

Oracle® Banking APIs

Single Sign-on Configuration-SAML



Innovation Release 25.1.2.0.0

G51536-01

April 2026

ORACLE®

Copyright © 2006, 2026, Oracle and/or its affiliates.

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.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 fail-safe, 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.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Purpose	i
Audience	i
Documentation Accessibility	i
Critical Patches	i
Diversity and Inclusion	ii
Conventions	ii
Related Resources	ii
Screenshot Disclaimer	ii
Acronyms and Abbreviations	ii

1 Introduction

2 Configuration

2.1 Identity Provider Configuration at IDCS	1
2.2 SAML Authentication Provider configuration	5
2.3 SQL Authentication Provider configuration	9
2.4 OHS Configuration	13
2.5 Database Configuration	14
2.6 IDCS OAuth Integration	15
2.7 WebLogic configuration for OAuth	21
2.8 OBAPI configuration for OAuth	25
2.9 Default Admin Configuration	26
2.10 Logout Configurations	26

Index

List of Figures

2-1	<u>Dashboard</u>	<u>1</u>
2-2	<u>Add Application</u>	<u>2</u>
2-3	<u>Add SAML Application</u>	<u>2</u>
2-4	<u>Add SAML Application</u>	<u>3</u>
2-5	<u>Add SAML Application</u>	<u>3</u>
2-6	<u>Edit Application</u>	<u>4</u>
2-7	<u>Edit Application</u>	<u>4</u>
2-8	<u>Edit Application</u>	<u>5</u>
2-9	<u>Assign Users</u>	<u>5</u>
2-10	<u>Security Realms</u>	<u>6</u>
2-11	<u>Providers</u>	<u>6</u>
2-12	<u>Default Authenticator</u>	<u>6</u>
2-13	<u>Create Authentication Provider</u>	<u>7</u>
2-14	<u>Management</u>	<u>7</u>
2-15	<u>Create a SAML 2.0 Web Single Sign-on Identity Provider Partner</u>	<u>8</u>
2-16	<u>Settings for Create a SAML 2.0 Web Single Sign-on Identity Provider Partner</u>	<u>8</u>
2-17	<u>Servers</u>	<u>9</u>
2-18	<u>SAML 2.0 General</u>	<u>9</u>
2-19	<u>Security Realms</u>	<u>10</u>
2-20	<u>Providers</u>	<u>10</u>
2-21	<u>Create New Authentication Provider</u>	<u>11</u>
2-22	<u>Settings for Read Only SQL Authentication Provider</u>	<u>11</u>
2-23	<u>Settings for Read Only SQL Authentication Provider</u>	<u>12</u>
2-24	<u>Authentication</u>	<u>12</u>
2-25	<u>Reorder Authentication Providers</u>	<u>13</u>
2-26	<u>Dashboard</u>	<u>15</u>
2-27	<u>Add Application</u>	<u>16</u>
2-28	<u>Add Confidential Application</u>	<u>16</u>
2-29	<u>Add Confidential Application</u>	<u>17</u>
2-30	<u>Add Confidential Application</u>	<u>17</u>
2-31	<u>Add Confidential Application</u>	<u>18</u>
2-32	<u>Add App Role</u>	<u>18</u>
2-33	<u>Add Confidential Application</u>	<u>18</u>
2-34	<u>Add Confidential Application</u>	<u>19</u>
2-35	<u>Add Confidential Application</u>	<u>19</u>
2-36	<u>Add Confidential Application</u>	<u>19</u>

2-37	<u>Add Confidential Application</u>	<u>20</u>
2-38	<u>Edit Application</u>	<u>20</u>
2-39	<u>Edit Application</u>	<u>21</u>
2-40	<u>Deployments</u>	<u>21</u>
2-41	<u>Outbound Connection Pools Configuration</u>	<u>22</u>
2-42	<u>Outbound Connection Group Configuration</u>	<u>22</u>
2-43	<u>JNDI Configuration for Outbound Connection</u>	<u>22</u>
2-44	<u>Deployments</u>	<u>23</u>
2-45	<u>Outbound Credentials Mappings</u>	<u>23</u>
2-46	<u>Create New Security Credentials Mappings</u>	<u>24</u>
2-47	<u>Create New Security Credentials Mappings</u>	<u>24</u>
2-48	<u>Configure EIS UIS Username / Password</u>	<u>25</u>

Preface

- [Purpose](#)
- [Audience](#)
- [Documentation Accessibility](#)
- [Critical Patches](#)
- [Diversity and Inclusion](#)
- [Conventions](#)
- [Related Resources](#)
- [Screenshot Disclaimer](#)
- [Acronyms and Abbreviations](#)

Purpose

This guide is designed to help acquaint you with the Oracle Banking application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

Audience

This document is intended for the following audience:

- Customers
- Partners

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>.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at [Critical Patches, Security Alerts and](#)

[Bulletins](#). All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by [Oracle Software Security Assurance](#).

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Related Resources

For more information on any related features, refer to the following documents:

- Oracle Banking APIs Installation Manuals

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

Acronyms and Abbreviations

The list of the acronyms and abbreviations used in this guide are as follows:

Table 1 Acronyms and Abbreviations

Abbreviation	Description
OBAPI	Oracle Banking APIs

1

Introduction

This document covers step-by-step details on configuration required at IDCS side (Application and User) and WebLogic console configurations for SAML and SQL Authentication Providers. Document also includes the configuration required on OHS to enable different URL's for internal and external user login.

2

Configuration

To enable SAML authentication it involves configuration at WebLogic server (console) and IDCS console.

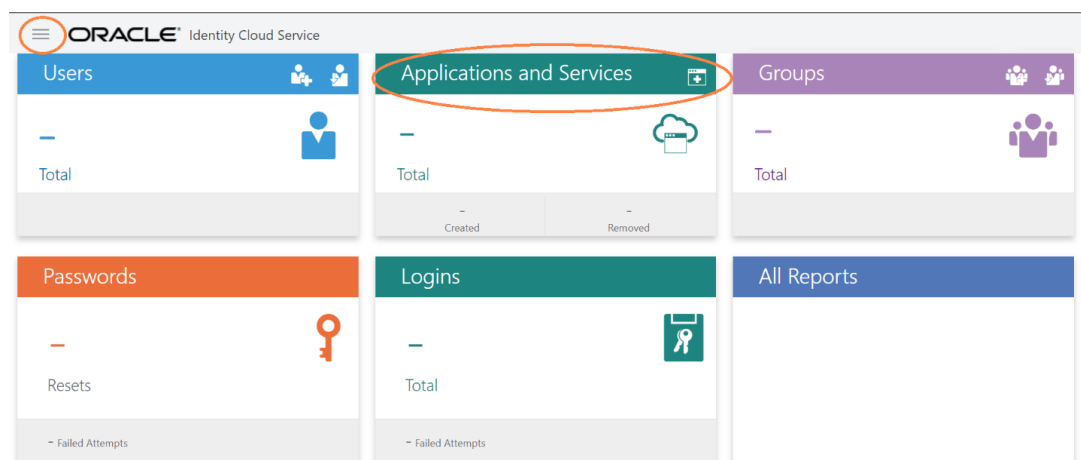
- [Identity Provider Configuration at IDCS](#)
- [SAML Authentication Provider configuration](#)
- [SQL Authentication Provider configuration](#)
- [OHS Configuration](#)
- [Database Configuration](#)
- [IDCS OAuth Integration](#)
- [WebLogic configuration for OAuth](#)
- [OBAPI configuration for OAuth](#)
- [Default Admin Configuration](#)
- [Logout Configurations](#)

2.1 Identity Provider Configuration at IDCS

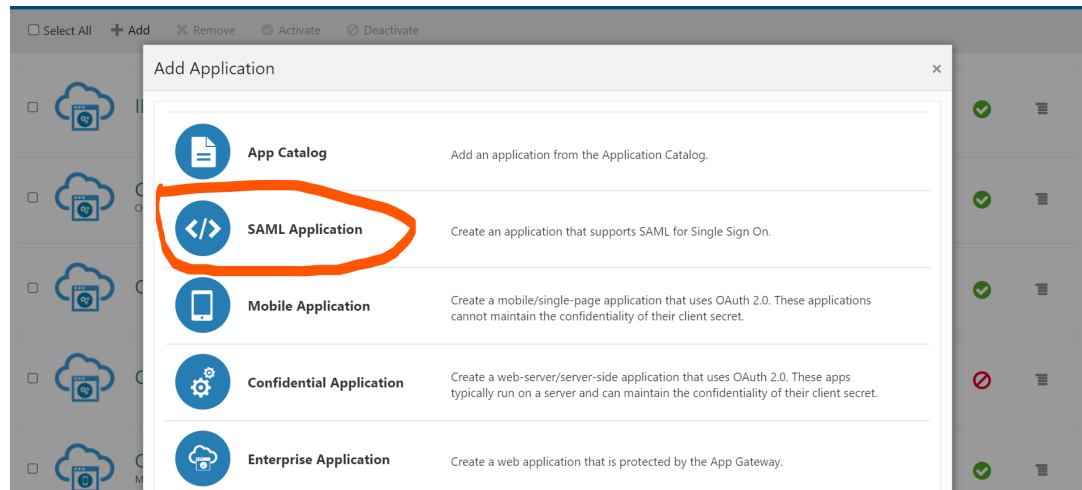
Steps to configure Identity Provide at IDCS

1. Login to Oracle Identity Cloud Service (IDCS) console with admin login. In dashboard click on **Add Application** in Application and Services widget or navigate through the breadcrumb menu as highlighted in screenshot.

Figure 2-1 Dashboard



2. In popup window select **SAML** Application.

Figure 2-2 Add Application

3. In **Add SAML Application** page provide below mentioned fields and click on **Next**.

- a. Name
- b. Description

Figure 2-3 Add SAML Application

Add SAML Application


Cancel Next >

1 ————— 2
Details SSO Configuration

App Details

* Name

Description

Application Icon 

Upload

Application URL / Relay State

Add Remove

4. Fill below mentioned fields as per section.

- a. General
 - i. Entity Id - A unique identifier / name for the service provider.
 - ii. Assertion Consumer URL - End point to which assertion will be sent by IDCS.
Recommended URL format `<OHS_URL>/saml2/sp/acs/pos`
e.g. `<PROTOCOL>://<OHS_HOST>:<OHS_PORT>/saml2/sp/acs/post`
`http://whf000xxx.bank.com:9999/saml2/sp/acs/post`
 - iii. NameID Format- Select value as "Unspecified".
 - iv. NameID Value- Select value as "User Name".

Figure 2-4 Add SAML Application

Add SAML Application

◀ Back

Details SSO Configuration

Download Signing Certificate Download Identity Provider Metadata

General

Use this section to define the required SSO attributes for the application and to upload the application's signing certificate.

* Entity ID OBDX_SAML

* Assertion Consumer URL http://example.com/saml2/sp/acs/post

* NameID Format Unspecified

* NameID Value User Name

Signing Certificate Upload

b. Advance Settings

- i. Signed SSO :- Select value as “Assertion”
- ii. Enable Single Logout: - This field should be checked.
- iii. Logout Binding: - Select value as “Redirect”.
- iv. Single Logout URL: - End point which IDCS will make call to do single logout functionality.
Recommended URL format <OHS_URL>/digx-infra/sso-logout
e.g. <PROTOCOL>: //<OHS_HOST>:<OHS_PORT>/digx-infra/sso-logout
<http://whf000xxx.bank.com:9999/digx-infra/sso-logout>
- v. Logout Response URL: -
Recommended URL format <OHS_URL>/digx-infra/sso-logout
e.g. <PROTOCOL>: //<OHS_HOST>:<OHS_PORT>/digx-infra/sso-logout
<http://whf000xxx.bank.com:9999/digx-infra/sso-logout>

Figure 2-5 Add SAML Application

Advanced Settings

This section contains additional configuration options.

Signed SSO Assertion

Include Signing Certificate in Signature ☐

Signature Hashing Algorithm SHA-256

Enable Single Logout ☒

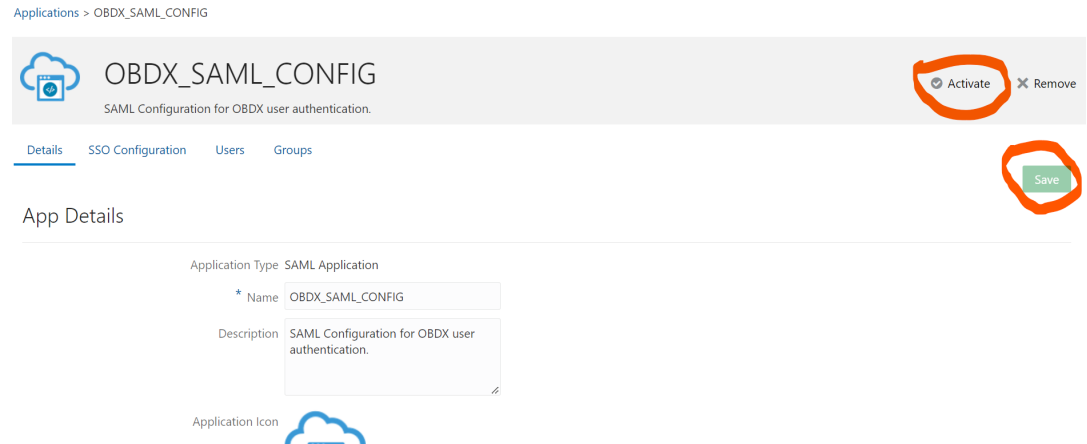
* Logout Binding Redirect

* Single Logout URL http://example.com:9999/digx-infra/ssc

* Logout Response URL http://example.com:9999

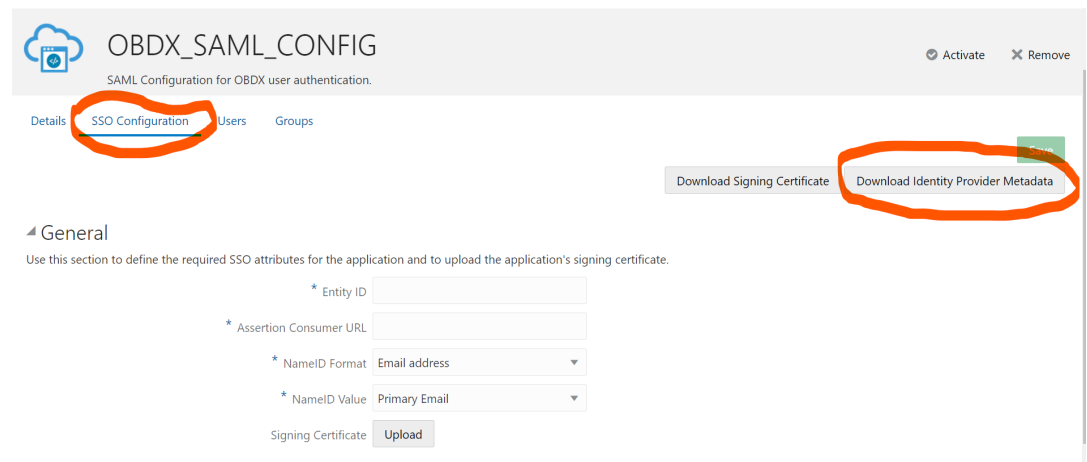
Encrypt Assertion ☐

5. Click on **Finish / Save**.
6. Click on **Activate** button to activate your application.

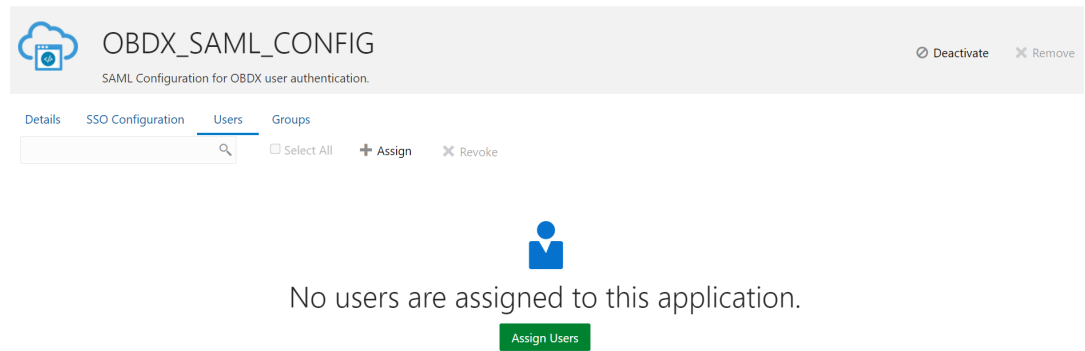
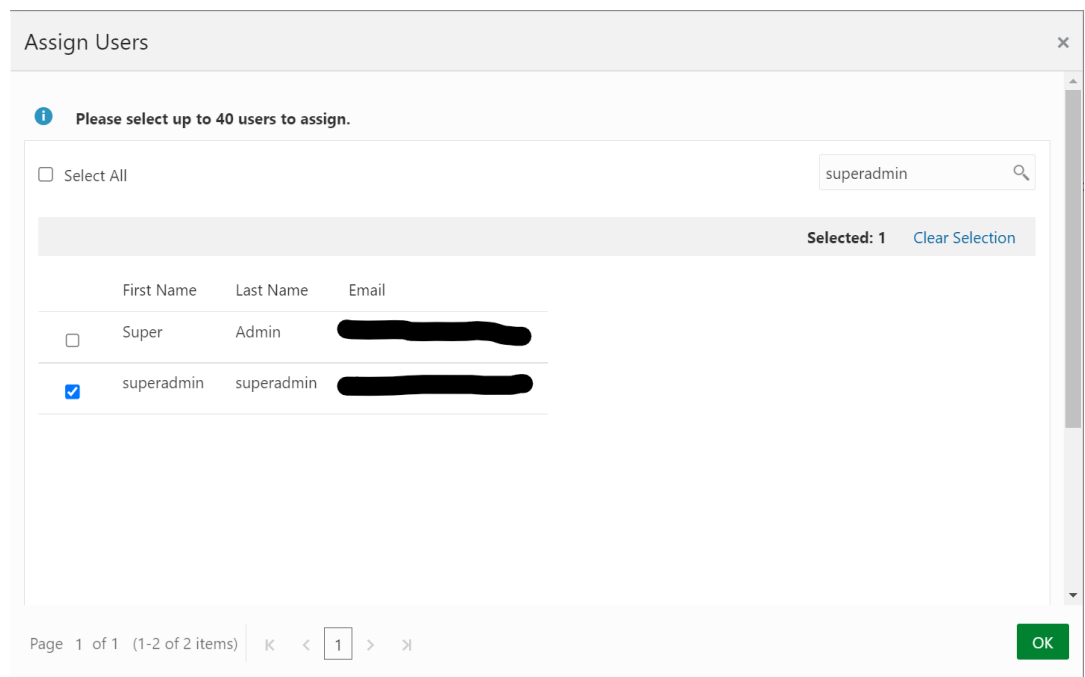
Figure 2-6 Edit Application

7. Navigate to Dashboard and search the application you have created.
8. Navigate to **SSO Configuration** tab and click on “**Download Identity Provider Metadata**”.

Keep the downloaded xml file, it will be required to upload in WebLogic console. Same is explain in WebLogic console configuration steps.

Figure 2-7 Edit Application

9. Copy / FTP the downloaded IDC metadata xml file to WebLogic server using winscp / putty.
 10. Navigate to **Users** tab in application to add the users related to application.
 11. Click on **Assign Users or Assign (+)** button to search and add the users into application.
- If user is not available follow steps mentioned in Section 1.3 to create new user.

Figure 2-8 Edit Application**Figure 2-9 Assign Users**

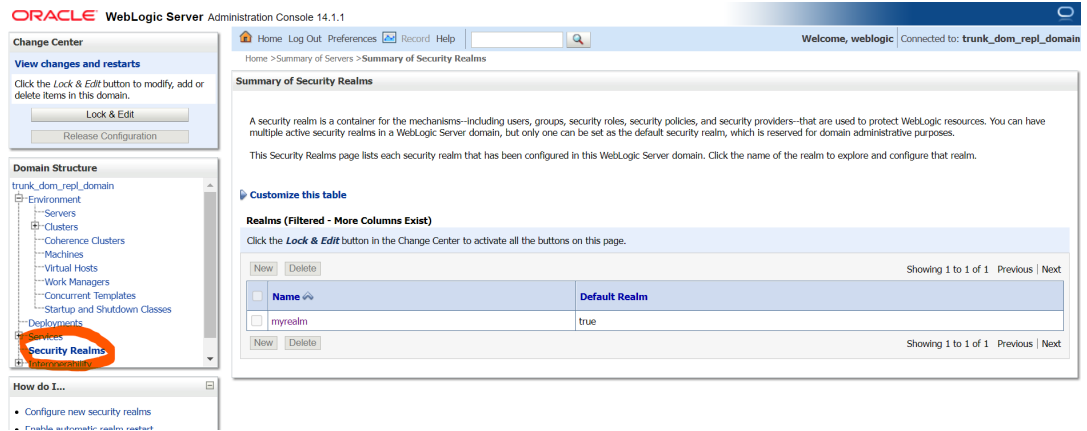
12. Logout from IDSC console.

2.2 SAML Authentication Provider configuration

Steps to configure SAML Authentication Providers changes into WebLogic console.

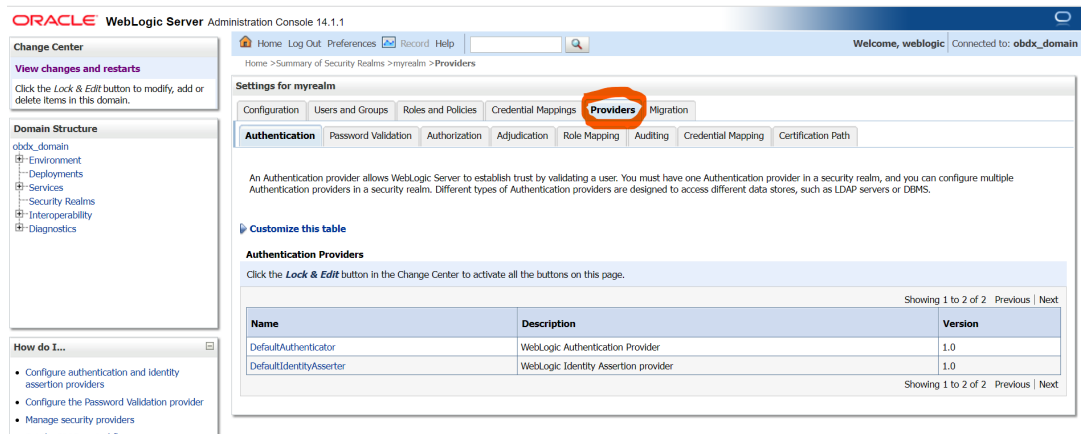
1. Login to WebLogic console with admin login and navigate to “Security Realms”.

Figure 2-10 Security Realms



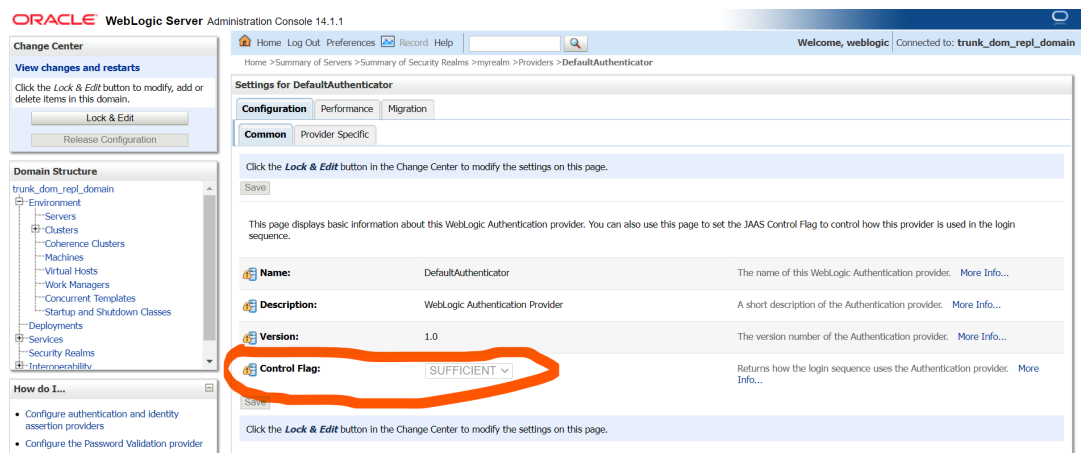
2. → Click on myrealm or your realm name present in screen. Navigate to “Providers” tab.

Figure 2-11 Providers



3. Select “DefaultAuthenticator” and change the Control Flag value to “SUFFICIENT”.

Figure 2-12 Default Authenticator

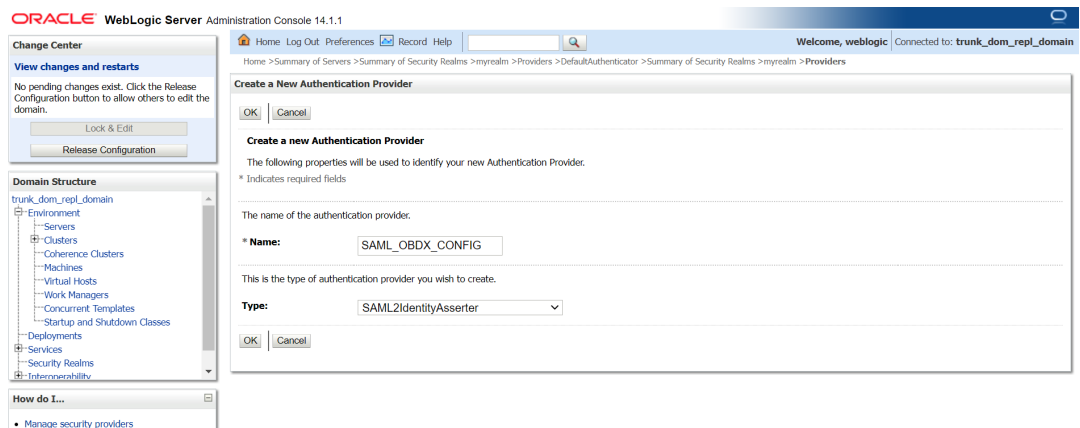


4. Again, navigate to **“Security Realms”** → myrealms → Providers and click on **New** button to create new Authentication Provider.

Fill the below mentioned fields with appropriate values and click on **OK**.

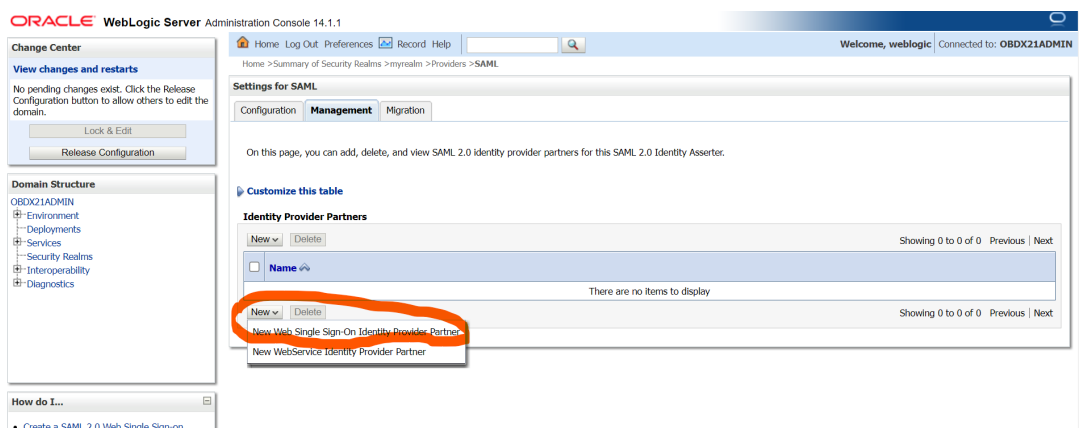
- a. Name: Name of authentication provider.
- b. Type : Select value as **“SAML2IdentityAsserter”**.

Figure 2-13 Create Authentication Provider



5. Restart Admin Server.
6. Login to WebLogic console and navigate to **“Security Realms”** → myrealms → Providers newly created authentication provider (e.g. SAML_OBDX_CONFIG) and navigate to **“Management”** tab.
7. Click on **New** button to add the Identity Provider Partner and select **“New Web Single Sign-On Identity Provider Partner”**.

Figure 2-14 Management



8. Provide the name for the identity partner and select the IDC metadata xml copied to WebLogic server.

Click **OK** button to save.

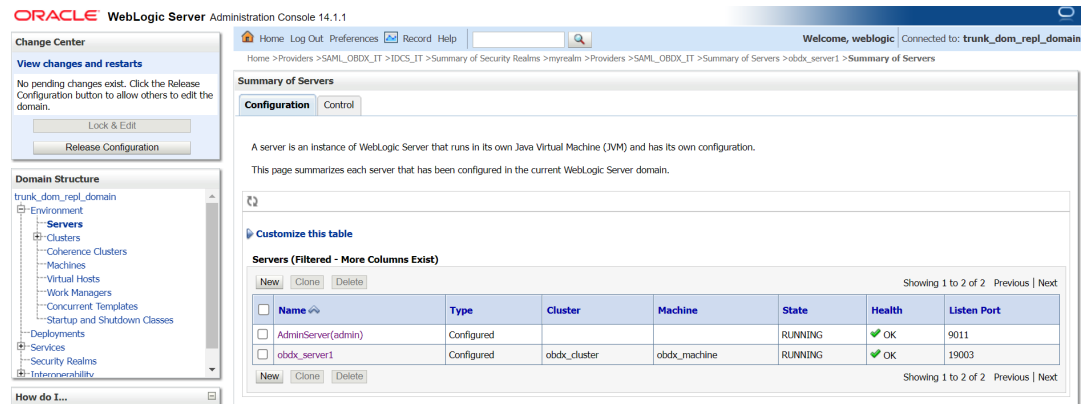
Figure 2-15 Create a SAML 2.0 Web Single Sign-on Identity Provider Partner

9. Open the newly added Identity Provider Partner and select below mentioned checkboxes and field and click on **Save**.
 - a. Enable: Checked
 - b. Virtual User: Checked
 - c. Redirect URIs: /digx-infra/admin-dashboard

Figure 2-16 Settings for Create a SAML 2.0 Web Single Sign-on Identity Provider Partner

10. Navigate to “Environment” → “Servers” and select the server on which SSO authentication application will be deployed.

Figure 2-17 Servers



11. Navigate to “Federation Services” → “SAML 2.0 General” and provide values to below mentioned fields. Click on **Save**.
 - a. Published Site URL: Recommended URL format <OHS_URL>/saml2
e.g. <PROTOCOL>://<OHS_HOST>:<OHS_PORT>/saml2

http://whf000xxx.bank.com:9999/saml2
 - b. Entity Id: Value should match with Entity Id provided in SAML configuration in IDCS console.
 - c. Recipient Check Enabled: unchecked.

Figure 2-18 SAML 2.0 General

The screenshot shows the 'SAML 2.0 General' configuration page. It has fields for 'Published Site URL' and 'Entity ID'. Below these is a 'Bindings' section with a checkbox for 'Recipient Check Enabled' which is unchecked. There are also 'More Info...' links for the URL and Entity ID fields.

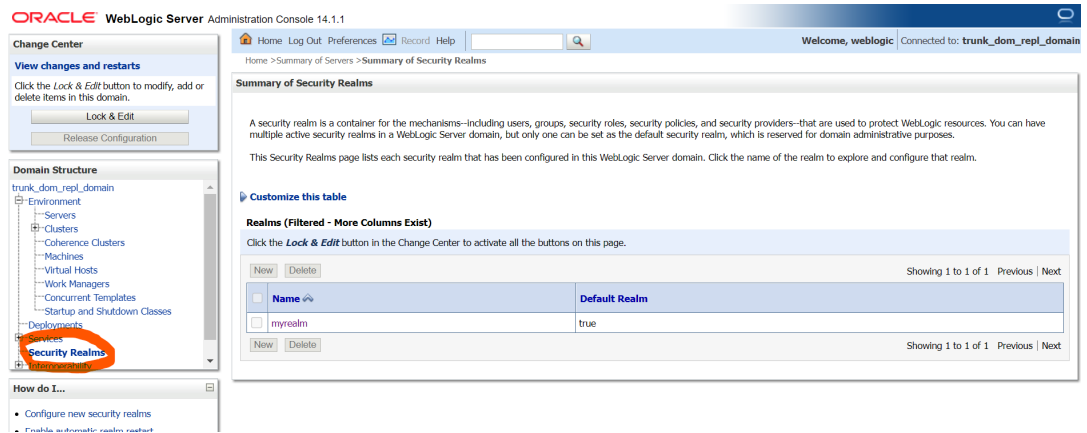
12. Navigate to “Federation Services” → “SAML 2.0 Service Provider” and provide values to below mentioned fields and click on **Save**.
 - a. Enabled: Check box should be checked.
 - b. Preferred Binding: Post
 - c. Default URL: <OHS_URL>/digx-infra/admin-dashboard

2.3 SQL Authentication Provider configuration

Steps to configure SQL Authentication Providers changes into WebLogic console.

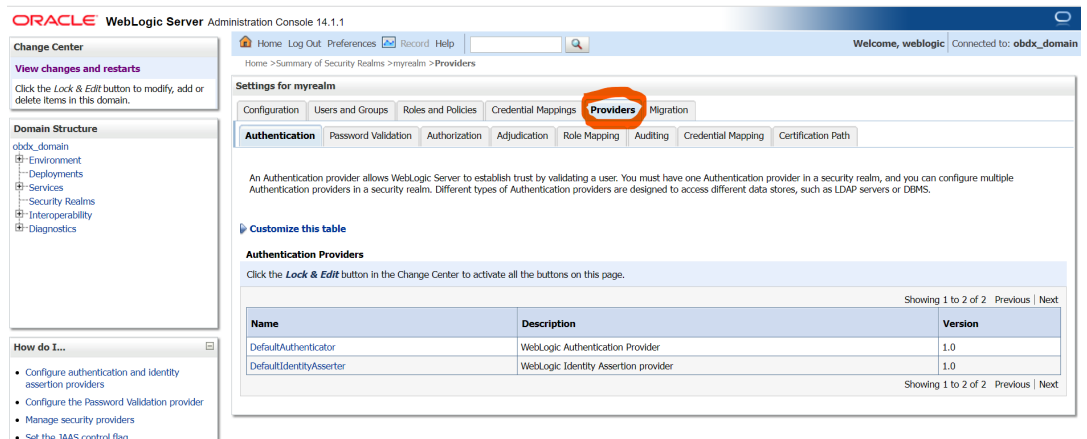
1. Login to WebLogic console with admin login and navigate to “Security Realms”.

Figure 2-19 Security Realms



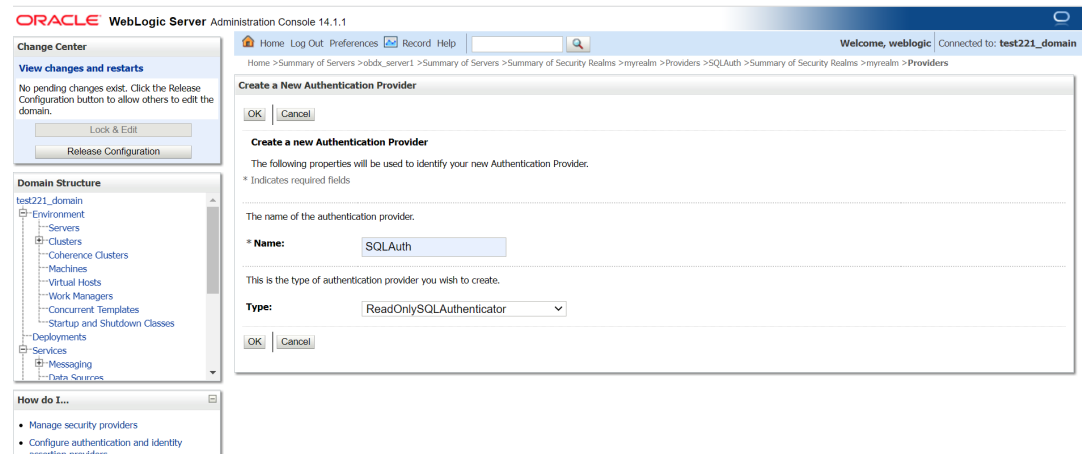
2. → Click on myrealm or your realm name present in screen. Navigate to “Providers” tab.

Figure 2-20 Providers



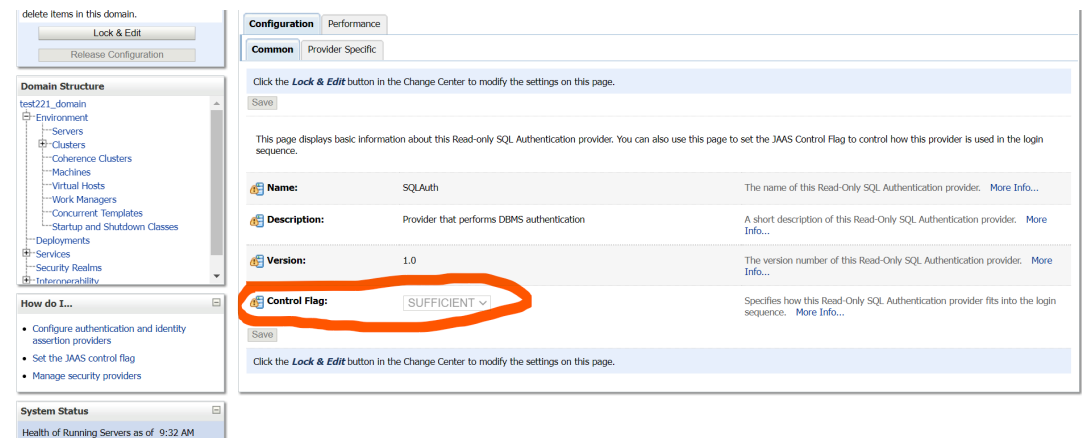
3. Click on **New** button to create new Authentication Provider.
Fill the below mentioned fields with appropriate values and click on **OK**.
 - a. Name: Name of authentication provider.
 - b. Type :Select value as “ReadOnlySQLAuthenticator”.

Figure 2-21 Create New Authentication Provider



4. Open newly created authentication provider (e.g. SQLAuth). Select the value of Control Flag as “SUFFICIENT”.

Figure 2-22 Settings for Read Only SQL Authentication Provider



5. Navigate to “Provider Specific” tab to configuration related to SQL Authentication.
6. Provide the values to fields mentioned below with given value in case it is not auto populated.
 - a. Data Source Name: NONXA
 - b. SQL Get Users Password: SELECT U_PASSWORD FROM USERS WHERE U_NAME = ?
 - c. SQL User Exists: SELECT U_NAME FROM USERS WHERE U_NAME = ?
 - d. SQL List Users: SELECT U_NAME FROM USERS WHERE U_NAME LIKE ?
 - e. SQL List Groups: SELECT G_NAME FROM GROUPS WHERE G_NAME LIKE ?
 - f. VI. SQL Group Exists: SELECT G_NAME FROM GROUPS WHERE G_NAME = ?
 - g. SQL Is Member: SELECT G_MEMBER FROM GROUPMEMBERS WHERE G_NAME = ? AND G_MEMBER = ?
 - h. SQL List Member Groups: SELECT G_NAME FROM GROUPMEMBERS WHERE G_MEMBER = ?

- i. SQL Get User Description: - SELECT U_DESCRIPTION FROM USERS WHERE U_NAME = ?
- j. SQL Get Group Description: - SELECT G_DESCRIPTION FROM GROUPS WHERE G_NAME = ?

Figure 2-23 Settings for Read Only SQL Authentication Provider

Data Source Name: NONXA [More Info...](#)

Group Membership Searching: unlimited [More Info...](#)

Max Group Membership Search Level: 0 [More Info...](#)

SQL Get Users Password: SELECT U_PASSWORD FROM [More Info...](#)

SQL User Exists: SELECT U_NAME FROM [More Info...](#)

SQL List Users: SELECT U_NAME FROM [More Info...](#)

SQL List Groups: SELECT G_NAME FROM [More Info...](#)

SQL Group Exists: SELECT G_NAME FROM [More Info...](#)

SQL Is Member: SELECT G_MEMBER FROM [More Info...](#)

SQL List Member Groups: SELECT G_NAME FROM [More Info...](#)

☒ **Descriptions Supported** [More Info...](#)

SQL Get User Description: SELECT U_DESCRIPTION [More Info...](#)

SQL Get Group Description: SELECT G_DESCRIPTION [More Info...](#)

[Save](#)

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

7. Click on **Save**.
8. Navigate to “**Security Realms**” → myrealms → Providers and click on **Reorder** button.

Figure 2-24 Authentication

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS.

[Customize this table](#)

Authentication Providers

[New](#) [Delete](#) [Reorder](#) Showing 1 to 4 of 4 Previous | Next

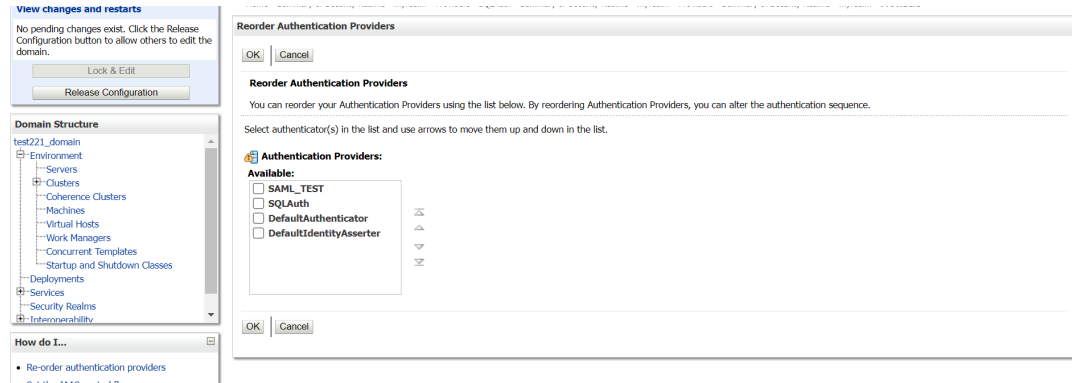
<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	SAML_TEST	SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0.	1.0
<input type="checkbox"/>	SQLAuth	Provider that performs DBMS authentication	1.0
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

[New](#) [Delete](#) [Reorder](#) Showing 1 to 4 of 4 Previous | Next

9. Reorder the authentication providers as given below.

- a. SAML Authentication Provider
- b. SQL Authentication Provider
- c. Default Authenticator

Figure 2-25 Reorder Authentication Providers



10. Restart all the servers in domain including Admin Server.

Note

Accessing /saml2 uri from OHS (<OHS_URL>/saml2), /saml2 uri has to be proxy bypassed from OHS

2.4 OHS Configuration

Provides details on configuration required on OHS to enable different URL's for internal and external users. i.e authentication with OBDX or external service provider.

1. Open obdx.conf file from OHS server. You can find the location of obdx.conf file from httpd.conf file.
2. Verify if proxypass URLs are configured in obdx.conf file. If not then add entries as mentioned in below format.

```
ProxyPassMatch "/digx(.*)" "<PROTOCOL>://<WL_HOST_NAME>:<WL_PORT>/digx$1"
ProxyPassReverse "/digx(.*)" "<PROTOCOL>://<WL_HOST_NAME>:<WL_PORT>/digx$1"
ProxyPassMatch "/saml2(.*)" "<PROTOCOL>://<WL_HOST_NAME>:<WL_PORT>/saml2$1"
ProxyPassReverse "/saml2(.*)" "<PROTOCOL>://<WL_HOST_NAME>:<WL_PORT>/saml2$1"
ProxyPassMatch "/digx(.*)" "http://whf000xxx.bank.com:19003/digx$1"
ProxyPassReverse "/digx(.*)" "http://whf000xxx.bank.com:19003/digx$1"
ProxyPassMatch "/saml2(.*)" "http://whf000xxx.bank.com:19001/saml2$1"
ProxyPassReverse "/saml2(.*)" "http://whf000xxx.bank.com:19001/saml2$1"
```

3. Add below virtual configuration into obdx.conf file.

```
##Virtual HostsListen <PORT_1><VirtualHost *: <PORT_1>>      ServerName
                        <HOST_NAME>
                        RewriteEngine On
                        RewriteOptions inherit
                        <Directory
                        "${DocumentRoot}">
```

```
Options FollowSymLinks
AllowOverride all
</Directory></VirtualHost> Listen <PORT_2><VirtualHost
*:<PORT_2>>
ServerName <HOST_NAME>
RewriteEngine On
RewriteRule      "^(.*)/config\.js$"
"<SERVER_PROTOCOL>://<HOST_NAME>:<PORT_2>/framework/js/
configurations/config-admin.js" [R]
<Directory
"${DocumentRoot}">
Options FollowSymLinks
AllowOverride all
</Directory>
</VirtualHost>
```

❗ Note

Replace the <PORT_1> & <PORT_2> with the ports which are expose to outside world. Replace <SERVER_PROTOCOL> and <HOST_NAME> with appropriate values. E.g. http and whfxxx.sample.com (if hostname is not available then <HOST_NAME> value can be IP address.)

```
# All other request passed through this rules.
ProxyPassMatch "/digx(.*)" "http://whf00qiw.in.oracle.com:19001/digx$1"
ProxyPassReverse "/digx(.*)" "http://whf00qiw.in.oracle.com:19001/digx$1"
ProxyPassMatch "/saml2(.*)" "http://whf00qiw.in.oracle.com:19001/saml2$1"
ProxyPassReverse "/saml2(.*)" "http://whf00qiw.in.oracle.com:19001/saml2$1"

##Virtual Hosts
Listen 8888
<VirtualHost *:8888>
    ServerName whf00qiw.in.oracle.com
    RewriteEngine On
    RewriteOptions inherit

    <Directory "${DocumentRoot}">
        Options FollowSymLinks
        AllowOverride all
        #Require all granted
    </Directory>
</VirtualHost>

Listen 9999
<VirtualHost *:9999>
    ServerName whf00qiw.in.oracle.com
    RewriteEngine On
    RewriteRule      "^(.*)/config\.js$" "http://whf00qiw.in.oracle.com:9999/framework/js/configurations/config-admin.js" [R]

    <Directory "${DocumentRoot}">
        Options FollowSymLinks
        AllowOverride all
        #Require all granted
    </Directory>
</VirtualHost>
```

4. Save obdx.conf file and restart ohs server.

2.5 Database Configuration

To enable SSO for external users below configuration need to be done in database.

1. To enable SSO authentication for user type / enterprise role execute below query on intended database environment. Replace <USER_TYPE> with the user type / enterprise role for which SSO authentication to be enabled.

```
UPDATE DIGX_FW_CONFIG_ALL_B SET PROP_VALUE = 'External' WHERE PROP_ID =
'<USER_TYPE>' AND CATEGORY_ID = ' AuthenticationConfiguration ';
```

For example: UPDATE DIGX_FW_CONFIG_ALL_B SET PROP_VALUE = 'External' WHERE PROP_ID = 'administrator' AND CATEGORY_ID = 'AuthenticationConfiguration';

2. Execute below query for redirection after authentication from SSO service provider back to OBDX. Replace the value of <OHS_URL_FOR_ADMIN_USER_LOGIN> with the OHS_URL with port enable for external / admin user login, the virtual host enabled in section 3.4, step 3.

```
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 ('SSO_PUBLIC_URL', 'dayoneconfig',
'<OHS_URL_FOR_ADMIN_USER_LOGIN>', 'N', null, 'Public SSO URL', 'ofssuser',
to_timestamp('29-09-22 10:05:56.000000000 AM', 'DD-MM-RR fmHH12:fmMI:SSXFF
AM'), 'ofssuser', to_timestamp('29-09-22 10:05:56.000000000 AM', 'DD-MM-RR
fmHH12:fmMI:SSXFF AM'), 'A', 1, 'N', null);
```

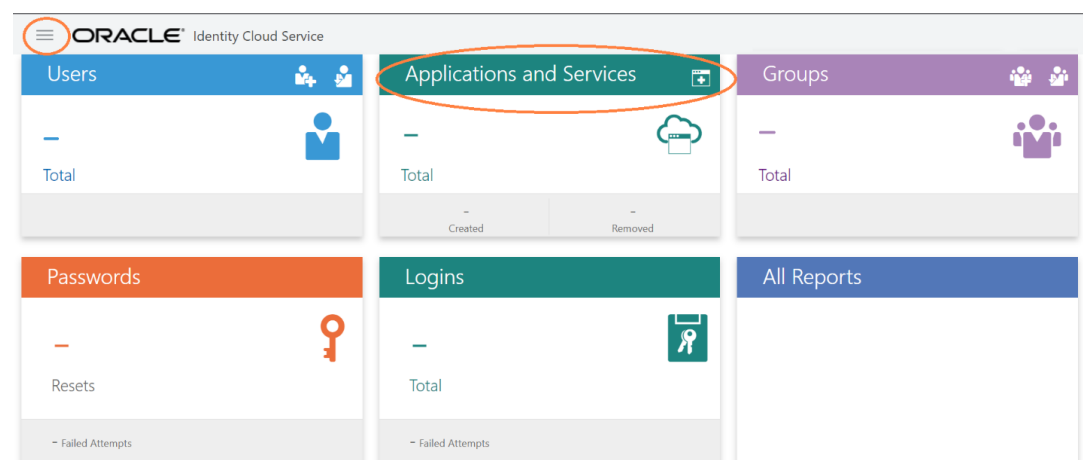
For Example: INSERT INTO DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER, EDITABLE, CATEGORY_DESCRIPTION) values ('SSO_PUBLIC_URL', 'dayoneconfig', 'http:// whf000xxx.bank.com:9999', 'N', null, 'Public SSO URL', 'ofssuser', to_timestamp('29-09-22 10:05:56.000000000 AM', 'DD-MM-RR fmHH12:fmMI:SSXFF AM'), 'ofssuser', to_timestamp('29-09-22 10:05:56.000000000 AM', 'DD-MM-RR fmHH12:fmMI:SSXFF AM'), 'A', 1, 'N', null);

2.6 IDCS OAuth Integration

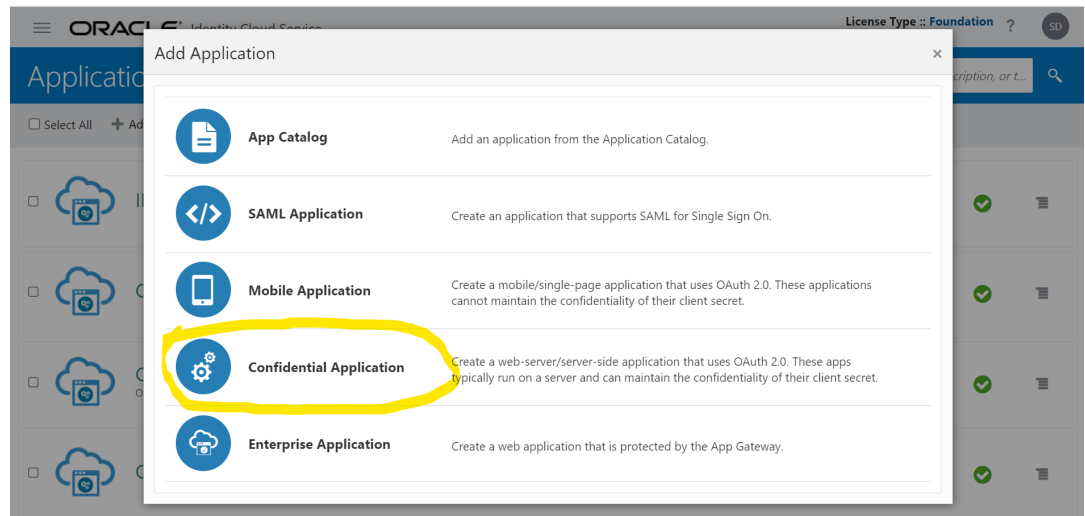
To fetch the user information from external SSO provider, application need to be registered as a client in IDCS. Below steps providers details on registering the application in IDCS.

1. Login to Oracle Identity Cloud Service (IDCS) console with admin login. In dashboard click on **Add Application** in **Application and Services** widget or navigate through the breadcrumb menu as highlighted in screenshot.

Figure 2-26 Dashboard



2. In popup window select Confidential Application.

Figure 2-27 Add Application

3. In **Add Confidential Application** page provide below mentioned fields and click on **Next**.
 - a. Name
 - b. Description

Figure 2-28 Add Confidential Application

4. Select **Configure this application as a client now** option in screen as shown in below screenshot.
 - a. Name
 - b. Description

Figure 2-29 Add Confidential Application

Add Confidential Application

← Back Details **Client** Resources Web Tier Policy Authorization Next >

☒ Configure this application as a client now ☐ Skip for later

Authorization

Allowed Grant Types ☐ Resource Owner ☐ Client Credentials ☐ JWT Assertion ☐ SAML2 Assertion ☐ Refresh Token ☐ Authorization Code ☐ Implicit

☐ Device Code

☐ TLS Client Authentication

Allow non-HTTPS URLs ☐

Redirect URL

Logout URL

Post Logout Redirect URL

Security ☐ Trusted Client Certificate **Import**

5. Fill below mentioned fields as per section.

a. Authorization

- i. Allowed Grant Types:- Select checkbox as “Client Credentials” and “JWT Assertion”

Figure 2-30 Add Confidential Application

← Back Details **Client** Resources Web Tier Policy Authorization Next >

☒ Configure this application as a client now ☐ Skip for later

Authorization

Allowed Grant Types ☐ Resource Owner ☒ Client Credentials ☒ JWT Assertion ☐ SAML2 Assertion ☐ Refresh Token ☐ Authorization Code ☐ Implicit

☐ Device Code

☐ TLS Client Authentication

Allow non-HTTPS URLs ☐

Redirect URL

Logout URL

Post Logout Redirect URL

Security ☐ Trusted Client Certificate **Import**

Allowed Operations ☐ Introspect ☐ On behalf Of

ID Token Encryption Algorithm

b. Token Issuance Policy

- i. Authorized Resources :Select value as “Specific”
- ii. Grant the client access to Identity Cloud Service Admin APIs: Click on **Add** button

Figure 2-31 Add Confidential Application

Token Issuance Policy ⓘ

Authorized Resources ☐ All ☐ Tagged ☒ Specific

Resources

+ Add Scope

Resource	Protected	Scope
No data to display.		

Grant the client access to Identity Cloud Service Admin APIs

+ Add

App Roles	Protected
No data to display.	

- iii. In popup window search for **“Identity Domain Administrator”** and click on **Add**.

Figure 2-32 Add App Role

Token Issuance Policy ⓘ

Authorized Resources ☐ All ☐ Tagged ☒ Specific

Resources

+ Add Scope

Resource	Protected	Scope
No data to display.		

Grant the client access to Identity Cloud Service Admin APIs

+ Add

App Roles	Protected
No data to display.	

Add App Role

Select All ☒ identity X

Selected: 1 Clear Selection

<input checked="" type="checkbox"/>	Identity Domain Administrator
-------------------------------------	-------------------------------

Page 1 of 1 (1 of 1 items) | < 1 > X

Add

- iv. Verify a row added in table for **App Roles** as shown like below screenshot.

Figure 2-33 Add Confidential Application

Token Issuance Policy ⓘ

Authorized Resources ☐ All ☐ Tagged ☒ Specific

Resources

+ Add Scope

Resource	Protected	Scope
No data to display.		

Grant the client access to Identity Cloud Service Admin APIs

+ Add

App Roles	Protected
Identity Domain Administrator	No

- v. Click on **Next** button on top.
- c. Expose APIs to Other Applications: Select **"Skip for later"** and click on **Next**.

Figure 2-34 Add Confidential Application

Add Confidential Application

< Back Details Client **Resources** Web Tier Policy Authorization Next >

Expose APIs to Other Applications

Specify the APIs that need to be protected.

☐ Configure this application as a resource server now ☒ Skip for later

No Resources are protected by OAuth

- d. Web Tier Policy: Select **"Skip for later"** and click on **Next** button.

Figure 2-35 Add Confidential Application

Add Confidential Application

< Back Details Client Resources **Web Tier Policy** Authorization Next >

Web Tier Policy

Use this page to configure, edit, and validate a web tier policy. Additionally, you can import and export existing policies.

☐ Configure Web Tier Policy for this application ☒ Skip for later

- e. Click on **"Finish"**.

Figure 2-36 Add Confidential Application

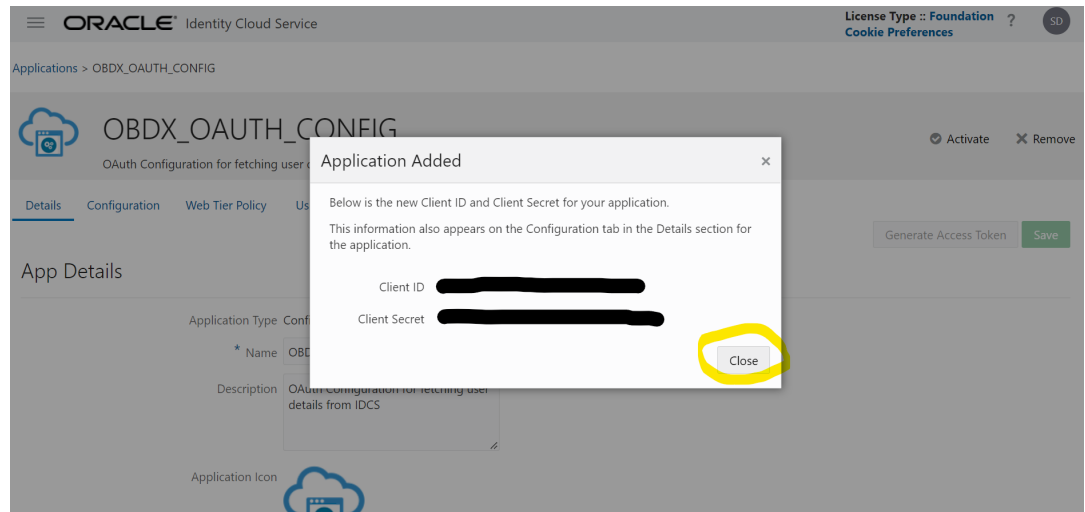
Add Confidential Application

< Back Details Client Resources Web Tier Policy **Authorization** Finish

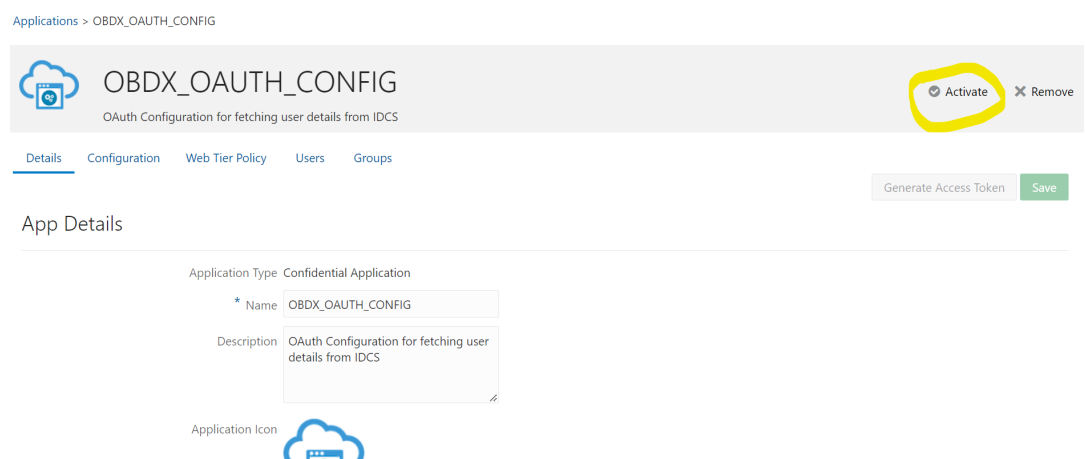
Authorization

Enforce Grants as Authorization ☐

- 6. After finish click a popup window will open with "Client ID" and "Client Secret" as shown in below screenshot. Copy the Client Id and Client Secret to text file to keep it handy as it will be required in further steps. Once copied click on "Close".

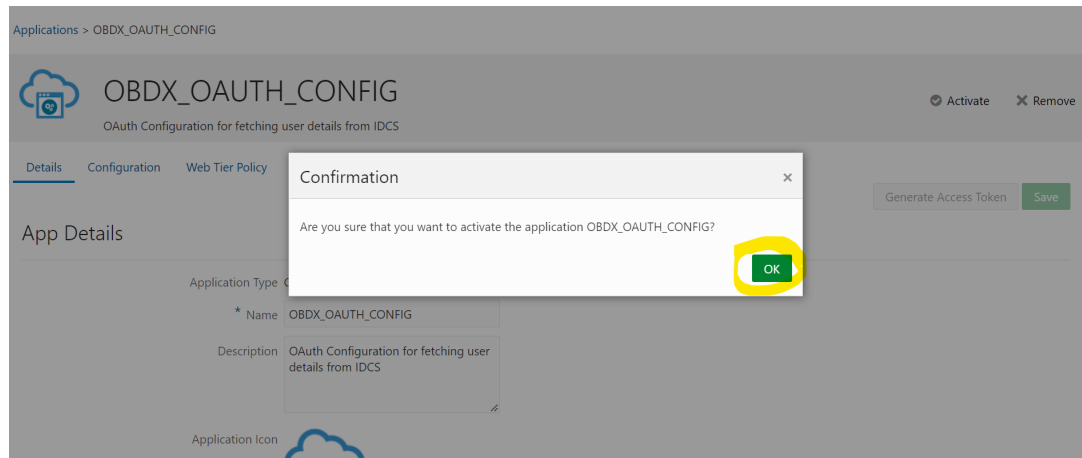
Figure 2-37 Add Confidential Application

7. Click on **"Activate"** button to activate the application.

Figure 2-38 Edit Application

8. Popup window asking confirmation to activate the application will open, click on **"OK"** to activate the application.

Figure 2-39 Edit Application



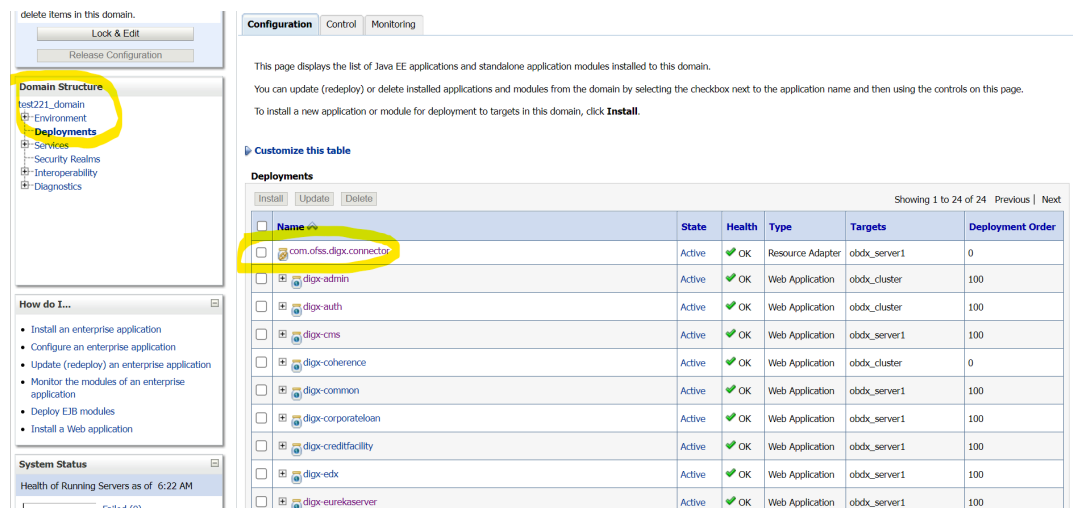
9. Logout from IDCS console.

2.7 WebLogic configuration for OAuth

To enable OAuth support on WebLogic server follow below mentioned steps.

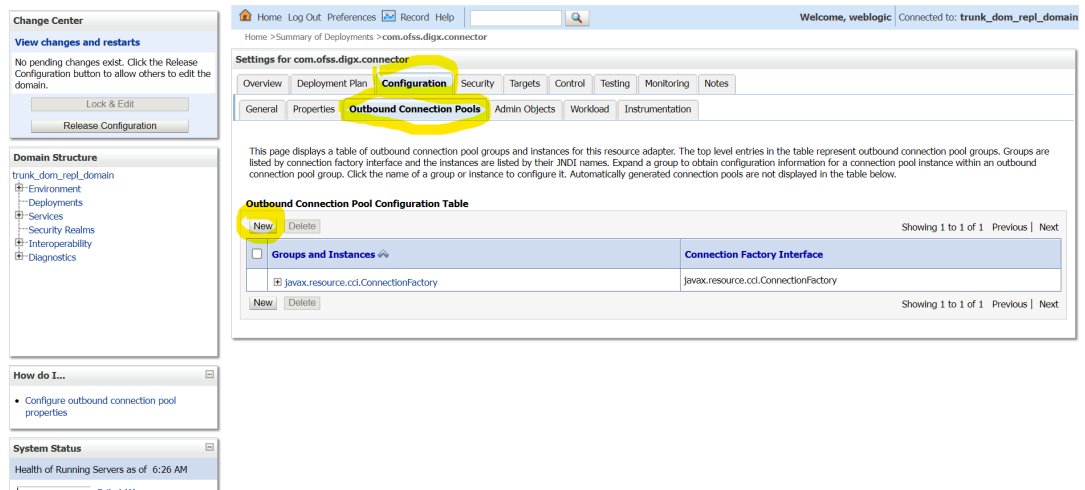
1. Login to WebLogic console with admin login and navigate to “Domain Structure” → “Deployments”.
2. Click on “com.ofss.digx.connector”

Figure 2-40 Deployments



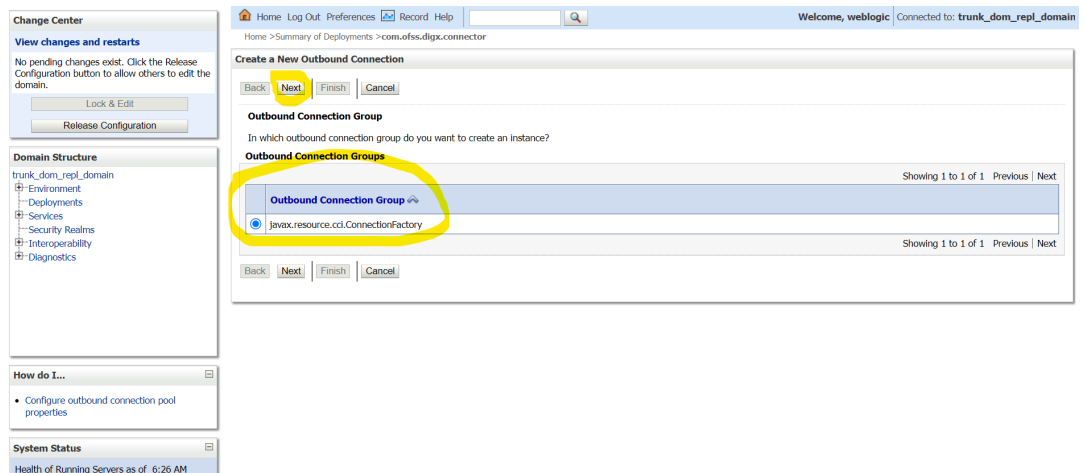
3. Navigate to “Configuration” → “Outbound Connection Pools” tab and click on **New**.

Figure 2-41 Outbound Connection Pools Configuration



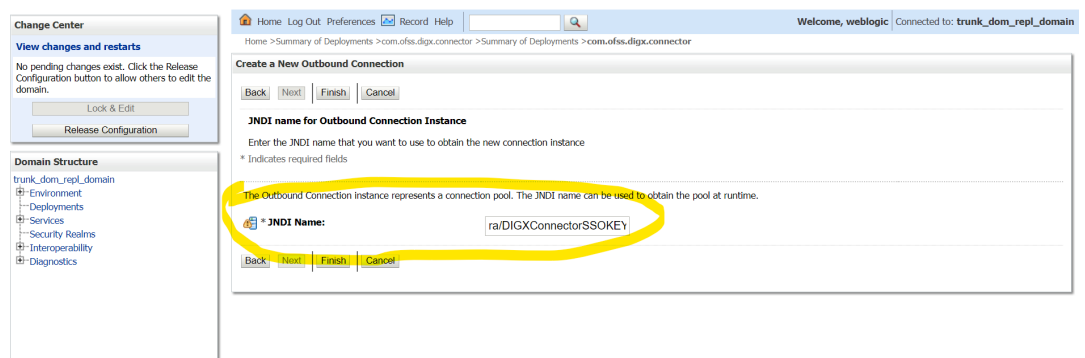
4. Select "javax.resource.cci.ConnectionFactory" and click on **Next**.

Figure 2-42 Outbound Connection Group Configuration



5. Enter JNDI name as ra/DIGXConnectorSSOKEY and click on **Finish**.

Figure 2-43 JNDI Configuration for Outbound Connection



6. Again navigate to “Domain Structure” → “Deployments”.
7. Click on “com.ofss.digx.connector”.

Figure 2-44 Deployments

The screenshot shows the WebLogic Administration Console's 'Deployments' page. On the left, the 'Domain Structure' tree has 'Deployments' selected. The main content area displays a table of installed applications. The application 'com.ofss.digx.connector' is highlighted with a yellow circle. Below the table, there are 'New' and 'Delete' buttons.

Name	State	Health	Type	Targets	Deployment Order
com.ofss.digx.connector	Active	OK	Resource Adapter	obdx_server1	0
digx-admin	Active	OK	Web Application	obdx_cluster	100
digx-auth	Active	OK	Web Application	obdx_cluster	100
digx-cms	Active	OK	Web Application	obdx_server1	100
digx-coherence	Active	OK	Web Application	obdx_cluster	0
digx-common	Active	OK	Web Application	obdx_server1	100
digx-corporateloan	Active	OK	Web Application	obdx_server1	100
digx-creditfacility	Active	OK	Web Application	obdx_server1	100
digx-edx	Active	OK	Web Application	obdx_server1	100
digx-eurekaserver	Active	OK	Web Application	obdx_server1	100

8. Navigate to “Security” → “Outbound Credentials Mapping” tab and click on **New**.

Figure 2-45 Outbound Credentials Mappings

The screenshot shows the WebLogic Administration Console's 'Outbound Credentials Mappings' page. On the left, the 'Domain Structure' tree has 'Security' selected. The main content area displays the 'Outbound Credentials Mappings' tab. The 'New' button is highlighted with a yellow circle. Below the table, there are 'New' and 'Delete' buttons.

WLS User	EIS User	Outbound Connection Pool
There are no items to display		

9. Select “ra/DIGXConnectorSSOKEY” by navigating using next button. Once selected as shown in below screenshot, click on **Next**.

Figure 2-46 Create New Security Credentials Mappings

The screenshot shows the 'Create a New Security Credential Mapping' wizard in the Oracle WebLogic console. The left sidebar contains the 'Change Center' and 'Domain Structure' panels. The main area displays the 'Outbound Connection Pool' step, which includes a message: '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.' Below this is a table titled 'Customize this table' with the heading 'Create a New Security Credential Map Entry for:'. The table lists several outbound connection pools, with 'ra/DIGXConnectorSSOKEY' selected and highlighted by a yellow circle. The 'Next' button at the bottom of the wizard is also highlighted with a yellow circle.

10. Select "Default User" and click on Next.

Figure 2-47 Create New Security Credentials Mappings

The screenshot shows the 'Create a New Security Credential Mapping' wizard in the Oracle WebLogic console, specifically the 'WebLogic Server User' step. The left sidebar is the same as in Figure 2-46. The main area displays instructions for selecting a WebLogic Server user. There are three radio button options: 'User for creating initial connections', 'Default User' (which is selected and highlighted with a yellow circle), and 'Unauthenticated WLS User'. Below these options is a text field for 'WebLogic Server User Name:'. The 'Next' button at the bottom of the wizard is also highlighted with a yellow circle.

11. Provide the below mentioned field values as given below.
 - a. EIS User Name: - Client ID save in txt file generated from IDCS in section 3.5, step 6.
 - b. EIS Password: - Client Secret save in txt file generated from IDCS in section 3.5, step 6.
 - c. EIS User Name: - Client Secret save in txt file generated from IDCS section 3.5, step 6.

Figure 2-48 Configure EIS UIS Username / Password

The screenshot shows the Oracle WebLogic Server Administration Console interface. On the left, there's a sidebar with 'Change Center' and 'Domain Structure'. The main area displays the 'Create a New Security Credential Mapping' wizard. The current step is 'EIS User Name and Password', which is highlighted with a yellow circle. The wizard prompts the user to 'Configure the EIS User Name and Password that you would like to map the WebLogic Server User to:'. It includes three input fields: 'EIS User Name' (containing 'XXXXXXXXXXXXXXXXXX'), 'EIS Password' (masked with dots), and 'Confirm Password' (masked with dots). Navigation buttons 'Back', 'Next', 'Finish', and 'Cancel' are at the bottom of the wizard.

12. Click on **Finish** to save the configuration.

2.8 OBAPI configuration for OAuth

To enable IDCS out of the box support for OAuth follow below mentioned steps.

```
update DIGX_FW_CONFIG_ALL_B set prop_value = <SSO_PROVIDER_URL> where prop_id = 'SSO_PROVIDER_URL';
```

1. Replace <SSO_PROVIDER_URL> with respective SSO provider URL.
2. Restart all the managed servers.

For configuring any other service provider, a custom class needs to be written which implements `com.ofss.digx.app.sms.service.user.external.IExternalUser` interface.

The entry for the new custom class has to be made in database using the below script -

```
update DIGX_FW_CONFIG_ALL_B set prop_value = <SSO_PROVIDER_CLASS> where prop_id = 'SSO_PROVIDER_CLASS';
```

3. Replace <SSO_PROVIDER_CLASS> with the fully qualified name of the new custom class.
4. Also below queries need to be executed as well if there are any changes in the configuration-

```
update DIGX_FW_CONFIG_ALL_B set prop_value = <SSO_PROVIDER_TOKEN_SCOPE> where prop_id = 'SSO_PROVIDER_TOKEN_SCOPE';
update DIGX_FW_CONFIG_ALL_B set prop_value = <SSO_PROVIDER_TOKEN_URI> where prop_id = 'SSO_PROVIDER_TOKEN_URI';
update DIGX_FW_CONFIG_ALL_B set prop_value = <SSO_PROVIDER_URL> where prop_id = 'SSO_PROVIDER_URL';
update DIGX_FW_CONFIG_ALL_B set prop_value = <SSO_PROVIDER_USER_READ_URI> where prop_id = 'SSO_PROVIDER_USER_READ_URI';
```

5. Restart all the servers in domain.

2.9 Default Admin Configuration

OBAPI installer comes pre-shipped admin user with name “superadmin”,so in order to login into the OBAPI application for completing Day 1 maintenances the same user need to be created in SSO Provider with same name post SSO integration.

2.10 Logout Configurations

Below query needs to be executed as part of the logout configurations.

```
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  
( 'SSO_LOGOUT_URL' , 'dayoneconfig' , '<LOGOUT_URL>' , 'Y' , null , 'SSO logout Url' ,  
'ofssuser' , sysdate , 'ofssuser' , sysdate , 'A' , 1 , 'N' , null );
```

Replace <LOGOUT_URL> with respective url.

Index

C

Configuration, [1](#)

D

Database Configuration, [14](#)

Default Admin Configuration, [26](#)

I

IDCS OAuth Integration, [15](#)

Identity Provider Configuration at IDCS, [1](#)

L

Logout Configurations, [26](#)

O

OBAPI configuration for OAuth, [25](#)

OHS Configuration, [13](#)

S

SAML Authentication Provider configuration, [5](#)

SQL Authentication Provider configuration, [9](#)

W

WebLogic configuration for OAuth, [21](#)