

Single Sign-on Configuration Guide -SAML  
Oracle Banking Digital Experience  
Patchset Release 22.2.5.0.0

Part No. F72987-01

October 2024

Single Sign-on Configuration Guide -SAML

October 2024

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/](http://www.oracle.com/financialservices/)

Copyright © 2006, 2024, 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

<b>1. Preface .....</b>	<b>1-1</b>
1.1 Purpose .....	1-1
1.2 Audience .....	1-1
1.3 Documentation Accessibility .....	1-1
1.4 Critical Patches .....	1-1
1.5 Diversity and Inclusion .....	1-1
1.6 Conventions .....	1-1
1.7 Screenshot Disclaimer .....	1-2
1.8 Acronyms and Abbreviations .....	1-2
<b>2. Introduction .....</b>	<b>2-1</b>
<b>3. Configuration .....</b>	<b>3-1</b>
3.1 Identity Provider Configuration at IDCS .....	3-1
3.2 SAML Authentication Provider configuration. ....	3-6
3.3 SQL Authentication Provider configuration. ....	3-9
3.4 OHS Configuration .....	3-13
3.5 Database Configuration .....	3-15
3.6 IDCS OAuth Integration .....	3-16
3.7 WebLogic configuration for OAuth .....	3-22
3.8 OBDX configuration for OAuth .....	3-26
3.9 Default Admin Configuration .....	3-27
3.10 Logout Configurations .....	3-28

---

# 1. Preface

## 1.1 Purpose

Welcome to the User Guide for Oracle Banking Digital Experience. This guide explains the operations that the user will follow while using the application.

## 1.2 Audience

This manual is intended for Customers and Partners who setup and use Oracle Banking Digital Experience.

## 1.3 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 customers that have purchased support 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 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](#).

## 1.5 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.

## 1.6 Conventions

The following text conventions are used in this document:

Convention	Meaning
------------	---------

<b>boldface</b>	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.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

## 1.7 **Screenshot Disclaimer**

The images of screens used in this user manual are for illustrative purpose only, to provide improved understanding of the functionality; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

## 1.8 **Acronyms and Abbreviations**

The list of the acronyms and abbreviations that you are likely to find in the manual are as follows:

<b>Abbreviation</b>	<b>Description</b>
<b>OBDX</b>	Oracle Banking Digital Experience

---

## 2. 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.

## 3. Configuration

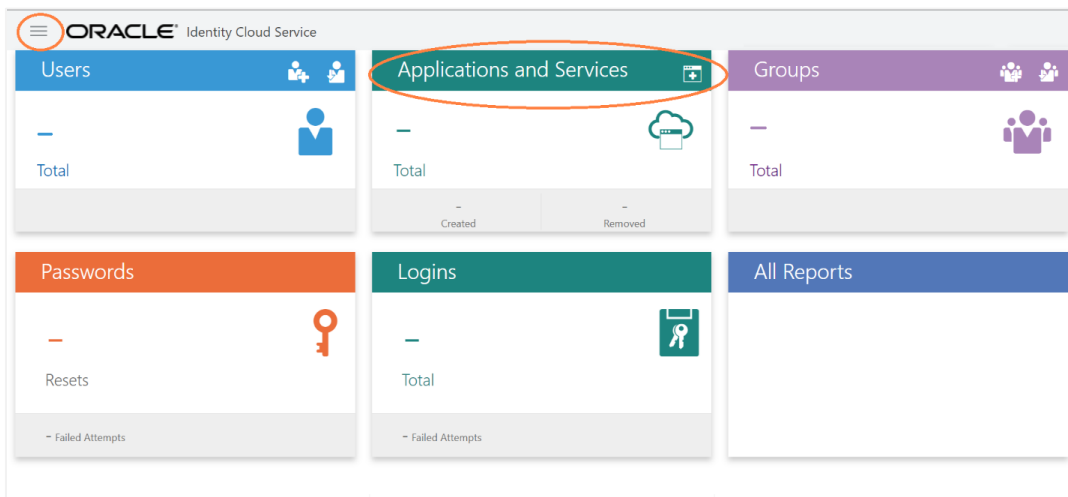
To enable SAML authentication it involves configuration at WebLogic server (console) and IDCS console.

### 3.1 Identity Provider Configuration at IDCS

Steps to configure Identity Provide at IDCS

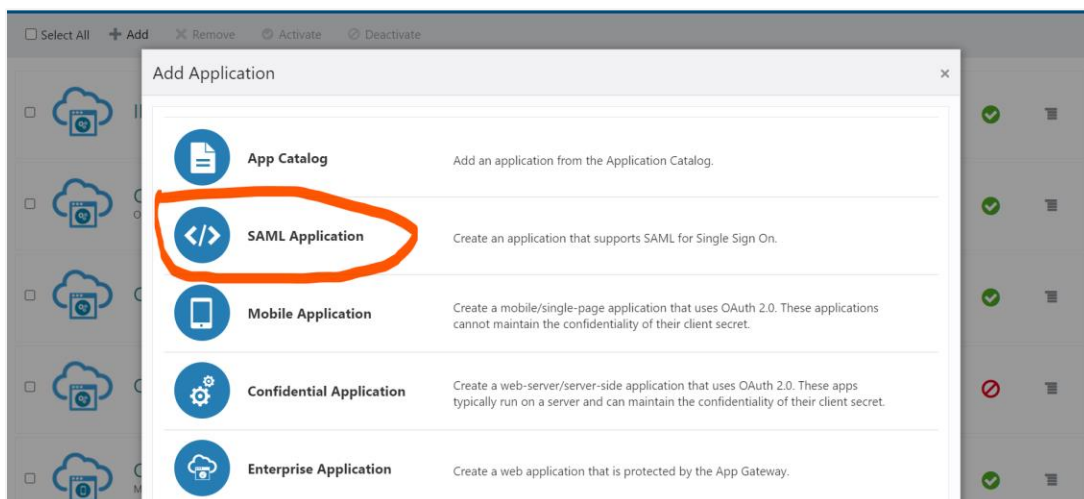
1. Login to Oracle Identity Cloud Service (IDCS) console with admin login. In dashboard click on **Add Application** in Application and Services widget or navigate through the breadcrumb menu as highlighted in screenshot.

#### Dashboard



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

#### Add Application



3. In **Add SAML Application** page provide below mentioned fields and click on **Next**.
  - i. Name
  - ii. Description

### Add SAML Application

**Add SAML Application**


Cancel 1 2 Next >

Details SSO Configuration

**App Details**

\* Name OBDX\_SAML\_CONFIG

Description SAML Configuration for OBDX user authentication.

Application Icon 

Upload

Application URL / Relay State

Add Remove

4. Fill below mentioned fields as per section.
  - i. General
    - a. Entity Id: - A unique identifier / name for the service provider.
    - b. Assertion Consumer URL: - End point to which assertion will be sent by IDCS.  
Recommended URL format [<OHS\\_URL>/saml2/sp/acs/post](#)  
e.g. [<PROTOCOL>://<OHS\\_HOST>:<OHS\\_PORT>/saml2/sp/acs/post](#)  
[http://whf000xxx.bank.com:9999/saml2/sp/acs/post](#)
    - c. NameID Format: - Select value as “Unspecified”.
    - d. NameID Value:- Select value as “User Name”.

### Add SAML Application

**Add SAML Application**

< Back ✓ 2 Finish

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

## ii. Advance Settings

- a. Signed SSO :- Select value as "Assertion"
- b. Enable Single Logout: - This field should be checked.
- c. Logout Binding: - Select value as "Redirect".
- d. 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)  
<http://whf000xxx.bank.com:9999/digx-infra/sso-logout>
- e. 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)  
<http://whf000xxx.bank.com:9999/digx-infra/sso-logout>

## Add SAML Application

### Advanced Settings


This section contains additional configuration options.

Signed SSO	Assertion
Include Signing Certificate in Signature	<input type="checkbox"/>
Signature Hashing Algorithm	SHA-256
Enable Single Logout	<input checked="" type="checkbox"/>
* Logout Binding	Redirect
* Single Logout URL	http://example.com:9999/digx-infra/ssc
* Logout Response URL	http://example.com:9999
Encrypt Assertion	<input type="checkbox"/>

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

## Edit Application

Applications > OBDX\_SAML\_CONFIG

 **OBDX\_SAML\_CONFIG**  
SAML Configuration for OBDX user authentication.

Activate Remove


Details SSO Configuration Users Groups

App Details

Application Type: SAML Application

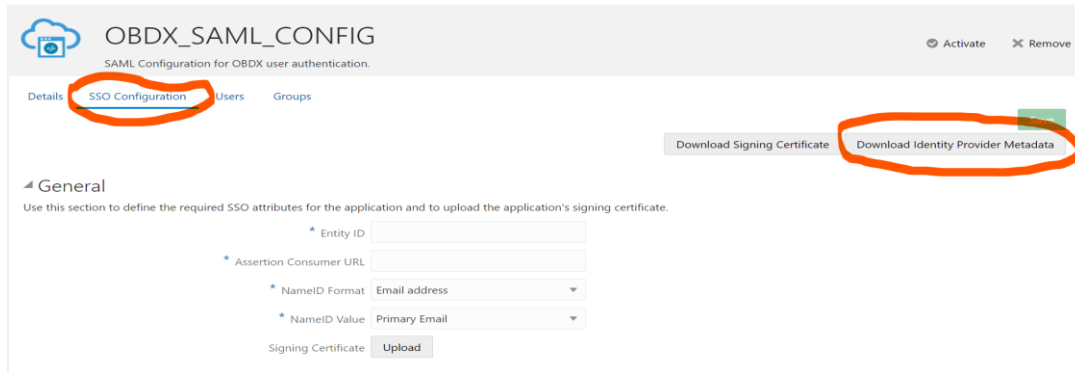
\* Name: OBDX\_SAML\_CONFIG

Description: SAML Configuration for OBDX user authentication.

Application Icon: 

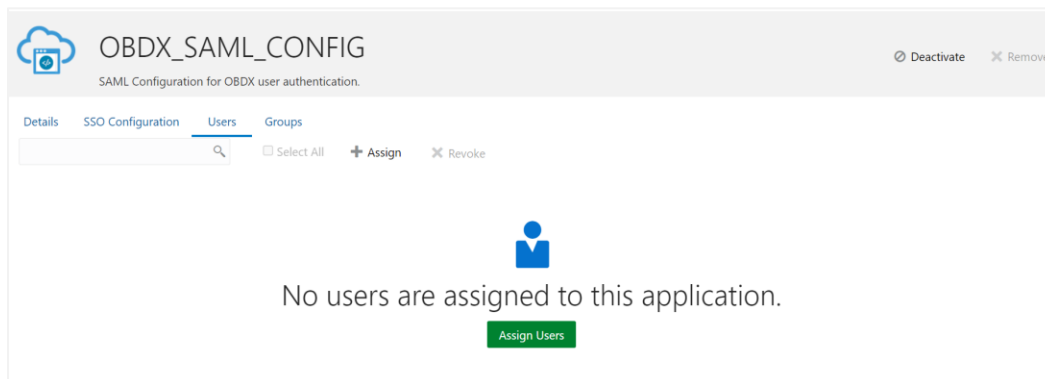
7. Navigate to Dashboard and search the application you have created.
8. Navigate to **SSO Configuration** tab and click on “**Download Identity Provider Metadata**”. Keep the downloaded xml file, it will be required to upload in WebLogic console. Same is explain in WebLogic console configuration steps.

### 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.

### Edit Application



### Assign Users

Assign Users

Please select up to 40 users to assign.

☐ Select All

superadmin

Selected: 1

Clear Selection

	First Name	Last Name	Email
<input type="checkbox"/>	Super	Admin	
<input checked="" type="checkbox"/>	superadmin	superadmin	

Page 1 of 1 (1-2 of 2 items)

<

1

>

OK

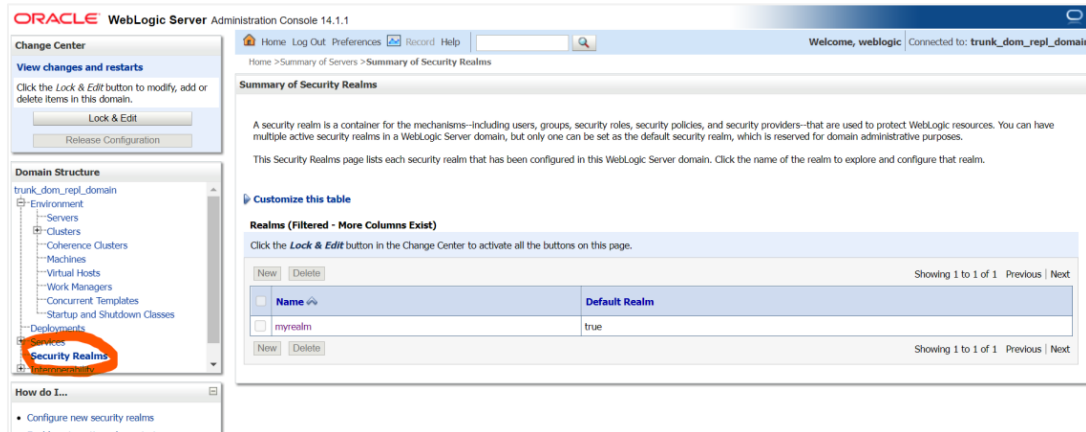
12. Logout from IDCS console.

## 3.2 SAML Authentication Provider configuration.

Steps to configure SAML Authentication Providers changes into WebLogic console.

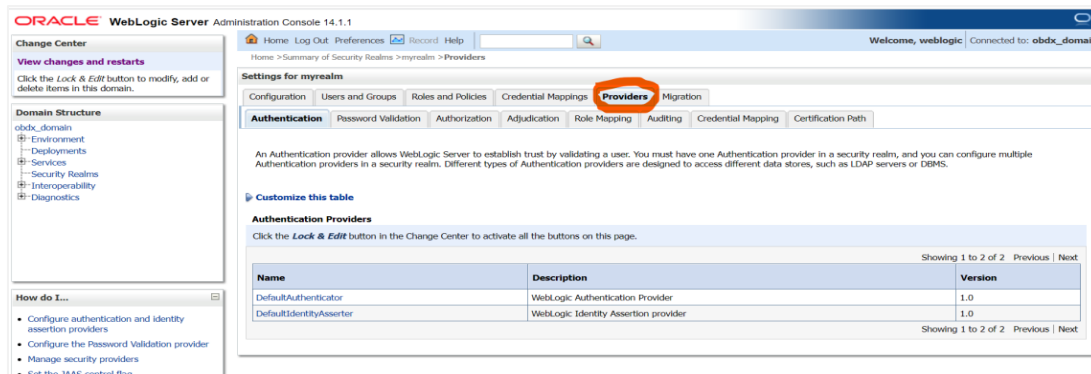
1. Login to WebLogic console with admin login and navigate to “Security Realms”.

### Security Realms



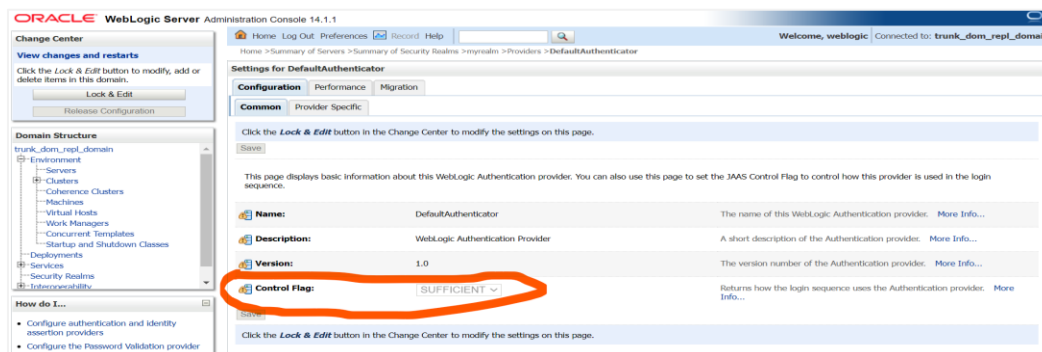
2. → Click on **myrealm** or your realm name present in screen. Navigate to “Providers” tab.

### Providers



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

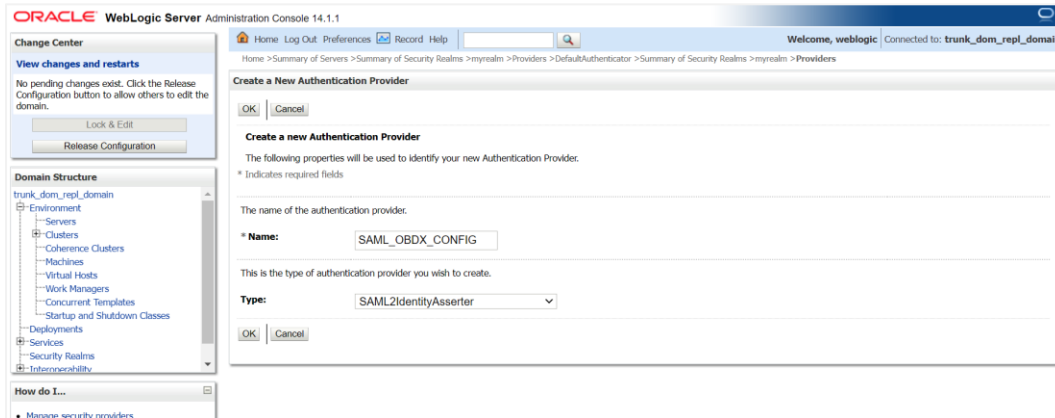
### Default Authenticator



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**.

- i. Name: - Name of authentication provider.
- ii. Type :- Select value as “SAML2IdentityAsserter”.

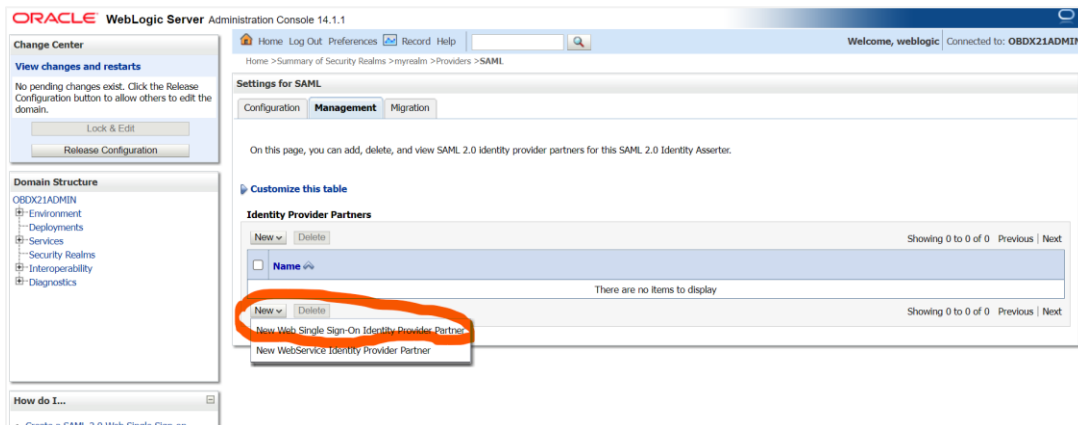
## Create Authentication Provider



The screenshot shows the Oracle WebLogic Server Administration Console. On the left, the 'Domain Structure' tree is visible, with 'Security Realms' expanded. The main area displays the 'Create a New Authentication Provider' dialog. The 'Name' field is set to 'SAML\_OBDX\_CONFIG' and the 'Type' dropdown is set to 'SAML2IdentityAsserter'. The 'OK' button is highlighted.

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**”

## Management



The screenshot shows the 'Settings for SAML' page in the Oracle WebLogic Server Administration Console. The 'Management' tab is selected. The page contains a table for 'Identity Provider Partners' with a 'New' button circled in red. The table is currently empty, showing 'Showing 0 to 0 of 0' items.

8. Provide the name for the identity partner and select the IDC metadata xml copied to WebLogic server. Click **OK** button to save.

## Create a SAML 2.0 Web Single Sign-on Identity Provider Partner

Use this page to:

- Enter the name of your new Single Sign-on Identity Provider partner
- Specify the name and location of the SAML 2.0 metadata file that you received from this new partner

\* Indicates required fields

Please specify the name of the partner:

\* **Name:**

Please specify the name of the file containing the partner metadata document.

**Path:**

**Recently Used Paths:**

**Current Location:**

bin  
common  
config  
init-info  
jms  
logs  
orchestration  
original  
servers  
IDCSMetadata.xml

OK Cancel

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

## Settings for Create a SAML 2.0 Web Single Sign-on Identity Provider Partner

The parameters that can be set on this Administration Console page can also be accessed programmatically via the Java interfaces that are identified in this help topic. For API information about those interfaces, see Related Topics.

— Overview —

**Name:** IDCS\_IT The name of this Identity Provider partner. [More Info...](#)

☒ **Enabled** Specifies whether interactions with this Identity Provider partner are enabled on this server. [More Info...](#)

**Description:**  A short description of this Identity Provider partner. [More Info...](#)

— Authentication Requests —

**Identity Provider Name Mapper Class Name:**  The Java class that overrides the default username mapper class with which the SAML 2.0 Identity Asserter provider is configured in this security realm. [More Info...](#)

**Issuer URI:**  The Issuer URI of this Identity Provider partner. [More Info...](#)

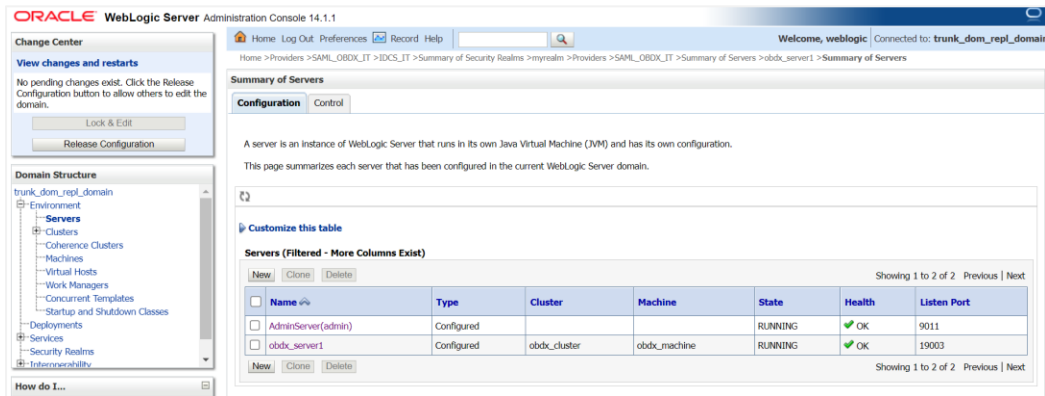
☒ **Virtual User** Specifies whether user information contained in assertions received from this Identity Provider partner are mapped to virtual users in this security realm. [More Info...](#)

**Redirect URIs:**  An optional set of URIs from which unauthenticated users will be redirected to the Identity Provider partner. [More Info...](#)

☒ **Process Attributes** Specifies whether the SAML 2.0 Identity Asserter provider consumes attribute statements contained in assertions received from this Identity Provider partner. [More Info...](#)

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

## Servers



11. Navigate to “Federation Services” → “SAML 2.0 General” and provide values to below mentioned fields. Click on **Save**.

- Published Site URL: - Recommended URL format <http://whf000xxx.bank.com:9999/saml2>  
e.g. <http://100.76.153.182:19003/saml2>
- Entity Id: - Value should match with [Entity Id](#) provided in SAML configuration in IDCS console.
- Recipient Check Enabled: - unchecked.

### SAML 2.0 General

Published Site URL:  The published site URL. [More Info...](#)

Entity ID:  The string that uniquely identifies the local site. [More Info...](#)

**Bindings**

☐ Recipient Check Enabled

Specifies whether the recipient/destination check is enabled. When true, the recipient of the SAML Request/Response must match the URL in the HTTP Request. [More Info...](#)

12. Navigate to “Federation Services” → “SAML 2.0 Service Provider” and provide values to below mentioned fields and click on **Save**.

- Enabled: - Check box should be checked.
- Preferred Binding: - Post
- Default URL: - <http://100.76.153.182:19003/digx-infra/admin-dashboard>

## 3.3 SQL Authentication Provider configuration.

Steps to configure SQL Authentication Providers changes into WebLogic console.

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

## Security Realms

**Oracle WebLogic Server Administration Console 14.1.1**

Home > Summary of Servers > Summary of Security Realms

**Summary of Security Realms**

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple active security realms in a WebLogic Server domain, but only one can be set as the default security realm, which is reserved for domain administrative purposes.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

**Customize this table**

**Realms (Filtered - More Columns Exist)**

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

Name	Default Realm
myrealm	true

Showing 1 to 1 of 1 Previous | Next

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

## Providers

**Oracle WebLogic Server Administration Console 14.1.1**

Home > Summary of Security Realms > myrealm > Providers

**Settings for myrealm**

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**

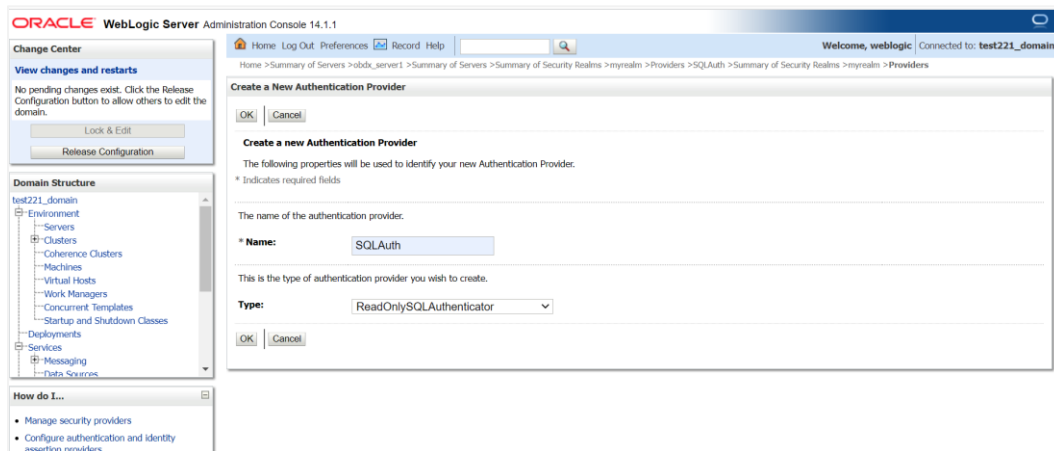
Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

Name	Description	Version
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

Showing 1 to 2 of 2 Previous | Next

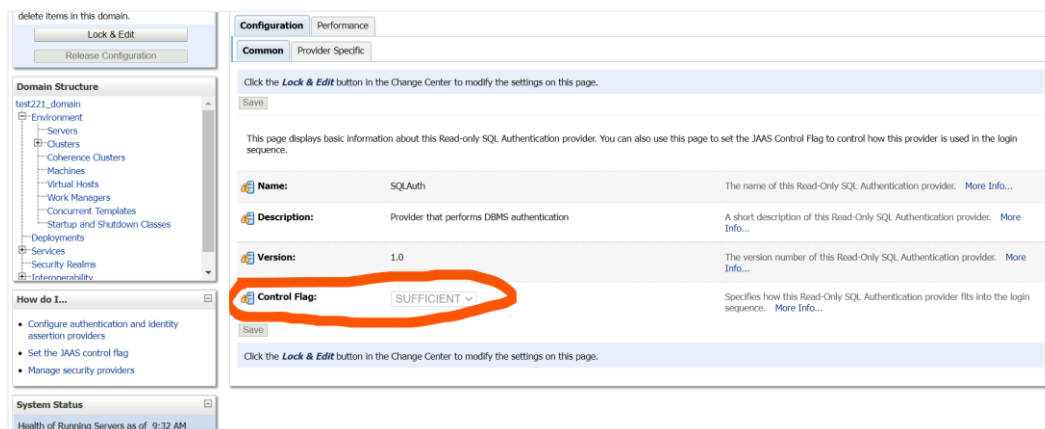
3. Click on **New** button to create new Authentication Provider. Fill the below mentioned fields with appropriate values and click on **OK**.
  - i. Name: - Name of authentication provider.
  - ii. Type :- Select value as “ReadOnlySQLAuthenticator”.

## Create New Authentication Provider



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

## 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.
  - i. Data Source Name: - NONXA
  - ii. SQL Get Users Password: - SELECT U\_PASSWORD FROM USERS WHERE U\_NAME = ?
  - iii. SQL User Exists: - SELECT U\_NAME FROM USERS WHERE U\_NAME = ?
  - iv. SQL List Users: - SELECT U\_NAME FROM USERS WHERE U\_NAME LIKE ?
  - v. SQL List Groups: - SELECT G\_NAME FROM GROUPS WHERE G\_NAME LIKE ?
  - vi. VI. SQL Group Exists: - SELECT G\_NAME FROM GROUPS WHERE G\_NAME = ?
  - vii. SQL Is Member: - SELECT G\_MEMBER FROM GROUPMEMBERS WHERE G\_NAME = ? AND G\_MEMBER = ?

- viii. SQL List Member Groups: - SELECT G\_NAME FROM GROUPMEMBERS WHERE G\_MEMBER = ?
- ix. SQL Get User Description: - SELECT U\_DESCRIPTION FROM USERS WHERE U\_NAME = ?
- x. SQL Get Group Description: - SELECT G\_DESCRIPTION FROM GROUPS WHERE G\_NAME = ?

## Settings for Read Only SQL Authentication Provider

**Data Source Name:** NONXA

**Group Membership Searching:** unlimited

**Max Group Membership Search Level:** 0

**SQL Get Users Password:** SELECT U\_PASSWORD FROM

**SQL User Exists:** SELECT U\_NAME FROM

**SQL List Users:** SELECT U\_NAME FROM

**SQL List Groups:** SELECT G\_NAME FROM

**SQL Group Exists:** SELECT G\_NAME FROM

**SQL Is Member:** SELECT G\_MEMBER FROM

**SQL List Member Groups:** SELECT G\_NAME FROM

**Descriptions Supported:** ☐ Indicates whether user and group descriptions are supported by the database used by the authentication provider.

**SQL Get User Description:** SELECT U\_DESCRIPTION

**SQL Get Group Description:** SELECT G\_DESCRIPTION

**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.

## Authentication

**Providers**

Name	Type	Status
Authentication Provider	Authentication	OK

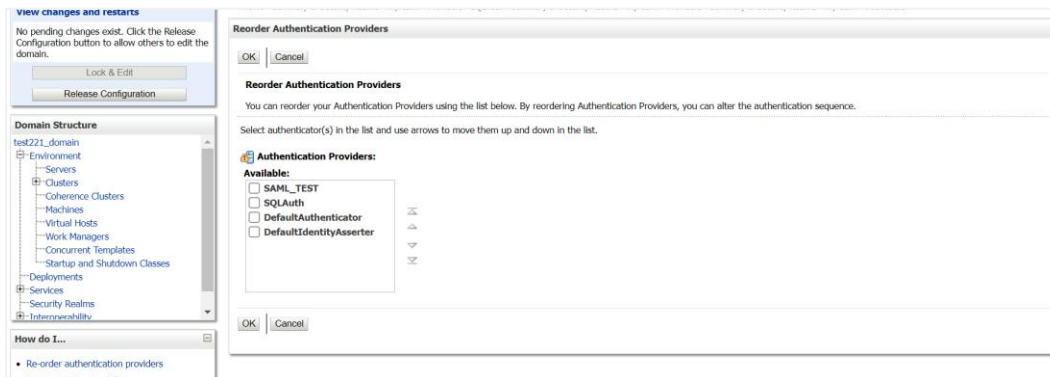
**Authentication Provider**

**Authentication**

**Providers**

9. Reorder the authentication providers as given below.
  - i. SAML Authentication Provider
  - ii. SQL Authentication Provider
  - iii. Default Authenticator

### 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

## 3.4 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 Hosts

Listen <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.

## 3.5 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);
```

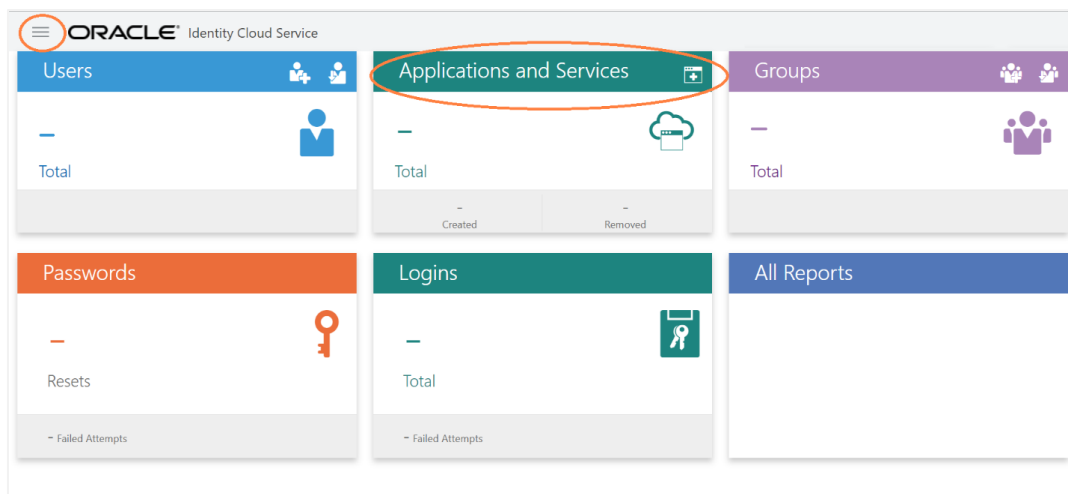
For Example: - INSERT INTO DIGX\_FW\_CONFIG\_ALL\_B (PROP\_ID, CATEGORY\_ID, PROP\_VALUE, FACTORY\_SHIPPED\_FLAG, PROP\_COMMENTS, SUMMARY\_TEXT, CREATED\_BY, CREATION\_DATE, LAST\_UPDATED\_BY, LAST\_UPDATED\_DATE, OBJECT\_STATUS, OBJECT\_VERSION\_NUMBER, EDITABLE, CATEGORY\_DESCRIPTION) values ('SSO\_PUBLIC\_URL', '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);

## 3.6 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.

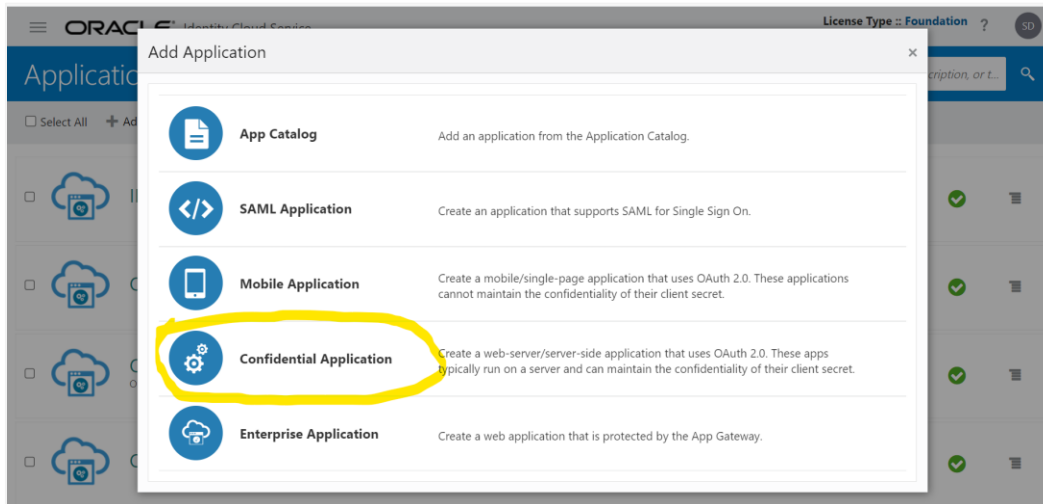
1. Login to Oracle Identity Cloud Service (IDCS) console with admin login. In dashboard click on Add Application in Application and Services widget or navigate through the breadcrumb menu as highlighted in screenshot.

### Dashboard



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

### Add Application



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

### Add Confidential Application

The screenshot shows the 'Add Confidential Application' page in the Oracle Identity Cloud Service interface. The page has a progress bar at the top with five steps: 'Details' (active), 'Client', 'Resources', 'Web Tier Policy', and 'Authorization'. Below the progress bar, there is a section titled 'App Details'. It contains three fields: 'Name' (OBDX\_OAUTH\_CONFIG), 'Description' (OAuth Configuration for fetching user details from IDCS), and 'Application Icon' (a cloud icon). An 'Upload' button is located below the icon field.

4. Select Configure this application as a client now option in screen as shown in below screenshot.

## Add Confidential Application

**Add Confidential Application**

Navigation: Details (1) → **Client (2)** → Resources (3) → Web Tier Policy (4) → Authorization (5)

Options: ☒ 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

5. Fill below mentioned fields as per section.

i. Authorization

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

## Add Confidential Application

**Add Confidential Application**

Navigation: Details (1) → **Client (2)** → Resources (3) → Web Tier Policy (4) → Authorization (5)

Options: ☒ 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

Allowed Operations: ☐ Introspect ☐ On behalf Of

ID Token Encryption Algorithm:

ii. Token Issuance Policy

a. Authorized Resources :- Select value as “Specific”

b. Grant the client access to Identity Cloud Service Admin APIs: - Click on **Add** button

## 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.	

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

## 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

+ Add

App Roles

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 >

Add

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

## 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	Scope
Identity Domain Administrator	No	x

e. Click on **Next** button on top.

iii. Expose APIs to Other Applications: - Select “**Skip for later**” and click on **Next**.

## 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

iv. Web Tier Policy: - Select “Skip for later” and click on Next button.

## Add Confidential Application

Add Confidential Application

< Back

Details Client Resources Web Tier Policy Authorization

Next >

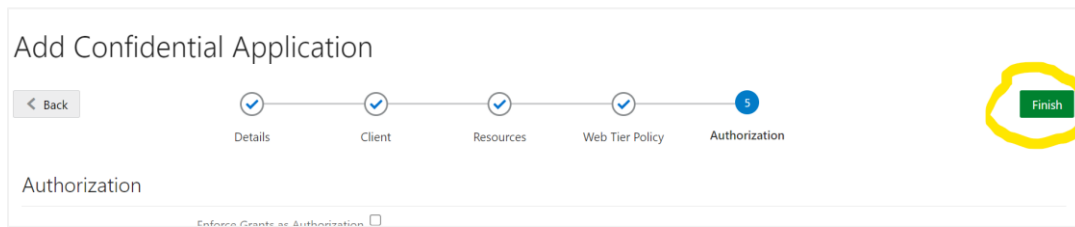
Web Tier Policy

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

v. Click on “Finish”

## Add Confidential Application



Add Confidential Application

< Back

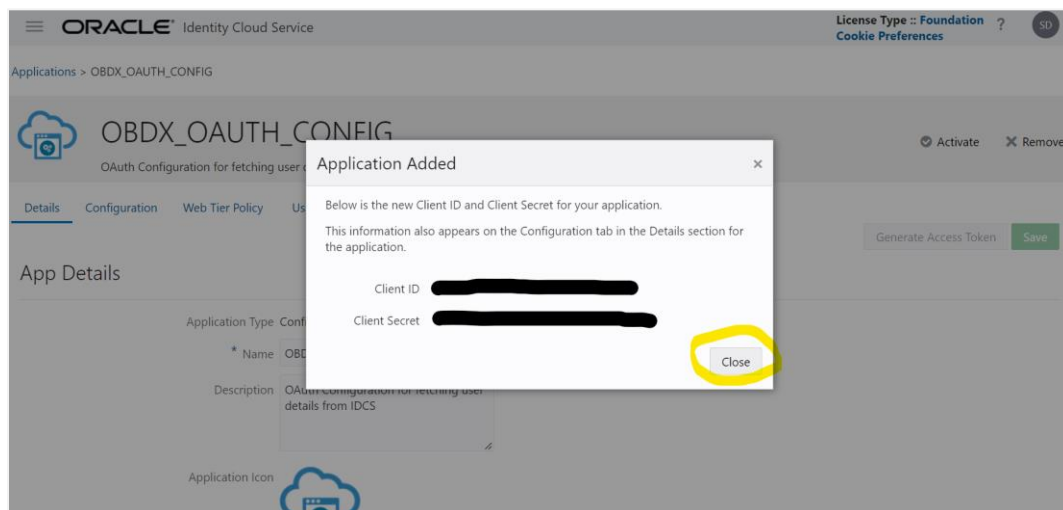
Details Client Resources Web Tier Policy Authorization 5

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”.

## Add Confidential Application



ORACLE Identity Cloud Service

License Type :: Foundation ?

Cookie Preferences

Applications > OBDX\_OAUTH\_CONFIG

OBDX\_OAUTH\_CONFIG

OAuth Configuration for fetching user details from IDCS

Activate Remove

Generate Access Token Save

App Details

Application Type Confidential Application

\* Name OBDX\_OAUTH\_CONFIG

Description OAuth Configuration for fetching user details from IDCS

Application Icon

Application Added

Below is the new Client ID and Client Secret for your application.  
This information also appears on the Configuration tab in the Details section for the application.

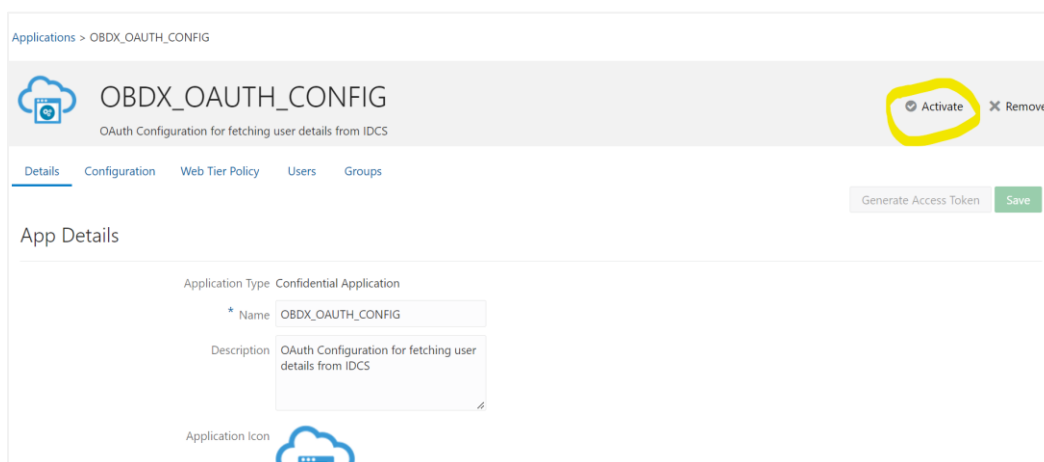
Client ID [Redacted]

Client Secret [Redacted]

Close

7. Click on “Activate” button to activate the application.

## Edit Application



Applications > OBDX\_OAUTH\_CONFIG

OBDX\_OAUTH\_CONFIG

OAuth Configuration for fetching user details from IDCS

Activate Remove

Generate Access Token Save

App Details

Application Type Confidential Application

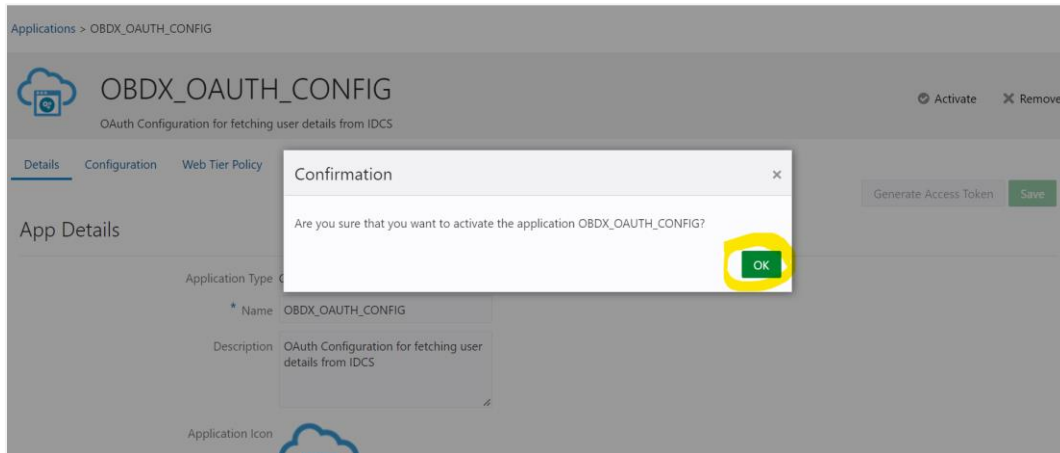
\* Name OBDX\_OAUTH\_CONFIG

Description OAuth Configuration for fetching user details from IDCS

Application Icon

8. Popup window asking confirmation to activate the application will open, click on “Ok” to activate the application.

## Edit Application



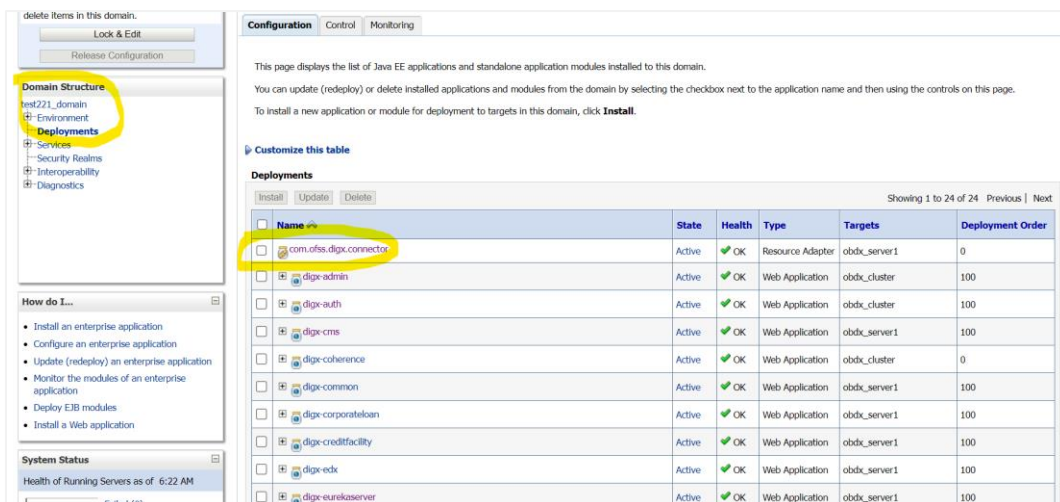
9. Logout from IDCS console.

## 3.7 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”

## Deployments



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

## Outbound Connection Pools Configuration

The screenshot shows the Oracle WebLogic Console interface. On the left is the 'Change Center' sidebar with sections for 'View changes and restarts', 'Domain Structure', 'How do I...', and 'System Status'. The main content area is titled 'Settings for com.oracle.digx.connector'. The 'Configuration' tab is selected, and the 'Outbound Connection Pools' sub-tab is highlighted. Below the tabs is a table titled 'Outbound Connection Pool Configuration Table'. The table has two columns: 'Groups and Instances' and 'Connection Factory Interface'. The entry 'javax.resource.cci.ConnectionFactory' is selected, and the 'Next' button is highlighted.

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

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

## Outbound Connection Groups Configuration

The screenshot shows the Oracle WebLogic Console interface. On the left is the 'Change Center' sidebar. The main content area is titled 'Create a New Outbound Connection'. The 'Next' button is highlighted. Below the buttons is a section titled 'Outbound Connection Groups'. It contains a table with one entry: 'javax.resource.cci.ConnectionFactory'. The 'Next' button is highlighted.

Outbound Connection Group
javax.resource.cci.ConnectionFactory

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

## JNDI Configuration for Outbound Connection

Change Center

View changes and restarts

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Lock & Edit

Release Configuration

Domain Structure

trunk\_dom\_rep1\_domain

- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: trunk\_dom\_rep1\_domain

Create a New Outbound Connection

Back Next Finish Cancel

JNDI name for Outbound Connection Instance

Enter the JNDI name that you want to use to obtain the new connection instance

\* Indicates required fields

The Outbound Connection instance represents a connection pool. The JNDI name can be used to obtain the pool at runtime.

\* JNDI Name: ra/DIGXConnectorSSOKEY

Back Next Finish Cancel

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

## Deployments

delete items in this domain.

Lock & Edit

Release Configuration

Domain Structure

trunk\_dom\_rep1\_domain

- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...?

- Install an enterprise application
- Configure an enterprise application
- Update (redeploy) an enterprise application
- Monitor the modules of an enterprise application
- Deploy EJB modules
- Install a Web application

System Status

Health of Running Servers as of 6:22 AM

Failed (0)

Configuration Control Monitoring

This page displays the list of Java EE applications and standalone application modules installed to this domain.

You can update (redeploy) or delete installed applications and modules from the domain by selecting the checkbox next to the application name and then using the controls on this page.

To install a new application or module for deployment to targets in this domain, click **Install**.

Customize this table

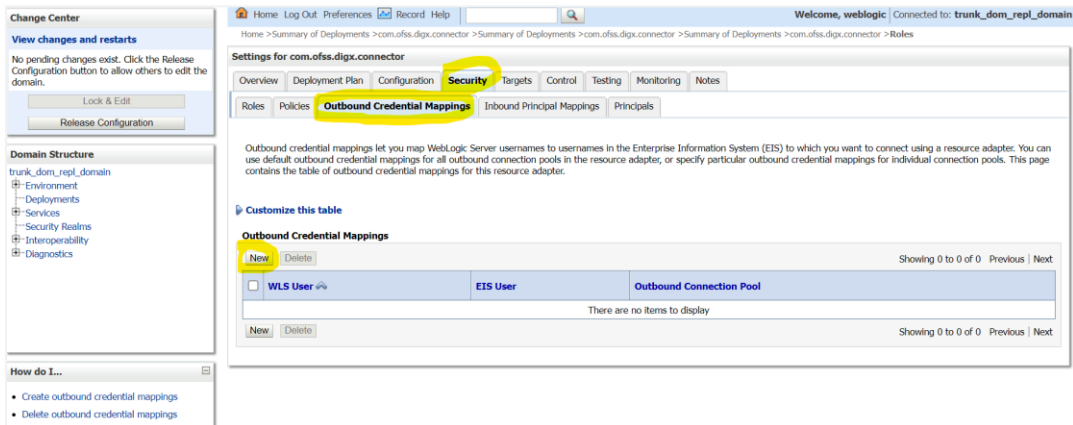
Install Update Delete

Showing 1 to 24 of 24 Previous Next

<input type="checkbox"/>	Name	State	Health	Type	Targets	Deployment Order
<input type="checkbox"/>	com.ofss.digx.connector	Active	OK	Resource Adapter	obdx_server1	0
<input type="checkbox"/>	digx-admin	Active	OK	Web Application	obdx_cluster	100
<input type="checkbox"/>	digx-auth	Active	OK	Web Application	obdx_cluster	100
<input type="checkbox"/>	digx-cms	Active	OK	Web Application	obdx_server1	100
<input type="checkbox"/>	digx-coherence	Active	OK	Web Application	obdx_cluster	0
<input type="checkbox"/>	digx-common	Active	OK	Web Application	obdx_server1	100
<input type="checkbox"/>	digx-corporateloan	Active	OK	Web Application	obdx_server1	100
<input type="checkbox"/>	digx-creditfacility	Active	OK	Web Application	obdx_server1	100
<input type="checkbox"/>	digx-edx	Active	OK	Web Application	obdx_server1	100
<input type="checkbox"/>	digx-eureka-server	Active	OK	Web Application	obdx_server1	100

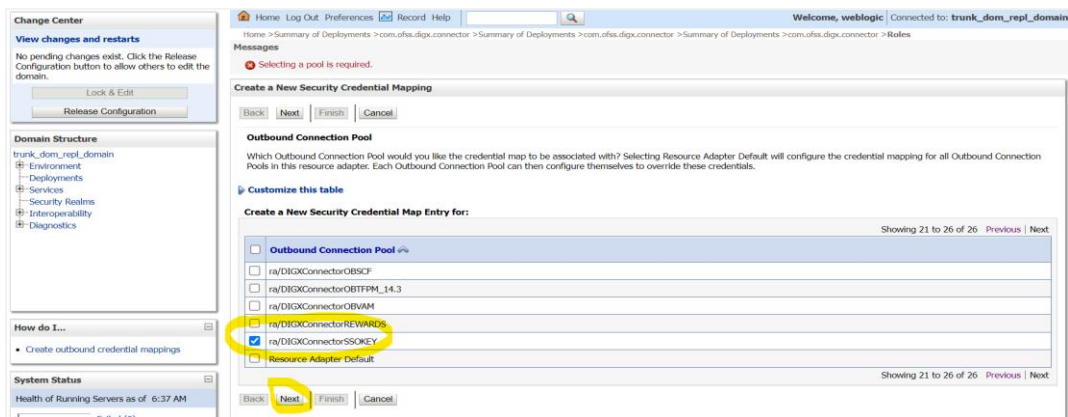
- Navigate to “Security” → “Outbound Credentials Mapping” tab and click on New.

## Outbound Credentials Mappings



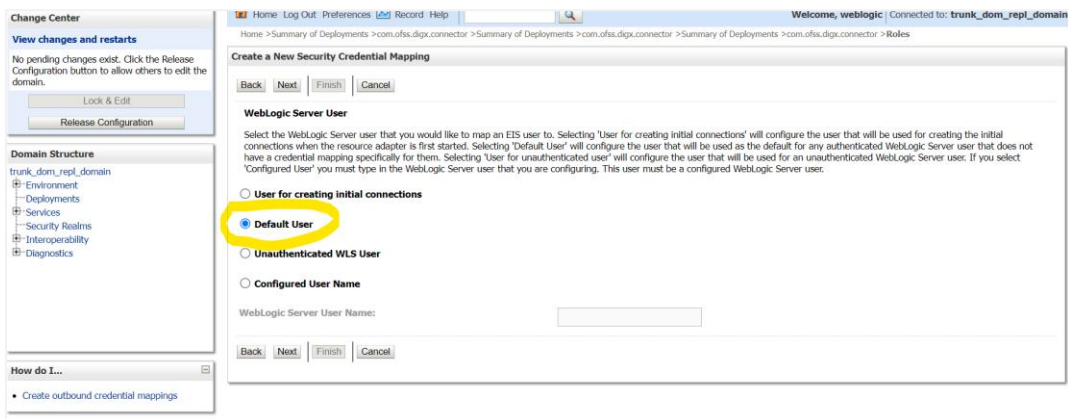
9. Select “ra/DIGXConnectorSSOKEY” by navigating using next button. Once selected as shown in below screenshot, click on Next.

## Create New Security Credentials Mappings



10. Select “Default User” and click on Next.

## Create New Security Credentials Mappings



11. Provide the below mentioned field values as given below.

- i. EIS User Name: - Client ID save in txt file generated from IDCS in section 3.5, step 6.
- ii. EIS Password: - Client Secret save in txt file generated from IDCS in section 3.5, step 6.
- iii. EIS User Name: - Client Secret save in txt file generated from IDCS section 3.5, step 6.

### Configure EIS UIS Username / Password

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main window displays the 'Create a New Security Credential Mapping' page. The page title is 'EIS User Name and Password'. Below the title, there is a section for 'Enter the EIS User Name:' with a text input field containing 'XXXXXXXXXXXXXXXXXX'. Below this, there is a section for 'Enter the EIS Password:' with a text input field containing 'XXXXXXXXXXXXXXXXXX'. Below that, there is a section for 'Confirm Password:' with a text input field containing 'XXXXXXXXXXXXXXXXXX'. The 'EIS User Name' field is highlighted with a yellow circle. The 'EIS Password' and 'Confirm Password' fields are also highlighted with a yellow circle. The page includes navigation buttons (Back, Next, Finish, Cancel) and a 'Release Configuration' button in the top left corner.

12. Click on Finish to save the configuration.

## 3.8 OBDX configuration for OAuth

To enable IDCS out of the box support for OAuth, execute the below query.

**update DIGX\_FW\_CONFIG\_ALL\_B set prop\_value = <SSO\_PROVIDER\_URL> where prop\_id = 'SSO\_PROVIDER\_URL';**

Replace <SSO\_PROVIDER\_URL> with respective SSO provider URL.

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';**

Replace <SSO\_PROVIDER\_CLASS> with the fully qualified name of the new custom class.

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';
```

Restart all the servers in domain.

### 3.9 **Default Admin Configuration**

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

### 3.10 **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,S
UMMARY_TEXT,CREATED_BY,CREATION_DATE,LAST_UPDATED_BY,LAST_UPDATED_D
ATE,OBJECT_STATUS,OBJECT_VERSION_NUMBER,EDITABLE,CATEGORY_DESCRIPTOR
N)
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.