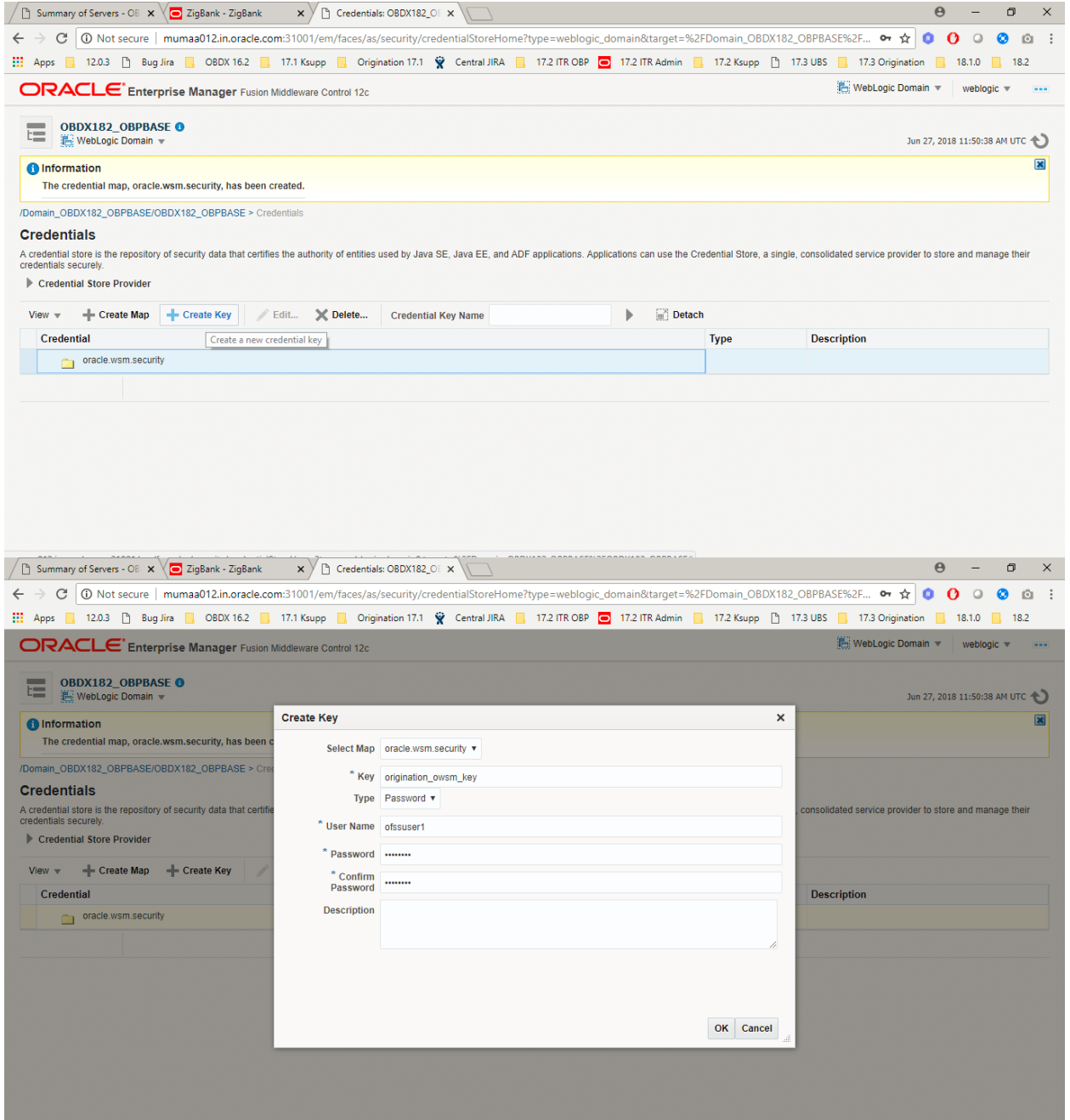
The screenshot shows the 'Credentials' configuration page in Oracle Enterprise Manager. The page title is 'Credentials' and it includes a description: 'A credential store is the repository of security data that certifies the authority of entities used by Java SE, Java EE, and ADF applications. Applications can use the Credential Store, a single, consolidated service provider to store and manage their credentials securely.' Below the description, there is a section for 'Credential Store Provider' with buttons for '+ Create Map', '+ Create Key', 'Edit...', and 'Delete...'. A 'Credential Key Name' field is present with a 'Detach' button. A table with columns 'Credential', 'Type', and 'Description' is shown, but it contains the text 'No credentials found.' The URL at the bottom of the page is 'mumaa012.in.oracle.com:31001/em/faces/as/security/credentialStoreHome?type=weblogic_domain&target=%2FDomain_OBDX182_OBPBASE%2FOBDX182_OBPBASE#'. The page timestamp is 'Jun 27, 2018 11:50:38 AM UTC'.

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.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	com.ofss.digx.app.connector	Active
	<input checked="" type="checkbox"/>	Modules	
	<input checked="" type="checkbox"/>	com.ofss.digx.connector.rar	
	<input checked="" type="checkbox"/>	EJBs com.ofss.digx.connector.rar, Level 3, 1 of 1	
		None to display	
	<input checked="" type="checkbox"/>	Web Services	
		None to display	

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

Anonymous User Configuration

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled "Settings for com.ofss.digx.connector.rar". It has tabs for Overview, Configuration, Security, Control, Testing, and Monitoring. Under the Configuration tab, there are sub-tabs for General, Properties, Outbound Connection Pools, Admin Objects, and Workload. The "Outbound Connection Pools" sub-tab is active, displaying a table titled "Outbound Connection Pool Configuration Table". The table has two columns: "Groups and Instances" and "Connection Factory Interface". There is one entry in the table with the JNDI name "javax.resource.ci.ConnectionFactory".

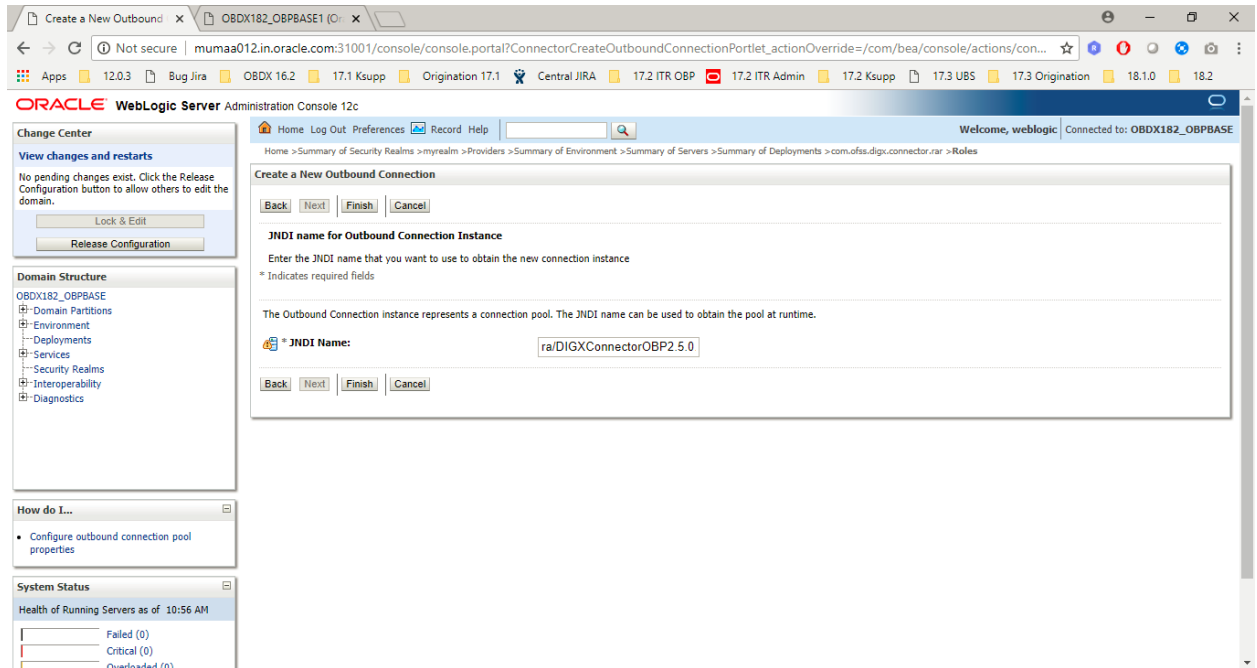
Groups and Instances	Connection Factory Interface
javax.resource.ci.ConnectionFactory	javax.resource.ci.ConnectionFactory

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

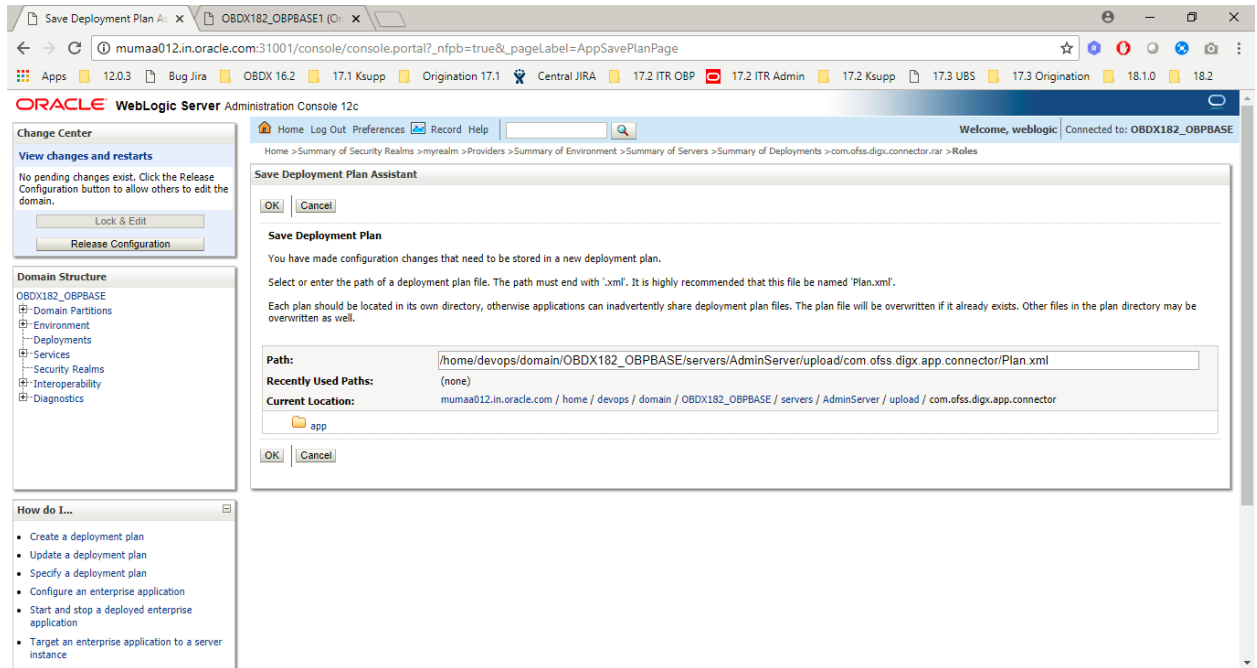
The screenshot shows the "Create a New Outbound Connection" wizard in the Oracle WebLogic Server Administration Console. The wizard is at the "Outbound Connection Groups" step. It asks "In which outbound connection group do you want to create an instance?". Below this question, there is a table titled "Outbound Connection Groups" with one entry: "javax.resource.ci.ConnectionFactory". The "Next" button is highlighted.

- 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



- Click on “Ok” to confirm.



- Click on Activate changes.

Anonymous User Configuration

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area displays the following information:

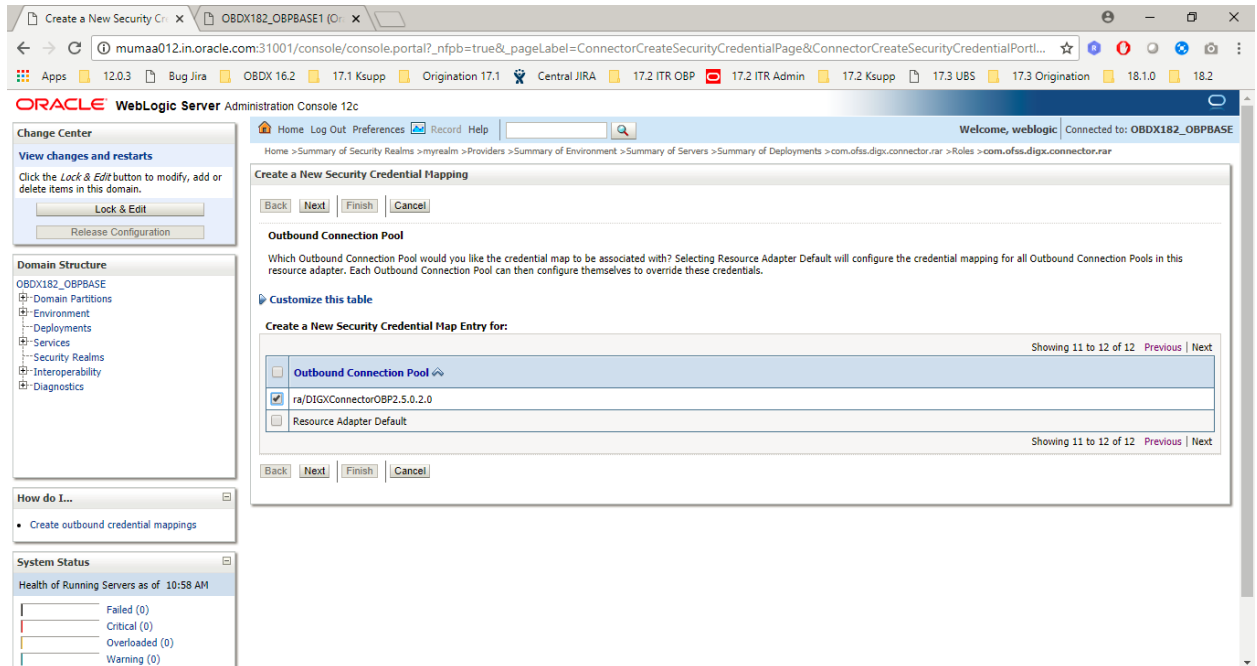
- Messages:**
 - A new deployment plan has been successfully created in /home/devops/domain/OBDX182_OBPBASE/servers/AdminServer/upload/com.ofss.digx.app.connector/Plan.xml.
 - Your deployment configuration has been updated to include the new plan.
- Settings for com.ofss.digx.connector.rar:**
 - Overview:** This page displays basic information about this resource adapter.
 - Name:** com.ofss.digx.connector.rar (The name of this application deployment. [More Info...](#))
 - Source Path:** servers/AdminServer/upload/com.ofss.digx.app.connector/app/com.ofss.digx.app.connector.ear (The path to the source of the deployable unit on the Administration Server. [More Info...](#))

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area displays the following information:

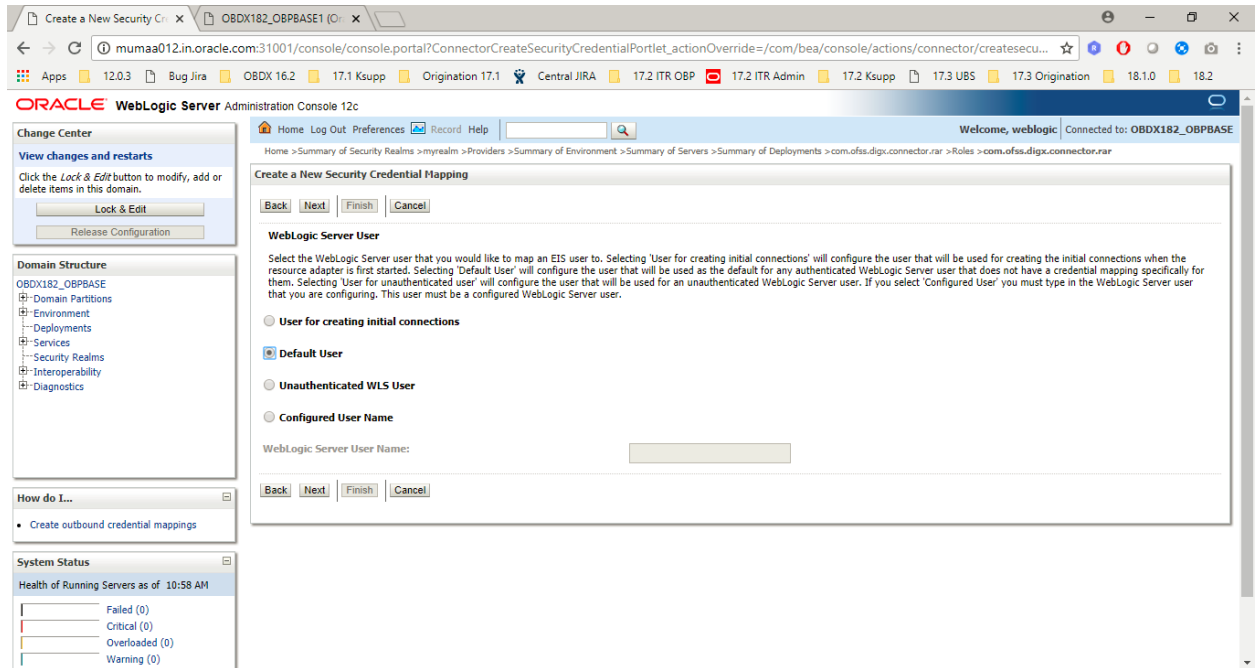
- Messages:**
 - All changes have been activated. No restarts are necessary.
- Settings for com.ofss.digx.connector.rar:**
 - Overview:** This page displays basic information about this resource adapter.
 - Name:** com.ofss.digx.connector.rar (The name of this application deployment. [More Info...](#))
 - Source Path:** servers/AdminServer/upload/com.ofss.digx.app.connector/app/com.ofss.digx.app.connector.ear (The path to the source of the deployable unit on the Administration Server. [More Info...](#))

- 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



- Select the default user and Click on "Next".



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

Anonymous User Configuration

The screenshot displays the Oracle WebLogic Server Administration Console interface. The main content area is titled "Settings for com.ofss.digx.connector.rar" and is under the "Security" tab. A message at the top states: "The new security credential map entry for this resource adapter was successfully created." Below this, there is a section for "Outbound Credential Mappings" with a table of configurations.

WLS User	EIS User	Outbound Connection Pool
Default	AES_KEY	ra/DIGXConnectorAES
Default	ofsuser1	ra/DIGXConnectorOBP2.5.0.2.0

- Restart managed server to take effects.