Oracle Banking APIs

Web Service Username Token Configuration Guide

Release 18.3.0.0.0

Part No. F12055-01

December 2018

ORACLE

Web Service Username Token Configurations Guide

December 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

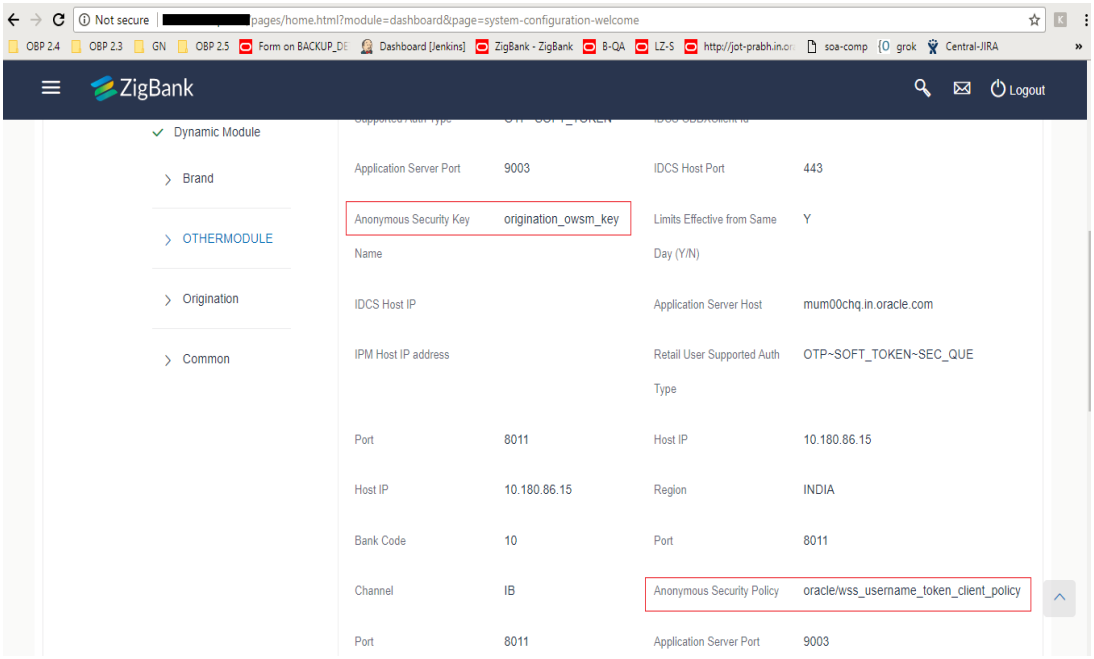
1.5 Related Information Sources

For more information on Oracle Banking APIs Release 18.3.0.0.0, refer to the following documents:

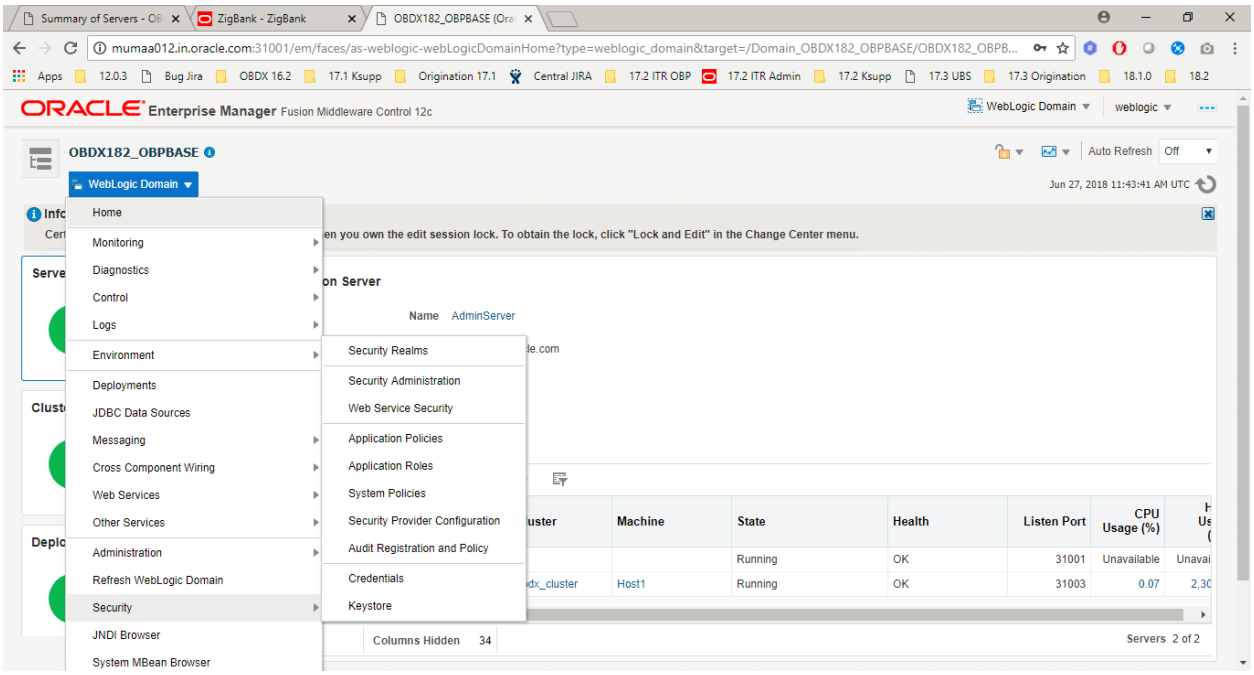
- Oracle Banking APIs Licensing Guide
- Oracle Banking APIs Security Guide

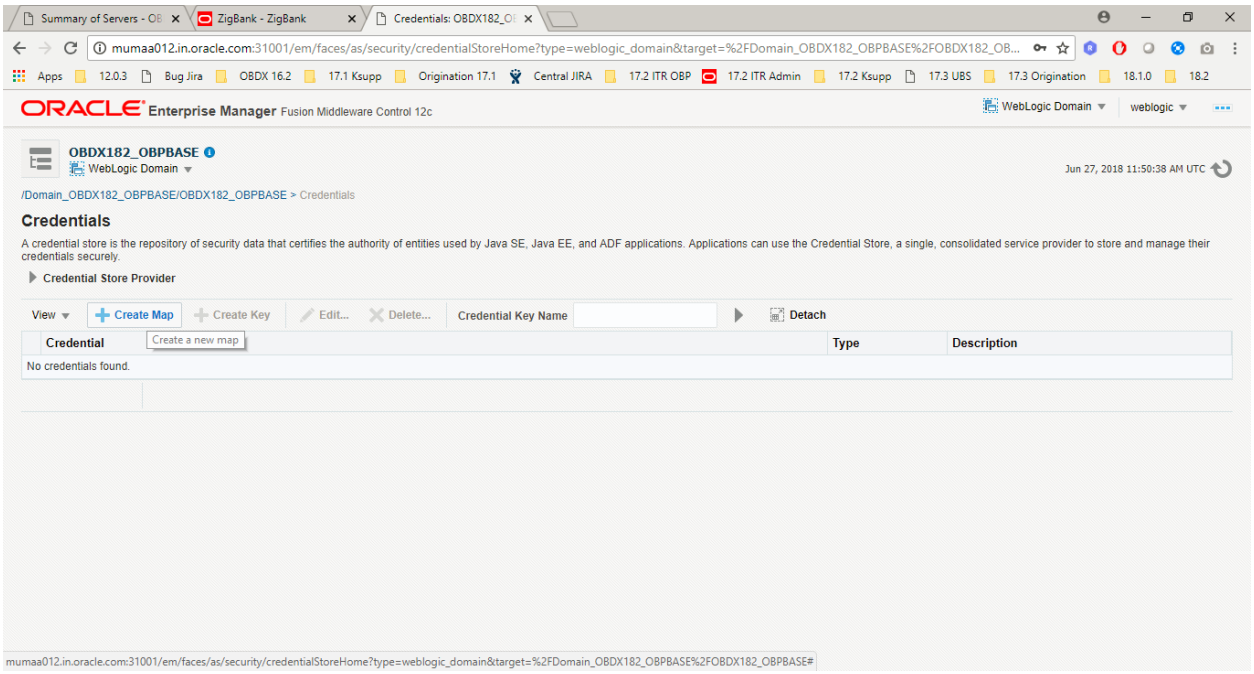
2. Anonymous User Configuration

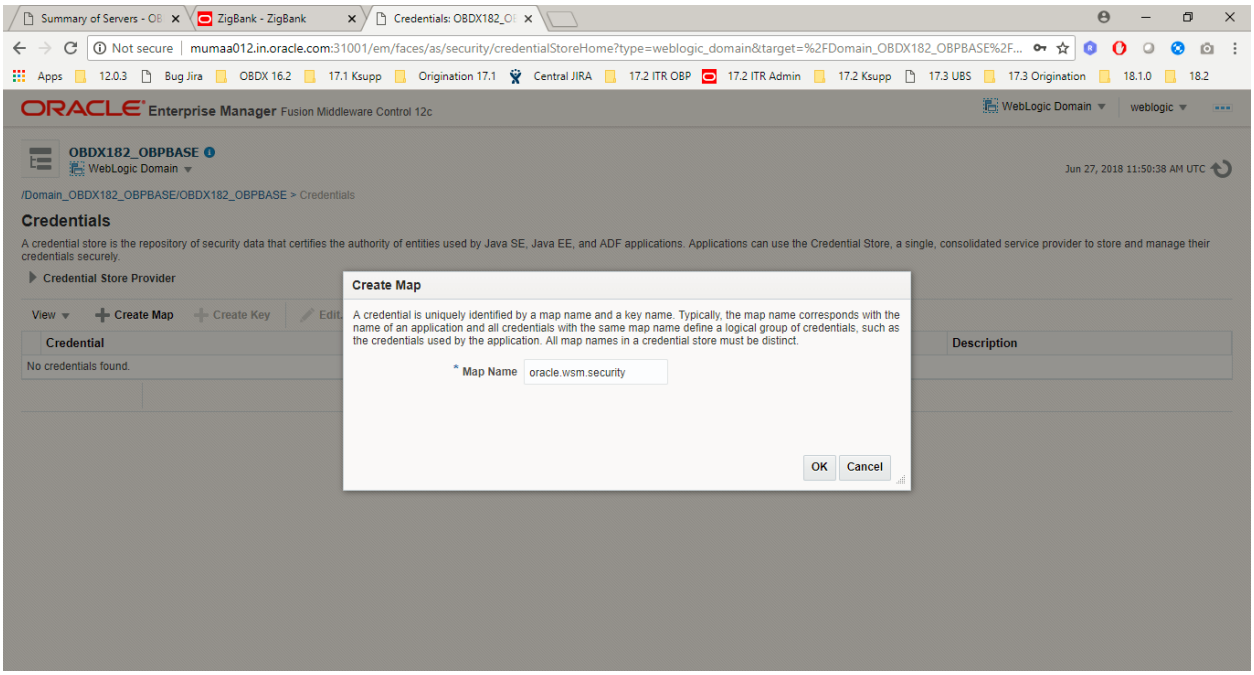
- Insert/Update security policy to be used in the field **in *Anonymous Security Policy*** at Day1 (defaulted to “oracle/wss_username_token_client_policy”)



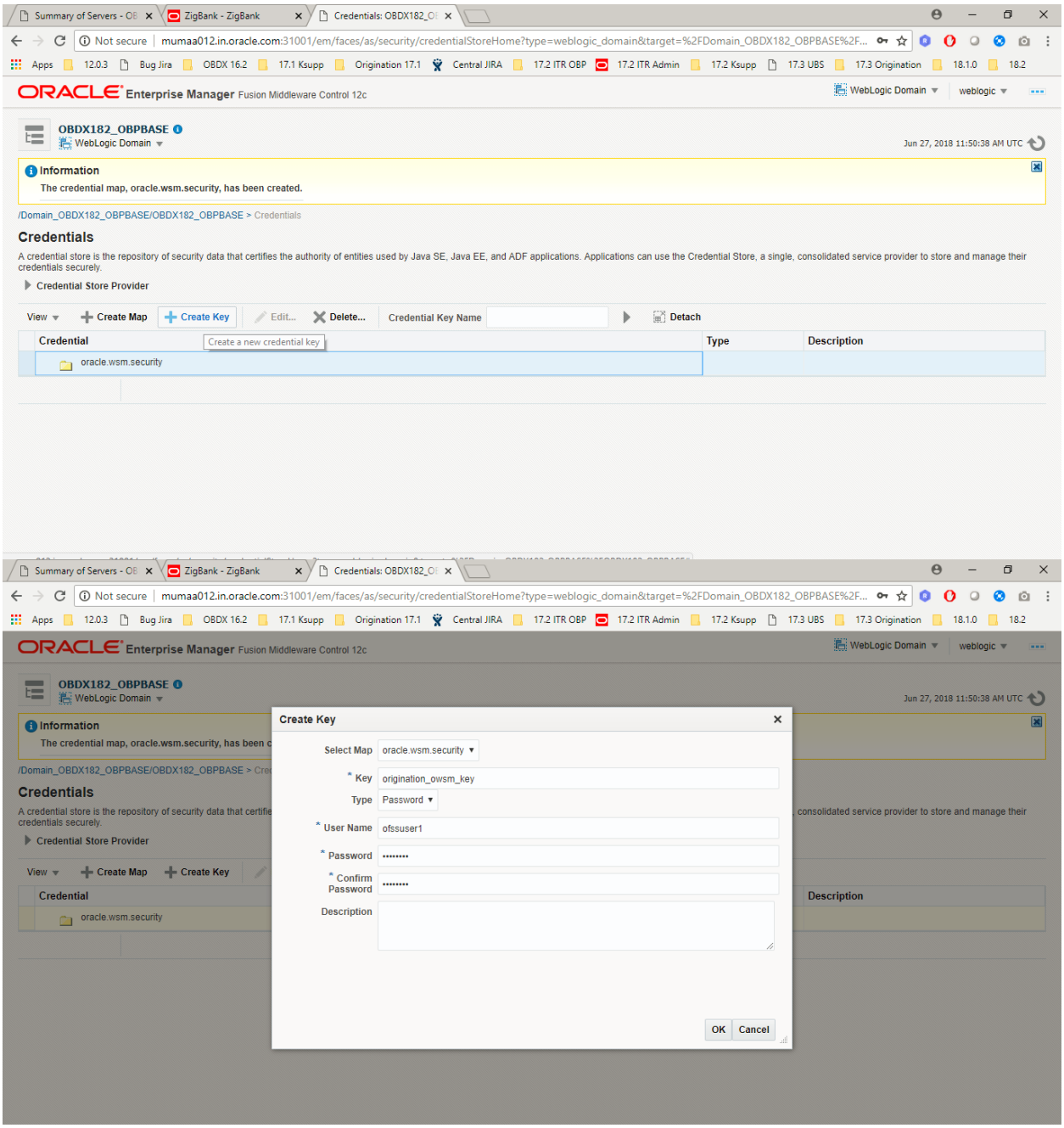
- Insert/Update security policy key to be used in the field **in *Anonymous Security Key*** at Day1 (defaulted to “origination_owsm_key”)
- Name should match with credential key stored inside the credential store repository.
- Create a map named “**oracle.wsm.security**” in credential store provider.


Summary of Servers - OB
ZigBank - ZigBank
OBDX182_OBPBASE (Ora
mumaa012.in.oracle.com:31001/em/faces/as-weblogic-webLogicDomainHome?type=weblogic_domain&target=/Domain_OBDX182_OBPBASE/OBDX182_OBPB...
Apps 12.0.3 Bug Jira OBDX 16.2 17.1 Ksupp Origination 17.1 Central JIRA 17.2 ITR OBP 17.2 ITR Admin 17.2 Ksupp 17.3 UBS 17.3 Origination 18.1.0 18.2
ORACLE Enterprise Manager Fusion Middleware Control 12c
WebLogic Domain
weblogic
OBDX182_OBPBASE
WebLogic Domain
Auto Refresh
Off
Jun 27, 2018 11:43:41 AM UTC
Home
Monitoring
Diagnostics
Control
Logs
Environment
Deployments
JDBC Data Sources
Messaging
Cross Component Wiring
Web Services
Other Services
Administration
Refresh WebLogic Domain
Security
JNDI Browser
System MBean Browser
Security Realms
Security Administration
Web Service Security
Application Policies
Application Roles
System Policies
Security Provider Configuration
Audit Registration and Policy
Credentials
Keystore
en you own the edit session lock. To obtain the lock, click "Lock and Edit" in the Change Center menu.
on Server
Name AdminServer
Machine
State
Health
Listen Port
CPU Usage (%)
Running
OK
31001
Unavailable
Host1
Running
OK
31003
0.07
Columns Hidden 34
Servers 2 of 2


Summary of Servers - OB
ZigBank - ZigBank
Credentials: OBDX182_OB
mumaa012.in.oracle.com:31001/em/faces/as/security/credentialStoreHome?type=weblogic_domain&target=%2FDomain_OBDX182_OBPBASE%2FOBDX182_OB...
Apps 12.0.3 Bug Jira OBDX 16.2 17.1 Ksupp Origination 17.1 Central JIRA 17.2 ITR OBP 17.2 ITR Admin 17.2 Ksupp 17.3 UBS 17.3 Origination 18.1.0 18.2
ORACLE Enterprise Manager Fusion Middleware Control 12c
WebLogic Domain
weblogic
OBDX182_OBPBASE
WebLogic Domain
Jun 27, 2018 11:50:38 AM UTC
/Domain_OBDX182_OBPBASE/OBDX182_OBPBASE > Credentials
Credentials
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.
Credential Store Provider
View
Create Map
Create Key
Edit...
Delete...
Credential Key Name
Detach
Credential
Create a new map
Type
Description
No credentials found.
mumaa012.in.oracle.com:31001/em/faces/as/security/credentialStoreHome?type=weblogic_domain&target=%2FDomain_OBDX182_OBPBASE%2FOBDX182_OBPBASE#



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


Summary of Servers - OB
ZigBank - ZigBank
Credentials: OBDX182_OB
Not secure
mumaa012.in.oracle.com:31001/em/faces/as/security/credentialStoreHome?type=weblogic_domain&target=%2FDomain_OBDX182_OBPBASE%2F...
Apps
12.0.3
Bug Jira
OBDX 16.2
17.1 Ksupp
Origination 17.1
Central JIRA
17.2 ITR OBP
17.2 ITR Admin
17.2 Ksupp
17.3 UBS
17.3 Origination
18.1.0
18.2
ORACLE Enterprise Manager Fusion Middleware Control 12c
WebLogic Domain
weblogic
OBDX182_OBPBASE
WebLogic Domain
Jun 27, 2018 11:50:38 AM UTC
Information
The credential map, oracle.wsm.security, has been created.
/Domain_OBDX182_OBPBASE/OBDX182_OBPBASE > Credentials
Credentials
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.
Credential Store Provider
View
Create Map
Create Key
Edit...
Delete...
Credential Key Name
Detach
Credential
Create a new credential key
Type
Description
oracle.wsm.security
Create Key
Select Map
oracle.wsm.security
* Key
origination_owsm_key
Type
Password
* User Name
ofssuser1
* Password
* Confirm Password
Description
OK
Cancel

[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.

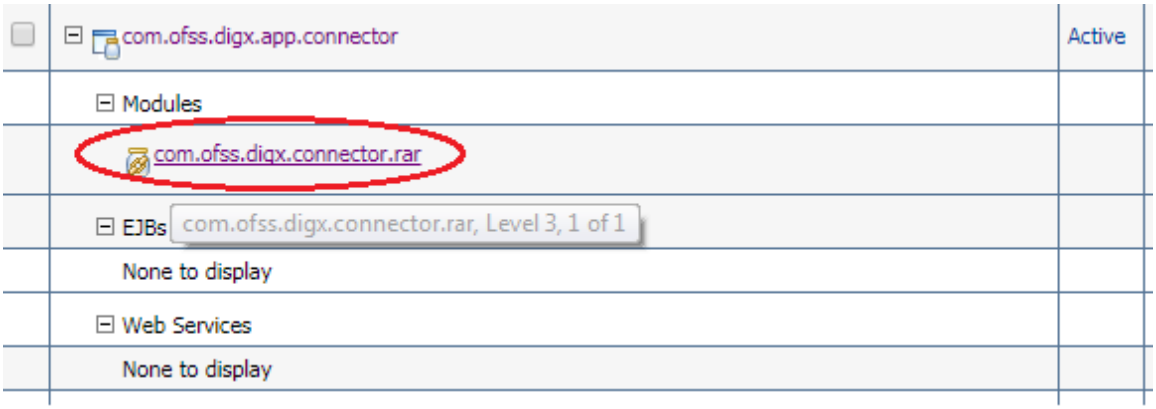
update DIGX_FW_CONFIG_OUT_WS_CFG_B set HTTP_BASIC_AUTH_CONNECTOR='OBP' where SECURITY_POLICY='oracle/wss10_saml_token_client_policy';

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

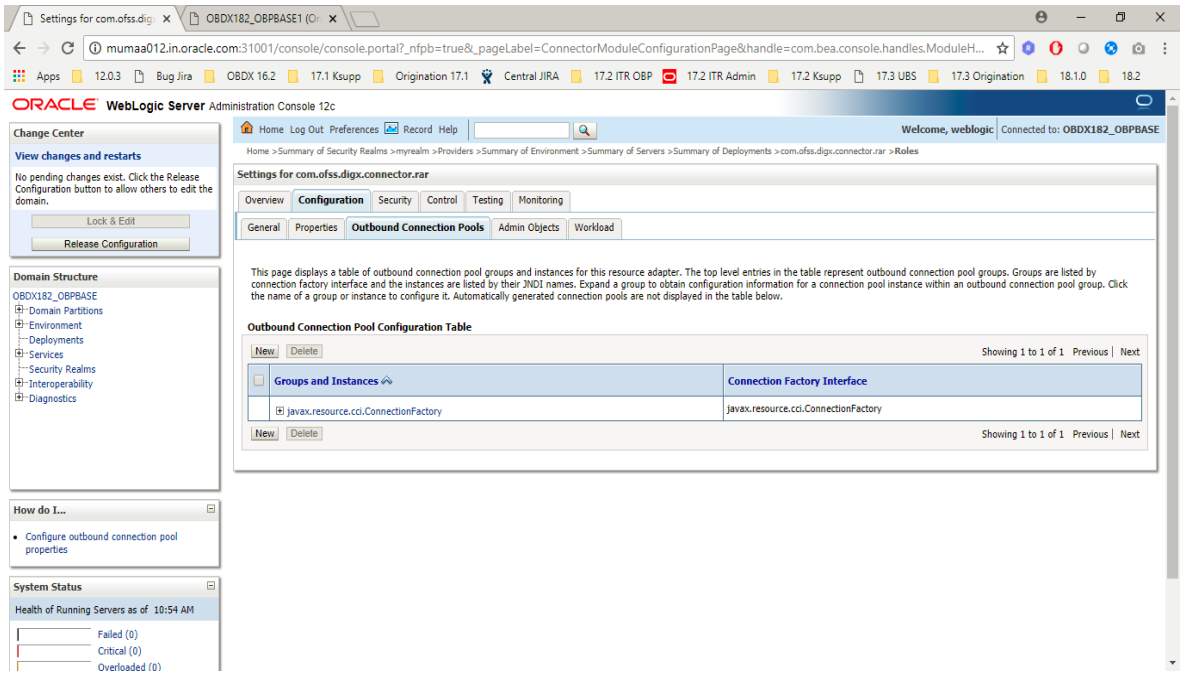
update DIGX_FW_CONFIG_OUT_WS_CFG_B set SECURITY_POLICY='oracle/wss_username_token_client_policy' where SECURITY_POLICY='oracle/wss10_saml_token_client_policy';

- 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.

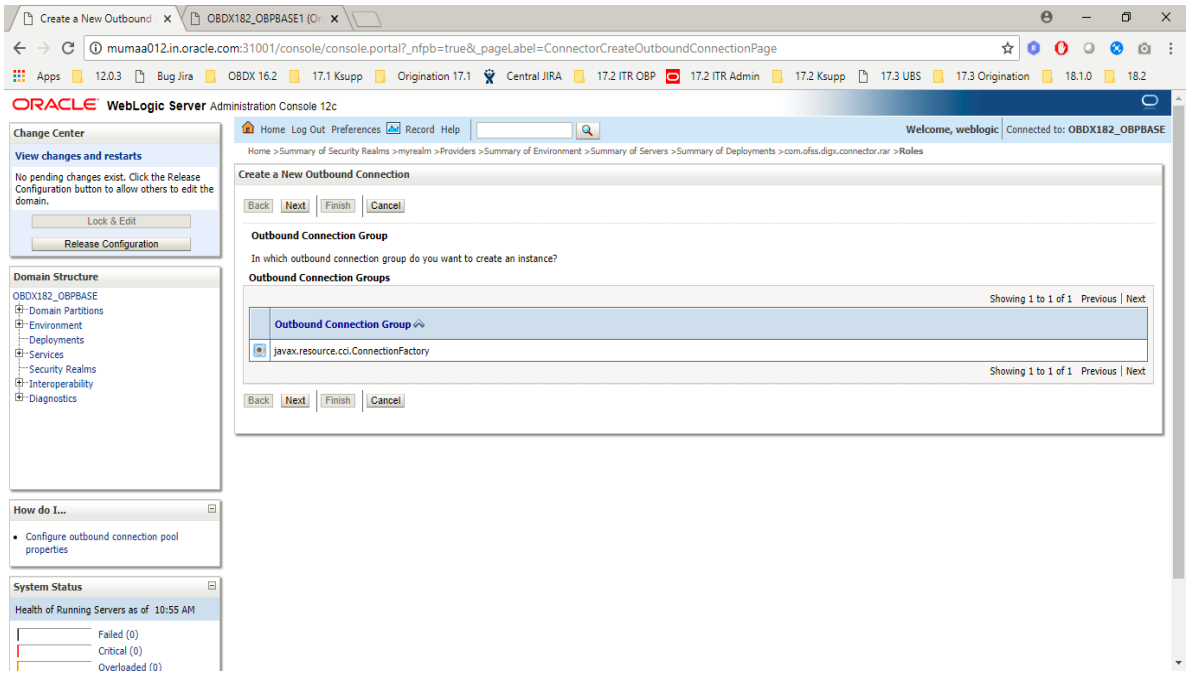
- Click **com.ofss.digx.connector.rar** as shown below.



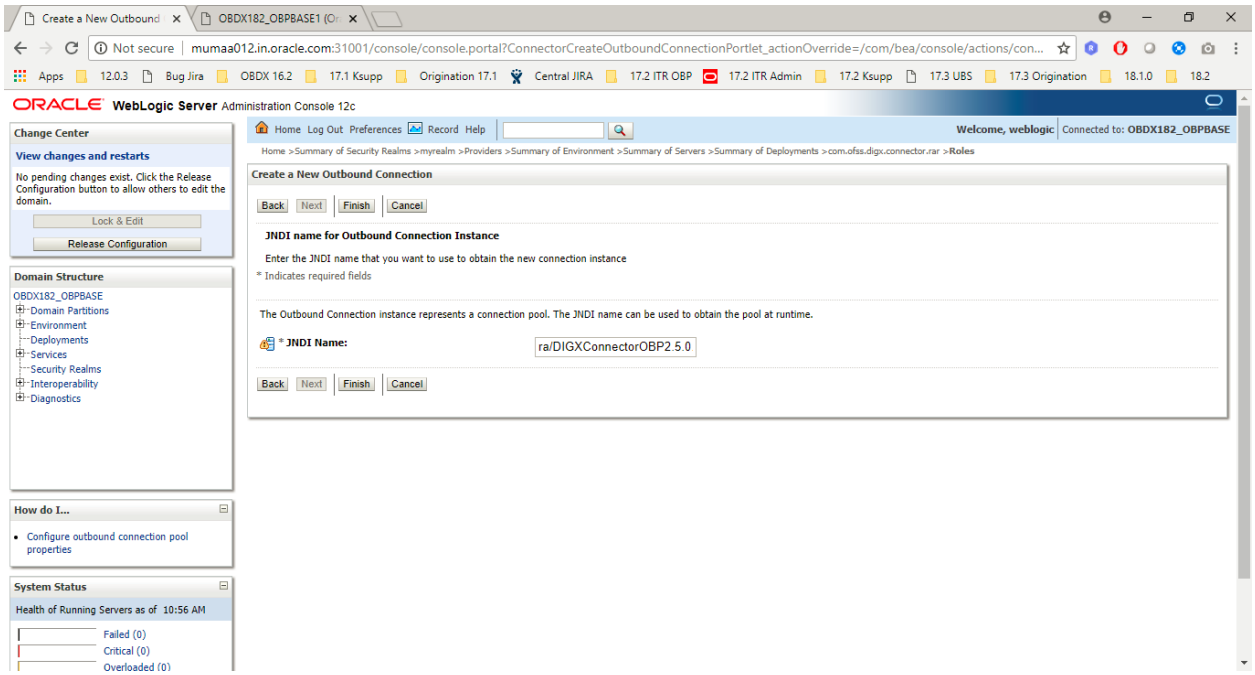
- Click On “configuration” tab as shown in figure.



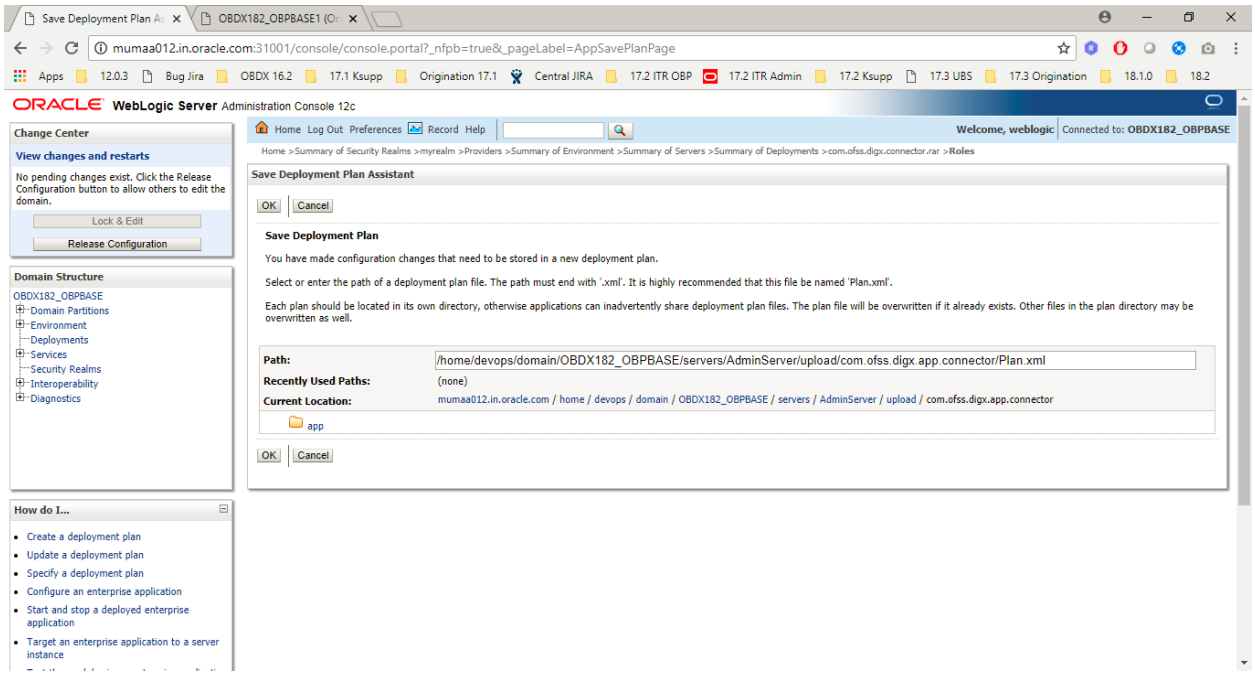
- Click on “New” button and select connection factory. Refer Screenshot.



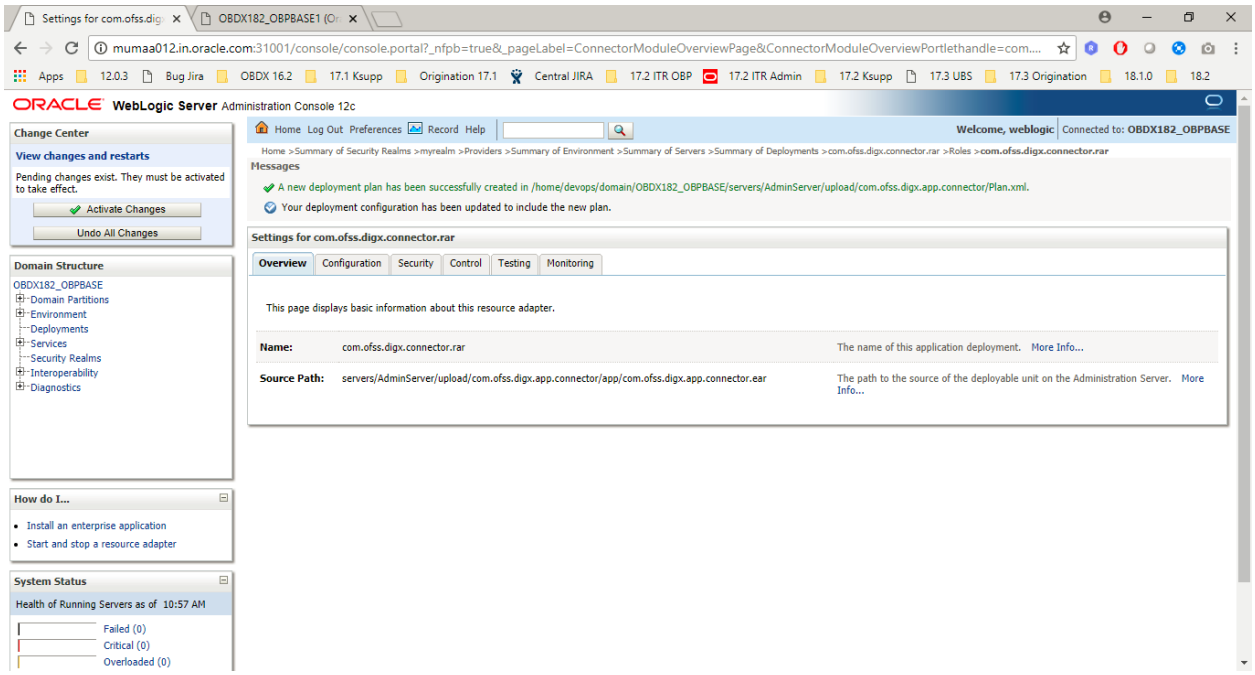
- Provide JINDI name as inserted in previous scripts. In this case name will be “ra/DIGXConnectorOBP”. After providing the name and Click on “Next”.

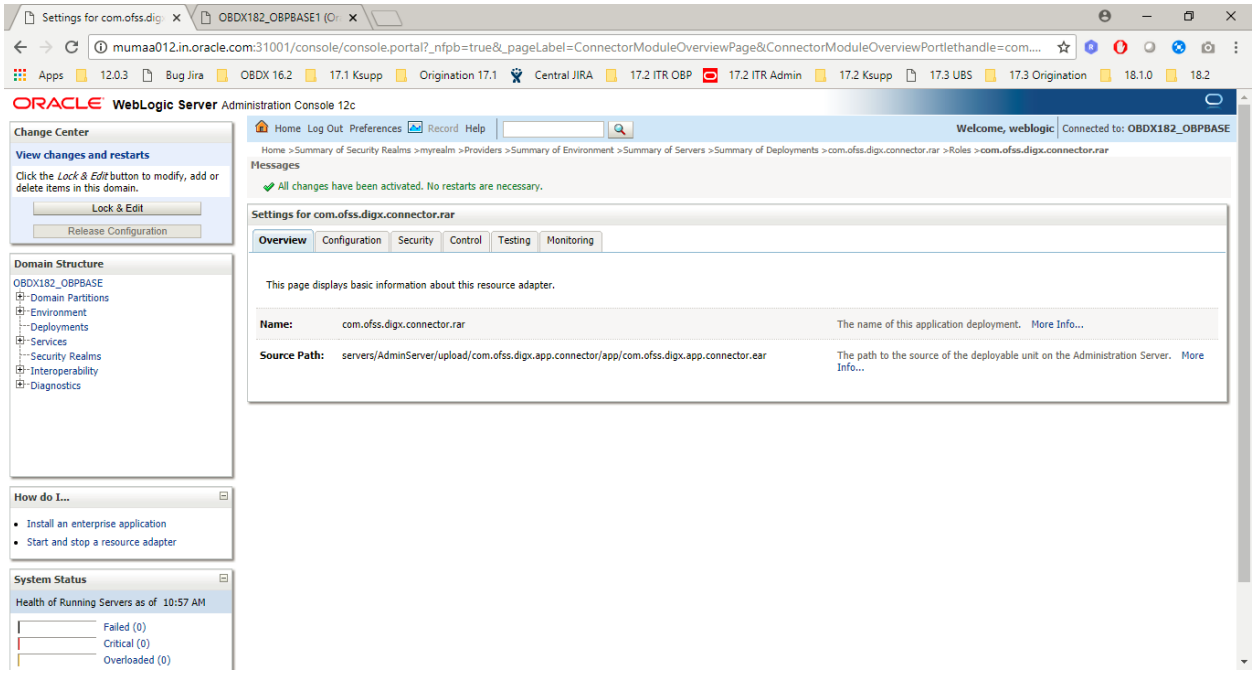


- Click on “Ok” to confirm.

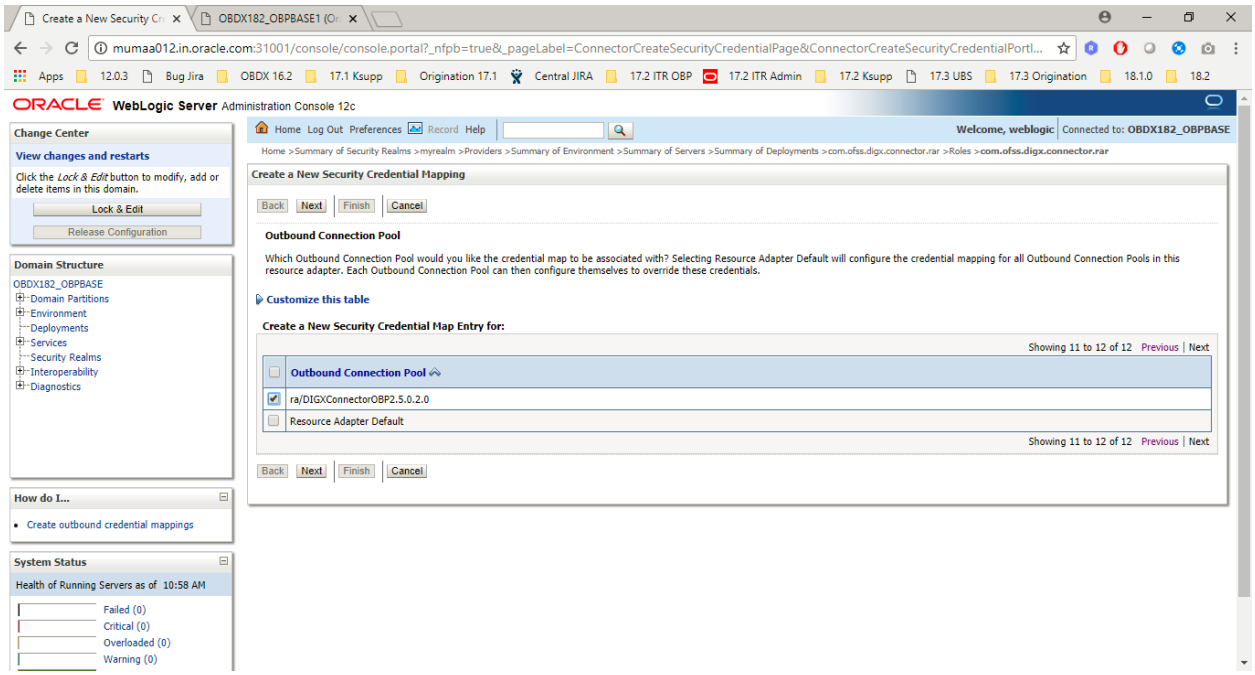


- Click on Activate changes.

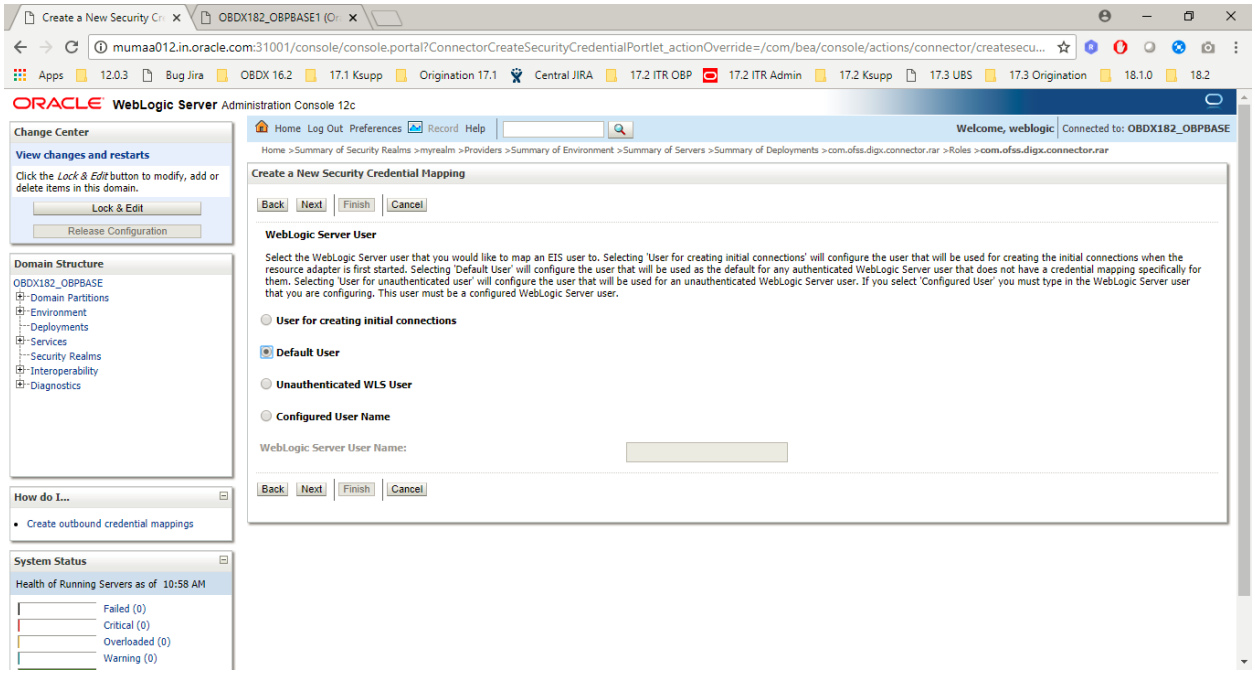




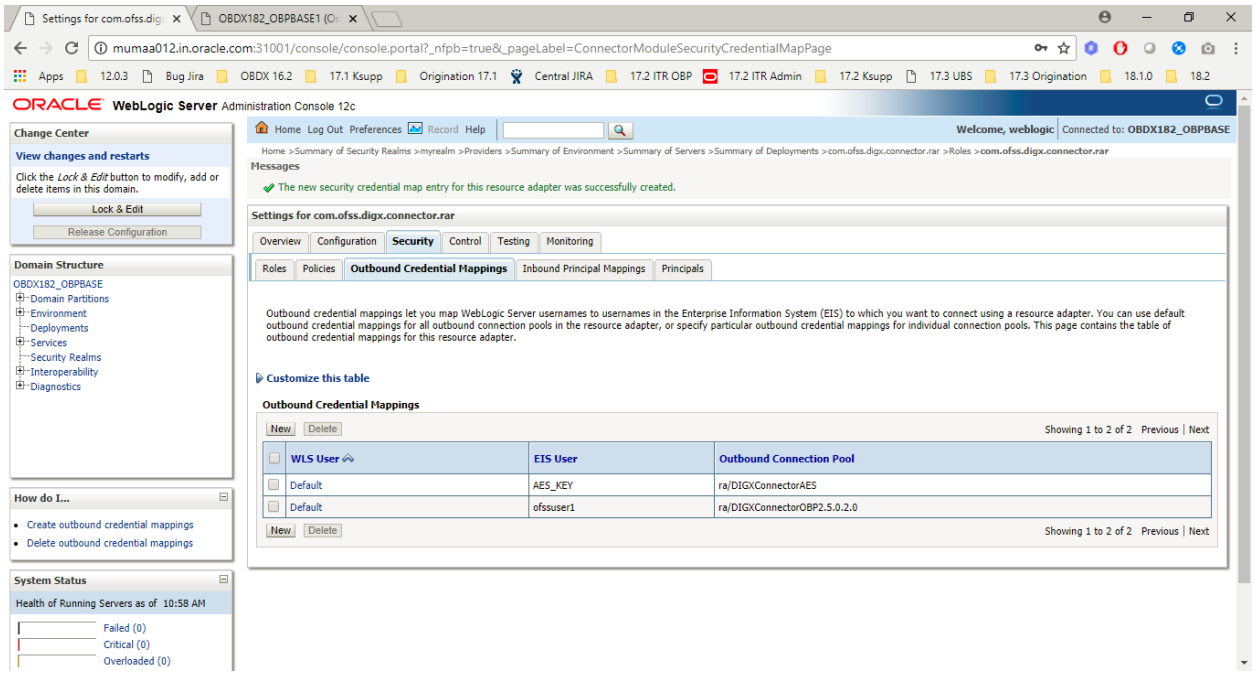
- Click on Security tab of connector, click on “Outbound credentials mapping”, click on “New” and select the newly created provider “ra/DIGXConnectorOBP” and click on “Next”.



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



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



- Restart managed server to take effects.