IDCS-OBAPI Setup Guide
Oracle Banking APIs
Patchset Release 21.1.3.0.0

Part No. F40802-01

November 2021

ORACLE

IDCS-OBAPI Setup Guide

November 2021

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax:+91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2006, 2021, Oracle and/or its affiliates. All rights reserved.

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

1. Preface 1–1

1.1 Intended Audience 1–1

1.2 Documentation Accessibility 1–1

1.3 Access to Oracle Support 1–1

1.4 Structure 1–1

1.5 Related Information Sources 1–1

2. Pre-requisite step: 2–1

2.1 To create groups and user in IDCS 2–1

2.2 Install OpenSSL 2–8

2.3 OAM installation not required 2–8

3. Apply Oracle OPSS SCIM Identity Store OPatch on Weblogic server 3–1

4. Extending Weblogic Domain to load 'Oracle OPSS SCIM Identity Store' template 4–1

5. Change JPS configurations 5–1

6. Create an OBAPI Client Application in IDCS Console 6–1

7. Configure OPSS IDCS Identity Store Service 7–1

8. Adding IDCS as an Identity Provider in Weblogic Security Realms 8–1

9. Application Server Changes 9–1

9.1 Add below argument to Managed server: 9–1

9.2 Managed Server Start Configurations 9–2

10. Change in Weblogic Deployments 10–1

10.1 Creating a Connection in Connector ear 10–1

11. Create Client Applications for Internal OBAPI Apps in IDCS Console 11–1

12. Database Scripts (to be executed after day0 scripts) 12–1

13. Apply Webgate Patch on OHS using OPatch 13–1

14. cloud.config 14–1

15. cloud.policy 15–1

16. CWallet configuration 16–1

17. Enabling webgate in httpd.conf 17–1

18. Change in mod_wl_ohs.conf 18–1

19. UI Changes 19–1

19.1 constants.js: 19–1

19.2 idcs-config.json: 19–1

1. Preface

1.1 Intended Audience

This document is intended for the following audience:

- Customers
- Partners

1.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

1.3 Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1.4 Structure

This manual is organized into the following categories:

Preface gives information on the intended audience. It also describes the overall structure of the User Manual.

The subsequent chapters describes following details:

- Introduction
- Preferences & Database
- Configuration / Installation.

1.5 Related Information Sources

For more information on Oracle Banking APIs Patchset Release 21.1.3.0.0, refer to the following documents:

- Oracle Banking APIs Installation Manuals

2. Pre-requisite step:

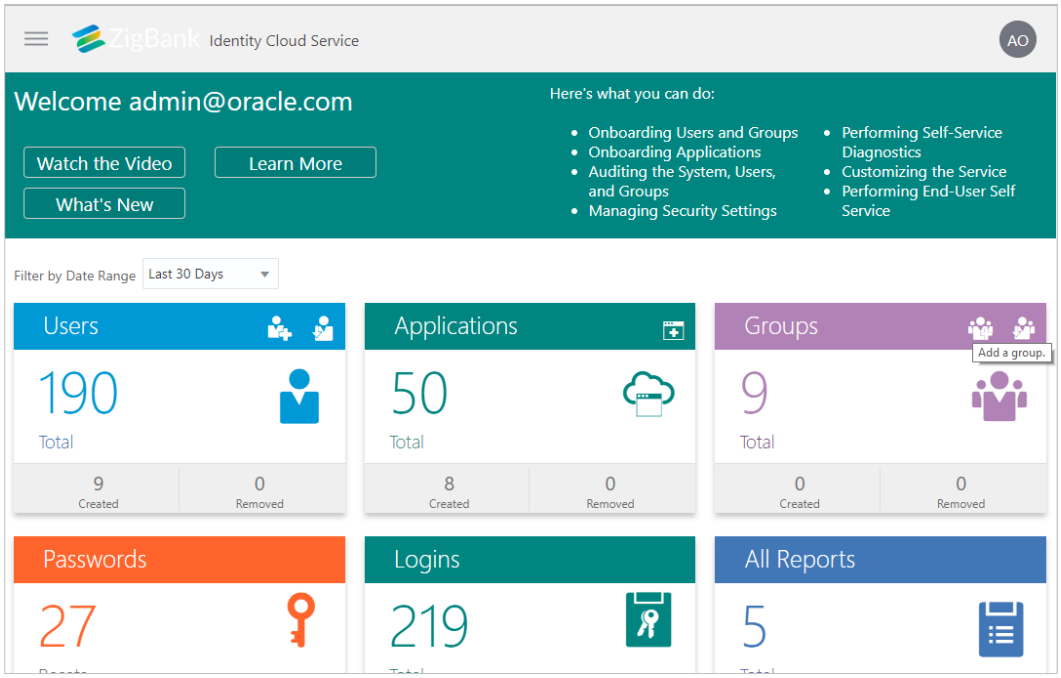
2.1 To create groups and user in IDCS

1. Access your Oracle Identity Cloud Service instance (for example: https://<tenant-base-url>/ui/v1/adminconsole) and log in with your Identity Domain Administrator credentials.

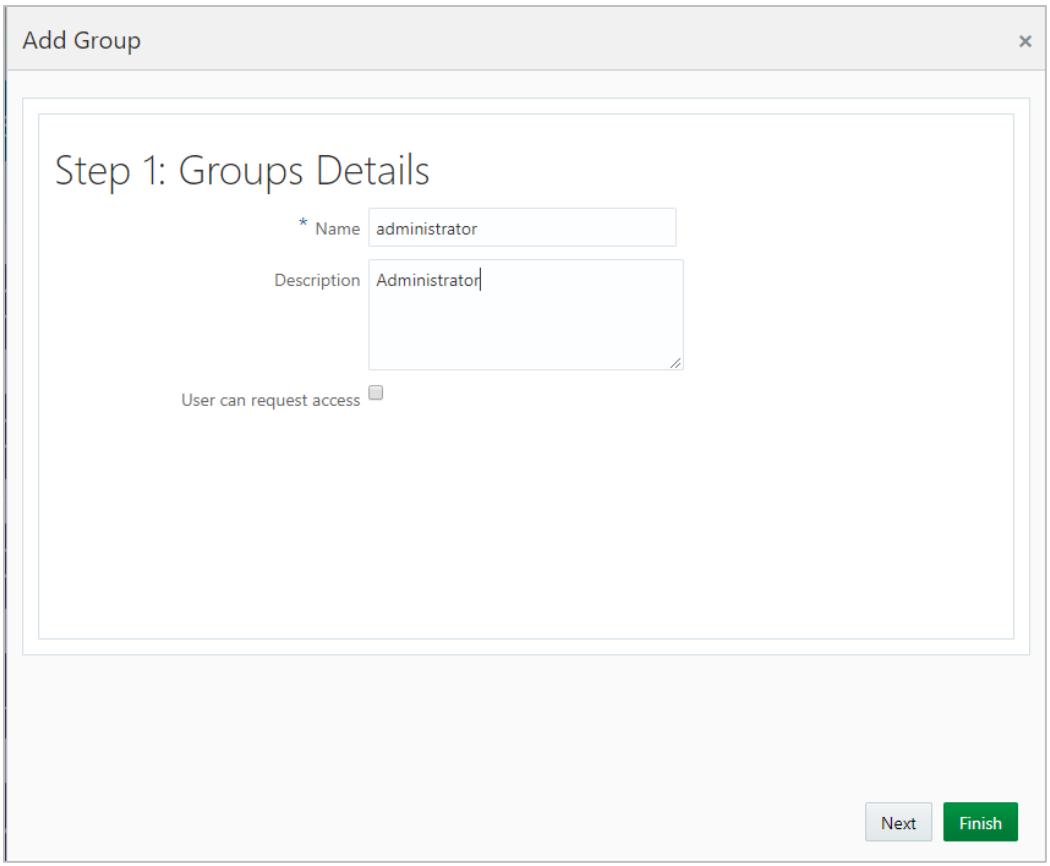
Glossary of Parameters:

<tenant-name>	Tenant name of your IDCS instance
<tenant-base-url>	Tenant base URL used to access your IDCS instance
<base-url>	Base URL used to access your IDCS instance without tenant name

2. Click on **Add a group** button shown below.

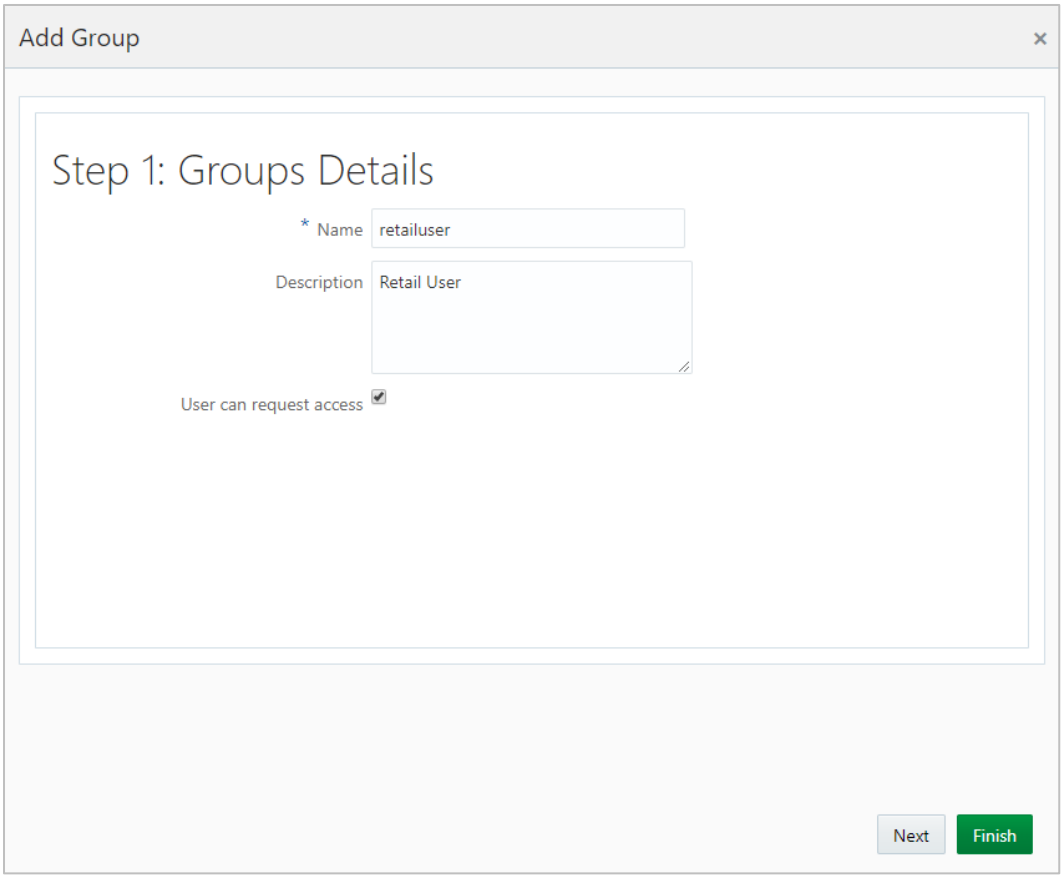


3. Enter the group name and group description for ‘administrator’ as shown below.



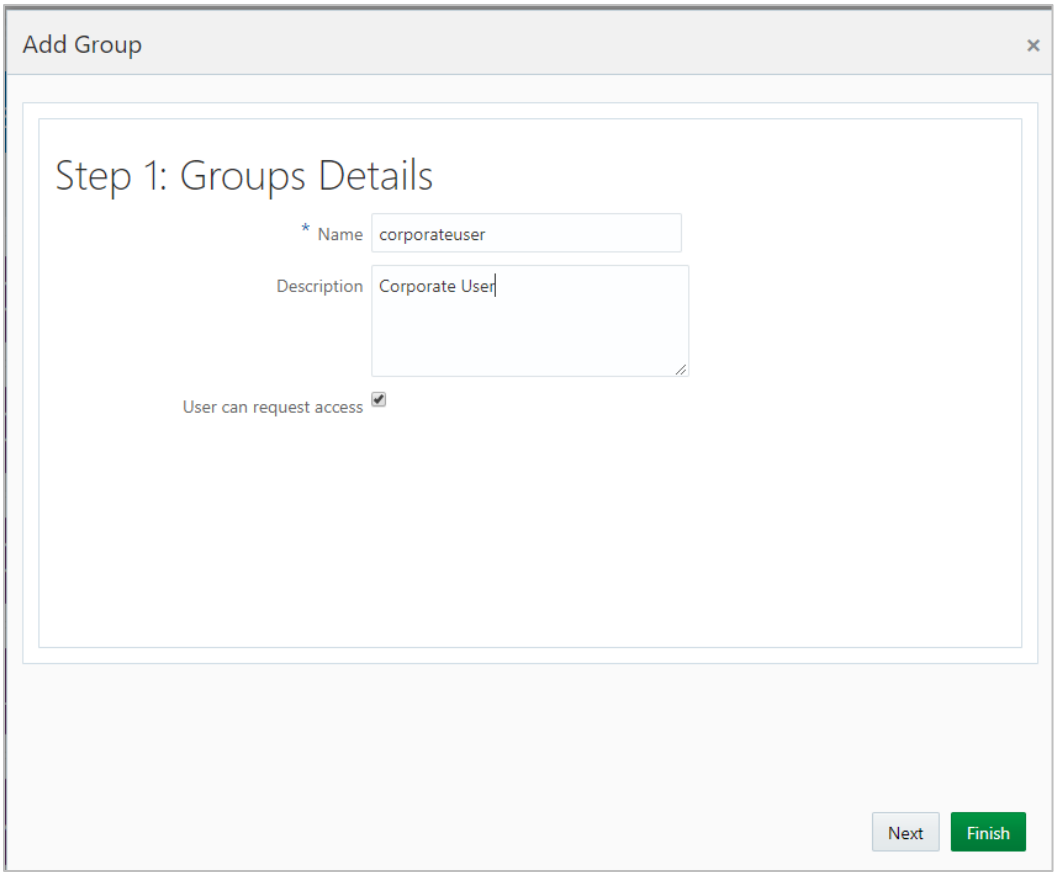
4. Click **Finish**. You will get a message ‘Group administrator has been successfully added.’

5. On **Groups** screen, click on **Create a group** button. Enter the group name and group description for ‘retailuser’ as shown below.



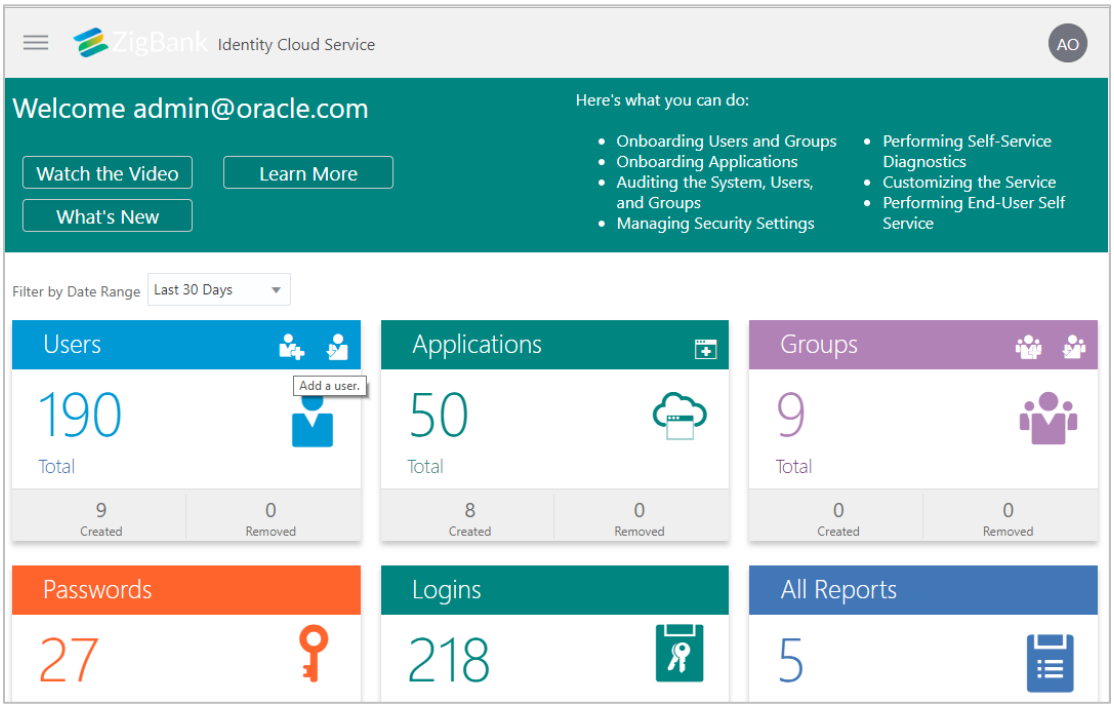
6. Click **Finish**. You will get a message ‘Group retailuser has been successfully added.’

7. On **Groups** screen, click on **Create a group** button. Enter the group name and group description for ‘corporateuser’ as shown below.

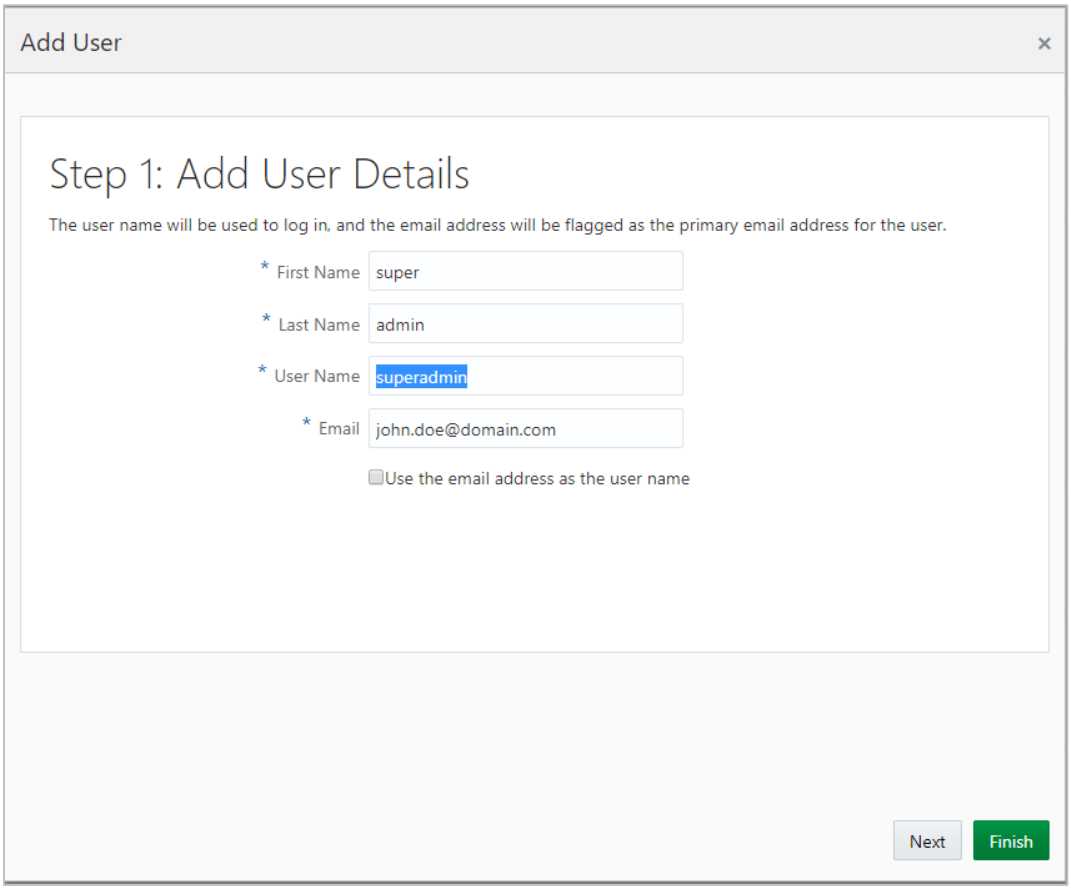


8. Click **Finish**. You will get a message ‘Group corporateuser has been successfully added.’

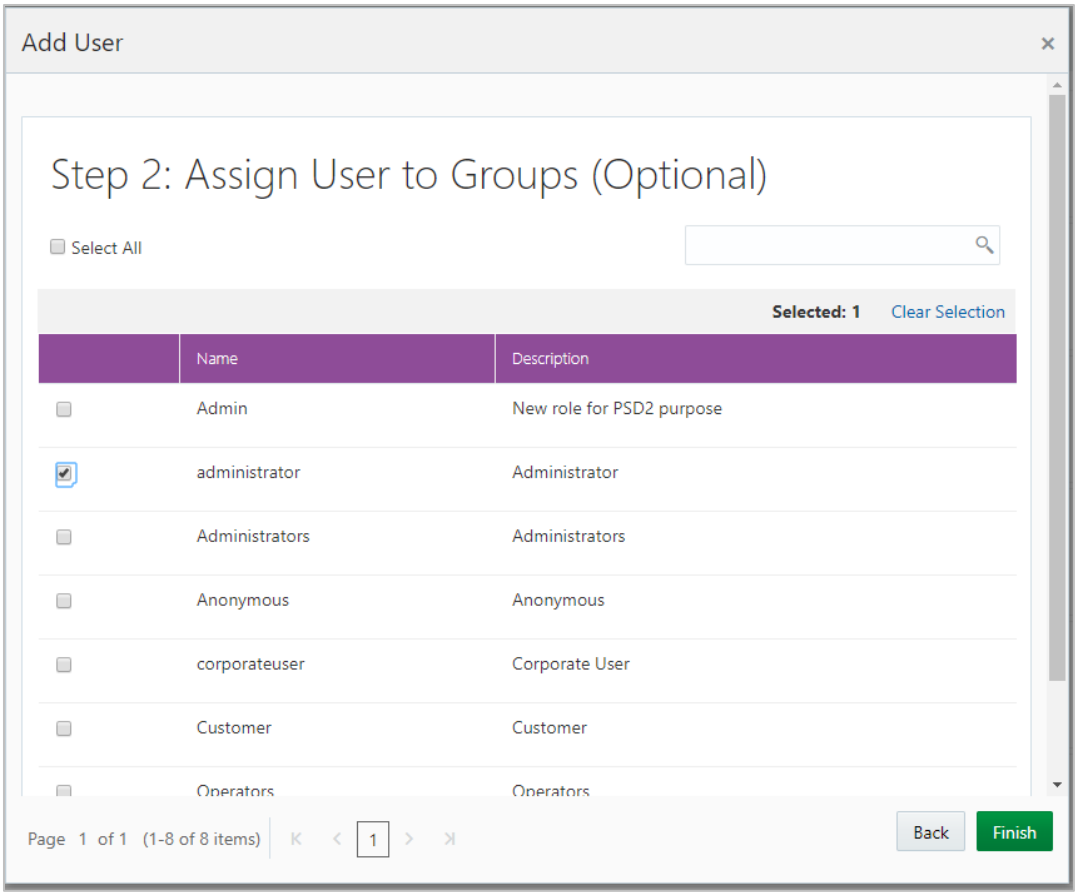
9. Click on **Add a user** button on **Dashboard** screen as shown below.



10. On the next screen, enter details of a new user ‘superadmin’ shown below.



11. Click **Next**. You will get a list of existing groups in IDCS to which the user ‘superadmin’ can be assigned. Select group ‘**administrator’**.



12. Click **Finish**. The user ‘superadmin’ will be created and assigned ‘administrator’ group.

2.2 Install OpenSSL

Eg. [root@obapiohs devops]# yum install openssl*

2.3 OAM installation not required

Oracle Access Manager installation is not required for this setup.

Home

3. Apply Oracle OPSS SCIM Identity Store OPatch on Weblogic server

1. Download the patch from the below link.

   ARU 22260908

2. Extract the zip on weblogic machine.
3. Shutdown Managed and Admin weblogic server.

   Glossary of Parameterized path:

oracle-home-path	Oracle Home path of Fusion Middleware Application (Weblogic/OHS)
jre-path	Location where jre is installed
local-patch-path	Location where relevant patch folder is stored locally. Eg. Location of 27644158 folder
weblogic-domain-path	Location where weblogic domain is installed
jdk-path	Location of JDK
ohs-domain-path	Location where OHS domain is installed

4. Run below commands on Weblogic machine.

[devops@obapiwls ~]$ export ORACLE_HOME=<oracle-home-path>

Eg. export ORACLE_HOME=/home/devops/Oracle/Middleware/Oracle_Home/

[devops@obapiwls ~]$ export PATH=$PATH:<oracle-home-path>/OPatch/

Eg. export PATH=$PATH:/home/devops/Oracle/Middleware/Oracle_Home/OPatch/

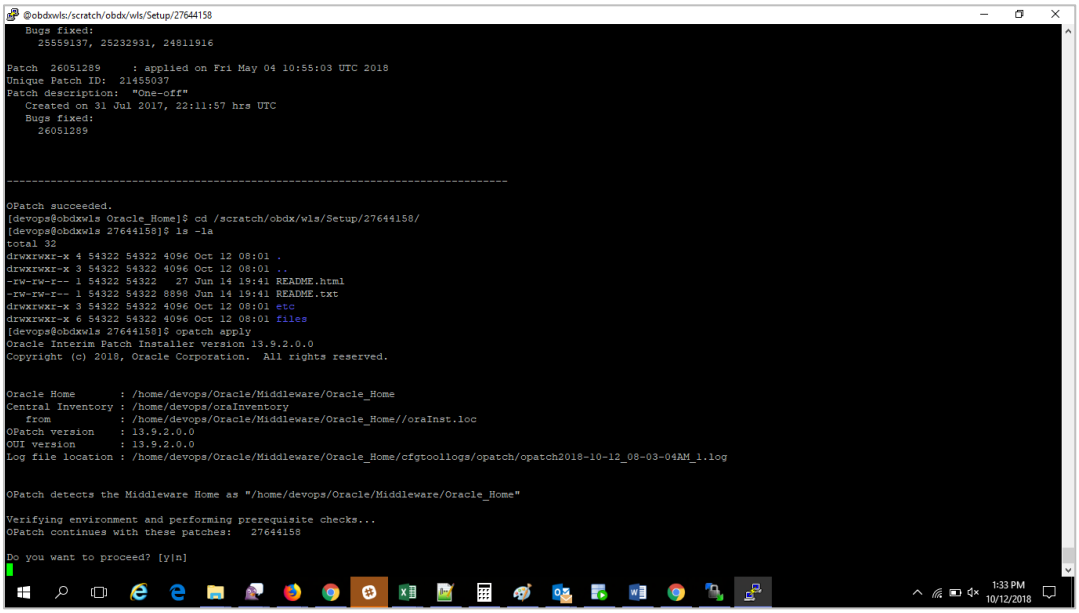
[devops@obapiwls ~]$ opatch lsinventory -jre <jre-path>

Eg. opatch lsinventory -jre /home/devops/jdk18/jre/

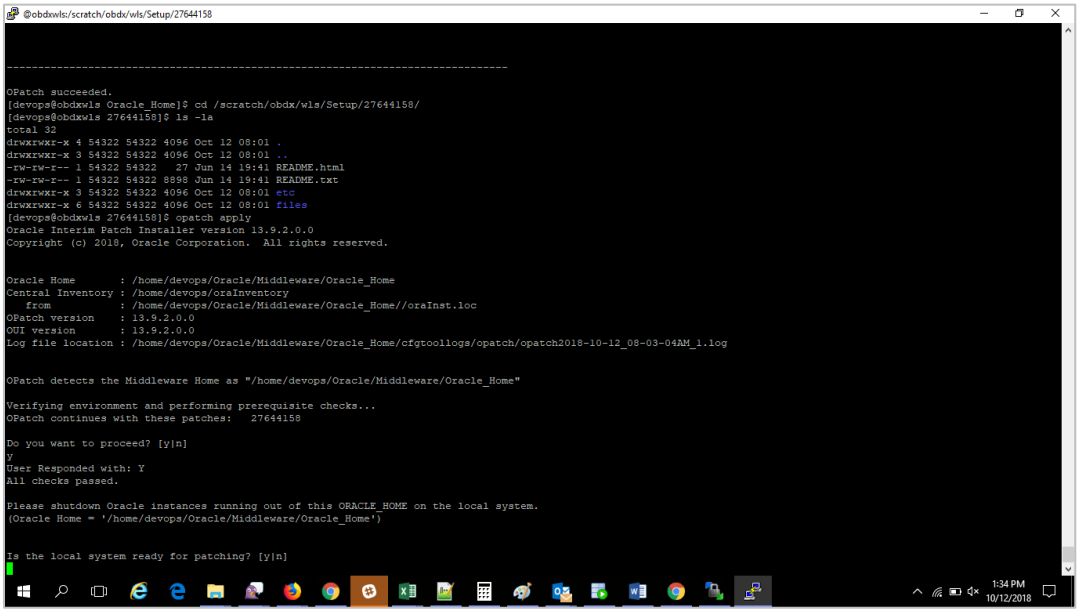
[devops@obapiwls ~]$ cd <local-patch-path>

Eg. cd /scratch/obapi/wls/p27644158_122130_Generic/27644158/

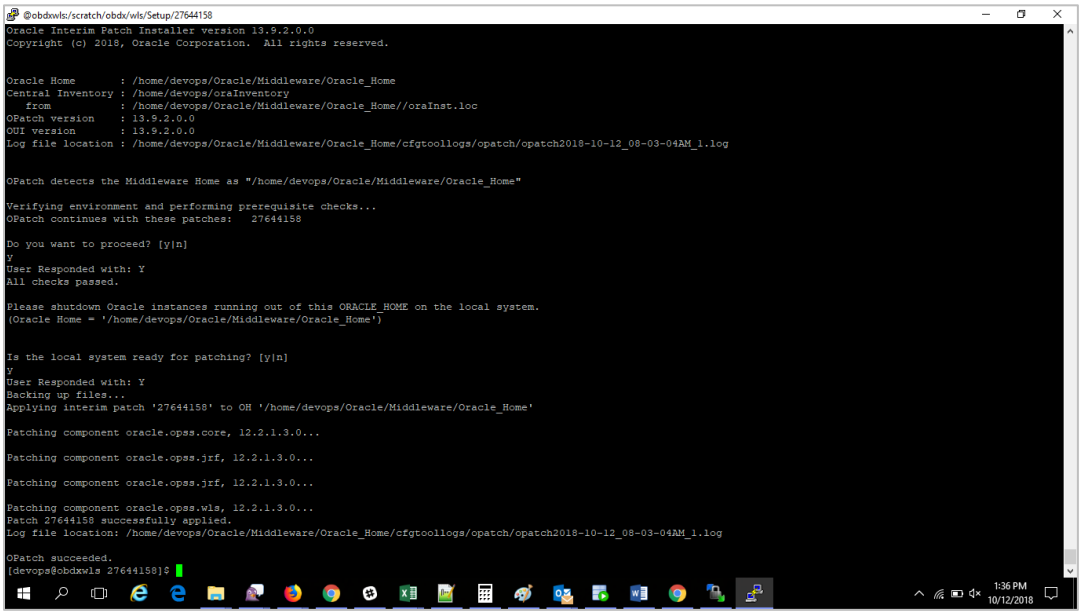
[devops@obapiwls 27644158]$ opatch apply



5. Press '**y**'



6. Press '**y**'



Home

4. Extending Weblogic Domain to load ‘Oracle OPSS SCIM Identity Store’ template

1. Run the below commands.

[devops@obapiwls fmwconfig]$ cd <ORACLE-HOME-PATH>/oracle_common/common/bin/

Eg. cd /home/devops/Oracle/Middleware/Oracle_Home/oracle_common/common/bin/

[devops@obapiwls bin]$ ./wlst.sh

[This will take you to Weblogic Server Administration Scripting Shell]

2. Run the below commands in wlst :

wls:/offline>readDomain("<weblogic-domain-path>")

Eg. readDomain("/home/devops/domain/obapi_domain")

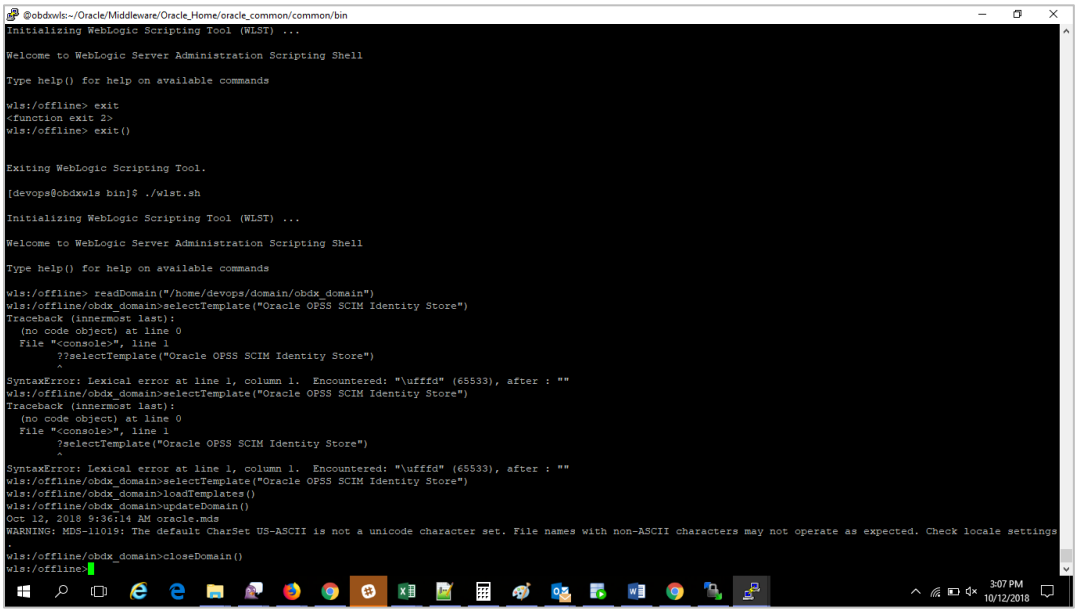
wls:/offline/obapi_domain>selectTemplate("Oracle OPSS SCIM Identity Store")

wls:/offline/obapi_domain>loadTemplates()

wls:/offline/obapi_domain>updateDomain()

wls:/offline/obapi_domain>closeDomain()

wls:/offline/obapi_domain>exit()


@obdxwls:~/Oracle/Middleware/Oracle_Home/oracle_common/common/bin
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands
wls:/offline> exit
<function exit 2>
wls:/offline> exit()
Exiting WebLogic Scripting Tool.
[devops@obdxwls bin]$ ./wlst.sh
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands
wls:/offline> readDomain("/home/devops/domain/obdx_domain")
wls:/offline/obdx_domain>selectTemplate("Oracle OPSS SCIM Identity Store")
Traceback (innermost last):
(no code object) at line 0
File "<console>", line 1
??selectTemplate("Oracle OPSS SCIM Identity Store")
^
SyntaxError: Lexical error at line 1, column 1. Encountered: "\ufffd" (65533), after : ""
wls:/offline/obdx_domain>selectTemplate("Oracle OPSS SCIM Identity Store")
Traceback (innermost last):
(no code object) at line 0
File "<console>", line 1
?selectTemplate("Oracle OPSS SCIM Identity Store")
^
SyntaxError: Lexical error at line 1, column 1. Encountered: "\ufffd" (65533), after : ""
wls:/offline/obdx_domain>selectTemplate("Oracle OPSS SCIM Identity Store")
wls:/offline/obdx_domain>loadTemplates()
wls:/offline/obdx_domain>updateDomain()
Oct 12, 2018 9:36:14 AM oracle.mds
WARNING: MDS-11019: The default CharSet US-ASCII is not a unicode character set. File names with non-ASCII characters may not operate as expected. Check locale settings
.
wls:/offline/obdx_domain>closeDomain()
wls:/offline>
3:07 PM
10/12/2018

Home

5. Change JPS configurations

1. Add the following to the **jps-config.xml** at **<weblogic-domain-path>/config/fmwconfig/**
2. Remove *GenericIdentityStoreProvider serviceProvider* inside **<serviceProviders>** tag:
   - <serviceProvider
     class="oracle.security.jps.internal.idstore.generic.GenericIdentityStoreProvider"
     name="custom.provider" type="IDENTITY_STORE">
     <description>Custom IdStore Provider</description>
     </serviceProvider>
3. Remove *idstore.custom serviceInstance* inside **<serviceInstances>** tag:
   - *<serviceInstance location="dumb" name="idstore.custom" provider="custom.provider">*
     <description>Custom Identity Store Service Instance</description>
     <property name="idstore.type" value="CUSTOM"/>
     <property name="ADF_IM_FACTORY_CLASS"
     value="com.ofss.sms.dbAuthenticator.providers.db.DBIdentityStoreFactory"/>
     <property name="DATASOURCE_NAME" value="DIGX"/>
     </serviceInstance>

Inside the <jpsContext name="default"> tag, if *idstore.custom* is present, then:

- *Change <serviceInstanceRef ref="idstore.custom"/>* to *<serviceInstanceRef ref="idstore.scim"/>*

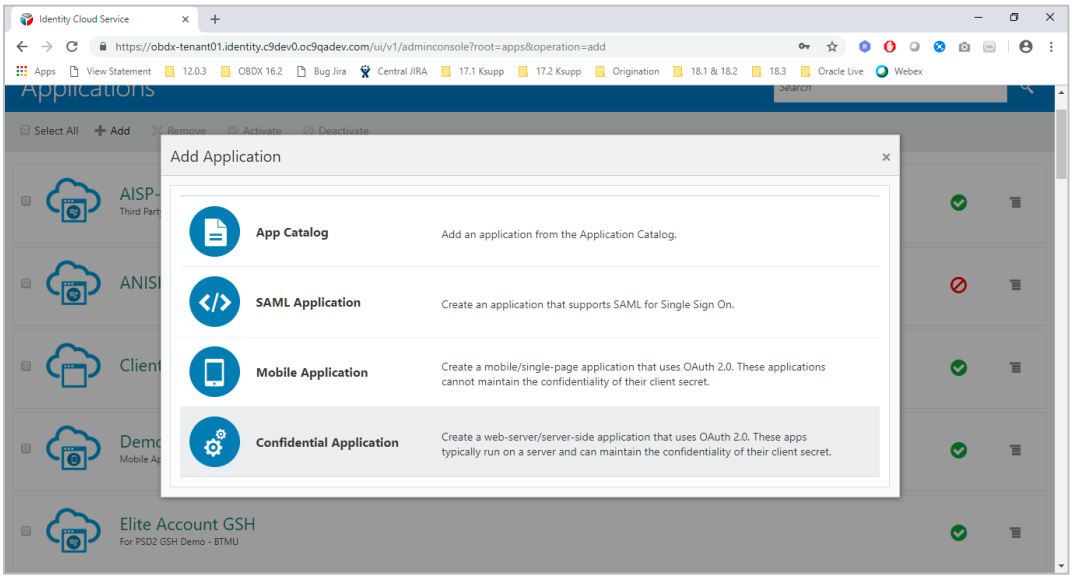
Home

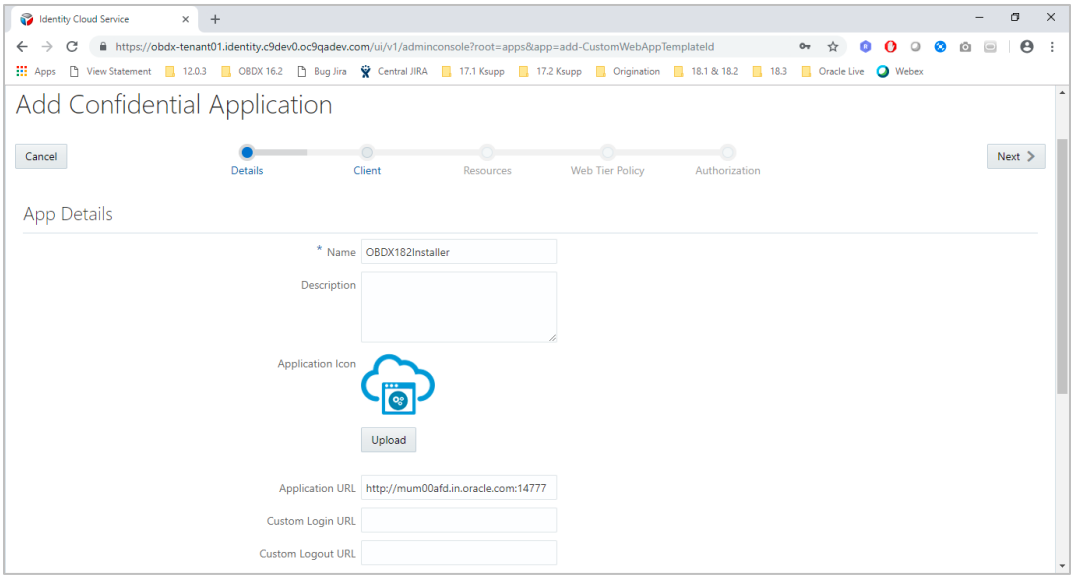
6. Create an OBAPI Client Application in IDCS Console

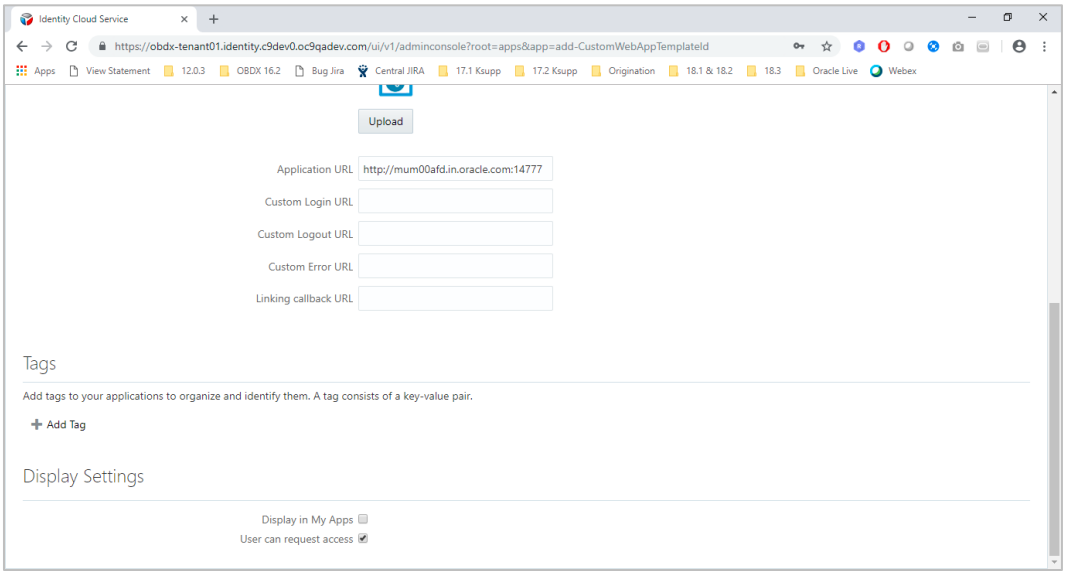
1. Go to IDCS Admin Console → Enter Admin user name and Password.
2. On Applications tab → Click on + sign →Confidential Application

OBAPI Client application details in IDCS:

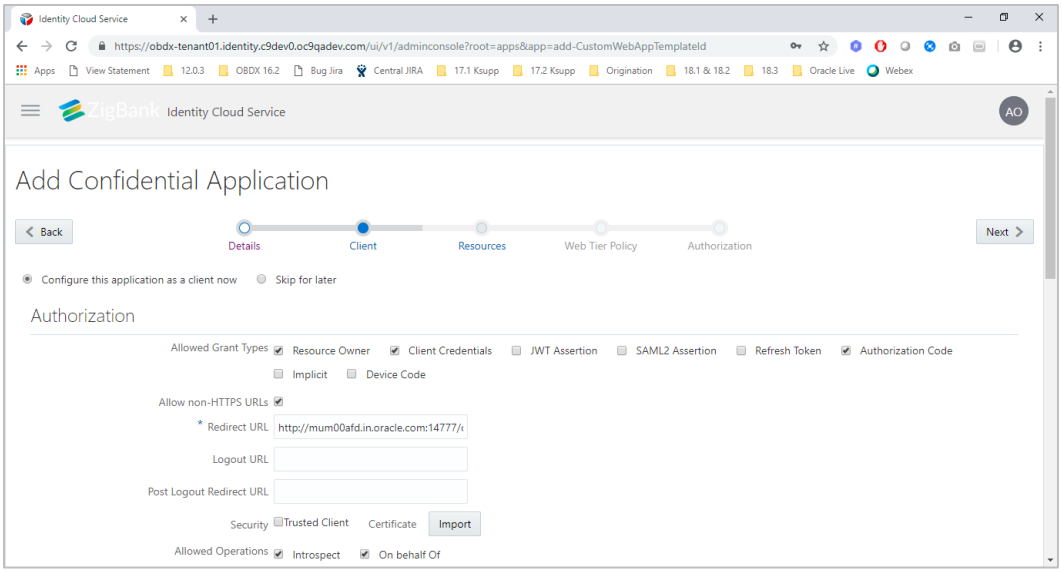
Name	Is the OBAPI Client Application Name in IDCS. Give a suitable name.
connection_scheme	http or https
webserver_host_name	Host name of web server
webserver_port	Port of web server
Application URL	<connection_scheme>://<webserver_host_name>:<webserver_port>
Redirect URL	<Application URL>/oauth/callback
Primary Audience	<Name>
Secondary Audience	<Application URL>

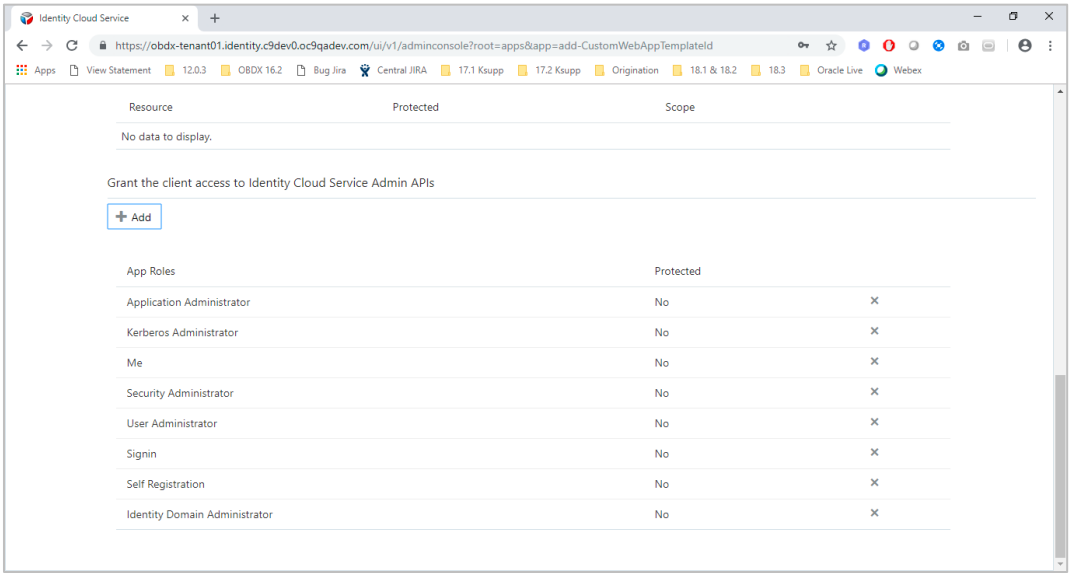



Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
Add Confidential Application
Cancel
Details
Client
Resources
Web Tier Policy
Authorization
Next
App Details
* Name
OBDX182Installer
Description
Application Icon
Upload
Application URL
http://mum00afd.in.oracle.com:14777
Custom Login URL
Custom Logout URL

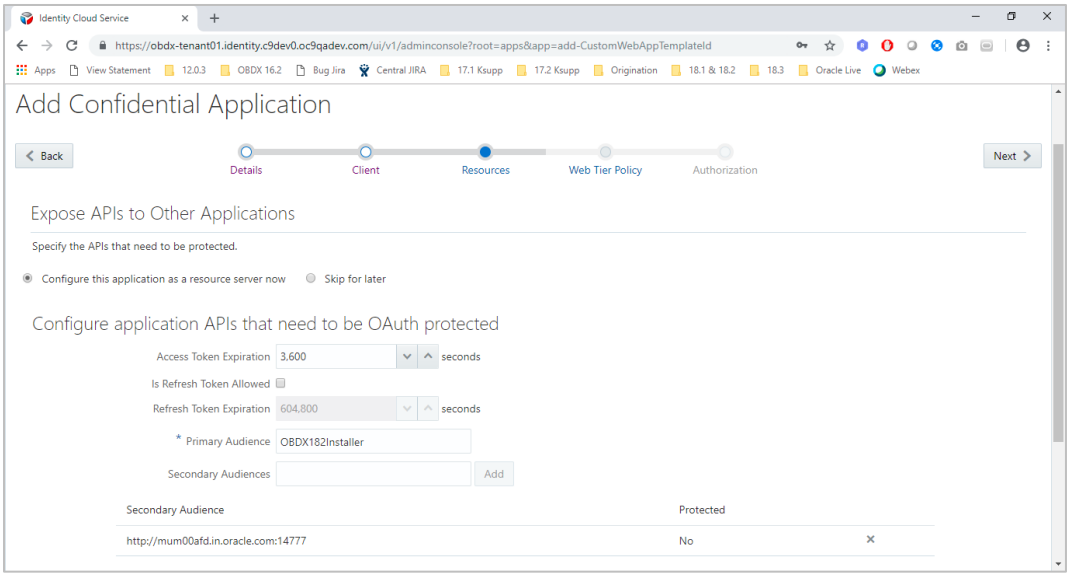

Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
Upload
Application URL
http://mum00afd.in.oracle.com:14777
Custom Login URL
Custom Logout URL
Custom Error URL
Linking callback URL
Tags
Add tags to your applications to organize and identify them. A tag consists of a key-value pair.
Add Tag
Display Settings
Display in My Apps
User can request access

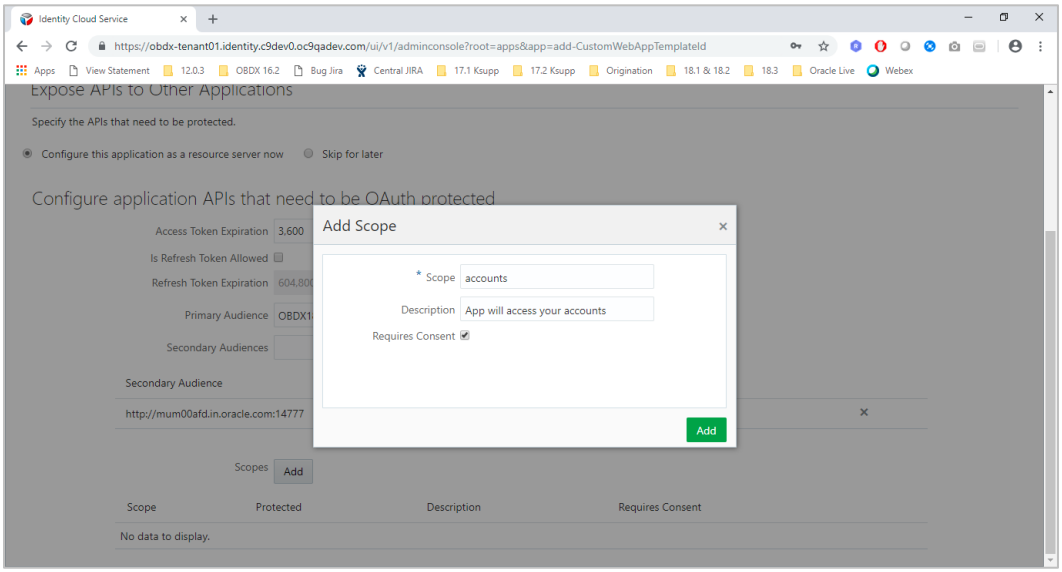
3. Click **Next**

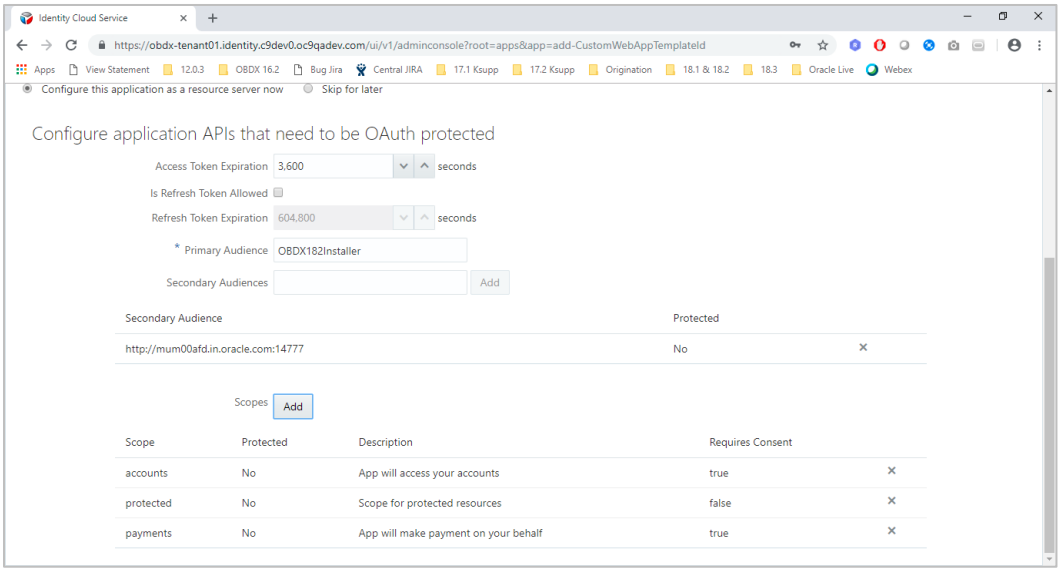

Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
Identity Cloud Service
AO
Add Confidential Application
Back
Details
Client
Resources
Web Tier Policy
Authorization
Next
Configure this application as a client now
Skip for later
Authorization
Allowed Grant Types
Resource Owner
Client Credentials
JWT Assertion
SAML2 Assertion
Refresh Token
Authorization Code
Implicit
Device Code
Allow non-HTTPS URLs
* Redirect URL
http://mum00afd.in.oracle.com:14777/
Logout URL
Post Logout Redirect URL
Security
Trusted Client
Certificate
Import
Allowed Operations
Introspect
On behalf Of


Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
Resource
Protected
Scope
No data to display.
Grant the client access to Identity Cloud Service Admin APIs
Add
App Roles
Protected
Application Administrator
No
Kerberos Administrator
No
Me
No
Security Administrator
No
User Administrator
No
Signin
No
Self Registration
No
Identity Domain Administrator
No

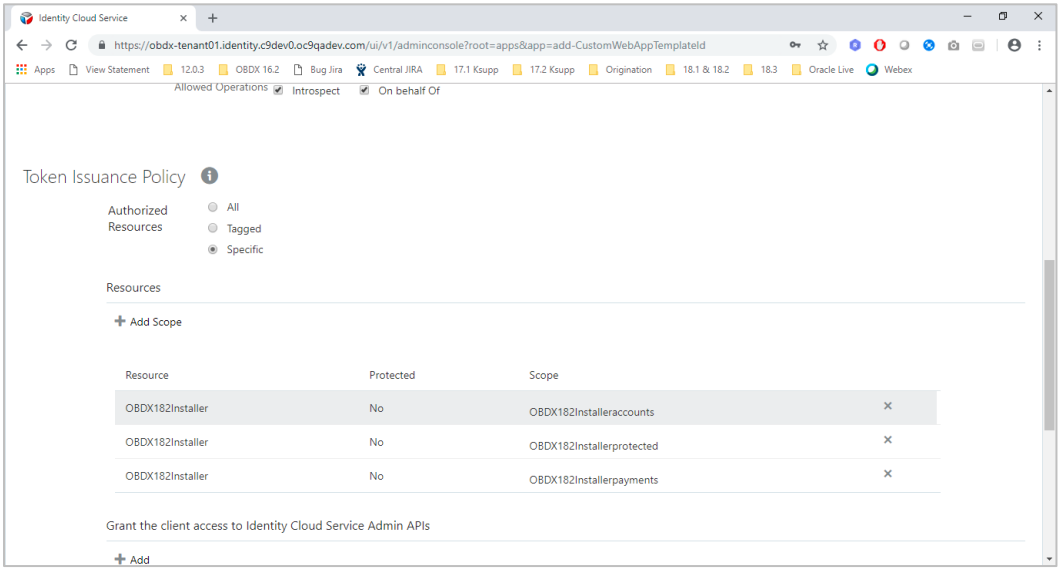
4. Click **Next**


Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
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
Configure application APIs that need to be OAuth protected
Access Token Expiration 3,600 seconds
Is Refresh Token Allowed
Refresh Token Expiration 604,800 seconds
* Primary Audience OBDX182Installer
Secondary Audiences
Add
Secondary Audience
Protected
http://mum00afd.in.oracle.com:14777
No


Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
Expose APIs to Other Applications
Specify the APIs that need to be protected.
Configure this application as a resource server now
Skip for later
Configure application APIs that need to be OAuth protected
Add Scope
* Scope accounts
Description App will access your accounts
Requires Consent
Add
Scopes
Add
Scope
Protected
Description
Requires Consent
No data to display.



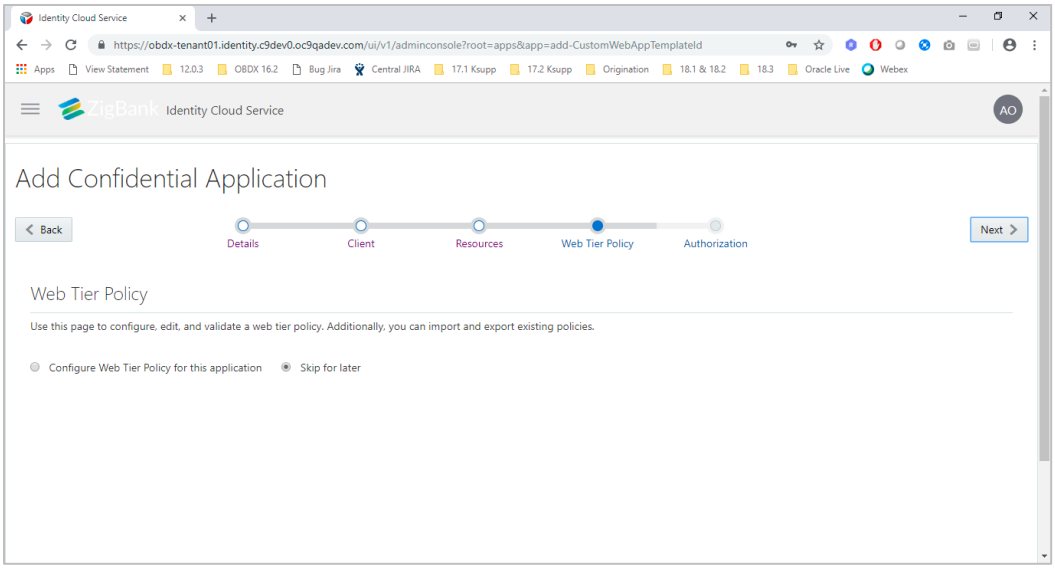
5. Go Back to **Client** tab and **Add Scope**



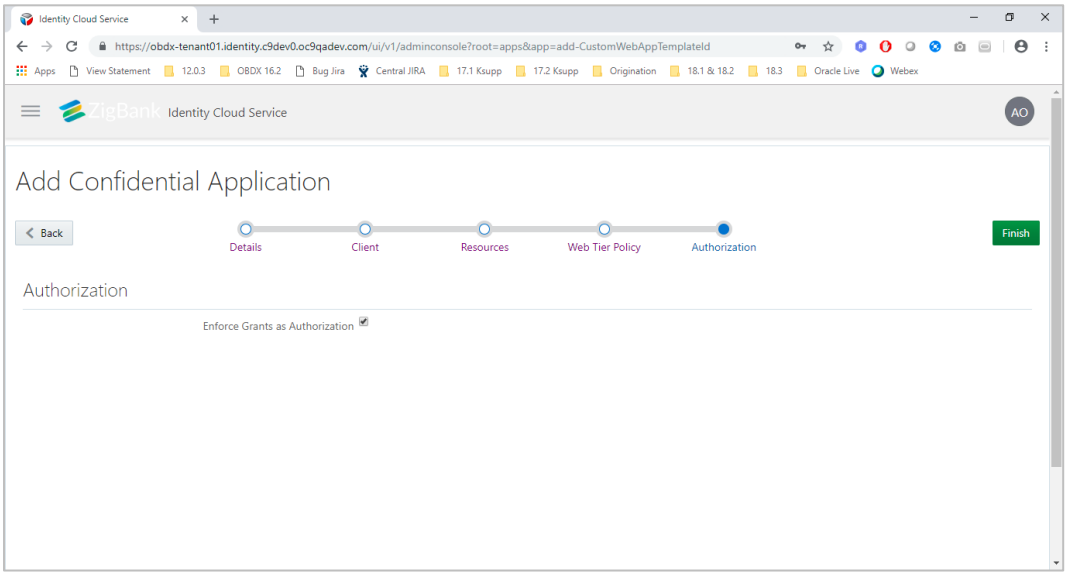
6. Note down the name of protected scope above.

allowed_scope_name_of_protected_in_OBAPI_Client_App	Name of Protected scope. Eg. OBAPI182Installerprotected

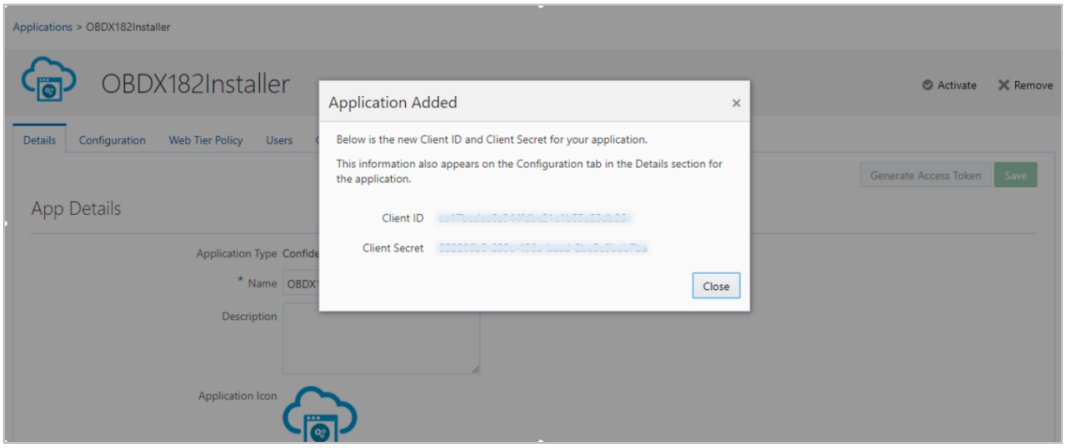
7. Next Go to **Web Tier Policy** tab.



8. Click **Next**



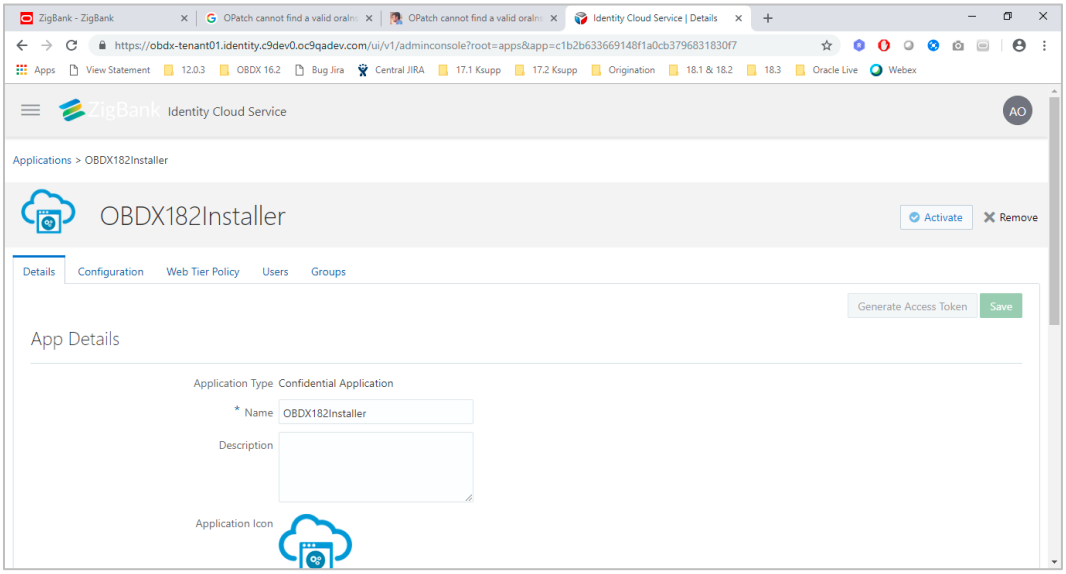
9. Click on **Finish**.



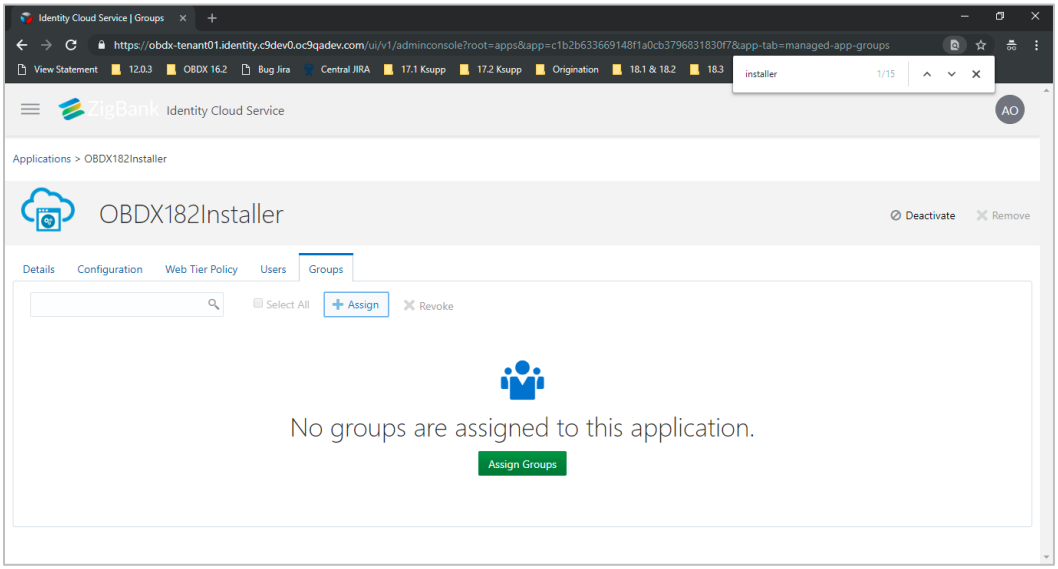
10. You will get **Client ID** and **Client Secret** on successful creation.

Glossary of parameters:

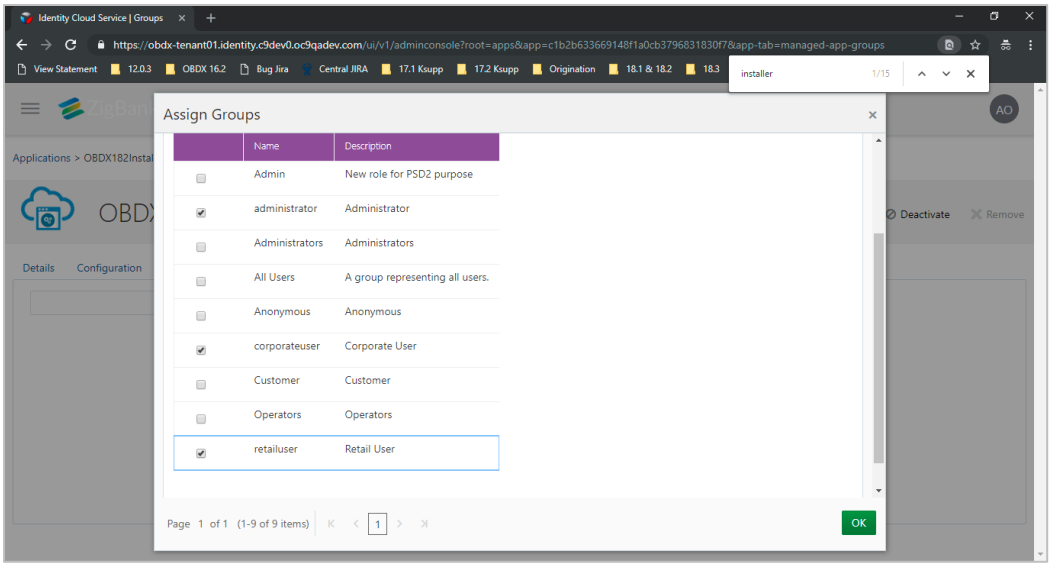
<client_id_of_OBAPI_client_in_IDCS>	Client ID given above
<client_secret_of_OBAPI_client_in_IDCS>	Client Secret given above



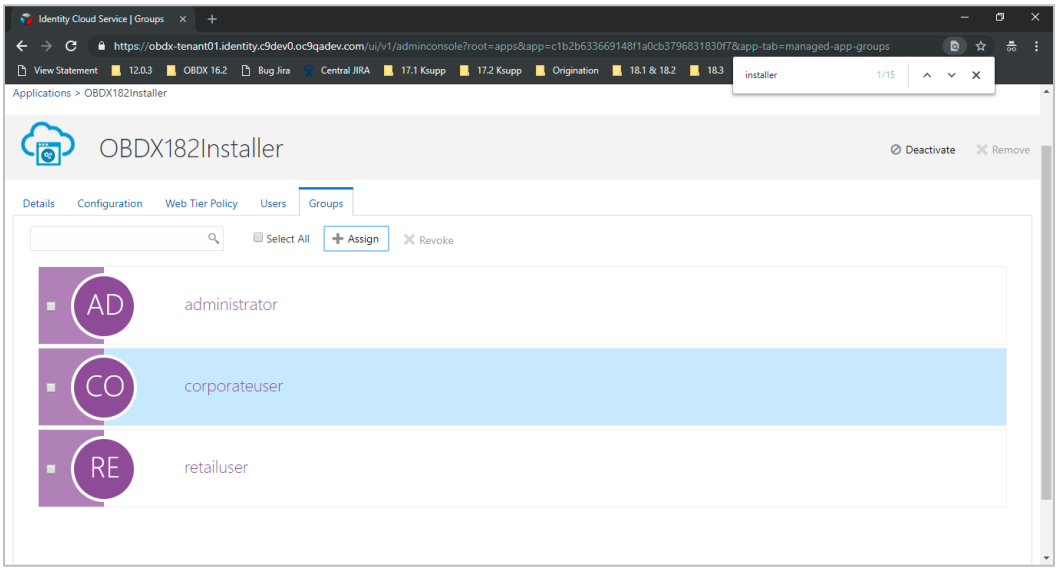
11. Click on **Activate** button.
12. Search for created application and go to **Groups** tab.



13. Click on **Assign**.



14. Click **Add**.



15. Above groups are added.

Home

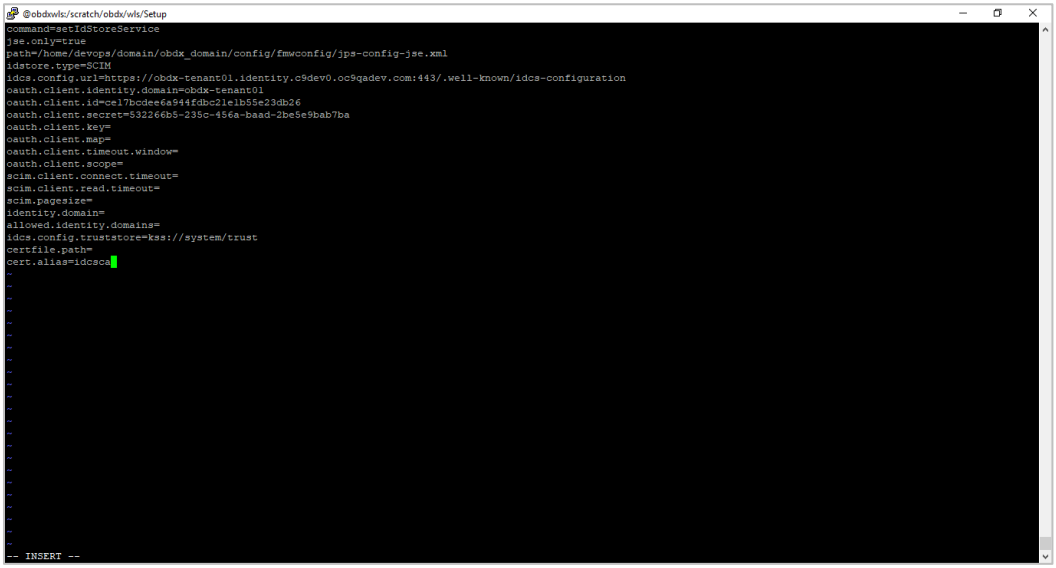
7. Configure OPSS IDCS Identity Store Service

1. Back up **jps-config-jse.xml** at **<weblogic-domain-path>/config/fmwconfig/**

Prepare a command property file named opss_idcs_cmd.props

opss_idcs_cmd.props:

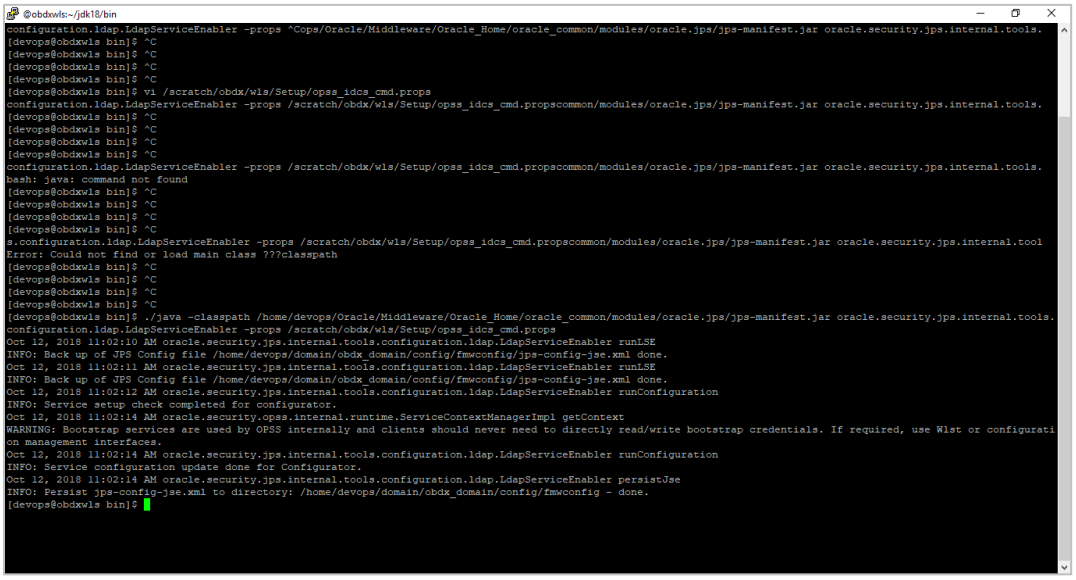
command=setIdStoreService
jse.only=true
path=<weblogic-domain-path>/config/fmwconfig/jps-config-jse.xml
idstore.type=SCIM
idcs.config.url=https://<tenant-base-url>:443/.well-known/idcs-configuration
oauth.client.identity.domain=<tenant-name>
oauth.client.id=<client_id_of_OBAPI_client_in_IDCS>
oauth.client.secret=<client_secret_of_OBAPI_client_in_IDCS>
oauth.client.key=
oauth.client.map=
oauth.client.timeout.window=
oauth.client.scope=
scim.client.connect.timeout=
scim.client.read.timeout=
scim.pagesize=
identity.domain=
allowed.identity.domains=
idcs.config.truststore=kss://system/trust
certfile.path=
cert.alias=idcsca



2. Go to <jdk-path>/bin

Run below command

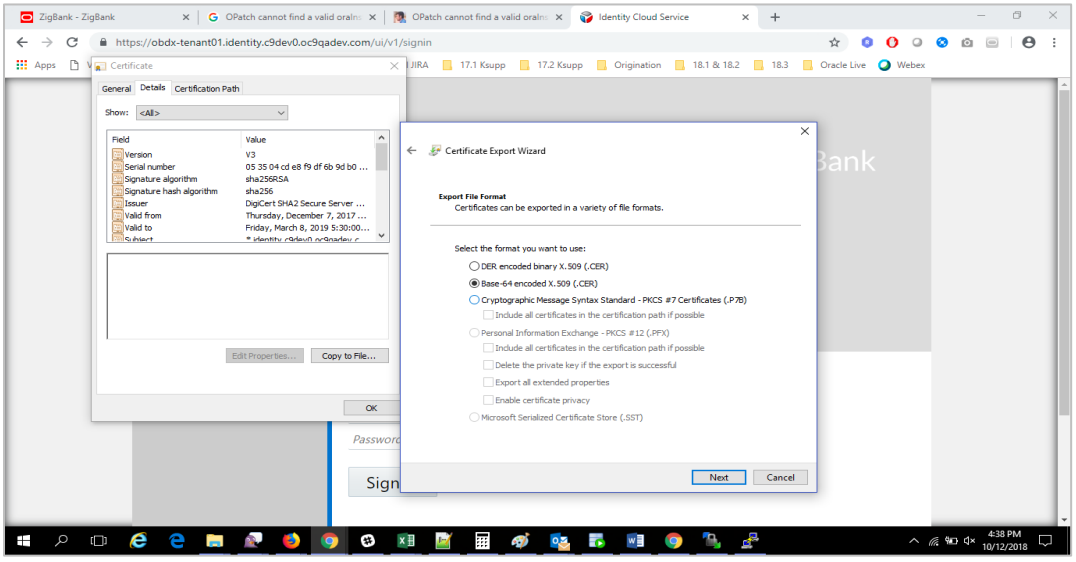
java –classpath <oracle-home-path>/oracle_common/modules/oracle.jps/jps-manifest.jar oracle.security.jps.internal.tools.configuration.ldap.LdapServiceEnabler -props <local-path-of-opss_idcs_cmd.props>



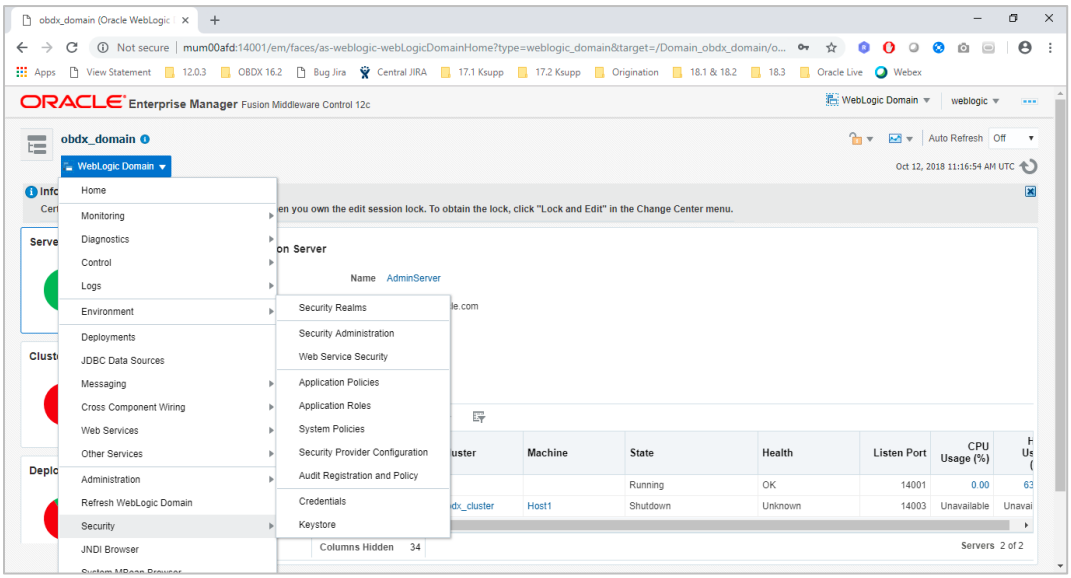
3. To provide cert to SSL connection:

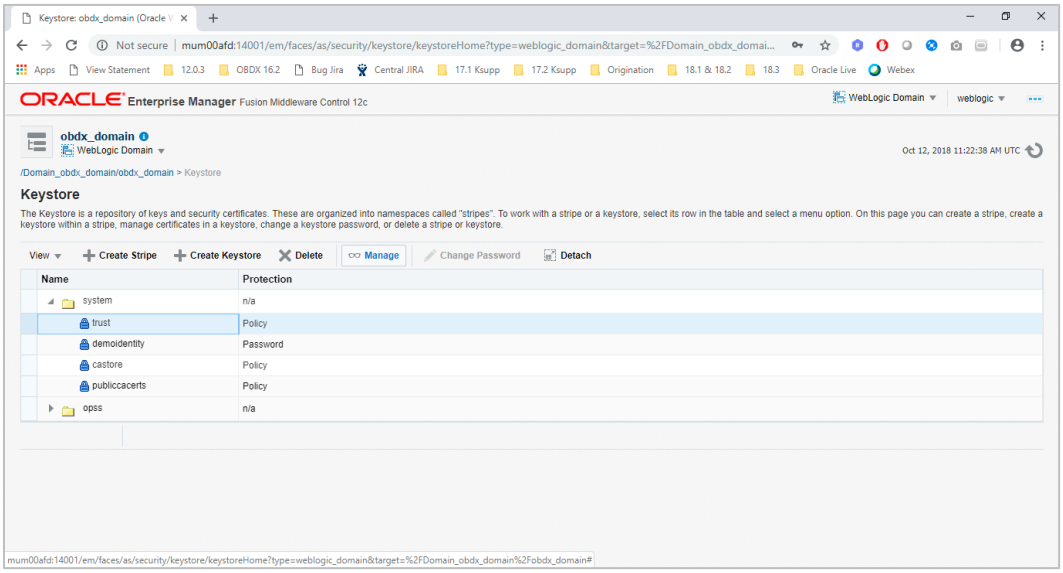
   Start the Weblogic Admin server.

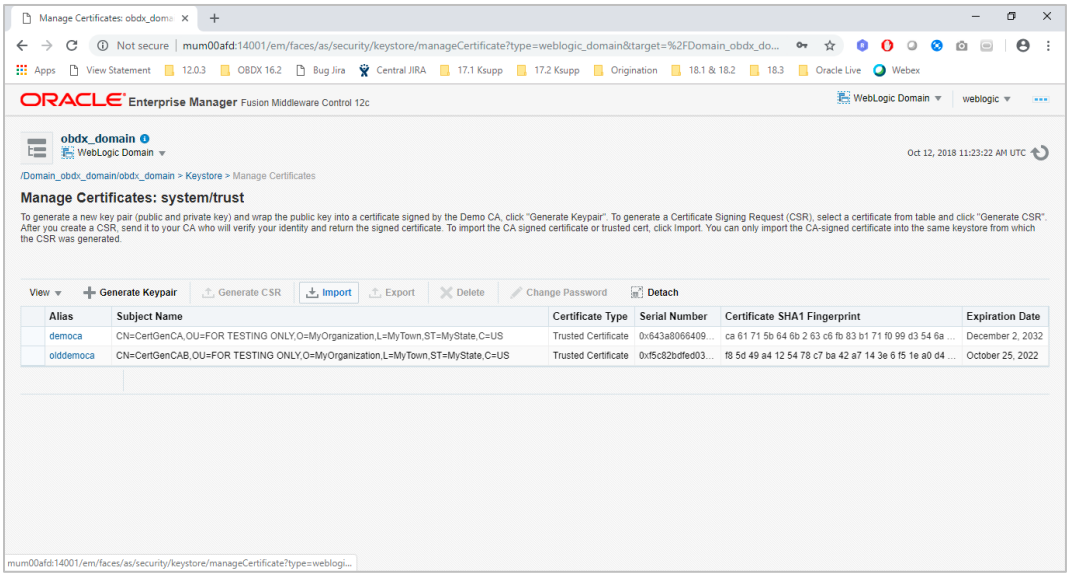
   Download the IDCS certificate from IDCS My console. ‘https://<tenant-base-url> /ui/v1/myconsole’.

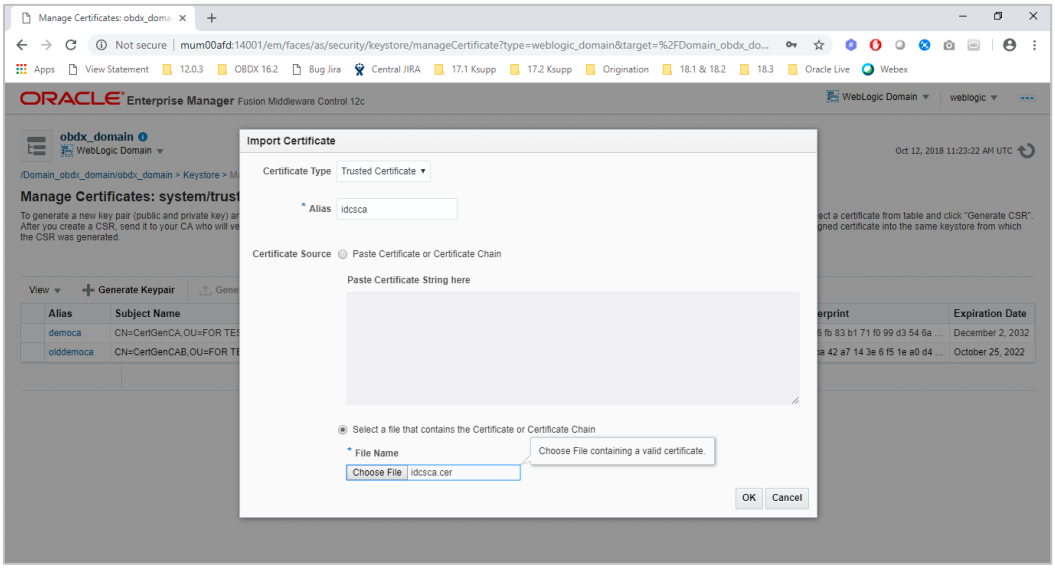


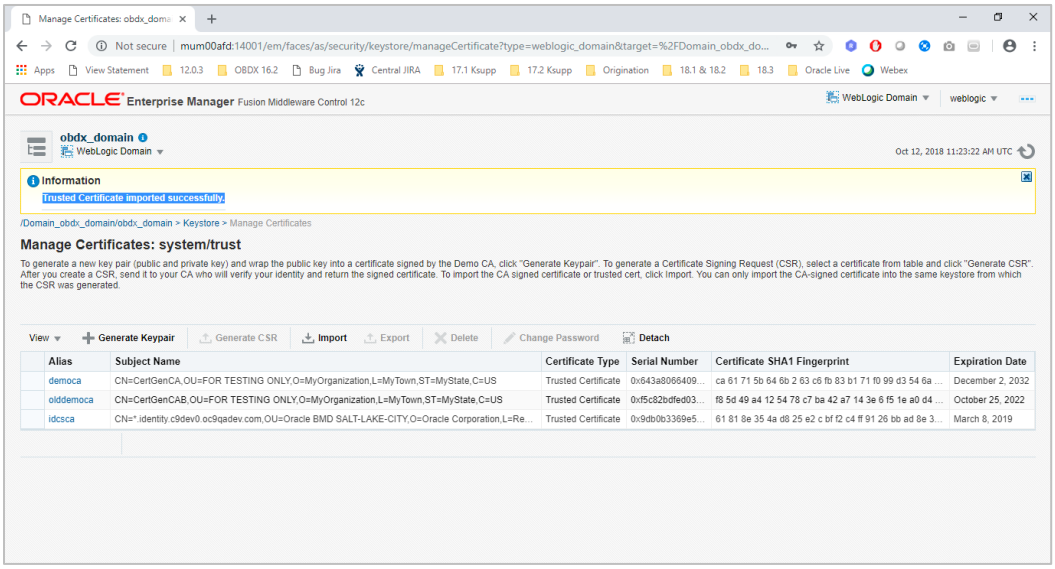
4. Login to weblogic Enterprise Manager (EM) and Import this certificate in EM as '*idcsca*' under kss://system/trust.





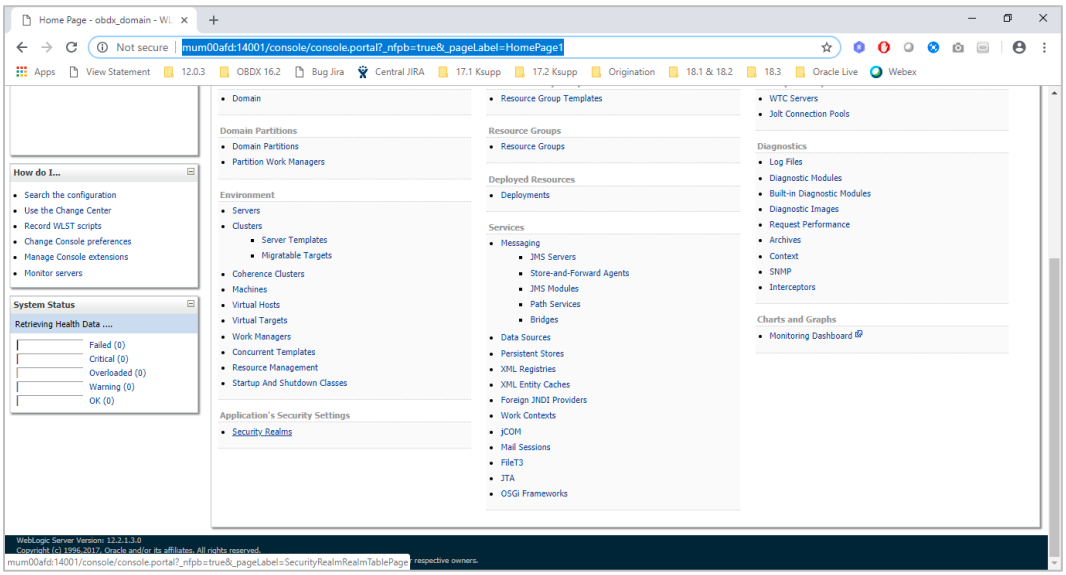

Manage Certificates: obdx_doma
Not secure | mum00afd:14001/em/faces/as/security/keystore/manageCertificate?type=weblogic_domain&target=%2FDomain_obdx_do...
Apps View Statement 12.0.3 OBDX 16.2 Bug Jira Central JIRA 17.1 Ksupp 17.2 Ksupp Origination 18.1 & 18.2 18.3 Oracle Live Webex
ORACLE Enterprise Manager Fusion Middleware Control 12c
WebLogic Domain weblogic
obdx_domain
WebLogic Domain
Oct 12, 2018 11:23:22 AM UTC
/Domain_obdx_domain/obdx_domain > Keystore > Manage Certificates
Manage Certificates: system/trust
To generate a new key pair (public and private key) and wrap the public key into a certificate signed by the Demo CA, click "Generate Keypair". To generate a Certificate Signing Request (CSR), select a certificate from table and click "Generate CSR". After you create a CSR, send it to your CA who will verify your identity and return the signed certificate. To import the CA signed certificate or trusted cert, click Import. You can only import the CA-signed certificate into the same keystore from which the CSR was generated.
View Generate Keypair Generate CSR Import Export Delete Change Password Detach
Alias Subject Name Certificate Type Serial Number Certificate SHA1 Fingerprint Expiration Date
democa CN=CertGenCA,OU=FOR TESTING ONLY,O=MyOrganization,L=MyTown,ST=MyState,C=US Trusted Certificate 0x643a8066409... ca 61 71 5b 64 6b 2 63 c6 fb 83 b1 71 f0 99 d3 54 6a ... December 2, 2032
olddemoca CN=CertGenCAB,OU=FOR TESTING ONLY,O=MyOrganization,L=MyTown,ST=MyState,C=US Trusted Certificate 0xf5c82bdfed03... f8 5d 49 a4 12 54 78 c7 ba 42 a7 14 3e 6 f5 1e a0 d4 ... October 25, 2022
mum00afd:14001/em/faces/as/security/keystore/manageCertificate?type=weblogi...

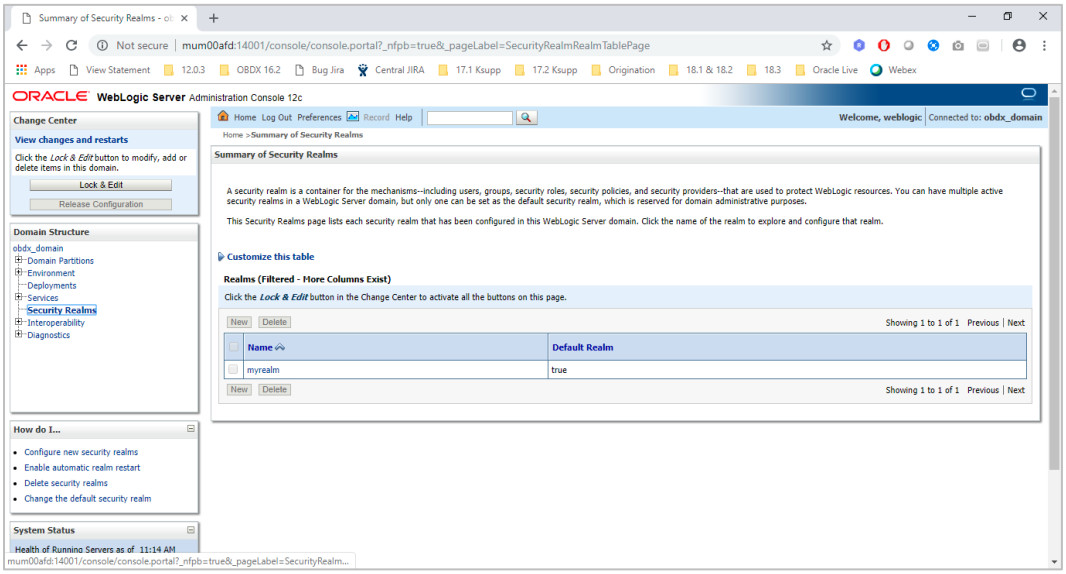

Import Certificate
Certificate Type Trusted Certificate
Alias idcsca
Certificate Source Paste Certificate or Certificate Chain
Paste Certificate String here
Select a file that contains the Certificate or Certificate Chain
File Name
Choose File idcsca.cer
Choose File containing a valid certificate.
OK Cancel

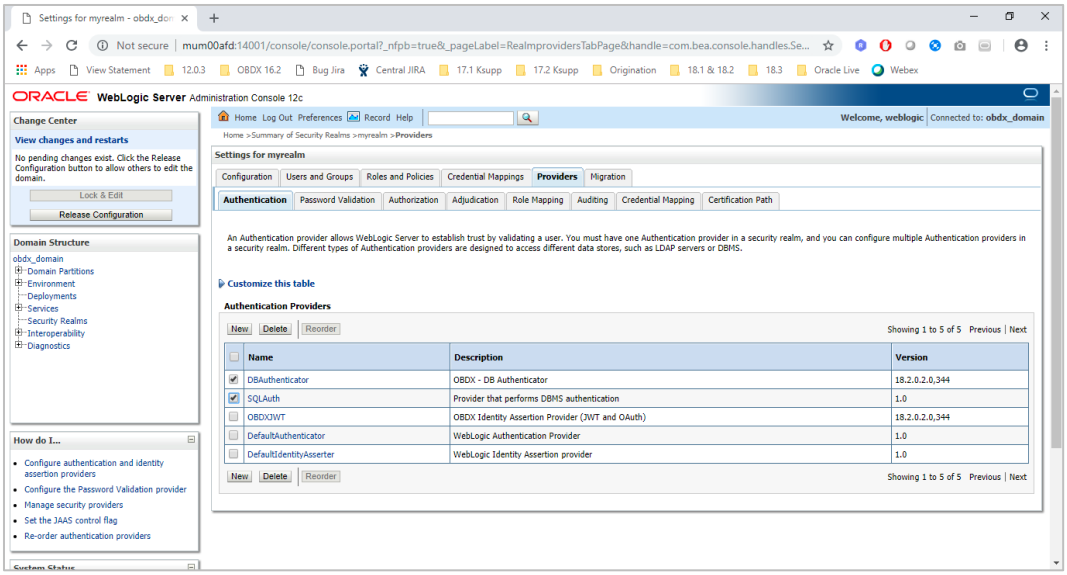

Manage Certificates: obdx_doma
Not secure
mum00afd:14001/em/faces/as/security/keystore/manageCertificate?type=weblogic_domain&target=%2FDomain_obdx_do...
Apps
View Statement
12.0.3
OBDX 16.2
Bug Jira
Central JIRA
17.1 Ksupp
17.2 Ksupp
Origination
18.1 & 18.2
18.3
Oracle Live
Webex
ORACLE Enterprise Manager Fusion Middleware Control 12c
WebLogic Domain
weblogic
obdx_domain
WebLogic Domain
Oct 12, 2018 11:23:22 AM UTC
Information
Trusted Certificate imported successfully.
/Domain_obdx_domain/obdx_domain > Keystore > Manage Certificates
Manage Certificates: system/trust
To generate a new key pair (public and private key) and wrap the public key into a certificate signed by the Demo CA, click "Generate Keypair". To generate a Certificate Signing Request (CSR), select a certificate from table and click "Generate CSR". After you create a CSR, send it to your CA who will verify your identity and return the signed certificate. To import the CA signed certificate or trusted cert, click Import. You can only import the CA-signed certificate into the same keystore from which the CSR was generated.
View
Generate Keypair
Generate CSR
Import
Export
Delete
Change Password
Detach
Alias
Subject Name
Certificate Type
Serial Number
Certificate SHA1 Fingerprint
Expiration Date
democa
CN=CertGenCA,OU=FOR TESTING ONLY,O=MyOrganization,L=MyTown,ST=MyState,C=US
Trusted Certificate
0x643a8066409...
ca 61 71 5b 64 6b 2 63 c6 fb 83 b1 71 f0 99 d3 54 6a ...
December 2, 2032
olddemoca
CN=CertGenCAB,OU=FOR TESTING ONLY,O=MyOrganization,L=MyTown,ST=MyState,C=US
Trusted Certificate
0xf5c82bdfed03...
f8 5d 49 a4 12 54 78 c7 ba 42 a7 14 3e 6 f5 1e a0 d4 ...
October 25, 2022
idcsca
CN=".identity.c9dev0.oc9qadev.com,OU=Oracle BMD SALT-LAKE-CITY,O=Oracle Corporation,L=Re...
Trusted Certificate
0x9db0b3369e5...
61 81 8e 35 4a d8 25 e2 c bf f2 c4 ff 91 26 bb ad 8e 3...
March 8, 2019

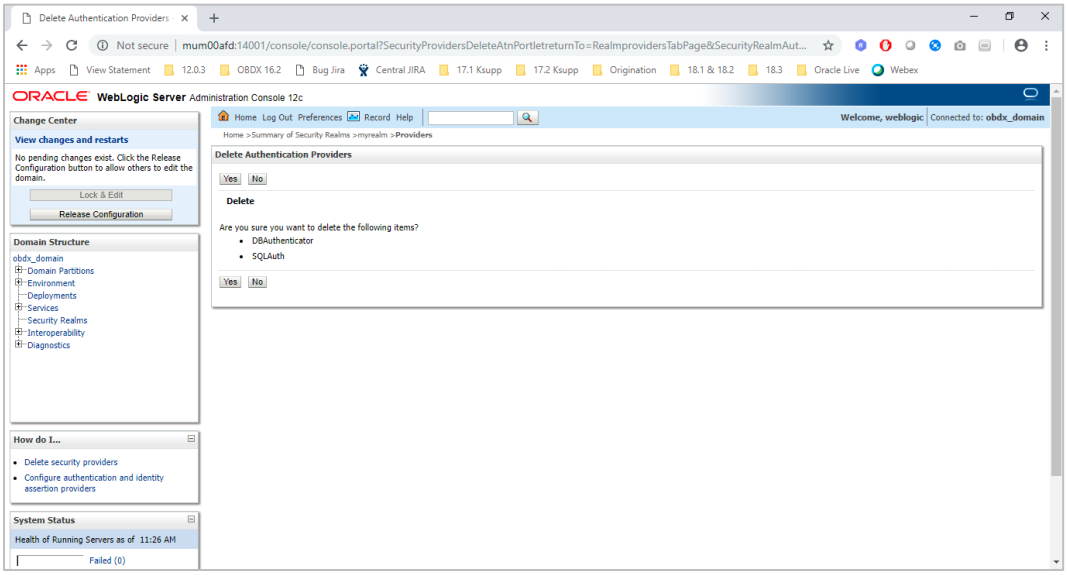
Home

8. Adding IDCS as an Identity Provider in Weblogic Security Realms

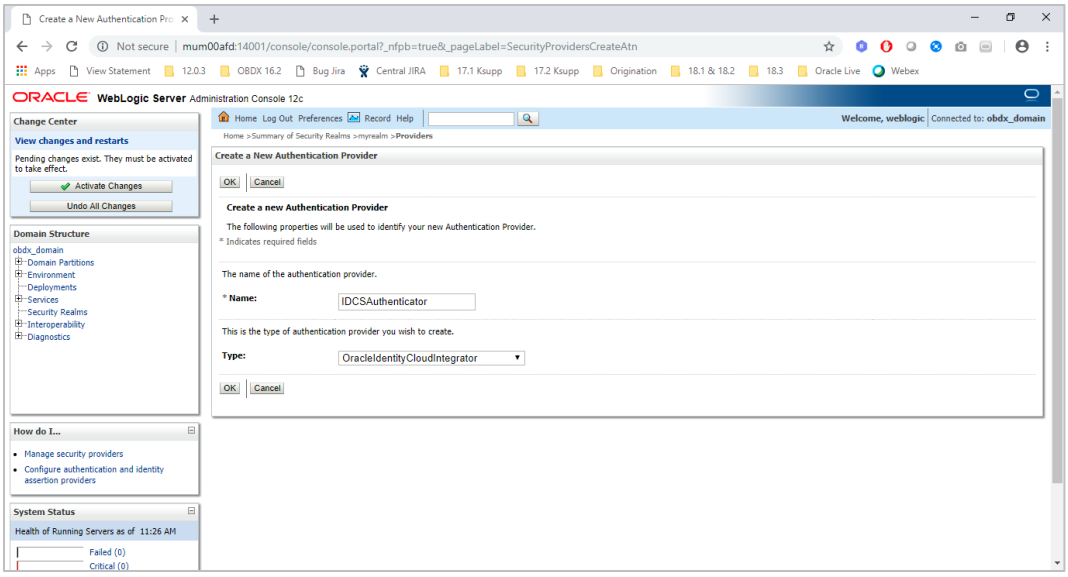




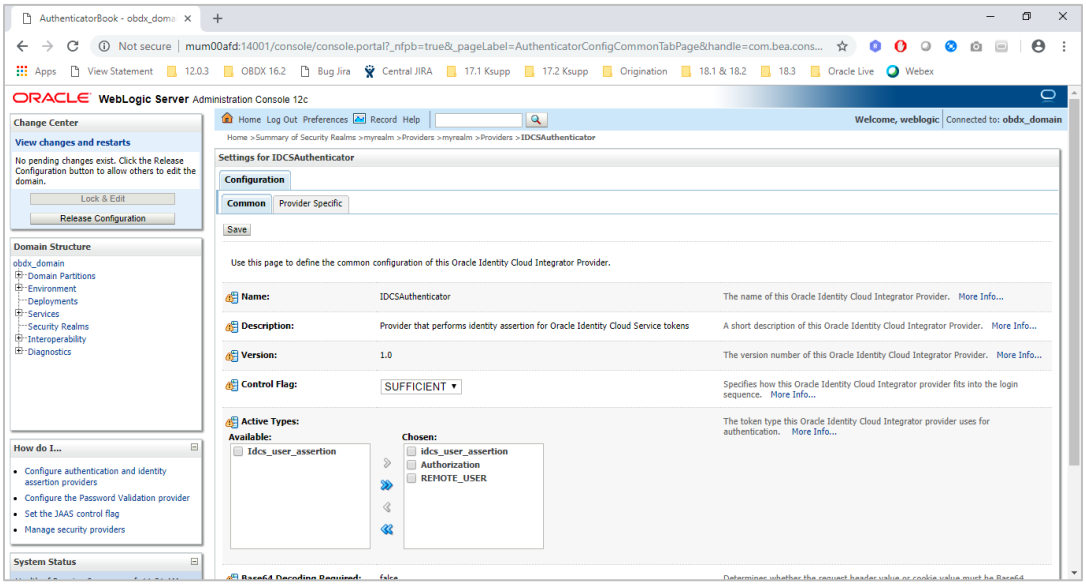




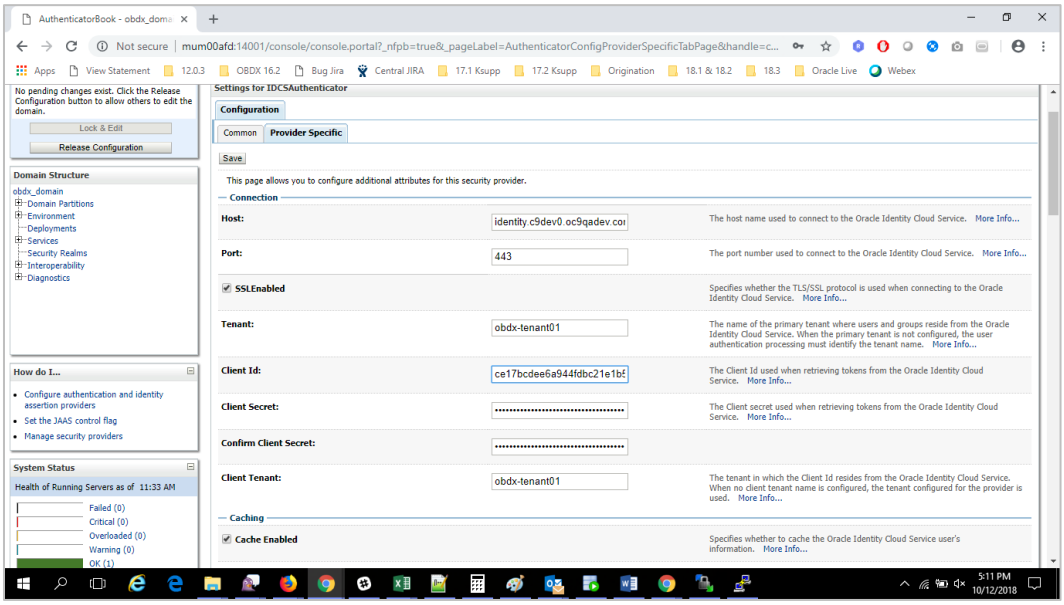
5. Delete *DBAuthenticator* and *SQLAuth* from the list of Authenticator Providers.
6. Create a New Provider.
    - Name : IDCSAuthenticator
    - Type : OracleIdentityCloudIntegrator

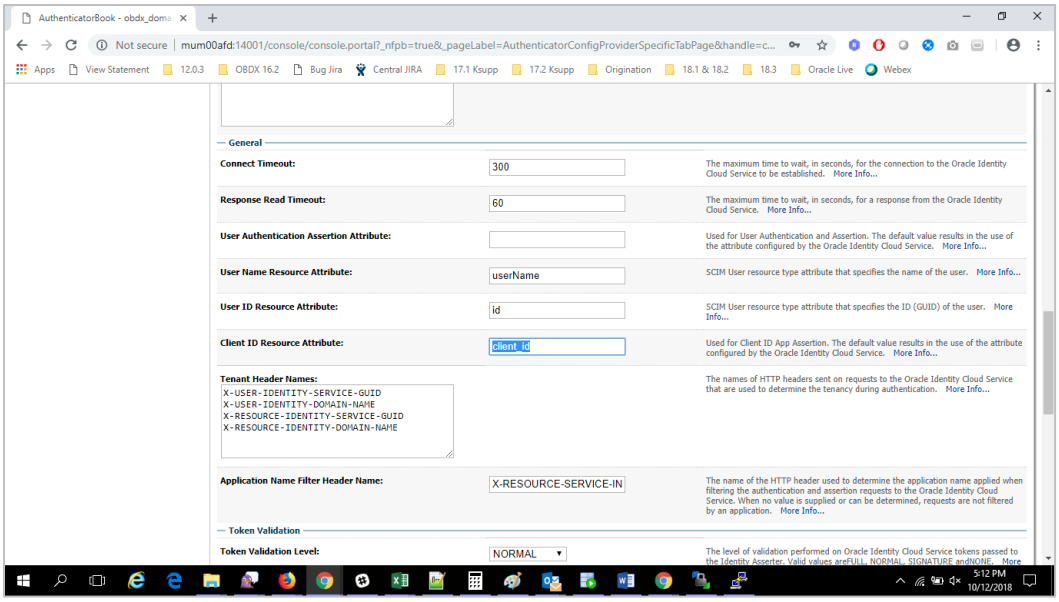


7. IDCSAuthenticator > Configurations > Common
   - Control Flag: SUFFICIENT
   - Active Types:
     i. Available: Idcs_user_assertion
     ii. Chosen: idcs_user_assertion, Authorization, IDCS_REMOTE_USER, REMOTE_USER

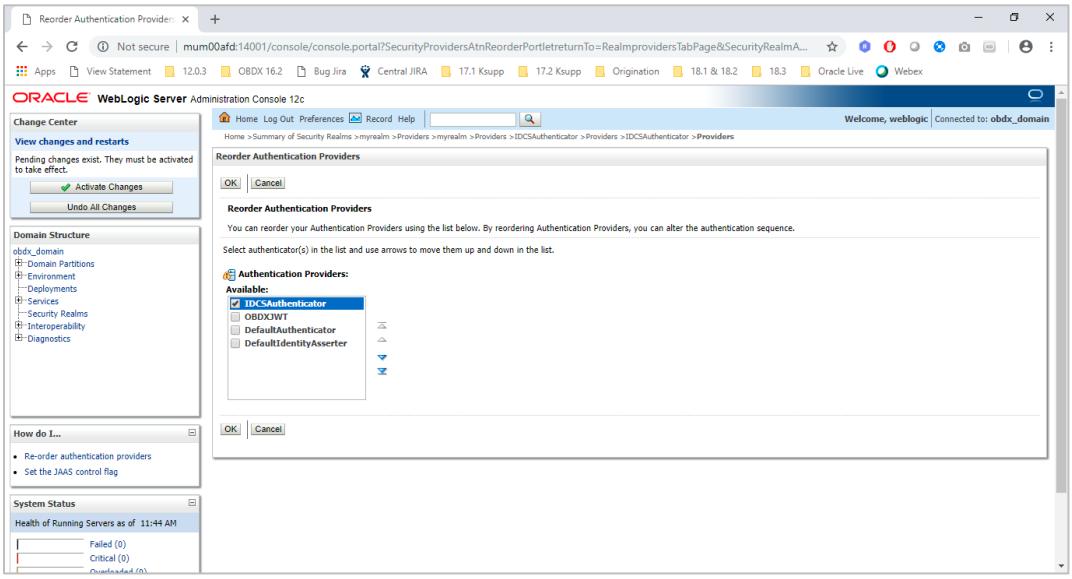


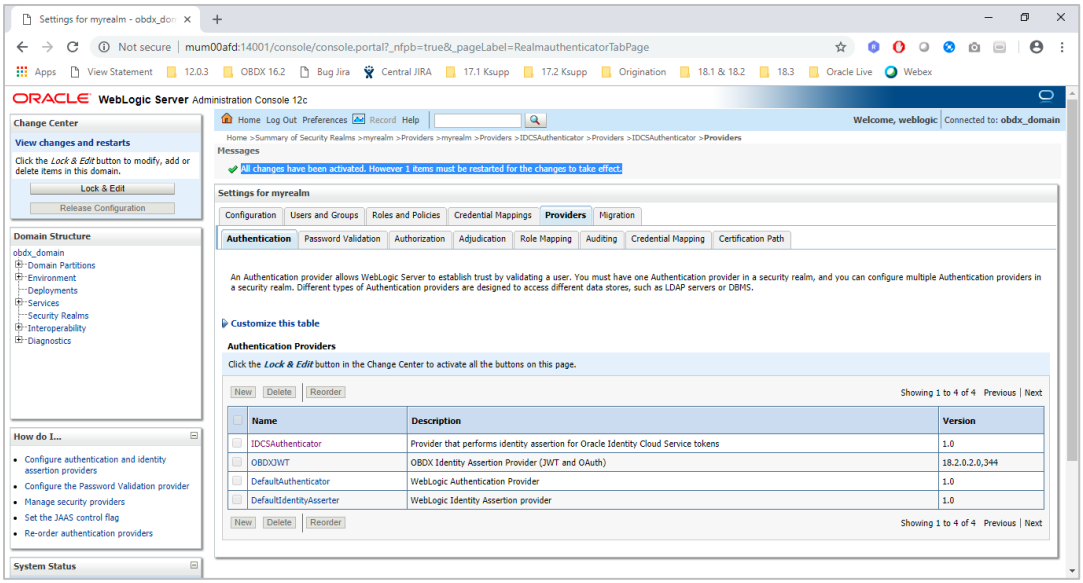
8. IDCSAuthenticator > Configurations > Provider Specific
    - Port: *443*
    - Tenant Names: *<tenant_name>*
    - SSLEnabled: *True*
    - Client IDResource Attribute: *client_id*
    - Client Id: *<client_ID_of_OBAPI_client_in_IDCS>*
    - Client Tenant: *<tenant_name>*
    - Tenant: *<tenant_name>*
    - Host: *<base-url>*
    - Client Secret: *<client_secret_of_OBAPI_client_in_IDCS>*





9. Reorder IDCSAuthenticator to the top of all providers.



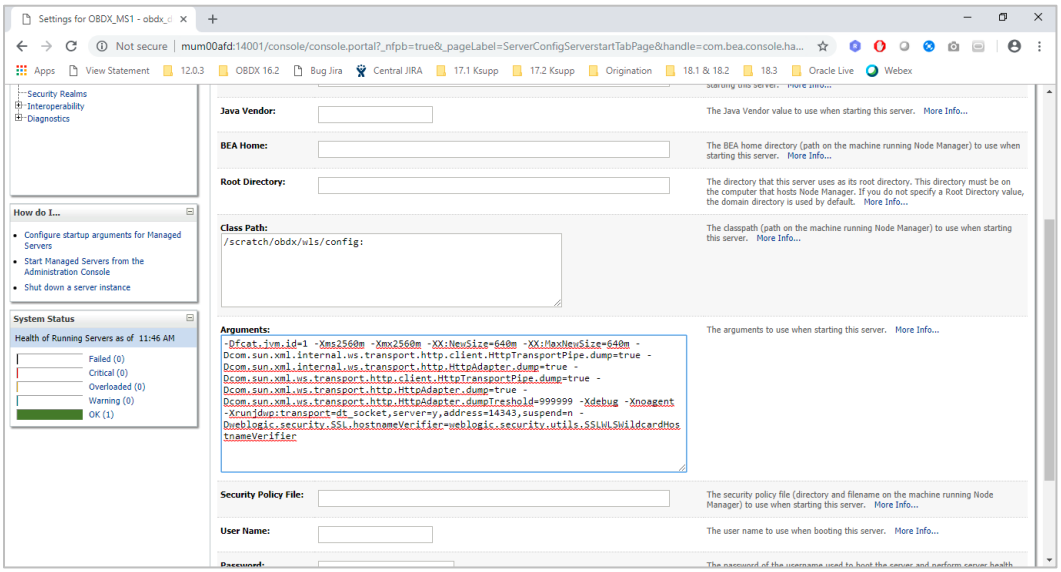

Settings for myrealm - obdx_dor
Not secure | mum00afd:14001/console/console.portal?_nfpb=true&_pageLabel=RealmauthenticatorTabPage
ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Click the Lock & Edit button to modify, add or delete items in this domain.
Lock & Edit
Release Configuration
Domain Structure
obdx_domain
Domain Partitions
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure authentication and identity assertion providers
Configure the Password Validation provider
Manage security providers
Set the JAAS control flag
Re-order authentication providers
System Status
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: obdx_domain
Home >Summary of Security Realms >myrealm >Providers >myrealm >Providers >IDCSAuthenticator >Providers >IDCSAuthenticator >Providers
Messages
All changes have been activated. However 1 items must be restarted for the changes to take effect.
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.
New | Delete | Reorder
Showing 1 to 4 of 4 Previous | Next
Name | Description | Version
IDCSAuthenticator | Provider that performs identity assertion for Oracle Identity Cloud Service tokens | 1.0
OBDXJWT | OBDX Identity Assertion Provider (JWT and OAuth) | 18.2.0.2.0,344
DefaultAuthenticator | WebLogic Authentication Provider | 1.0
DefaultIdentityAsserter | WebLogic Identity Assertion provider | 1.0
New | Delete | Reorder
Showing 1 to 4 of 4 Previous | Next

Home

9. Application Server Changes

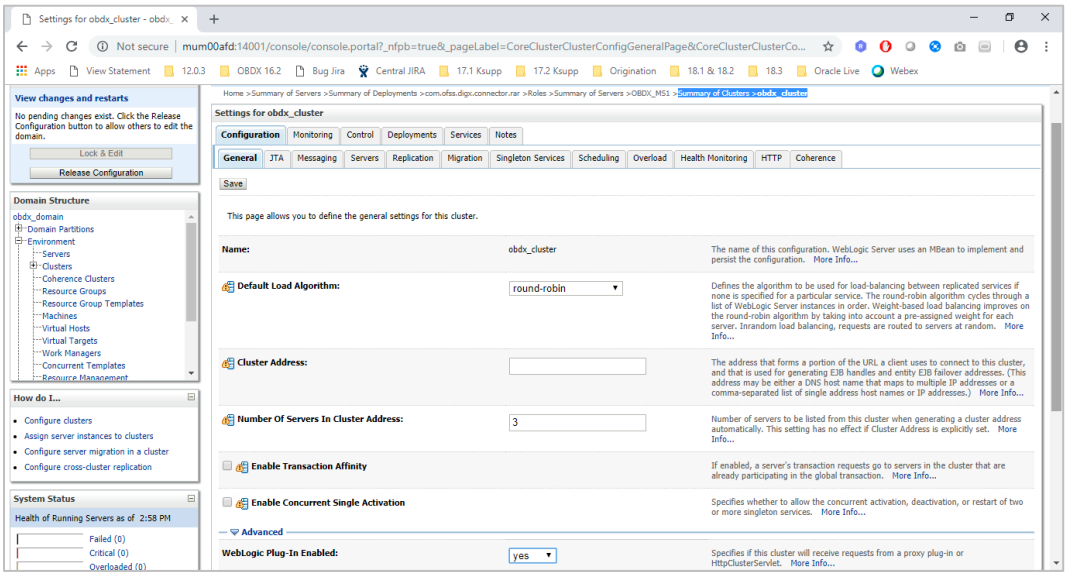
9.1 Add below argument to Managed server:

Dweblogic.security.SSL.hostnameVerifier=weblogic.security.utils.SSLWLSWildcardHostnameVerifier



9.2 Managed Server Start Configurations

1. Go to Home > Summary of Clusters > obapi_cluster > Configuration Tab > General Tab >
2. Expand **Advanced** Section.
3. Set the Value of **WebLogic Plug-In Enabled** to **yes**.

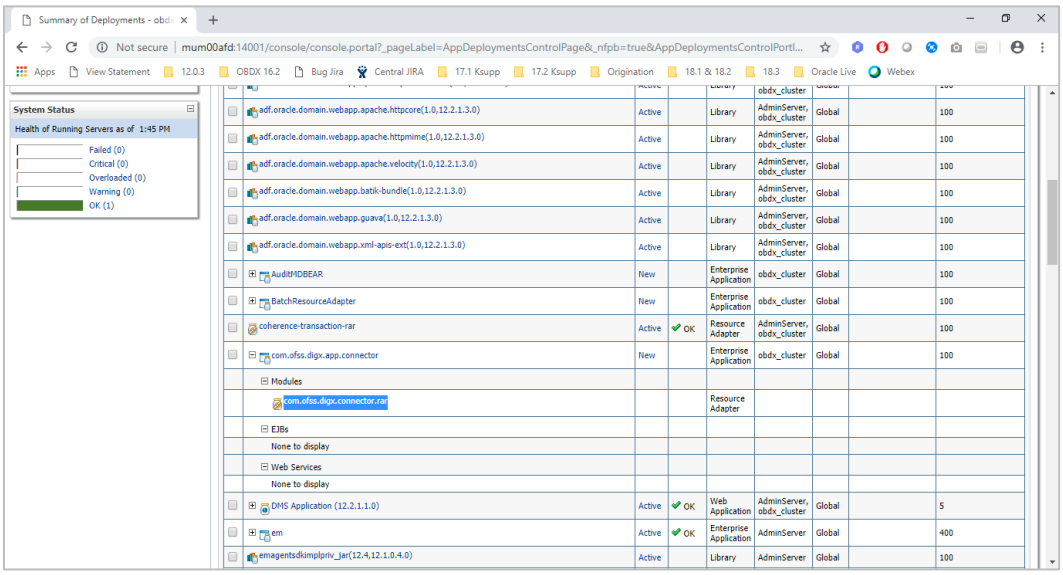


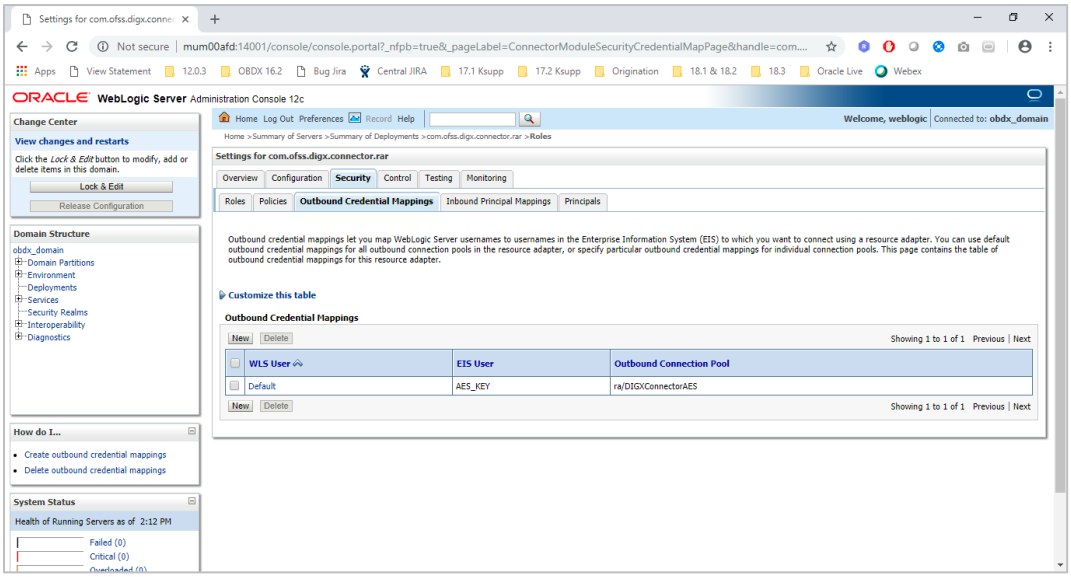
Home

10. Change in Weblogic Deployments

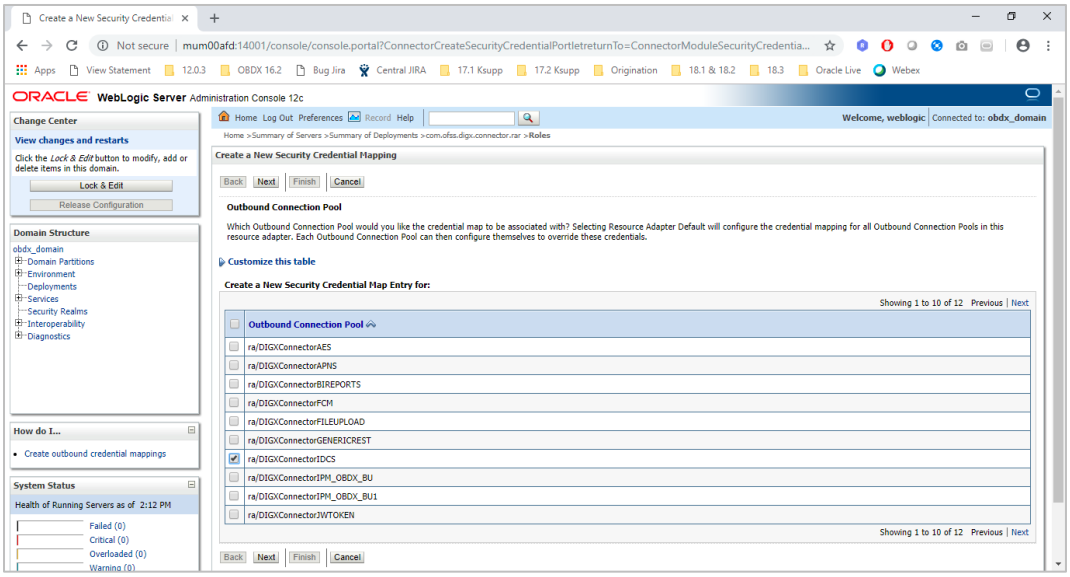
10.1 Creating a Connection in Connector ear

1. Start the managed server if it is down.
2. Summary of Deployments > com.ofss.digx.connector.rar > Security > Outbound Credential Mappings

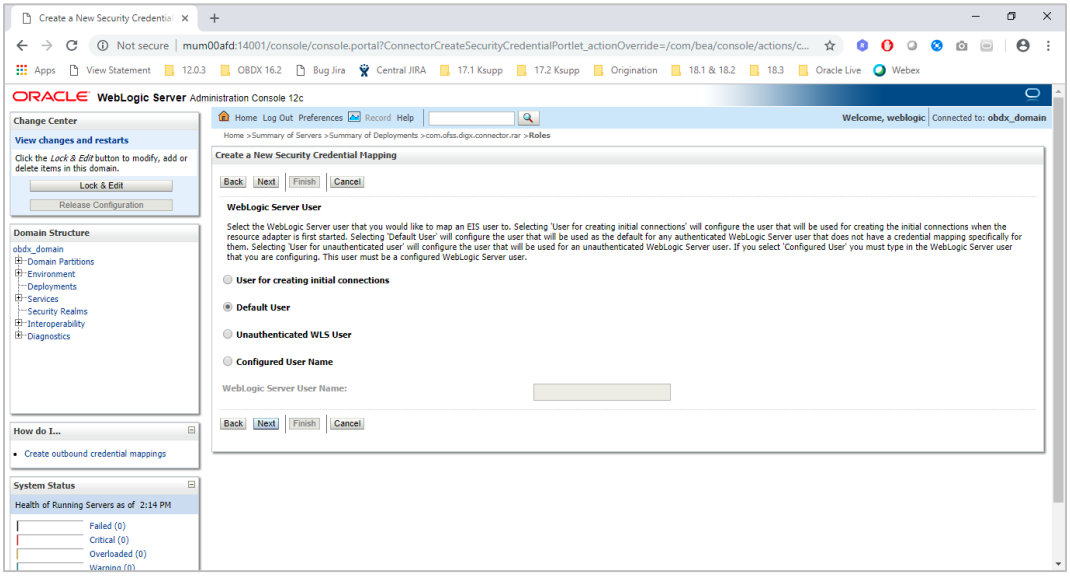




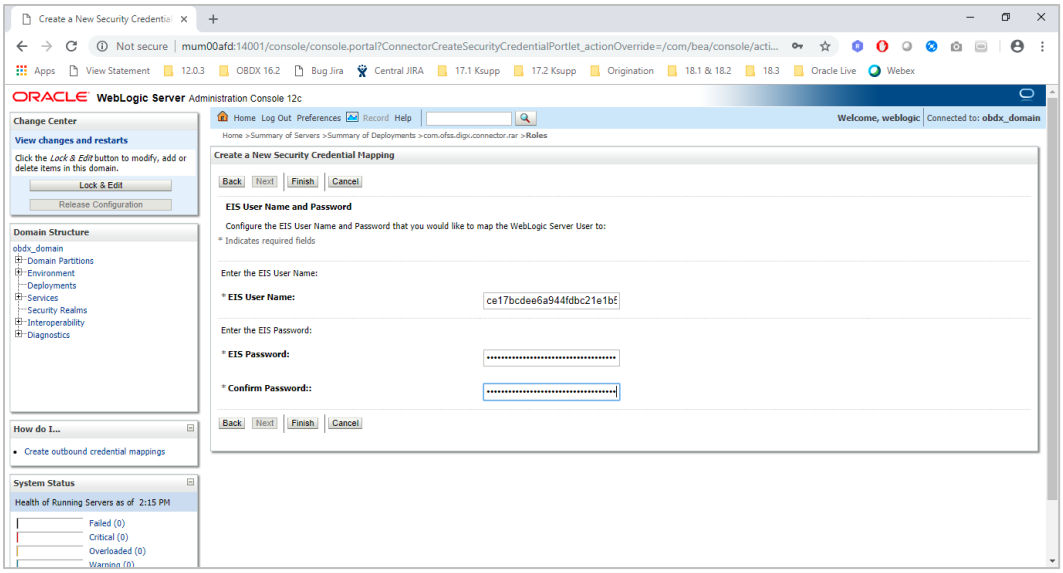
3. Click **New**



4. Click **Next**

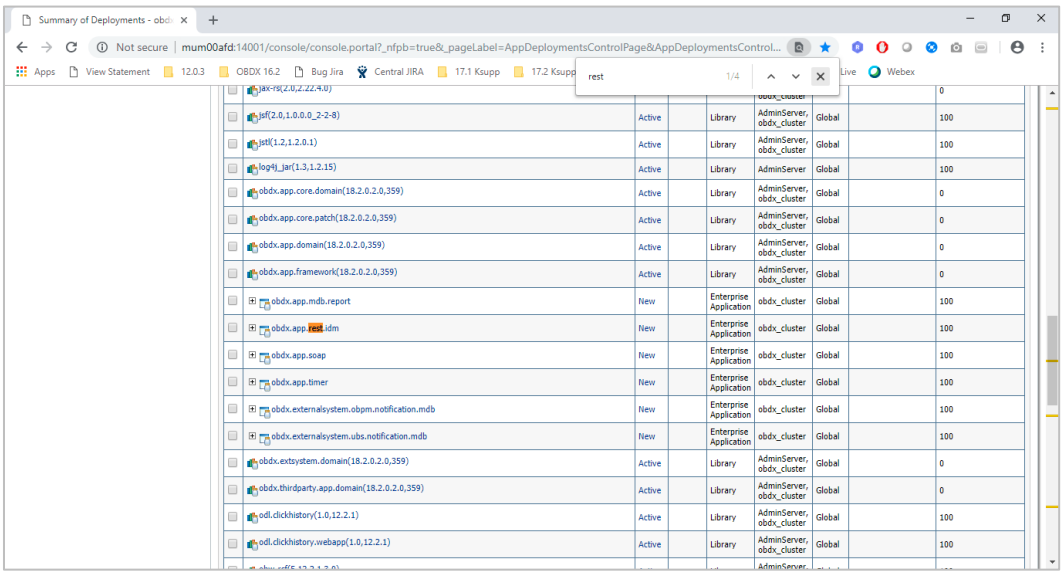


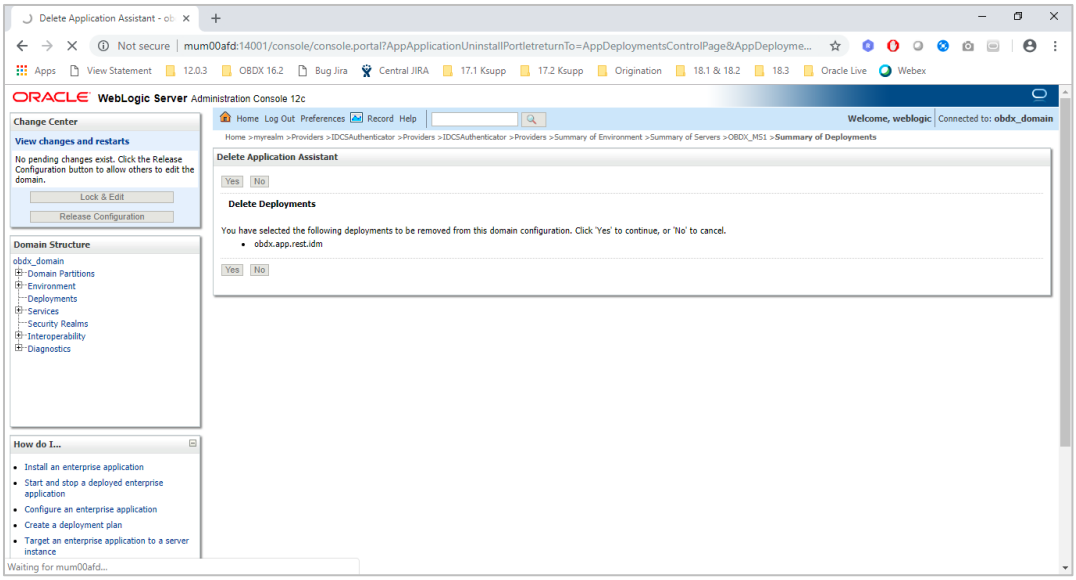
5. Click **Next**
6. Create a new Security Credential Mapping –
   - Outbound Connection Pool: **ra/DIGXConnectorIDCS**
   - WebLogic Server User: **Default**
   - EIS User Name: **<client_id_of_OBAPI_client_in_IDCS>**
   - EIS Password: **<client_secret_of_OBAPI_client_in_IDCS>**

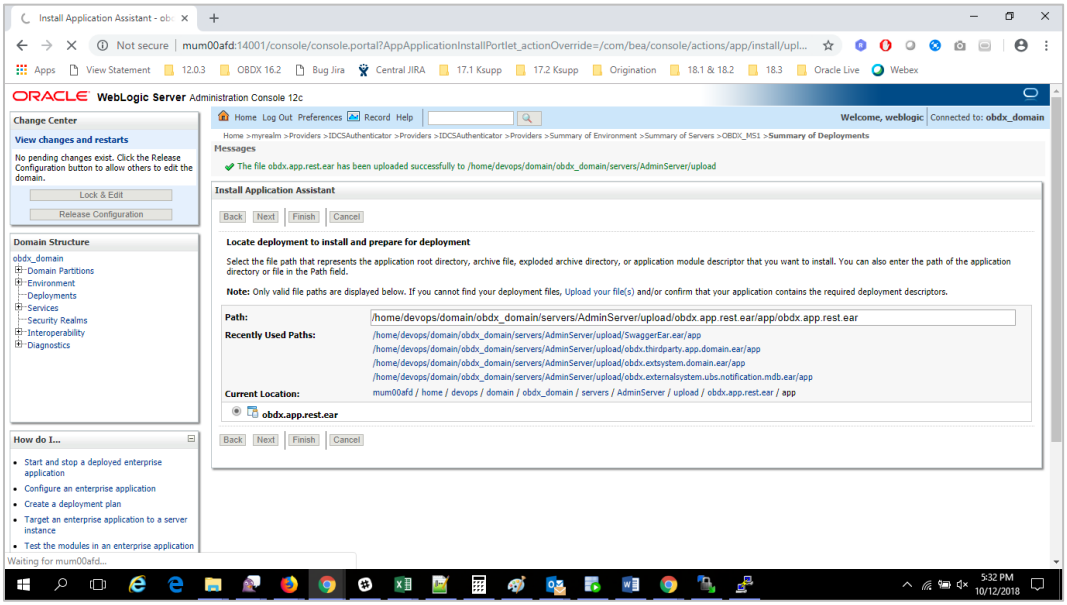


7. Click **Finish**

   a. Delete **obapi.app.rest.idm.ear** and install deployment **obapi.app.rest.ear** from <Installer_Path>\OBAPI_Patch_Installer\installables\app\components\obapi\deploy\obapi.app.rest.ear in **Installer.zip**.




Delete Application Assistant
Not secure
mum00afd:14001/console/console.portal?AppApplicationUninstallPortletreturnTo=AppDeploymentsControlPage&AppDeployme...
ORACLE WebLogic Server Administration Console 12c
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
obdx_domain
Domain Partitions
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Install an enterprise application
Start and stop a deployed enterprise application
Configure an enterprise application
Create a deployment plan
Target an enterprise application to a server instance
Welcome, weblogic
Connected to: obdx_domain
Delete Application Assistant
Yes
No
Delete Deployments
You have selected the following deployments to be removed from this domain configuration. Click 'Yes' to continue, or 'No' to cancel.
obdx.app.rest.idm
Waiting for mum00afd...

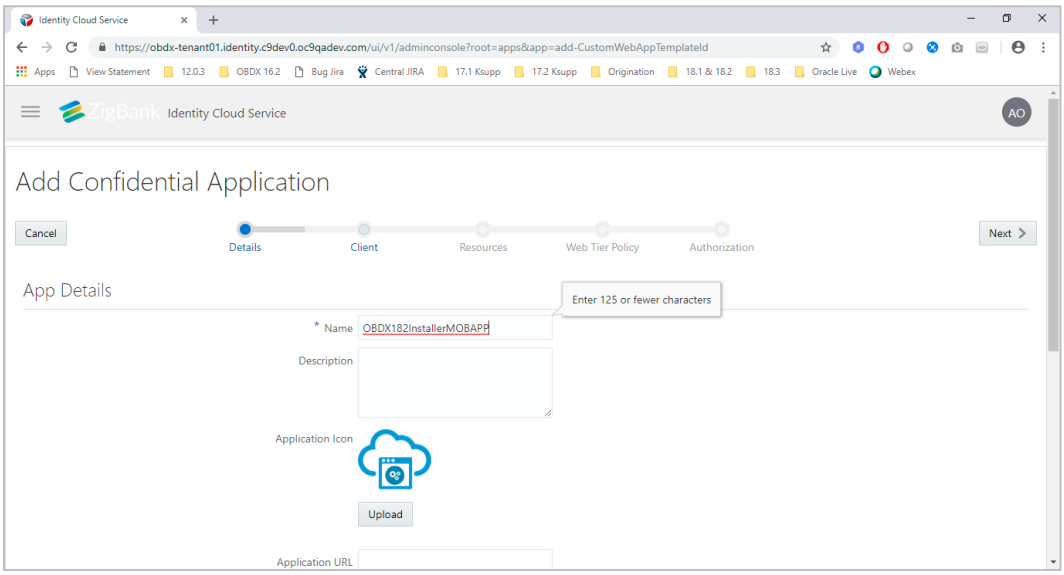

Install Application Assistant
Not secure
mum00afd:14001/console/console.portal?AppApplicationInstallPortlet_actionOverride=/com/bea/console/actions/app/install/upl...
ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.
Lock & Edit
Release Configuration
Domain Structure
obdx_domain
Domain Partitions
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed enterprise application
Configure an enterprise application
Create a deployment plan
Target an enterprise application to a server instance
Test the modules in an enterprise application
Welcome, weblogic
Connected to: obdx_domain
Messages
The file obdx.app.rest.ear has been uploaded successfully to /home/devops/domain/obdx_domain/servers/AdminServer/upload
Install Application Assistant
Back
Next
Finish
Cancel
Locate deployment to install and prepare for deployment
Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. You can also enter the path of the application directory or file in the Path field.
Note: Only valid file paths are displayed below. If you cannot find your deployment files, Upload your file(s) and/or confirm that your application contains the required deployment descriptors.
Path:
/home/devops/domain/obdx_domain/servers/AdminServer/upload/obdx.app.rest.ear/app/obdx.app.rest.ear
Recently Used Paths:
/home/devops/domain/obdx_domain/servers/AdminServer/upload/SwaggerEar.ear/app
/home/devops/domain/obdx_domain/servers/AdminServer/upload/obdx.thirdparty.app.domain.ear/app
/home/devops/domain/obdx_domain/servers/AdminServer/upload/obdx.extsystem.domain.ear/app
/home/devops/domain/obdx_domain/servers/AdminServer/upload/obdx.externalsystem.ubs.notification.mdb.ear/app
Current Location:
mum00afd / home / devops / domain / obdx_domain / servers / AdminServer / upload / obdx.app.rest.ear / app
obdx.app.rest.ear
Waiting for mum00afd...
5:32 PM
10/12/2018

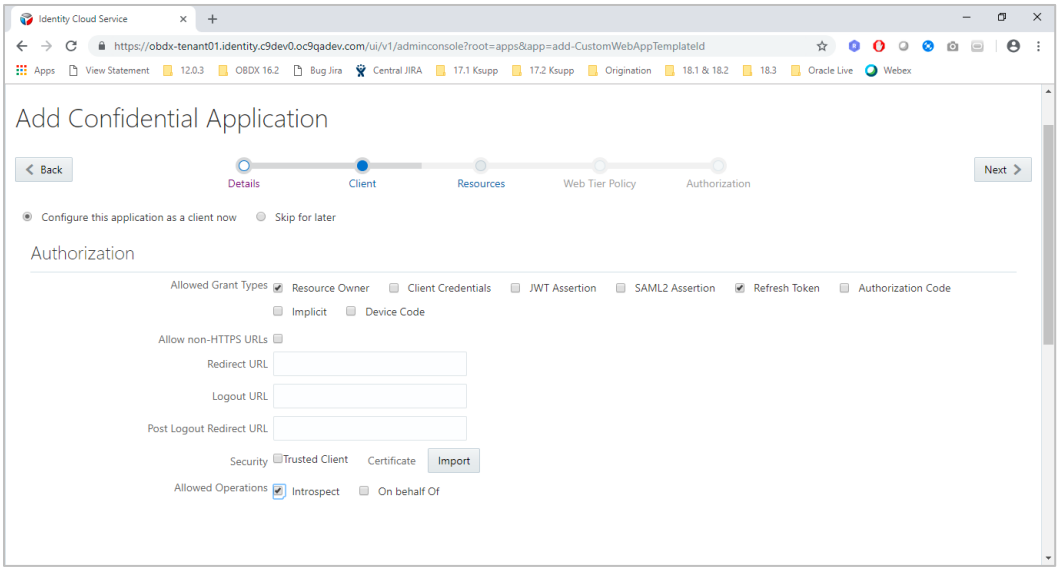
Home

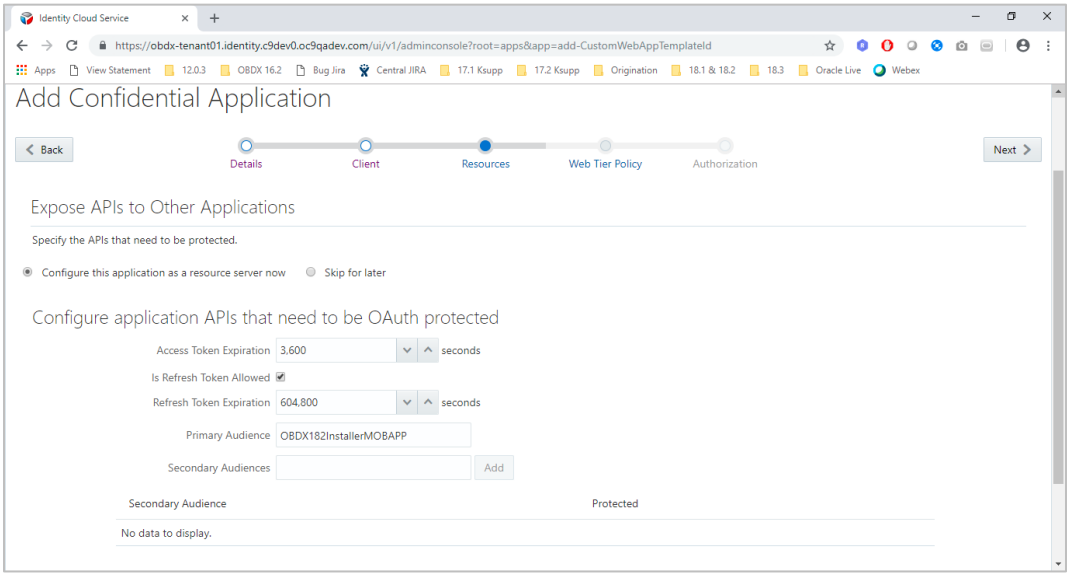
11. Create Client Applications for Internal OBAPI Apps in IDCS Console

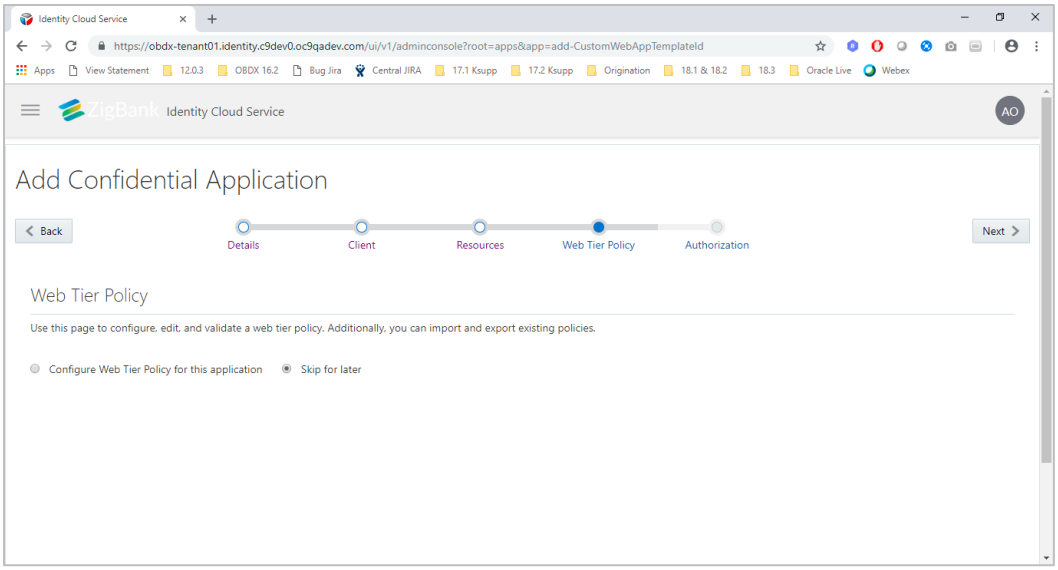
Client applications need to be created for below Internal applications.

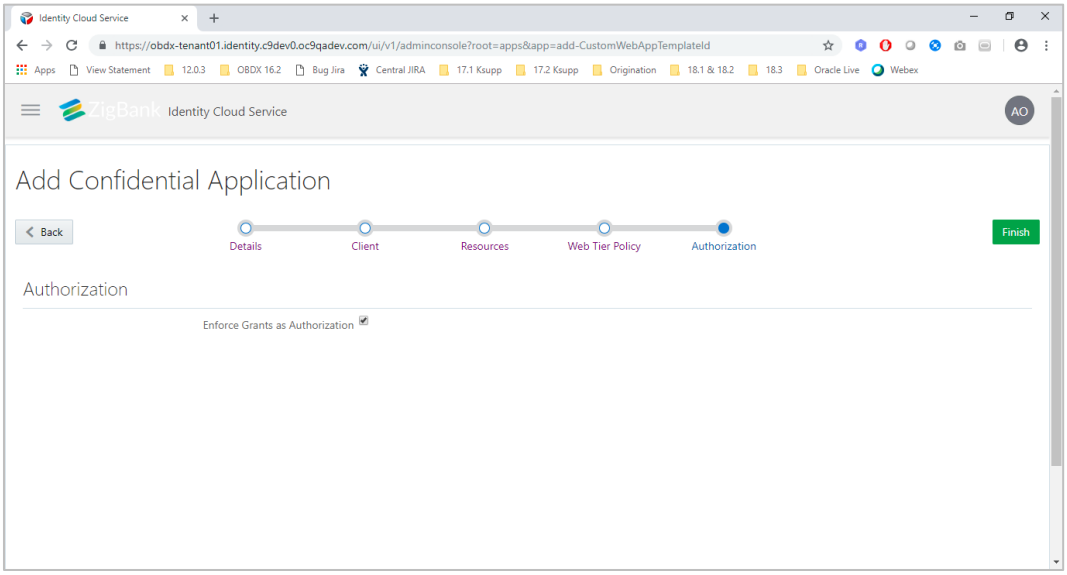
- Mobile App
- Siri Chatbot
- Snapshot
- Wearable

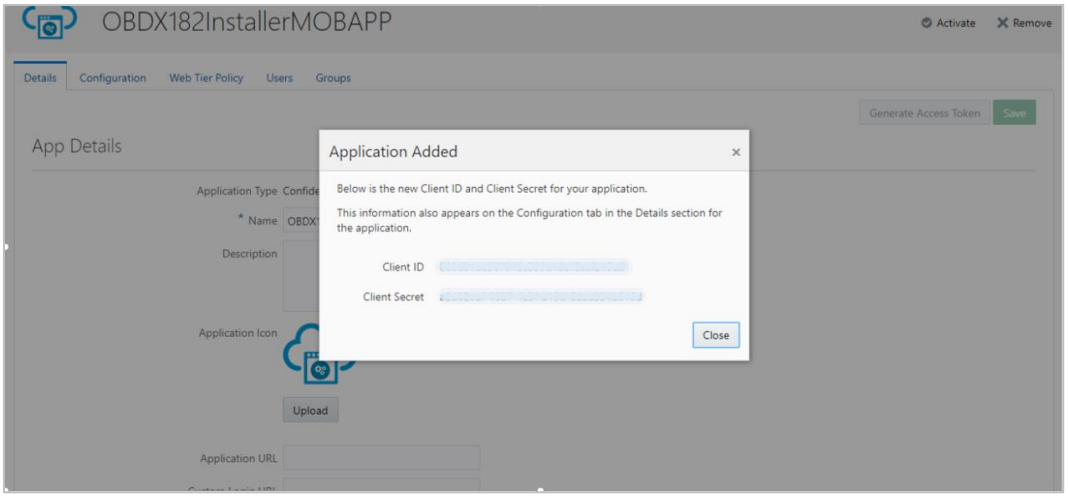



Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
Add Confidential Application
Back
Details
Client
Resources
Web Tier Policy
Authorization
Next
Configure this application as a client now
Skip for later
Authorization
Allowed Grant Types
Resource Owner
Client Credentials
JWT Assertion
SAML2 Assertion
Refresh Token
Authorization Code
Implicit
Device Code
Allow non-HTTPS URLs
Redirect URL
Logout URL
Post Logout Redirect URL
Security
Trusted Client
Certificate
Import
Allowed Operations
Introspect
On behalf Of


Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
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
Configure application APIs that need to be OAuth protected
Access Token Expiration
3,600
seconds
Is Refresh Token Allowed
Refresh Token Expiration
604,800
seconds
Primary Audience
OBDX182InstallerMOBAPP
Secondary Audiences
Add
Secondary Audience
Protected
No data to display.

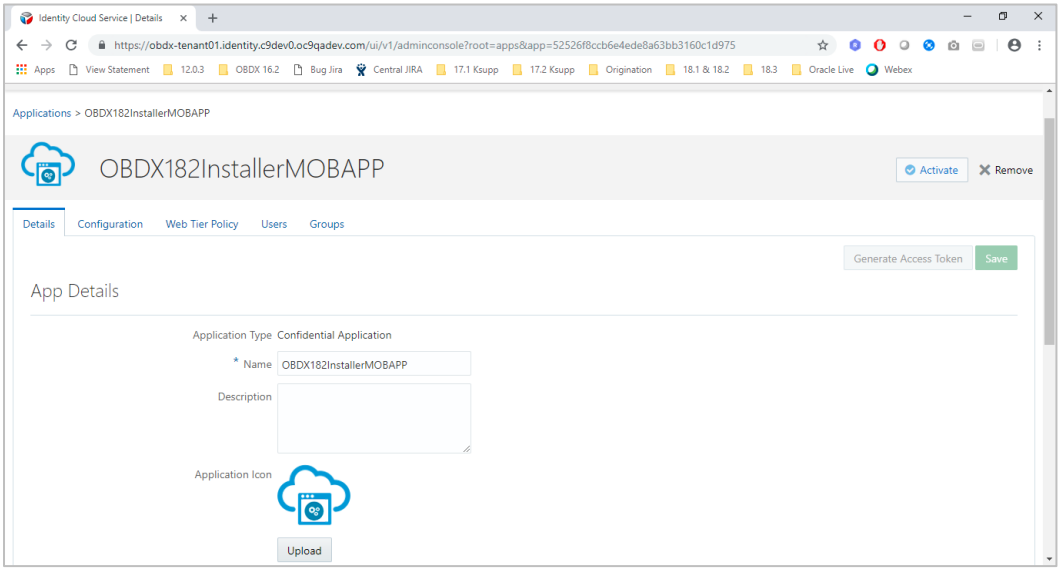

Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
Identity Cloud Service
AO
Add Confidential Application
Back
Details
Client
Resources
Web Tier Policy
Authorization
Next
Web Tier Policy
Use this page to configure, edit, and validate a web tier policy. Additionally, you can import and export existing policies.
Configure Web Tier Policy for this application
Skip for later


Identity Cloud Service
https://obdx-tenant01.identity.c9dev0.oc9qadev.com/ui/v1/adminconsole?root=apps&app=add-CustomWebAppTemplateId
Identity Cloud Service
AO
Add Confidential Application
Back
Details
Client
Resources
Web Tier Policy
Authorization
Finish
Authorization
Enforce Grants as Authorization



Glossary of parameters:

<client_id_of_SNAPSHOT_client>	Client Id of Snapshot app created in IDCS
<client_id_of_MobileApp_client>	Client Id of Mobile app created in IDCS created above
<client_id_of_SIRICHATBOT_client>	Client Id of Siri chatbot app created in IDCS
<client_id_of_WEARABLE_client>	Client Id of Wearable app created in IDCS



8. Click **Activate** button.

Similarly, do the same for the rest.

Home

12. Database Scripts (to be executed after day0 scripts)

Replace below parameters in database scripts with appropriate values as per glossary.

<tenant-base-url>

<client_id_of_SNAPSHOT_client>

<client_id_of_MobileApp_client>

<client_id_of_SIRICHATBOT_client>

<client_id_of_WEARABLE_client>

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 ('POLICY_STORE_UTIL','SecurityConstants','IGF','N',null,'Security Constant','ofssuser',sysdate,'ofssuser',sysdate,'Y',1,'N',null);

update DIGX_FW_CONFIG_ALL_B set prop_value = 'ipm1.0,ORACLEBI12.2.1.2,GENERIC1.0,IDCS18.2.4',SUMMARY_TEXT = 'Entry to set IPM,ORCALE BI and IDCS at enterprise level' where category_id = 'extxfaceadapterconfig' and prop_id='01';

Insert into DIGX_FW_CONFIG_VAR_B (PROP_ID,ENV_ID,PROP_VALUE,FACTORY_SHIPPED_FLAG,PROP_COMMENTS,CREATED_BY,CREATION_DATE,LAST_UPDATED_BY,LAST_UPDATED_DATE,OBJECT_STATUS,OBJECT_VERSION_NUMBER,MODULE,DETERMINANT_VALUE,TYPE,UI_DEFINITION) values ('HOST_IP_IDCS','OBAPI','<tenant-base-url>','Y','set host IP for IDCS REST calls','ofssuser',sysdate,'ofssuser',sysdate,null,null,'OTHERMODULE','OBDX_BU','TXT','{"title": "IDCS Host IP","validator":"","required":false}');

Insert into DIGX_FW_CONFIG_VAR_B (PROP_ID,ENV_ID,PROP_VALUE,FACTORY_SHIPPED_FLAG,PROP_COMMENTS,CREATED_BY,CREATION_DATE,LAST_UPDATED_BY,LAST_UPDATED_DATE,OBJECT_STATUS,OBJECT_VERSION_NUMBER,MODULE,DETERMINANT_VALUE,TYPE,UI_DEFINITION) values ('HOST_PORT_IDCS','OBAPI','443','Y','set host Port for IDCS REST calls ','ofssuser',sysdate,'ofssuser',sysdate,null,null,'OTHERMODULE','OBDX_BU','TXT','{"title": "IDCS Host Port","validator":"PORT","required":false}');

Insert into DIGX_FW_CONFIG_VAR_B
(PROP_ID,ENV_ID,PROP_VALUE,FACTORY_SHIPPED_FLAG,PROP_COMMENTS,CREATE
D_BY,CREATION_DATE,LAST_UPDATED_BY,LAST_UPDATED_DATE,OBJECT_STATUS,O
BJECT_VERSION_NUMBER,MODULE,DETERMINANT_VALUE,TYPE,UI_DEFINITION)
values ('IDCS_CONNECTION_SCHEME','OBAPI','https','Y','set host connection scheme for IDCS REST calls
','ofssuser',sysdate,'ofssuser',sysdate,null,null,'OTHERMODULE','OBDX_BU','TXT','{"title":
"IDCS Connection Scheme","validator":"","required":false}');

delete from DIGX_UM_PWD_POLICY_ROLE_MAP where PASSWORDPOLICYID in ('0000001','9999999');

delete from DIGX_UM_PWD_POLICY where PASSWORDPOLICYID in ('0000001','9999999');

Update DIGX_FW_ACCESSPOINT set CLIENT_ID = '*<client_id_of_SNAPSHOT_client>*' where ID = 'APSNAPSHOT';

Update DIGX_FW_ACCESSPOINT set CLIENT_ID = '*<client_id_of_MobileApp_client>*' where ID = 'APMOBAPP';

Update DIGX_FW_ACCESSPOINT set CLIENT_ID = '*<client_id_of_SIRICHATBOT_client>*' where ID = 'APSIRICHATBOT';

Update DIGX_FW_ACCESSPOINT set CLIENT_ID = '*<client_id_of_WEARABLE_client>*' where ID = 'APWEARABLE';

Home

13. Apply Webgate Patch on OHS using OPatch

1. Download the patch from the below link.

https://support.oracle.com/epmos/faces/PatchDetail?_adf.ctrl-state=hyoym65na_9&patch_name=28243743&releaseId=600000000073630&patchId=28243743&languageId=0&platformId=226&_afrLoop=441568515075199

2. Run below commands on webgate installation.

[devops@obapiohs ~]$ export ORACLE_HOME=<oracle-home-path>

Eg. export ORACLE_HOME=/home/devops/Oracle/Middleware/Oracle_Home/

[devops@obapiohs ~]$ export PATH=$PATH:<oracle-home-path>/OPatch/

Eg. export PATH=$PATH:/home/devops/Oracle/Middleware/Oracle_Home/OPatch/

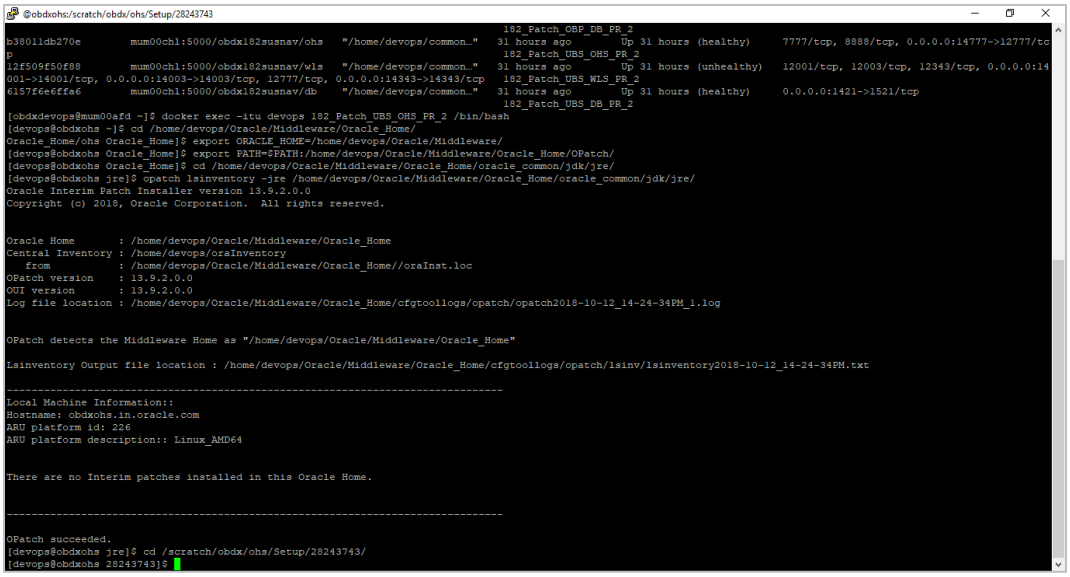
[devops@obapiohs ~]$ opatch lsinventory -jre <jre-path>

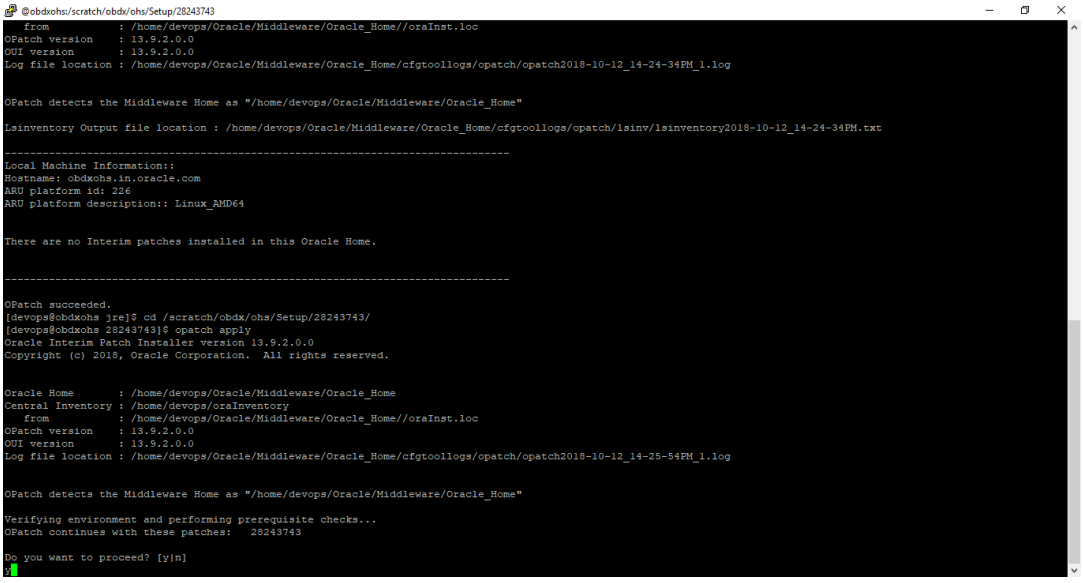
Eg. opatch lsinventory -jre /home/devops/Oracle/Middleware/Oracle_Home/oracle_common/jdk/jre/

[devops@obapiohs ~]$ cd <local-patch-path>

Eg. cd /scratch/obapi/ohs/p28243743_122130_Linux-x86-64/28243743/

[devops@obapiohs 28243743]$ opatch apply


@obdxohs:/scratch/obdx/ohs/Setup/28243743
182_Patch_OBP_DB_PR_2
b38011db270e mum00ch1:5000/obdx182susnav/ohs "/home/devops/common…" 31 hours ago Up 31 hours (healthy) 7777/tcp, 8888/tcp, 0.0.0.0:14777->12777/tcp
182_Patch_UBS_OHS_PR_2
12f509f50f88 mum00ch1:5000/obdx182susnav/wls "/home/devops/common…" 31 hours ago Up 31 hours (unhealthy) 12001/tcp, 12003/tcp, 12343/tcp, 0.0.0.0:14001->14001/tcp, 0.0.0.0:14003->14003/tcp, 12777/tcp, 0.0.0.0:14343->14343/tcp
182_Patch_UBS_WLS_PR_2
6157f6e6ffa6 mum00ch1:5000/obdx182susnav/db "/home/devops/common…" 31 hours ago Up 31 hours (healthy) 0.0.0.0:1421->1521/tcp
182_Patch_UBS_DB_PR_2
[obdxdevops@mum00afd ~]$ docker exec -itu devops 182_Patch_UBS_OHS_PR_2 /bin/bash
[devops@obdxohs ~]$ cd /home/devops/Oracle/Middleware/Oracle_Home/
Oracle_Home/ohs Oracle_Home]$ export ORACLE_HOME=/home/devops/Oracle/Middleware/
[devops@obdxohs Oracle_Home]$ export PATH=$PATH:/home/devops/Oracle/Middleware/Oracle_Home/OPatch/
[devops@obdxohs Oracle_Home]$ cd /home/devops/Oracle/Middleware/Oracle_Home/oracle_common/jdk/jre/
[devops@obdxohs jre]$ opatch lsinventory -jre /home/devops/Oracle/Middleware/Oracle_Home/oracle_common/jdk/jre/
Oracle Interim Patch Installer version 13.9.2.0.0
Copyright (c) 2018, Oracle Corporation. All rights reserved.
Oracle Home : /home/devops/Oracle/Middleware/Oracle_Home
Central Inventory : /home/devops/oraInventory
from : /home/devops/Oracle/Middleware/Oracle_Home//oraInst.loc
OPatch version : 13.9.2.0.0
OUI version : 13.9.2.0.0
Log file location : /home/devops/Oracle/Middleware/Oracle_Home/cfgtoollogs/opatch/opatch2018-10-12_14-24-34PM_1.log
OPatch detects the Middleware Home as "/home/devops/Oracle/Middleware/Oracle_Home"
Lsinventory Output file location : /home/devops/Oracle/Middleware/Oracle_Home/cfgtoollogs/opatch/lsinv/lsinventory2018-10-12_14-24-34PM.txt
Local Machine Information::
Hostname: obdxohs.in.oracle.com
ARU platform id: 226
ARU platform description:: Linux_AMD64
There are no Interim patches installed in this Oracle Home.
OPatch succeeded.
[devops@obdxohs jre]$ cd /scratch/obdx/ohs/Setup/28243743/
[devops@obdxohs 28243743]$


@obdxohs:/scratch/obdx/ohs/Setup/28243743
from : /home/devops/Oracle/Middleware/Oracle_Home//oraInst.loc
OPatch version : 13.9.2.0.0
OUI version : 13.9.2.0.0
Log file location : /home/devops/Oracle/Middleware/Oracle_Home/cfgtoollogs/opatch/opatch2018-10-12_14-24-34PM_1.log
OPatch detects the Middleware Home as "/home/devops/Oracle/Middleware/Oracle_Home"
Lsinventory Output file location : /home/devops/Oracle/Middleware/Oracle_Home/cfgtoollogs/opatch/lsinv/lsinventory2018-10-12_14-24-34PM.txt
Local Machine Information::
Hostname: obdxohs.in.oracle.com
ARU platform id: 226
ARU platform description:: Linux_AMD64
There are no Interim patches installed in this Oracle Home.
OPatch succeeded.
[devops@obdxohs jre]$ cd /scratch/obdx/ohs/Setup/28243743/
[devops@obdxohs 28243743]$ opatch apply
Oracle Interim Patch Installer version 13.9.2.0.0
Copyright (c) 2018, Oracle Corporation. All rights reserved.
Oracle Home : /home/devops/Oracle/Middleware/Oracle_Home
Central Inventory : /home/devops/oraInventory
from : /home/devops/Oracle/Middleware/Oracle_Home//oraInst.loc
OPatch version : 13.9.2.0.0
OUI version : 13.9.2.0.0
Log file location : /home/devops/Oracle/Middleware/Oracle_Home/cfgtoollogs/opatch/opatch2018-10-12_14-25-54PM_1.log
OPatch detects the Middleware Home as "/home/devops/Oracle/Middleware/Oracle_Home"
Verifying environment and performing prerequisite checks...
OPatch continues with these patches: 28243743
Do you want to proceed? [y|n]
y

3. Enter **y**

@obdxohs:/scratch/obdx/ohs/Setup/28243743
[devops@obdxohs jre]$ cd /scratch/obdx/ohs/Setup/28243743/
[devops@obdxohs 28243743]$ opatch apply
Oracle Interim Patch Installer version 13.9.2.0.0
Copyright (c) 2018, Oracle Corporation. All rights reserved.
Oracle Home : /home/devops/Oracle/Middleware/Oracle_Home
Central Inventory : /home/devops/oraInventory
from : /home/devops/Oracle/Middleware/Oracle_Home//oraInst.loc
OPatch version : 13.9.2.0.0
OUI version : 13.9.2.0.0
Log file location : /home/devops/Oracle/Middleware/Oracle_Home/cfgtoollogs/opatch/opatch2018-10-12_14-25-54PM_1.log
OPatch detects the Middleware Home as "/home/devops/Oracle/Middleware/Oracle_Home"
Verifying environment and performing prerequisite checks...
OPatch continues with these patches: 28243743
Do you want to proceed? [y|n]
y
User Responded with: Y
All checks passed.
Please shutdown Oracle instances running out of this ORACLE_HOME on the local system.
(Oracle Home = '/home/devops/Oracle/Middleware/Oracle_Home')
Is the local system ready for patching? [y|n]
y
User Responded with: Y
Backing up files...
Applying interim patch '28243743' to OH '/home/devops/Oracle/Middleware/Oracle_Home'
ApplySession: Optional component(s) [oracle.oamclient.webgate.otd, 12.2.1.3.0] , [oracle.oamclient.webgate.otd, 12.2.1.3.0] not present in the Oracle Home or a higher version is found.
Patching component oracle.oamclient.webgate.ohs, 12.2.1.3.0...
Patching component oracle.oamclient.webgate.ohs, 12.2.1.3.0...
Patch 28243743 successfully applied.
Log file location: /home/devops/Oracle/Middleware/Oracle_Home/cfgtoollogs/opatch/opatch2018-10-12_14-25-54PM_1.log
OPatch succeeded.
[devops@obdxohs 28243743]$

Home

14. cloud.config

1. *Go to this location <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/*

   Eg. /home/devops/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/

   CREATE THE FOLLOWING FILE NAMED as cloud.config:

2. *Replace below parameters in file:*

   <webserver_host_name>

   <webserver_port>

```
{
  "cloudgateConfig":{
    "bootstrap":{
      "callbackPrefix":"<connection_scheme>://<webserver_host_name>:<webserver_port>/oauth/callback",
      "externalIdUrl":"https://<tenant-base-url>",
      "refresh_token":false
    },
    "rest":{
      "httpsVerifyHost":false,
      "httpsVerifyServer":false,
      "httpsCertAuthFile":"",
      "httpsCrlFile":""
    }
  }
}
```

Home

15. cloud.policy

Go to this location <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/

E.g..
/home/devops/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/

CREATE THE FOLLOWING FILE NAMED as cloud.policy:

1. Replace below parameter.

   <allowed_scope_name_of_scope_protected_in_OBAPI_Client_App>

```
{
  "cloudgatePolicy":{
    "webtierPolicy":[
      {
        "policyName":"default",
        "resourceFilters":[
          {
            "comment":"Test Application OAuth+Logout Filter",
            "type":"text",
            "filter":"/logout",
            "method":"oauth+logout"
          },
          {
            "comment":"Test Application Public Filter",
            "type":"regex",
            "filter":"/*.js",
            "method":"anonymous",
            "headers":[
              {
                "PolicyName":"$request.policy_name"
              },
              {
                "PolicyResourceMatched":"$request.policy_res"
              }
            ]
          },
          {
            "comment":"Test Application OAuth Filter",
            "type":"regex",
            "filter":"/pages/*",
            "method":"oauth",
            "authorize":true,
            "scope":"<allowed_scope_name_of_protected_in_OBAPI_Client_App> openid",
            "idcsscope":"protected openid",
            "headers":[
              {
                "UserName":"$subject.user.name"
              },
              {
                "PrimaryEmail":"$subject.user.emails"
              },
              {
                "PolicyName":"$request.policy_name"
              },
              {
                "PolicyResourceMatched":"$request.policy_res"
              }
            ]
          },
          {
            "comment":"Test Application Public Filter",
            "type":"regex",
            "filter":"/**",
            "method":"anonymous",
                    "headers": [
                        {
```

```
                        "PolicyName":"$request.policy_name"
                    },
                    {
                        "PolicyResourceMatched":"$request.policy_res"
                    }
                ]
            }
        ]
    }
]
}
```

Home

16. CWallet configuration

[**devops@obapiohs ~]$** mkdir <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet

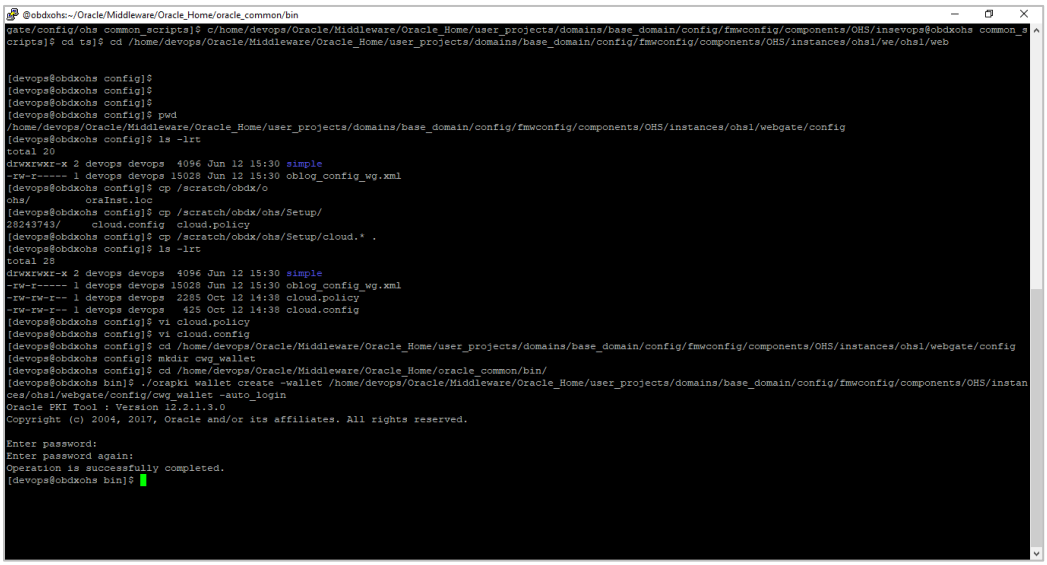
Eg. mkdir /home/devops/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet

[devops@obapiohs ~]$ cd <oracle-home-path>/oracle_common/bin/

[**devops@obapiohs bin]$** ./orapki wallet create -wallet <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet -auto_login

Eg. ./orapki wallet create -wallet /home/devops/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet -auto_login

You will be asked to create wallet password here.

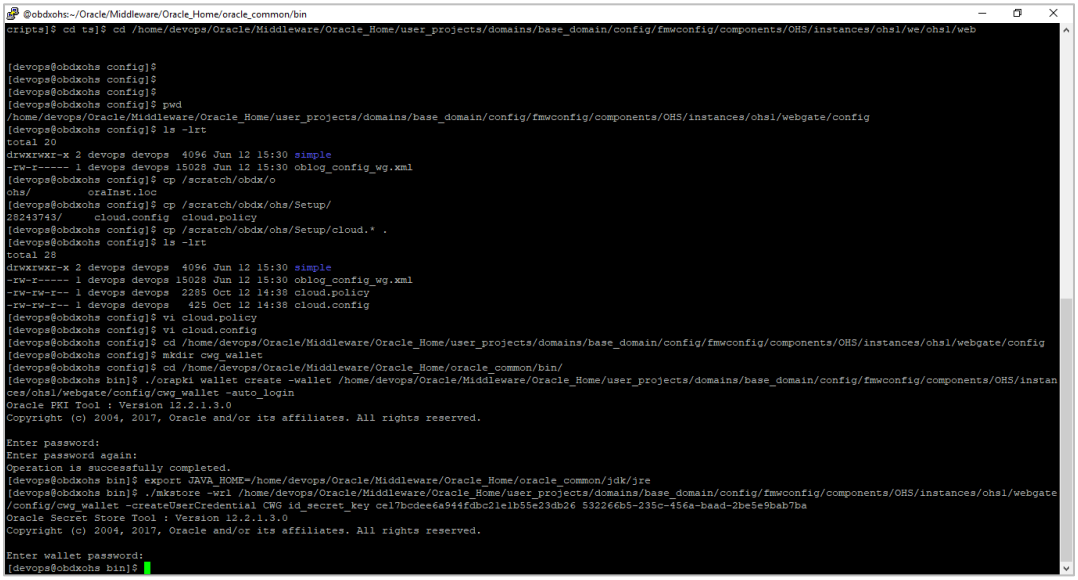


[devops@obapiohs bin]$ export JAVA_HOME=<jre-path>

Eg. export JAVA_HOME=/home/devops/Oracle/Middleware/Oracle_Home/oracle_common/jdk/jre

[devops@obapiohs bin]$ ./mkstore -wrl <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet -createUserCredential CWG id_secret_key **<client-id> <client-secret>**

Eg. ./mkstore -wrl /home/devops/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet -createUserCredential CWG id_secret_key <client-id> <client-secret>



<passphrase> is the password phrase used for encryption. Enter a passphrase in below command and execute it.

[root@obapiohs devops]# openssl enc -aes-128-cbc -k "<passphrase>" -P -md sha256

salt=4EBB2F22640F225F

key=701593B3EDE07C37FD09ECB532F7E0E5

iv =E5D3D73CED2C624900F952C05BC73A6E

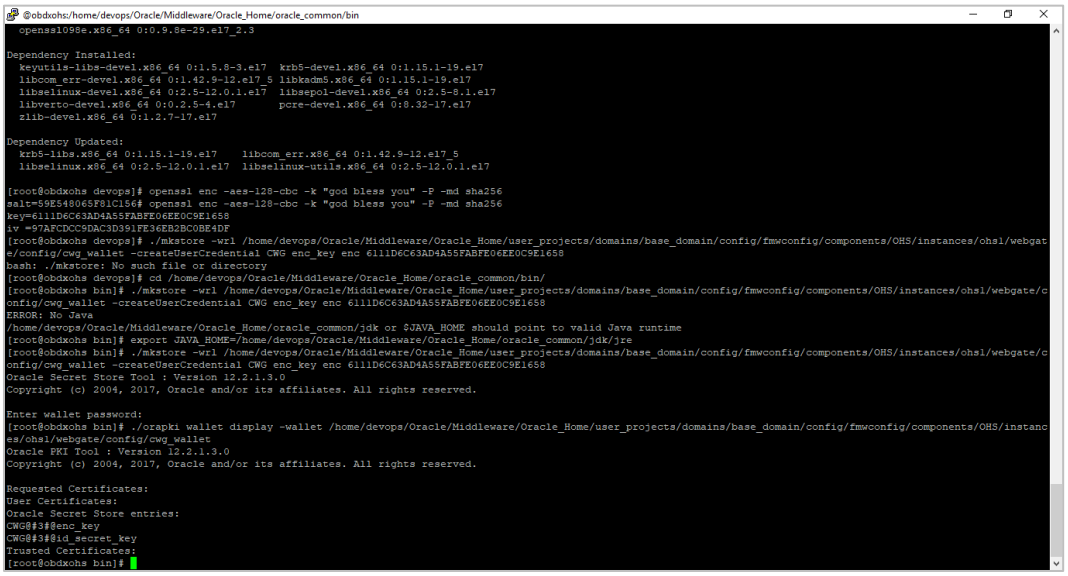
[devops@obapiohs bin]$ ./mkstore -wrl <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet -createUserCredential CWG enc_key enc <key>

Eg. ./mkstore -wrl /home/devops/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet -createUserCredential CWG enc_key enc <key>

Please enter the wallet password given above.

[devops@obapiohs bin]$ ./orapki wallet display -wallet <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet

Eg. ./orapki wallet display -wallet /home/devops/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/cwg_wallet



Home

17. Enabling webgate in httpd.conf

Go to <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/

Eg.
/home/devops/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1/

UNCOMMENT THE FOLLOWING:

include "webgate.conf"

Home

18. Change in mod_wl_ohs.conf

Go to <ohs-domain-path>/config/fmwconfig/components/OHS/instances/ohs1/

ADD THE FOLLOWING:

<IfModule weblogic_module>

WebLogicHost obapiwls.in.oracle.com

WebLogicPort 12003

Debug ON

WLLogFile /scratch/obapi/ohs/logs/weblogic.log

MatchExpression /digx/*

</IfModule>

<Location /digx>

WLSRequest On

WLProxySSL ON

WLProxySSLPassThrough ON

</Location>

Home

19. UI Changes

19.1 constants.js:

In UI deployments, go to channel\framework\js\constants\constants.js file, keep the value of 'authenticator' as below.

authenticator: "IDCSAuthenticator"

19.2 idcs-config.json:

In UI deployments, go to channel\json\index\login\idcs-config.json file, put the appropriate values of OBAPI Client Application in IDCS.

- **<name_of_obapi_client_app_in_idcs>** is the client application name. Eg. "OBAPIClient"
- **<client_id_of_obapi_client_app_in_idcs>** is client id of client application. Eg. "*00fa15d18cd147398ca4b53f957a4e3f"*
- **<client_secret_of_obapi_client_app_in_idcs>** is the client secret of client application.

Home