

Oracle® Banking Digital Experience

Single Sign-on Configuration-SAML



Release 25.1.0.0.0
G38614-01
September 2025

ORACLE®

Copyright © 2015, 2025, 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
Before you Begin	i
Pre-requisites	i
Audience	i
Documentation Accessibility	ii
Critical Patches	ii
Diversity and Inclusion	ii
Related Resources	ii
Conventions	ii
Screenshot Disclaimer	iii
Acronyms and Abbreviations	iii
Post-requisites	iii

1 Introduction

2 Configuration

2.1 Identity Provider Configuration at IDCS	1
2.2 SAML Authentication Provider configuration	6
2.3 SQL Authentication Provider configuration	10
2.4 OHS Configuration	14
2.5 Database Configuration	15
2.6 IDCS OAuth Integration	16
2.7 WebLogic configuration for OAuth	22
2.8 OBDX configuration for OAuth	26
2.9 Default Admin Configuration	27
2.10 Logout Configurations	27

Index

List of Figures

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

2-37	<u>Add Confidential Application</u>	<u>21</u>
2-38	<u>Edit Application</u>	<u>22</u>
2-39	<u>Edit Application</u>	<u>22</u>
2-40	<u>Deployments</u>	<u>23</u>
2-41	<u>Outbound Connection Pools Configuration</u>	<u>23</u>
2-42	<u>Outbound Connection Group Configuration</u>	<u>24</u>
2-43	<u>JNDI Configuration for Outbound Connection</u>	<u>24</u>
2-44	<u>Deployments</u>	<u>24</u>
2-45	<u>Outbound Credentials Mappings</u>	<u>25</u>
2-46	<u>Create New Security Credentials Mappings</u>	<u>25</u>
2-47	<u>Create New Security Credentials Mappings</u>	<u>25</u>
2-48	<u>Configure EIS UIS Username / Password</u>	<u>26</u>

Preface

- [Purpose](#)
- [Before you Begin](#)
- [Pre-requisites](#)
- [Audience](#)
- [Documentation Accessibility](#)
- [Critical Patches](#)
- [Diversity and Inclusion](#)
- [Related Resources](#)
- [Conventions](#)
- [Screenshot Disclaimer](#)
- [Acronyms and Abbreviations](#)
- [Post-requisites](#)

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.

Before you Begin

Kindly refer to our **Getting Started User Guide** for common elements, including Symbols and Icons, Conventions Definitions, and so forth.

Pre-requisites

Specify **User ID** and **Password**, and login to **Home** screen.

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 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.

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.

Related Resources

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

- Oracle Banking Digital Experience Installation Manuals
- Oracle Banking Digital Experience Licensing Manuals

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.

Convention	Meaning
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

Acronyms and Abbreviations

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

Table 1 Acronyms and Abbreviations

Abbreviation	Description
OBDX	Oracle Banking Digital Experience

Post-requisites

After finishing all the requirements, please log out from the **Home** screen.

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

This topic provides information on **Configuration**.

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

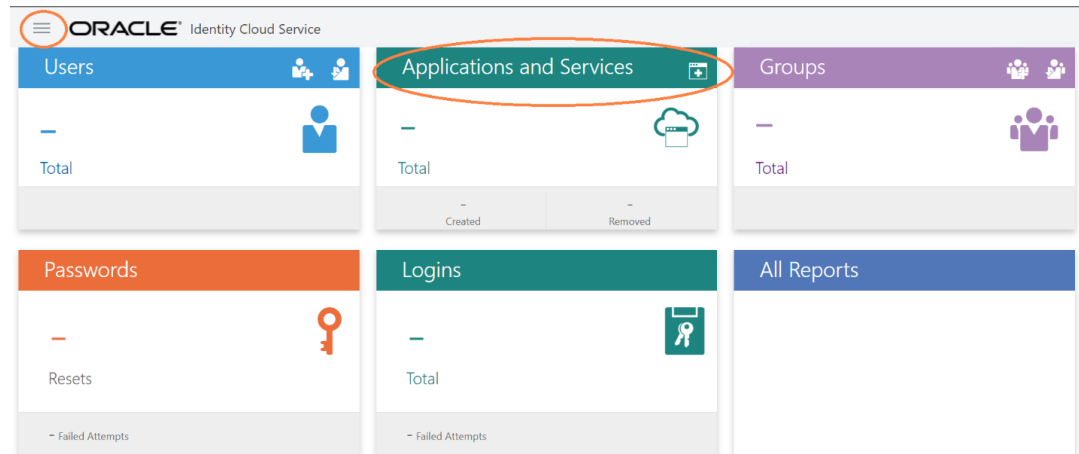
- [Identity Provider Configuration at IDCS](#)
This topic describes the systematic instruction to **Identity Provider Configuration at IDCS** option.
- [SAML Authentication Provider configuration](#)
This topic describes the systematic instruction to **SAML Authentication Provider configuration** option.
- [SQL Authentication Provider configuration](#)
This topic describes the systematic instruction to **SQL Authentication Provider configuration** option.
- [OHS Configuration](#)
This topic provides information on **OHS Configuration**.
- [Database Configuration](#)
This topic provides information on **Database Configuration**.
- [IDCS OAuth Integration](#)
This topic describes the systematic instruction to **IDCS OAuth Integration** option.
- [WebLogic configuration for OAuth](#)
This topic describes the systematic instruction to **WebLogic configuration for OAuth** option.
- [OBDX configuration for OAuth](#)
This topic provides information on **OBDX configuration for OAuth**.
- [Default Admin Configuration](#)
This topic provides information on **Default Admin Configuration**.
- [Logout Configurations](#)
This topic provides information on **Logout Configurations**.

2.1 Identity Provider Configuration at IDCS

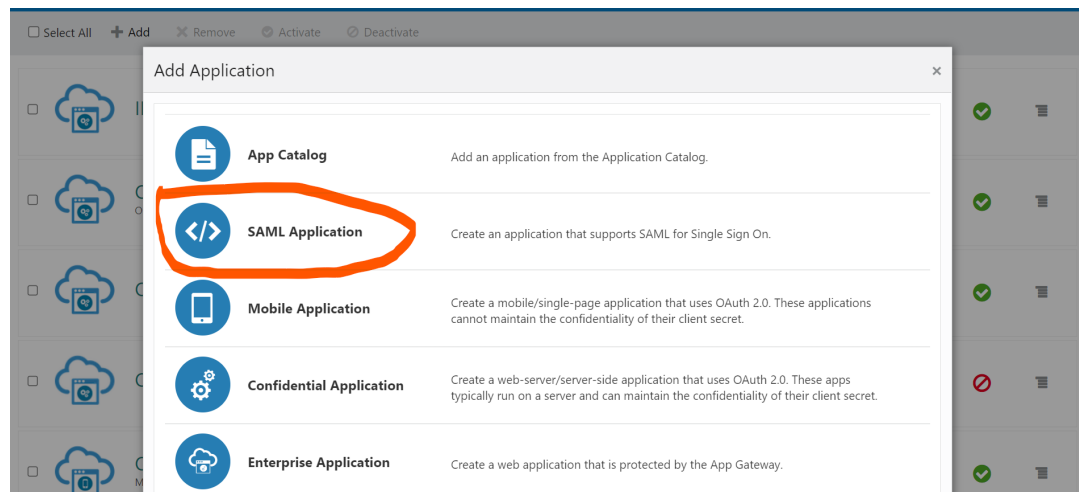
This topic describes the systematic instruction to **Identity Provider Configuration at IDCS** option.

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

1 Details

2 SSO Configuration

Next >

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.**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/post
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

2 SSO Configuration

Finish

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

Include Signing Certificate in Signature ☐

Signature Hashing Algorithm

Enable Single Logout ☒

* Logout Binding

* Single Logout URL

* Logout Response URL

Encrypt Assertion ☐

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

Figure 2-6 Edit Application

Applications > OBDX_SAML_CONFIG



OBDX_SAML_CONFIG
 SAML Configuration for OBDX user authentication.

Details SSO Configuration Users Groups

App Details

Application Type SAML Application

* Name

Description

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.

Figure 2-7 Edit Application

OBDX_SAML_CONFIG
SAML Configuration for OBDX user authentication.

Details **SSO Configuration** Users Groups

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

* Assertion Consumer URL

* NameID Format Email address

* NameID Value Primary Email

Signing Certificate

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

OBDX_SAML_CONFIG
SAML Configuration for OBDX user authentication.

Details SSO Configuration **Users** Groups


No users are assigned to this application.

Figure 2-9 Assign Users

Please select up to 40 users to assign.

☐ Select All

superadmin

Selected: 1 [Clear Selection](#)

	First Name	Last Name	Email
☐	Super	Admin	[REDACTED]
☒	superadmin	superadmin	[REDACTED]

Page 1 of 1 (1-2 of 2 items) [K](#) [<](#) [1](#) [>](#) [X](#) [OK](#)

12. Logout from IDSC console.

2.2 SAML Authentication Provider configuration

This topic describes the systematic instruction to **SAML Authentication Provider configuration** option.

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

ORACLE WebLogic Server Administration Console 14.1.1

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: trunk_dom_repl_domain

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

Showing 1 to 1 of 1 Previous Next

Change Center

View changes and restarts

Click the **Lock & Edit** button to modify, add or delete items in this domain.

[Lock & Edit](#)

[Release Configuration](#)

Domain Structure

trunk_dom_repl_domain

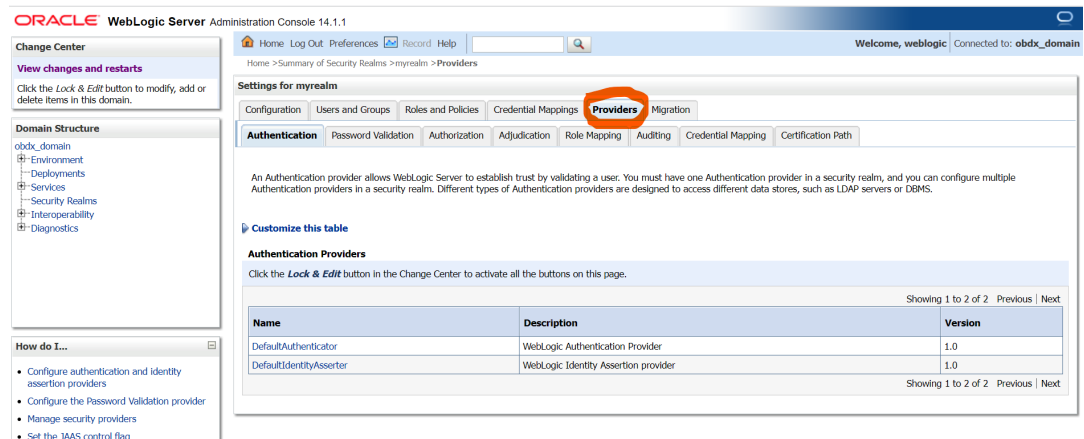
- Environment
 - Servers
 - Clusters
 - Coherence Clusters
 - Machines
 - Virtual Hosts
 - Work Managers
 - Concurrent Templates
 - Startup and Shutdown Classes
- Deployments
- Services**
 - Security Realms**

How do I...

- Configure new security realms
- Enable automatic realm restart

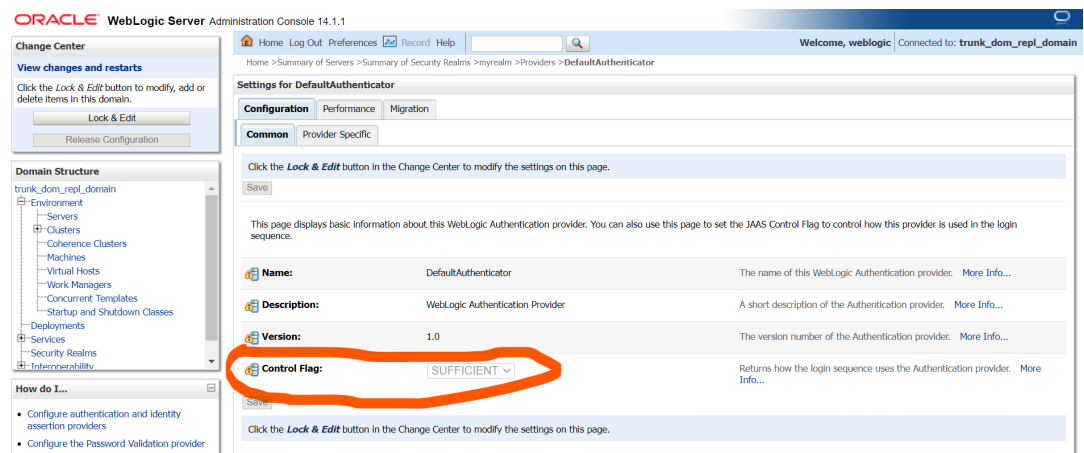
2. → Click on myrealm or your realm name present in screen. Navigate to “Providers” tab.

Figure 2-11 Providers



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

Figure 2-12 Default Authenticator

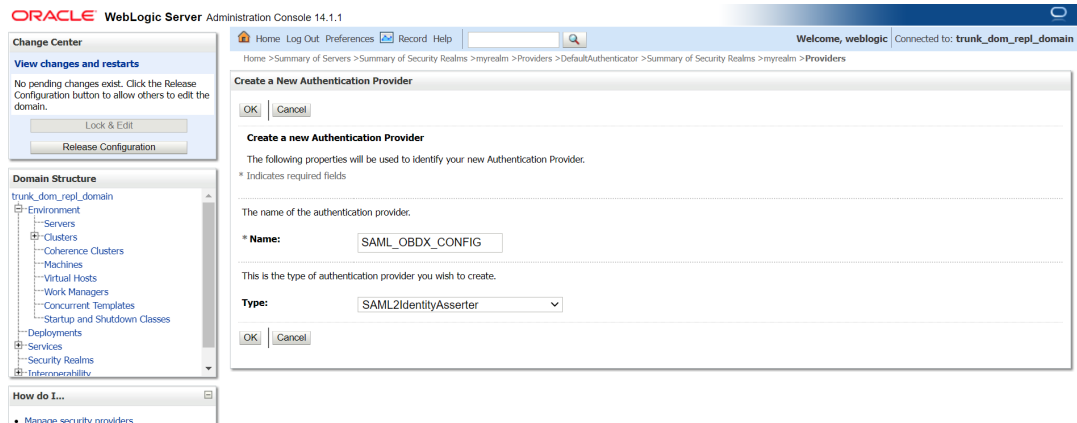


4. Again, navigate to “Security Realms” → myrealms → Providers and click on **New** button to create new Authentication Provider.

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

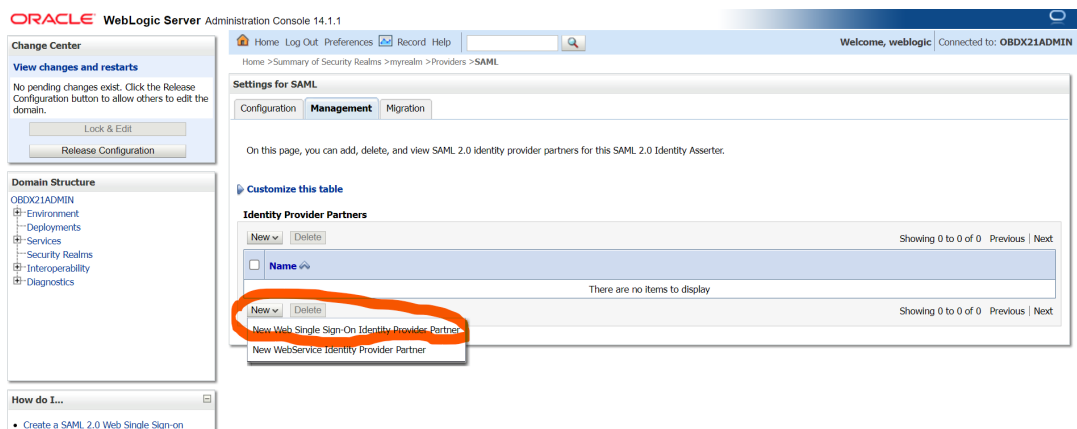
- a. Name: Name of authentication provider.
- b. Type : Select value as “SAML2IdentityAsserter”.

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

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**.
 - 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

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: 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 Assertion provider is configured in this security realm. [More Info...](#)

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

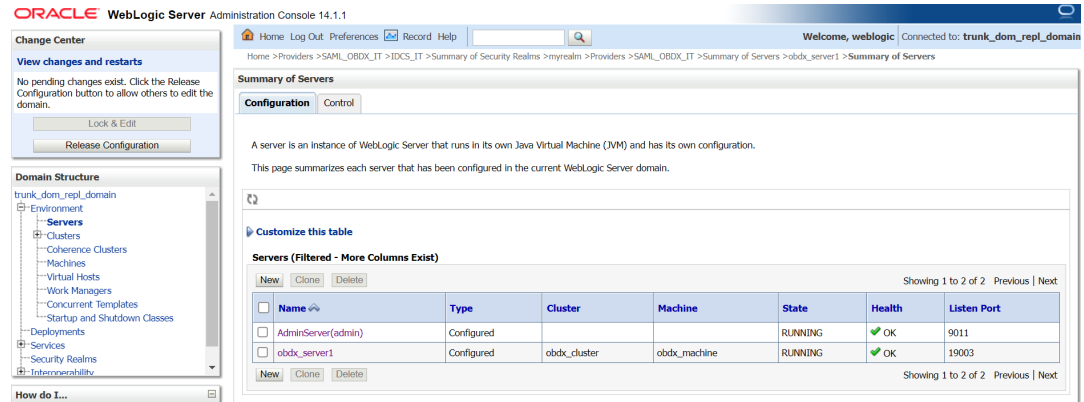
☒ Virtual User Specifies whether user information contained in assertions received from this Identity Provider partner are mapped to virtual users in this security realm. [More Info...](#)

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 Assertion 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.

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>/sam12
e.g. <PROTOCOL>://<OHS_HOST>:<OHS_PORT>/sam12

http://whf000xxx.bank.com:9999/sam12
 - 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

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**.
 - a. Enabled: Check box should be checked.
 - b. Preferred Binding: Post
 - c. Default URL: <OHS_URL>/digx-infra/admin-dashboard

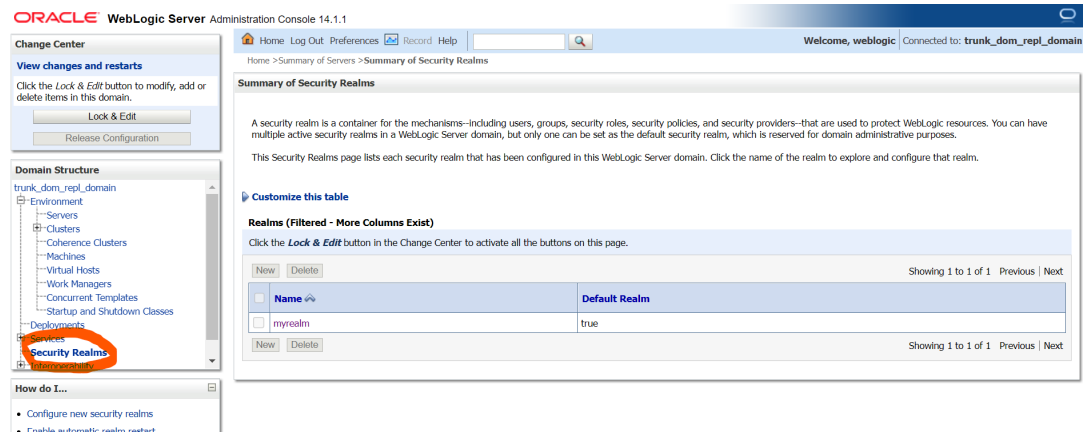
2.3 SQL Authentication Provider configuration

This topic describes the systematic instruction to **SQL Authentication Provider configuration** option.

Steps to configure SQL Authentication Providers changes into WebLogic console.

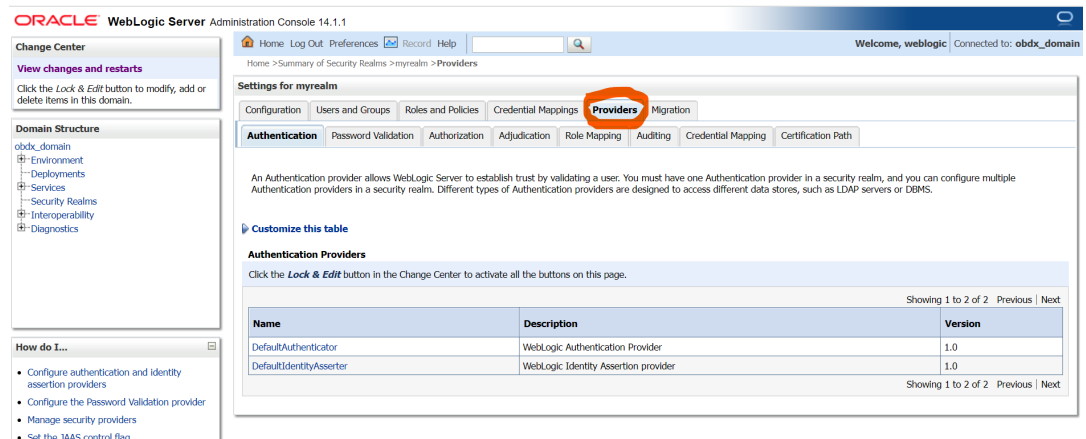
1. Login to WebLogic console with admin login and navigate to “Security Realms”.

Figure 2-19 Security Realms



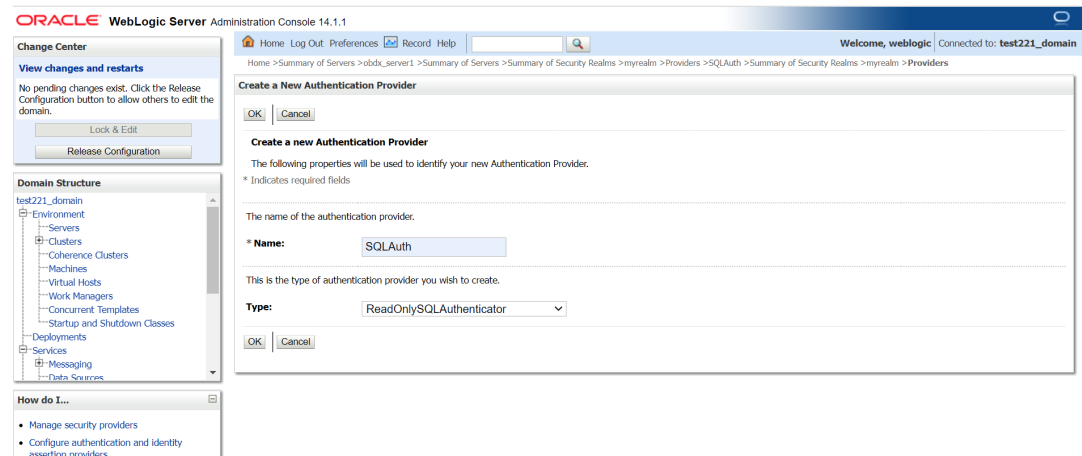
2. → Click on myrealm or your realm name present in screen. Navigate to “Providers” tab.

Figure 2-20 Providers



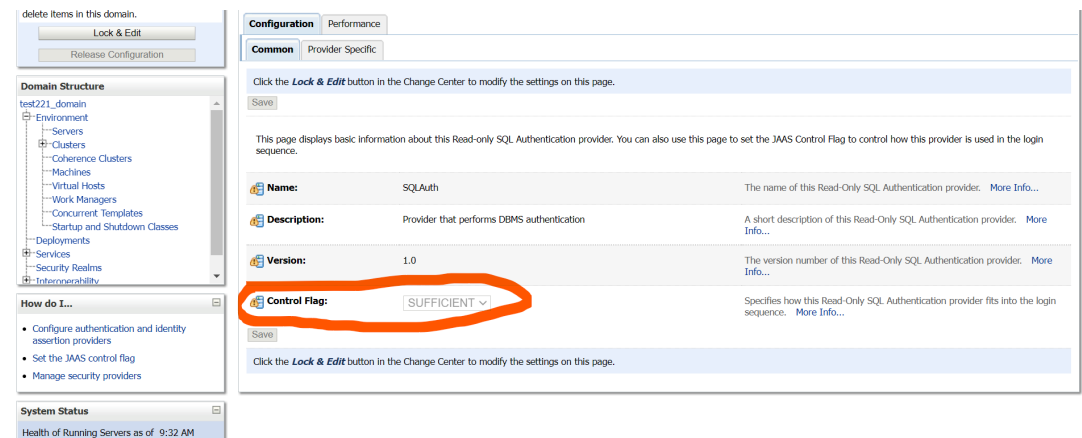
3. Click on **New** button to create new Authentication Provider.
Fill the below mentioned fields with appropriate values and click on **OK**.
 - a. Name: Name of authentication provider.
 - b. Type :Select value as “ReadOnlySQLAuthenticator”.

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

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**

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.

Figure 2-24 Authentication

Authentication Providers

Showing 1 to 4 of 4 Previous | Next

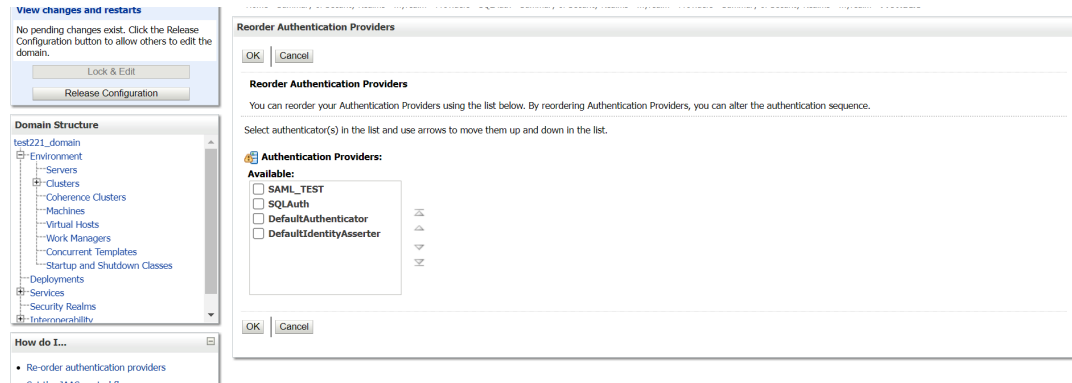
Name	Description	Version
SAML_TEST	SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0.	1.0
SQLAuth	Provider that performs DBMS authentication	1.0
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

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

This topic provides information on **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

This topic provides information on **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);
```

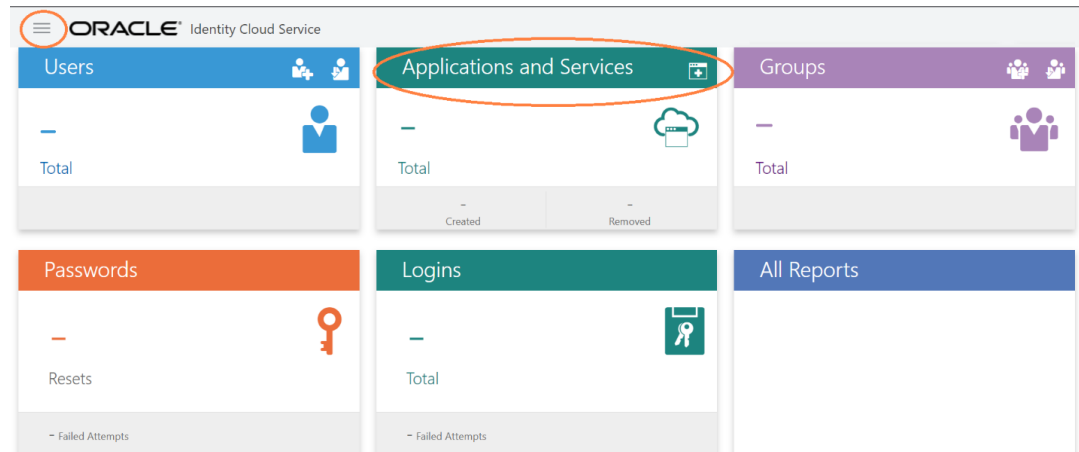
For Example: INSERT INTO DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER, EDITABLE, CATEGORY_DESCRIPTION) values ('SSO_PUBLIC_URL', 'dayoneconfig', '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

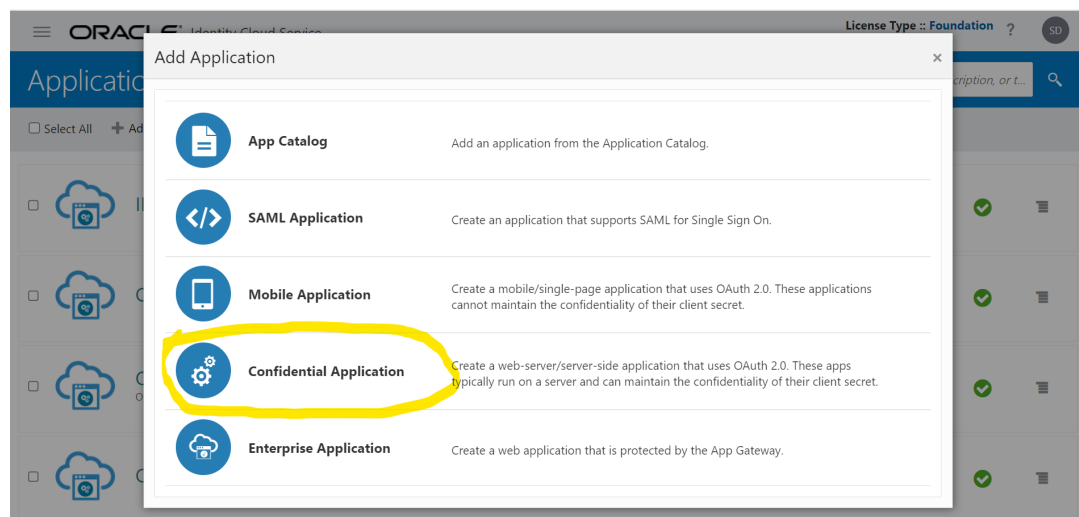
This topic describes the systematic instruction to **IDCS OAuth Integration** option.

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

Add Confidential Application

Cancel 1 2 3 4 5 Next >

Details Client Resources Web Tier Policy Authorization

App Details

* Name OBDX_OAUTH_CONFIG

Description OAuth Configuration for fetching user details from IDCS

Application Icon

Upload

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 ✓ 2 3 4 5 Next >

Details Client Resources Web Tier Policy Authorization

☒ 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.
 - 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

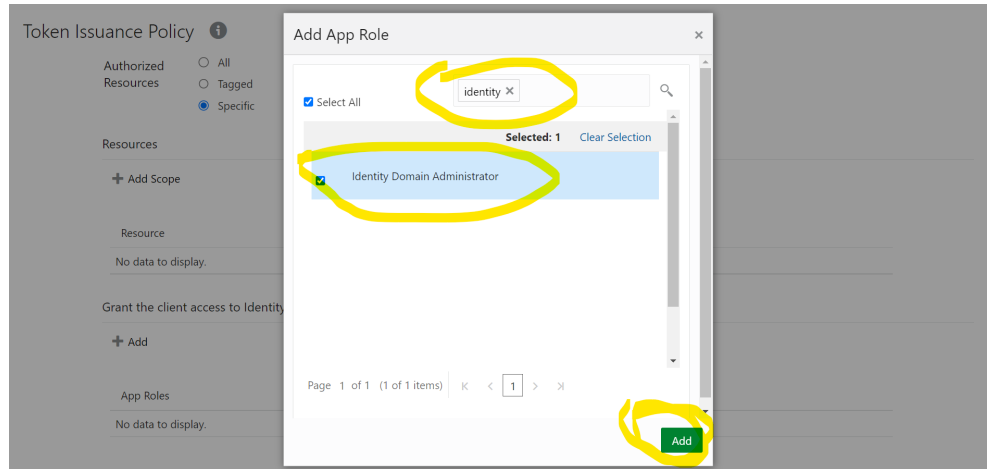
Resource	Protected	Scope
No data to display.		

Grant the client access to Identity Cloud Service Admin APIs

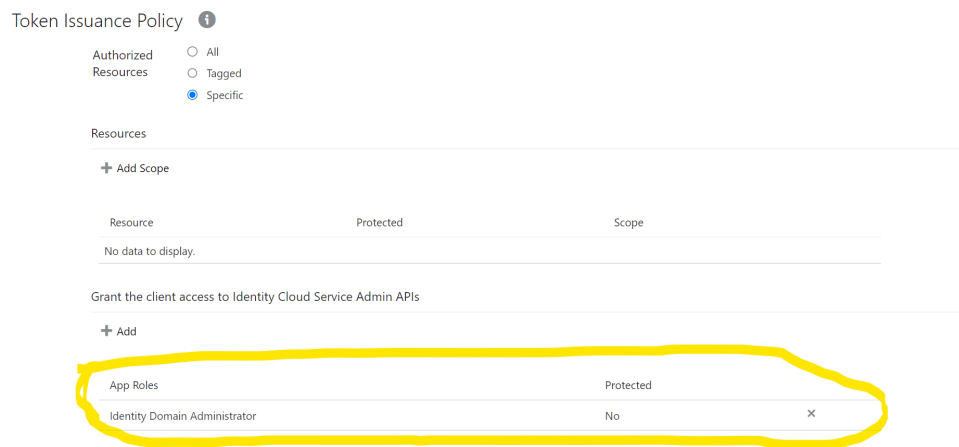
+ Add

App Roles	Protected
No data to display.	

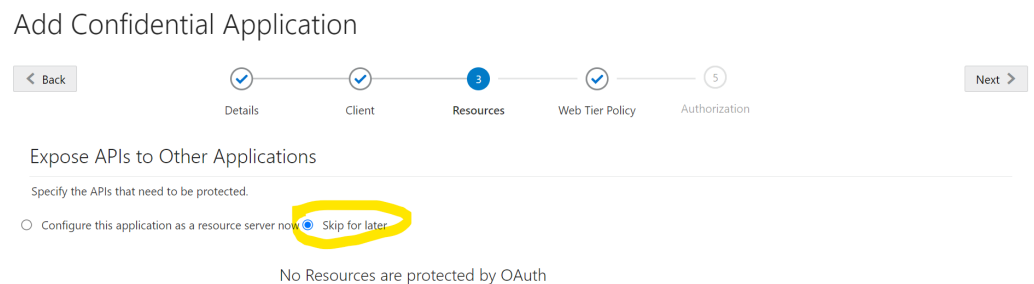
- iii. In popup window search for “**Identity Domain Administrator**” and click on **Add**.

Figure 2-32 Add App Role

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

Figure 2-33 Add Confidential Application

- 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

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

Figure 2-35 Add Confidential Application

Add Confidential Application

- e. Click on **“Finish”**.

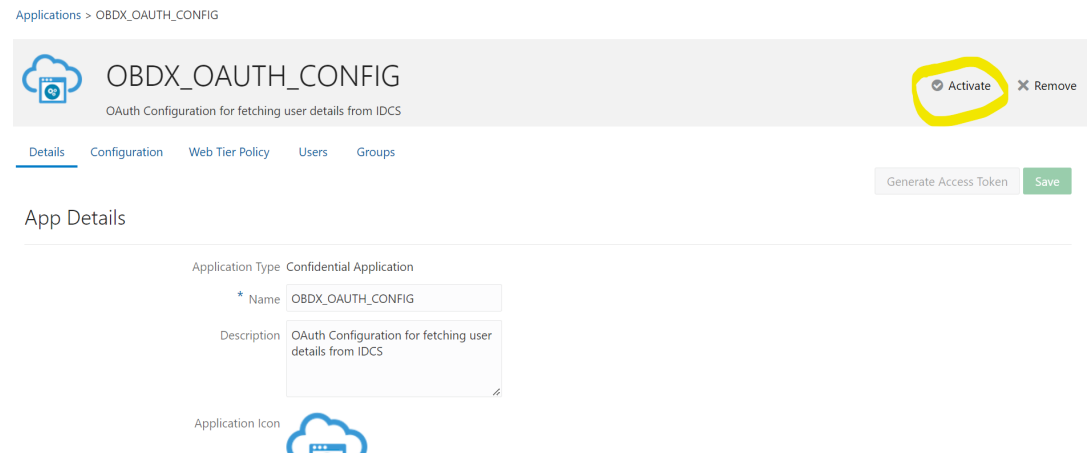
Figure 2-36 Add Confidential Application

Add Confidential Application

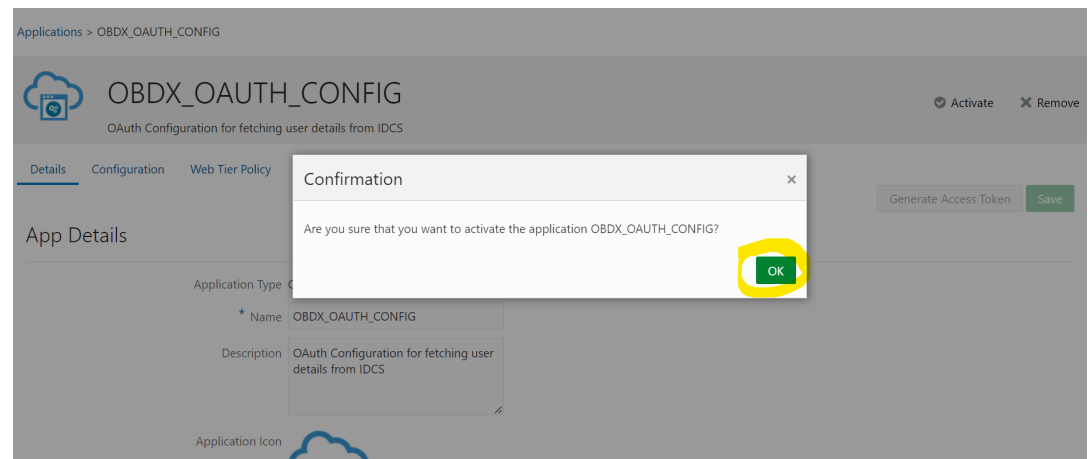
6. After finish click a popup window will open with “Client ID” and “Client Secret” as shown in below screenshot. Copy the Client Id and Client Secret to text file to keep it handy as it will be required in further steps. Once copied click on “Close”.

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

This topic describes the systematic instruction to **WebLogic configuration for OAuth** option.

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

delete items in this domain.
Lock & Edit
Release Configuration

Domain Structure
test221_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

Deployments
Install Update Delete Showing 1 to 24 of 24 Previous Next

☐	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-eureka-server	Active	OK	Web Application	obdx_server1	100

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

Figure 2-41 Outbound Connection Pools Configuration

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_rep_domain
├── Environment
├── Deployments
├── Services
├── Security Realms
├── Interoperability
└── Diagnostics

How do I...
• Configure outbound connection pool properties

System Status
Health of Running Servers as of 6:26 AM
Failed (0)

Home Log Out Preferences Record Help
Welcome, weblogic Connected to: trunk_dom_rep_domain
Home > Summary of Deployments > com.ofss.digx.connector

Settings for com.ofss.digx.connector
Overview Deployment Plan **Configuration** Security Targets Control Testing Monitoring Notes

General Properties **Outbound Connection Pools** Admin Objects Workload Instrumentation

This page displays a table of outbound connection pool groups and instances for this resource adapter. The top level entries in the table represent outbound connection pool groups. Groups are listed by connection factory interface and the instances are listed by their JNDI names. Expand a group to obtain configuration information for a connection pool instance within an outbound connection pool group. Click the name of a group or instance to configure it. Automatically generated connection pools are not displayed in the table below.

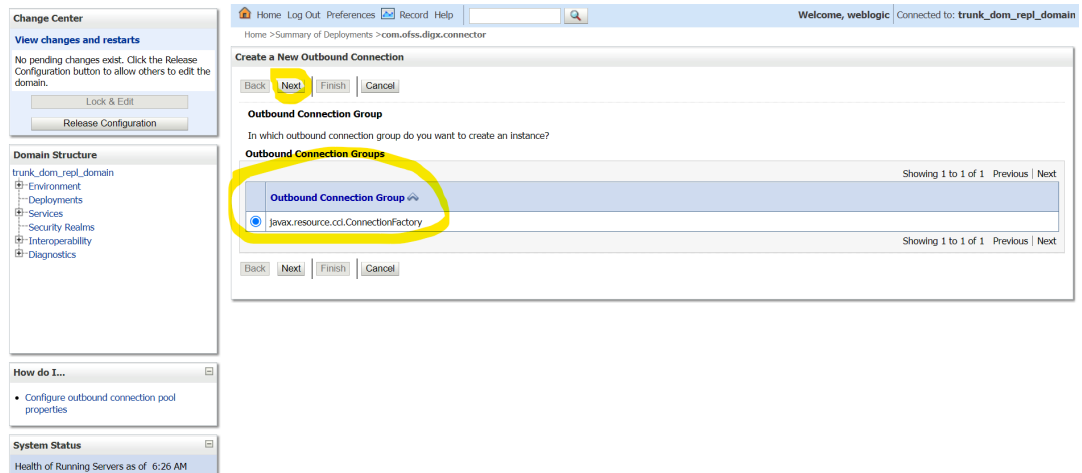
Outbound Connection Pool Configuration Table
New Delete Showing 1 to 1 of 1 Previous Next

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

New Delete Showing 1 to 1 of 1 Previous Next

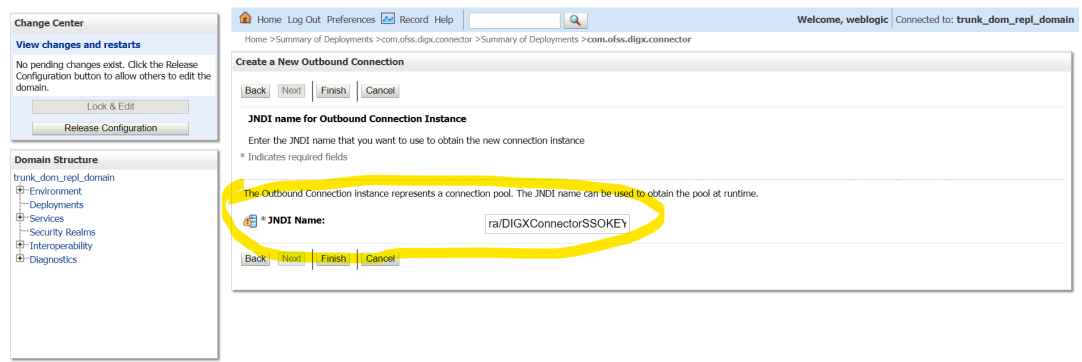
- Select “javax.resource.cci.ConnectionFactory” and click on **Next**.

Figure 2-42 Outbound Connection Group Configuration



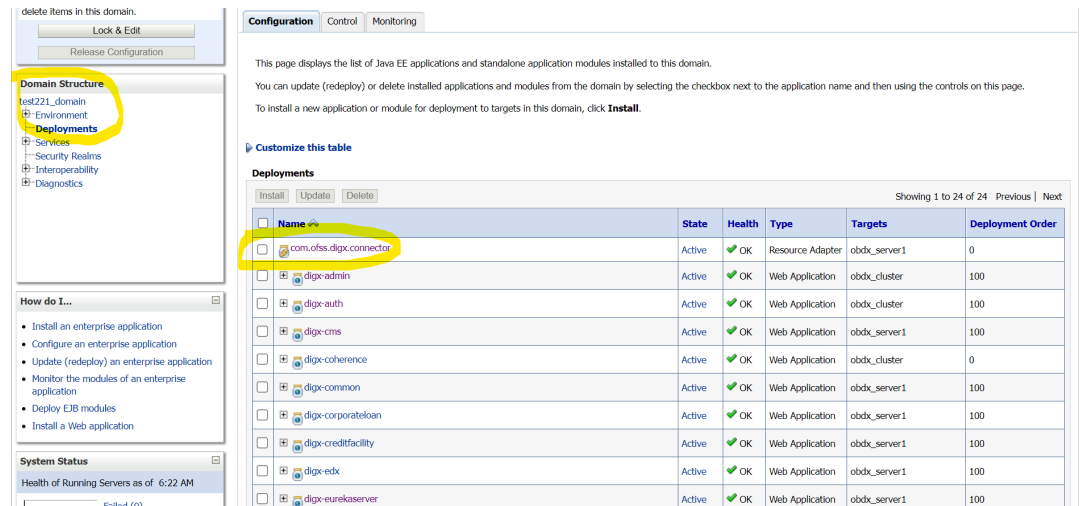
5. Enter JNDI name as ra/DIGXConnectorSSOKEY and click on **Finish**.

Figure 2-43 JNDI Configuration for Outbound Connection



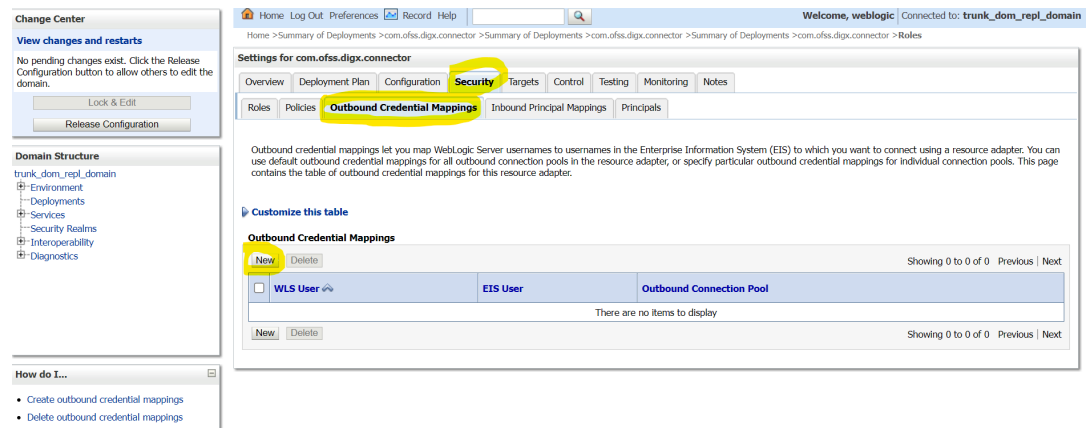
6. Again navigate to “Domain Structure” → “Deployments”.
7. Click on “com.ofss.digx.connector”.

Figure 2-44 Deployments



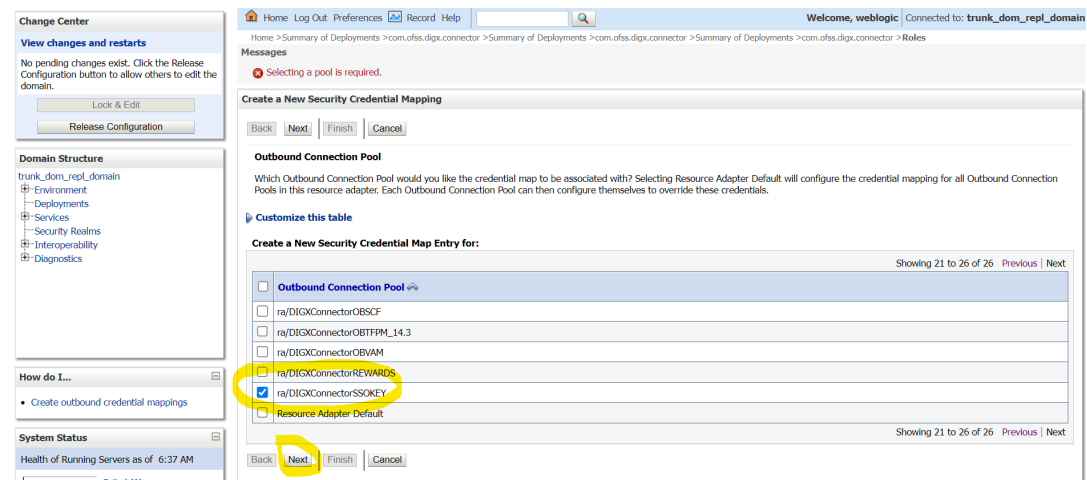
- Navigate to “Security” → “Outbound Credentials Mapping” tab and click on **New**.

Figure 2-45 Outbound Credentials Mappings



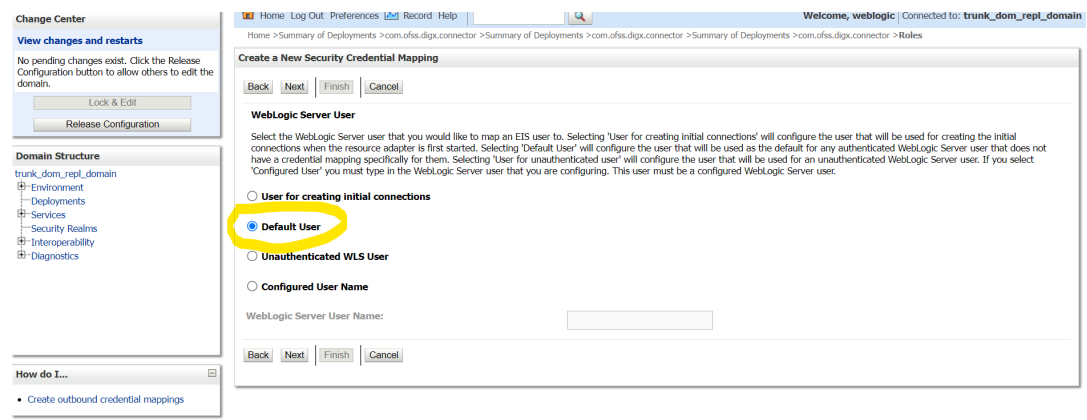
- Select “ra/DIGXConnectorSSOKEY” by navigating using next button. Once selected as shown in below screenshot, click on **Next**.

Figure 2-46 Create New Security Credentials Mappings



- Select “Default User” and click on **Next**.

Figure 2-47 Create New Security Credentials Mappings



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. On the left, there is a 'Change Center' panel with 'View changes and restarts' and 'Release Configuration' buttons. Below it is the 'Domain Structure' tree showing 'trunk_dom_rep1_domain' with sub-items like 'Environment', 'Deployments', 'Services', 'Security Realms', 'Interoperability', and 'Diagnostics'. At the bottom left is the 'System Status' panel showing 'Health of Running Servers as of 6:39 AM' with 'Failed (0)' and 'Critical (0)' counts. The main area displays the 'Create a New Security Credential Mapping' dialog. The dialog has a title bar with 'Back', 'Next', 'Finish', and 'Cancel' buttons. The main content area is titled 'EIS User Name and Password' and contains the instruction: 'Configure the EIS User Name and Password that you would like to map the WebLogic Server User to:'. Below this are three input fields: 'Enter the EIS User Name:', '* EIS User Name:', 'Enter the EIS Password:', '* EIS Password:', and '* Confirm Password:'. 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 dialog has 'Back', 'Next', 'Finish', and 'Cancel' buttons at the bottom.

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

2.8 OBDX configuration for OAuth

This topic provides information on **OBDX 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

This topic provides information on **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.

2.10 Logout Configurations

This topic provides information on **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, [15](#)

Default Admin Configuration, [27](#)

I

IDCS OAuth Integration, [16](#)

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

L

Logout Configurations, [27](#)

O

OBDX configuration for OAuth, [26](#)

OHS Configuration, [14](#)

S

SAML Authentication Provider configuration, [6](#)

SQL Authentication Provider configuration, [10](#)

W

WebLogic configuration for OAuth, [22](#)