Oracle Access Manager Integration
Oracle FLEXCUBE Universal Banking
Release 12.87.7.0.0

May 2021

Table of Contents

1. Preface

1.1 Introduction

This manual discusses the integration of Oracle FLEXCUBE Universal Banking and the Oracle Access Manager system**.** The configurations required for proper functioning of this integration and further processing are documented in this manual.

1.2 Audience

This manual is intended for the following User/User Roles:

Role	Function
Back office data entry Clerks	Input functions for maintenance related to the interface.
Implementation team	Implementation of Oracle FLEXCUBE Investor Servicing

1.3 Abbreviations

Abbreviation	Description
System	Unless specified, it shall always refer to Oracle FLECUBE
OAM	Oracle Access Manager
UBS	Universal Banking Solutions
SSO	Single Sign-on
LDAP	Lightweight Directory Access Protocol

1.4 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.

1.5 Organization

This manual is organized into the following chapters:

Chapter 1	*Preface* gives information on the intended audience. It also lists the various chapters covered in this User Manual.
Chapter 2	*Enabling Single Sign-on (SSO) with Oracle Access Manager* discusses the method to integrate Oracle FLEXCUBE with Oracle Access Manager for Single Sign-on.

1.6 Glossary of Icons

This User Manual may refer to all or some of the following icons.

Icons	Function
	Exit
	Add row
	Delete row
	Option List

1.6.1 Related Documents

You may refer the following manual for more information

- Oracle Access Manager User Manual (not included with Oracle FLEXCUBE User Manuals)

2. Enabling Single Sign-on with Oracle Access Manager

2.1 Introduction

For the purpose of single sign-on FLEXCUBE is qualified with Oracle Identity Management 11.1.2 (Fusion Middleware 11gR2) – specifically using the Access Manager component of Oracle Identity Management. This feature is available in FLEXCUE since the release FC UBS V.UM 7.3.0.0.0.0.0 .

This document provides an understanding as to how single sign-on can be enabled for a FLEXCUBE deployment using Oracle Fusion Middleware 11gR2.

In addition to providing a background to the various components of the deployment, this document also talks about Configuration to be done in FLEXCUBE and Oracle Access Manager to enable single sign-on using Oracle Internet Directory as a LDAP server.

2.2 Background and Prerequisites

2.2.1 Software Requirements

Oracle Identity and Access Management 11g R2 - 11.1.2.3.0

- Oracle Access Manager – 11.1.2.3.0
- Oracle Fusion Middleware Web Tier Utilities 11g Patch Set 6 - 11.1.1.9.0
  - Oracle HTTP Server
- Oracle Access Manager OHS 11gR2 WebGates - 11.1.2.3.0
- Optional: Oracle Adaptive Access Manager – 11.1.2.3.0 (Strong Authentication purpose only)

Note *: In case of **java.security.InvalidKeyException: Illegal key size** error in Admin Server, while starting the OAM Server based applications, then refer Oracle Support Document ID: **1901181.1**.

Note: Refer Oracle Support Document: **1935703.1**, to have skip the escape sequence \ (slash) infront of, (comma) in Oracle 11gR2 OAM request header values

LDAP Directory Server

Please make sure that the LDAP server to be used for FLEXCUBE Single Sign on deployment is certified to work with OAM.

List of few LDAP Directory servers supported as per OAM document (note – this is an indicative list. The conclusive list can be obtained from the Oracle Access Manager documentation. Though we have only use OID for our testing purposes):

- Oracle Internet Directory
- Active Directory
- ADAM
- ADSI
- Data Anywhere (Oracle Virtual Directory)

- IBM Directory Server
- NDS
- Sun Directory Server

Oracle Weblogic (10.3.6)

For the purpose of achieving single sign on for FLEXCUBE in FMW 11gR2, it is necessary for the weblogic instance to have an explicit **Oracle HTTP server (OHS).**

2.3 Background of SSO related components

2.3.1 Oracle Access Manager (OAM)

Oracle Access Manager consists of the Access System and the Identity System. The Access System secures applications by providing centralized authentication, authorization and auditing to enable single sign-on and secure access control across enterprise resources. The Identity System manages information about individuals, groups and organizations. It enables delegated administration of users, as well as self-registration interfaces with approval workflows. These systems integrate seamlessly.

The backend repository for the Access Manager is an LDAP-based directory service that can be a combination of a multiple directory servers, which is leveraged for two main purposes:

- As the store for policy, configuration and workflow related data, which is used and managed by the Access and Identity Systems
- As the identity store, containing the user, group and organization data that is managed through the Identity System and is used by the Access System to evaluate access policies.

2.3.2 LDAP Directory Server

To integrate Flexcube with OAM to achieve Single Sign-on feature, Flexcube's password policy management, like password syntax and password expiry parameters will no longer be handled by Flexcube. Instead, the password policy management can be delegated to the Directory Server. All password policy enforcements would be on the LDAP user id's password and NOT Flexcube application users' passwords.

2.3.3 WebGate/AccessGate

A WebGate is a Web server plug-in that is shipped out-of-the-box with Oracle Access Manager. The WebGate intercepts HTTP requests from users for Web resources and forwards it to the Access Server for authentication and authorization.

Whether you need a WebGate or an AccessGate depends on your use of the Oracle Access Manager Authentication provider. For instance, the:

Identity Asserter for Single Sign-On: Requires a separate WebGate and configuration profile for each application to define perimeter authentication. Ensure that the Access Management Service is On**.**

Authenticator or Oracle Web Services Manager: Requires a separate AccessGate and configuration profile for each application. Ensure that the Access Management Service is On**.**

2.3.4 Oracle Adaptive Access Manager

Oracle Adaptive Access Manager provides an innovative, comprehensive feature set to help organizations prevent fraud and misuse. Strengthening standard authentication mechanisms, innovative risk-based challenge methods, intuitive policy administration and integration across the Identity and Access Management Suite and with third party products make Oracle Adaptive Access Manager uniquely flexible and effective. Oracle Adaptive Access Manager provides real-time and batch risk analytics to combat fraud and misuse across multiple channels of access. Real-time evaluation of multiple data types helps stop fraud as it occurs. Oracle Adaptive Access Manager makes exposing sensitive data, transactions and business processes to consumers, remote employees or partners via your intranet and extranet safer.

Oracle Adaptive Access Manager provides an extensive set of capabilities including device fingerprinting, real-time behavioral profiling and risk analytics that can be harnessed across both Web and mobile channels. It also provides risk-based authentication methods including knowledge-based authentication (KBA) challenge infrastructure with Answer Logic and OTP Anywhere server-generated one-time passwords, delivered out of band via Short Message Service (SMS), e-mail or Instant Messaging (IM) delivery channels. Oracle Adaptive Access Manager also provides standard integration with Oracle Identity Management, the industry leading identity management and Web Single Sign-On products, which are integrated with leading enterprise applications.

2.4 Configuration

2.4.1 Pre-requisites

- The steps provided below assume that FLEXCUBE has already been deployed and is working (without single sign-on)
- The below provided steps assume that Oracle Access Manager and the LDAP server have been installed already and the requisite setup are already done with respect to connecting the two along with Weblogic's Identity Asserter.

2.5 Enabling SSL for Weblogic and OAM Console

2.5.1 Self-signed Certificate Creation:

To enable SSL mode, WebLogic requires a keystore which contains private and trusted certificates. We have to use the same version of JDK (which is used by Weblogic Domain) to create the keystore and certificates, otherwise it may lead to many difficulties (suggested by Oracle Support).

Keytool utility available in Java JDK will be used to create Keystore. In command prompt set PATH to the JDK\bin location. Follow the below steps to create keystore and self-signed certificates:

2.5.1.1 Keystore Creation

keytool -genkey -keystore <keystore_name.jks> -alias <alias_name> -dname "CN=<hostname>, OU=<Organization Unit>, O=<Organization>, L=<Location>, ST=<State>, C=<Country_Code>" -keyalg <Key Algorithm> -sigalg <Signature Algorithm> -keysize <key size> -validity <Number of Days> -keypass <Private key Password> -storepass <Store Password>

For example:

keytool -genkey -keystore AdminFlexcubeKeyStore.jks -alias FlexcubeCert -dname "CN=ofss00001.in.oracle.com, OU=OFSS, O=OFSS, L=Chennai, ST=TN, C=IN" -keyalg "RSA" -sigalg "SHA1withRSA" -keysize 2048 -validity 3650 -keypass Password@123 -storepass Password@123

Note: **CN=ofss00001.in.oracle.com** is the Host Name of the weblogic server

2.5.1.2 Export private key as certificate

keytool -export -v -alias <alias_name> -file <export_certificate_file_name_with_location.cer> -keystore <keystore_name.jks> > -keypass <Private key Password> -storepass <Store Password>

For example:

keytool -export -v -alias FlexcubeCert -file AdminFlexcubeCert.cer -keystore AdminFlexcubeKeyStore.jks -keypass Password@123 -storepass Password@123

If successful the following message will be displayed :

Certificate stored in file < AdminFlexcubeCert.cer>

2.5.1.3 Import as trusted certificate

keytool -import -v -trustcacerts -alias rootcacert -file <export_certificate_file_name_with_location.cer> -keystore <keystore_name.jks> > -keypass <Private key Password> -storepass <Store Password>

For example:

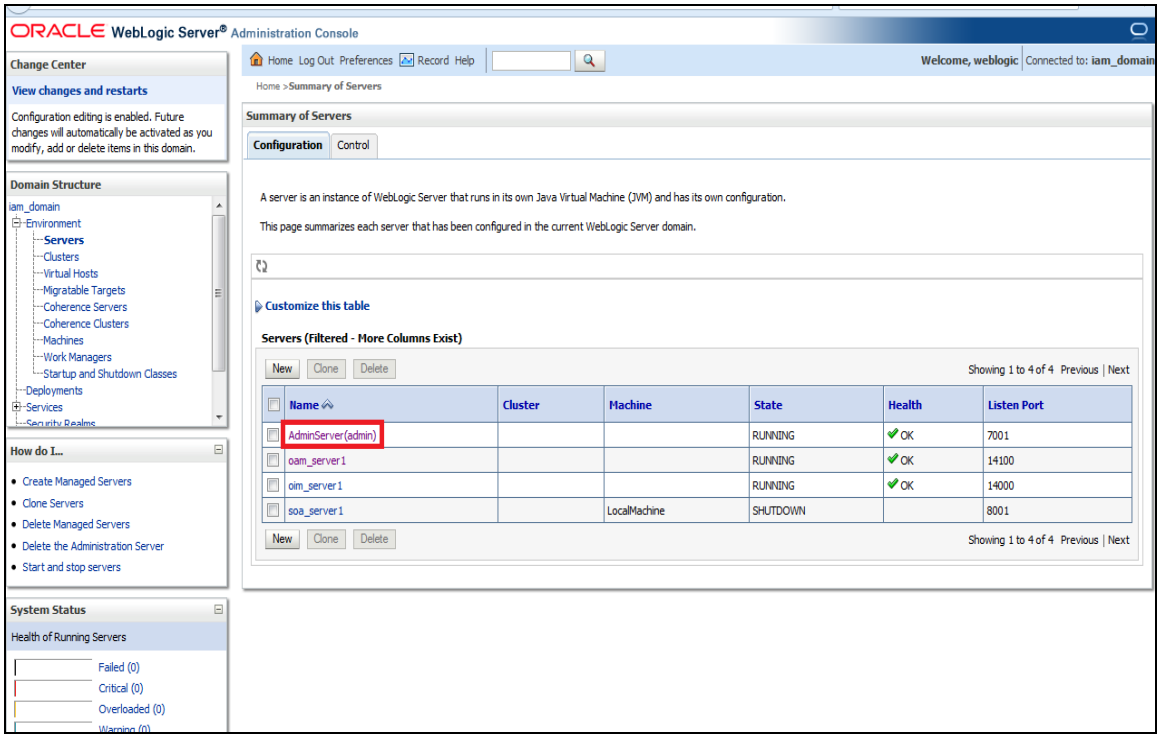
keytool -import -v -trustcacerts -alias rootcacert -file AdminFlexcubeCert.cer -keystore AdminFlexcubeKeyStore.jks -keypass Password@123 -storepass Password@123

References: Oracle Support Articles (Article ID 1281035.1, Article ID 1218695.1), in case of Certificates issued by the Trusted Authorities

2.5.2 Configuring Weblogic Console

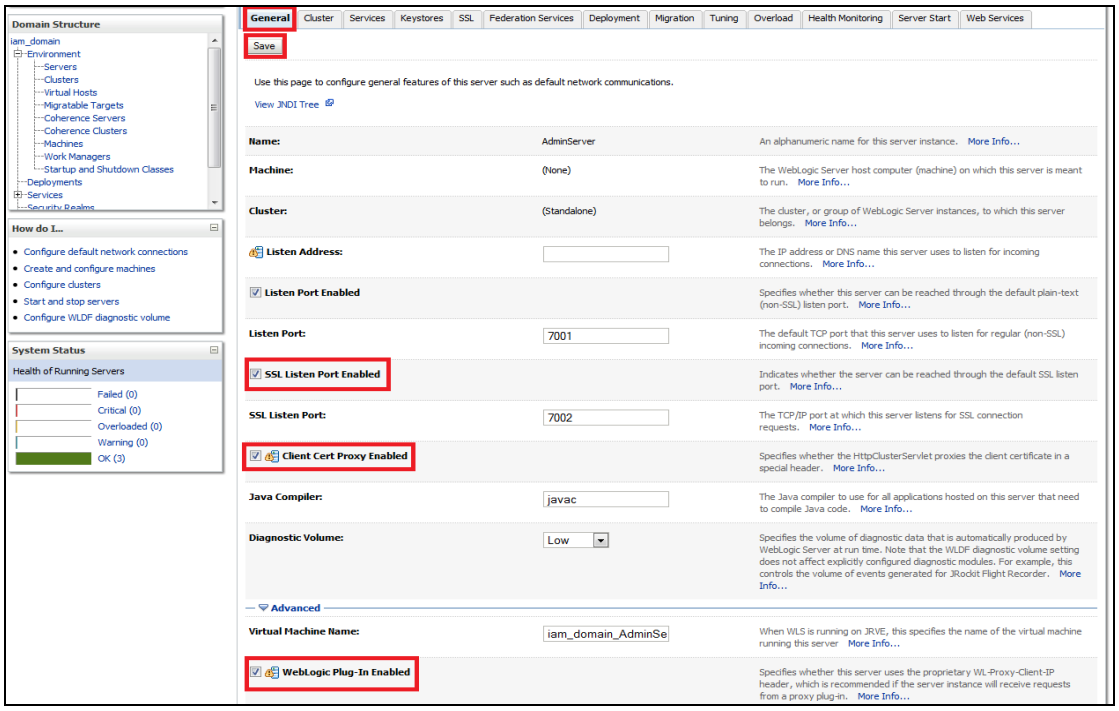
After domain creation, follow the below steps to enable SSL in weblogic Admin server and OAM Server.

2.5.2.1 Select Admin Server to enable SSL options



2.5.2.2 Follow the steps in General Tab as shown below:

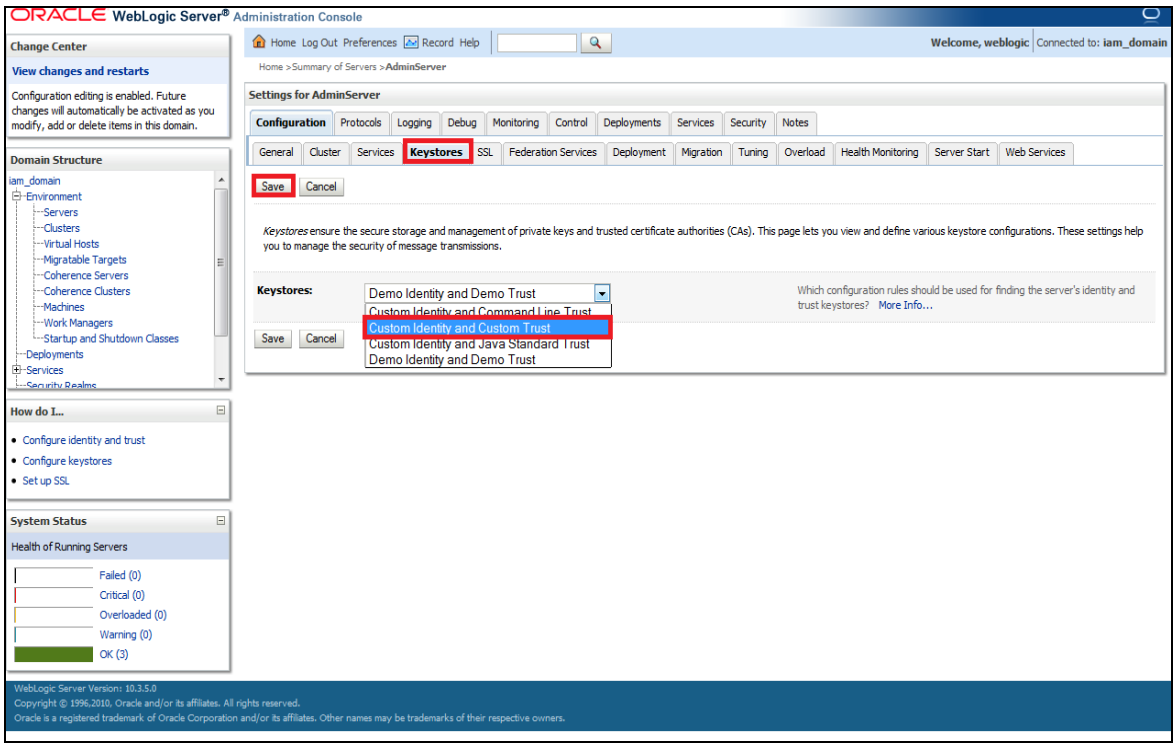
1. Select SSL Listen Port Enabled, Client Cert Proxy Enabled, Weblogic Plug-In Enabled.
2. Click on Save.



2.5.2.3 Follow the steps in Keystores Tab as shown below:

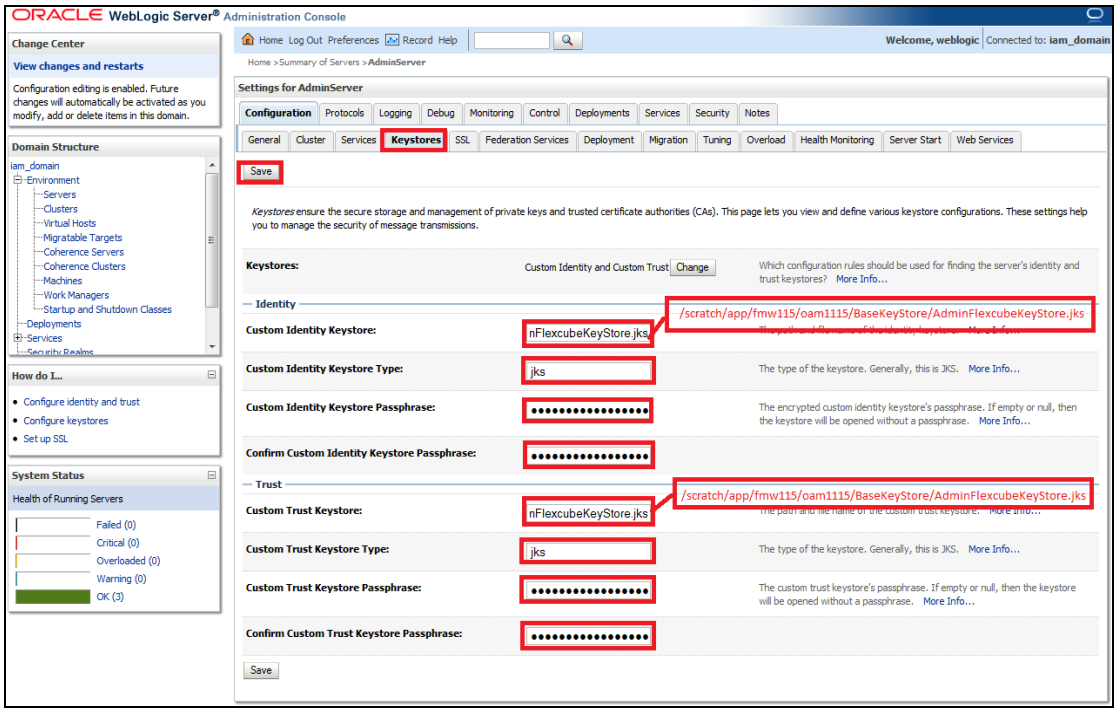
1. Click Change and select Keystores as Custom Identity and Custom Trust.
2. Click on Save.

   Keystores as Custom Identity and Custom Trust is as suggested by Oracle Support Team.



2.5.2.4 Follow the steps in Keystores Tab as shown below:

1. Enter Custom Identity Keystore and Custom Trust Keystore same as the Keystore Name created in step 3.2.1.1 with full path.
2. Enter Custom Identity Keystore Type and Custom Trust Keystore Type as jks.
3. Enter Custom Identity Keystore Passphrase, Confirm Custom Identity Keystore Passphrase, Custom Trust Keystore Passphrase and Confirm Custom Trust Keystore Passphrase same as the Store Password entered in step 3.2.1.1.
4. Click on Save.



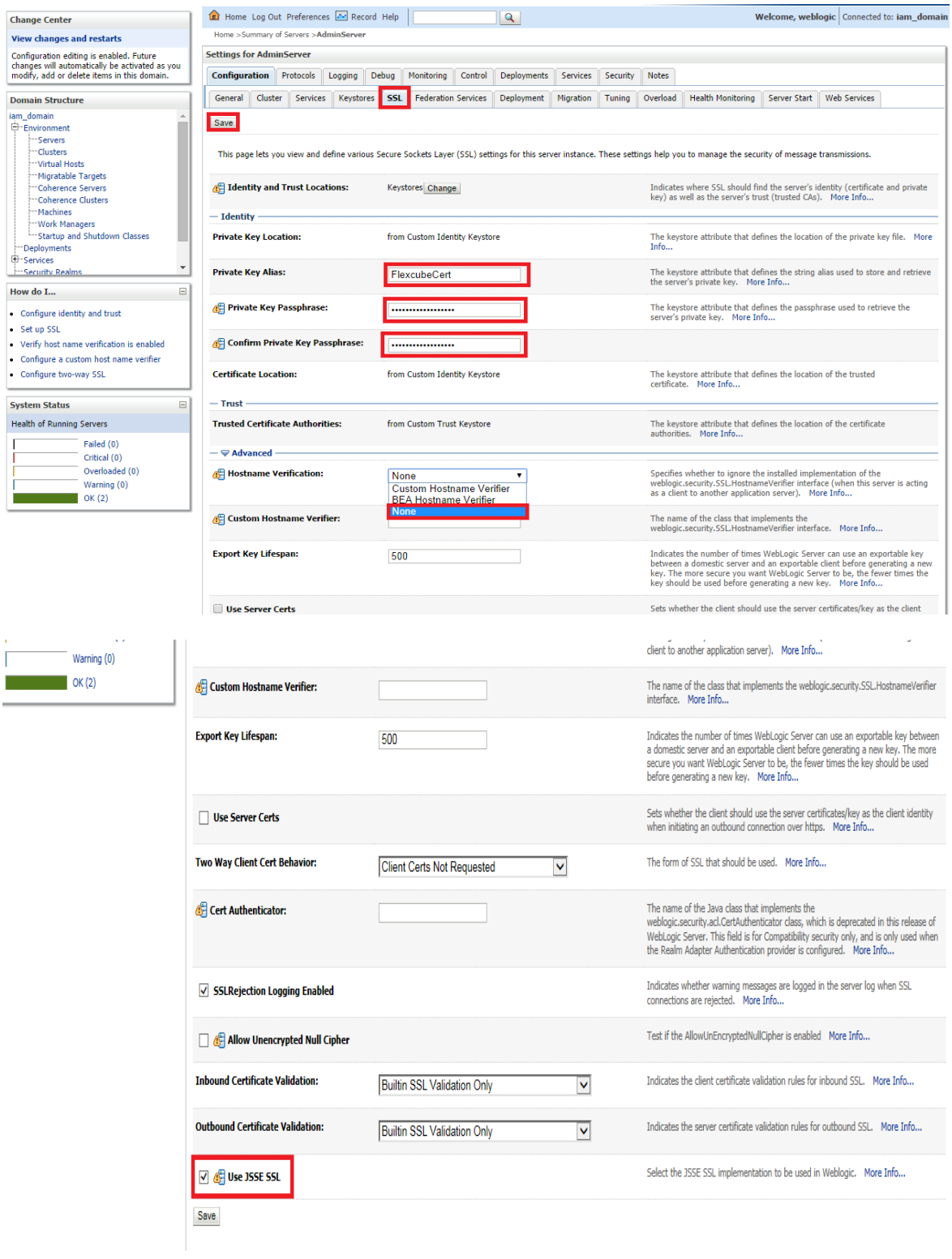
2.5.2.5 Follow the steps in SSL Tab as shown below:

1. Enter Private Key Alias as same as the alias name entered in step 3.2.1.1.
2. Enter Private Key Passphrase and Confirm Private Key Passphrase as same as the Private Key Password entered in step 3.2.1.1.
3. Change the Hostname Verification to None.
4. Select Use JSSE SSL option
5. Click on Save.

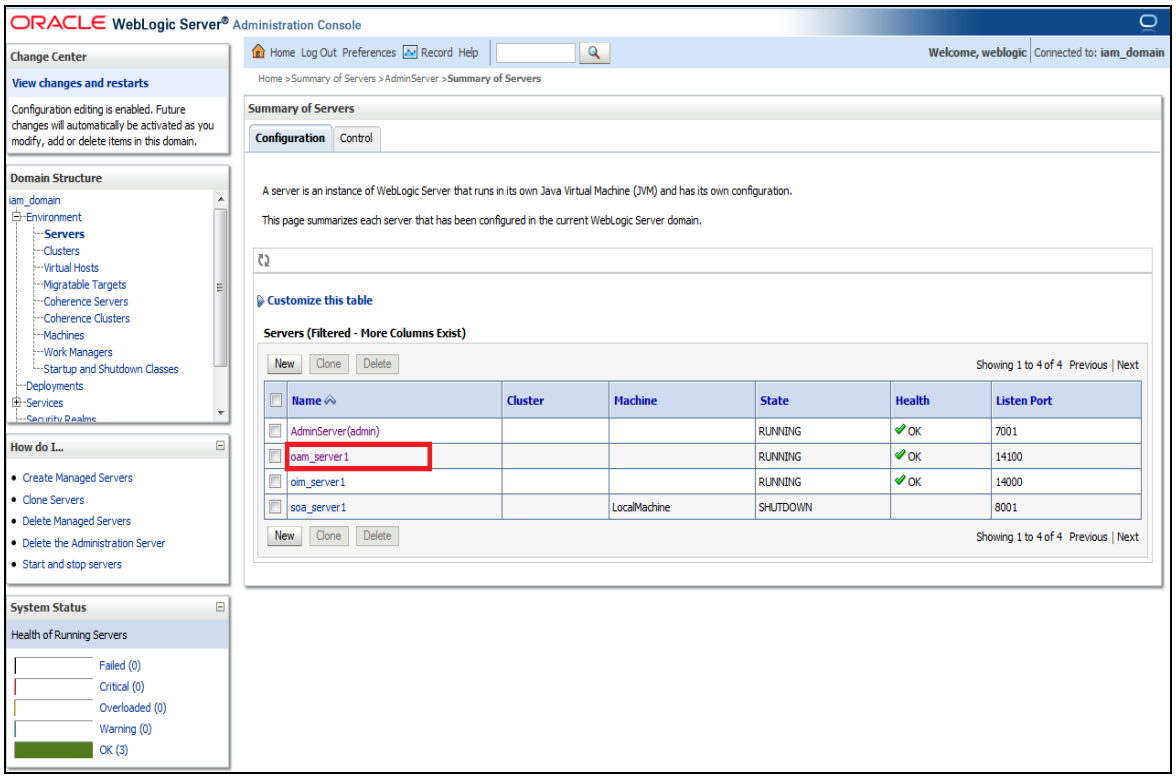
Note: For Weblogic 12c Server <DOMAIN_HOME>/bin setDomainEnv.cmd or setDomainEnv.sh update the JAVA_PROPERTIES from

JAVA_PROPERTIES=-Dwls.home=%WLS_HOME% -Dweblogic.home=%WLS_HOME%

To JAVA_PROPERTIES=-Dwls.home=%WLS_HOME% -Dweblogic.home=%WLS_HOME% -Dweblogic.security.SSL.minimumProtocolVersion=TLSv1



6. Select OAM Server to enable SSL options and Repeat the steps performed in 2.2.2.2 to 2.2.2.5

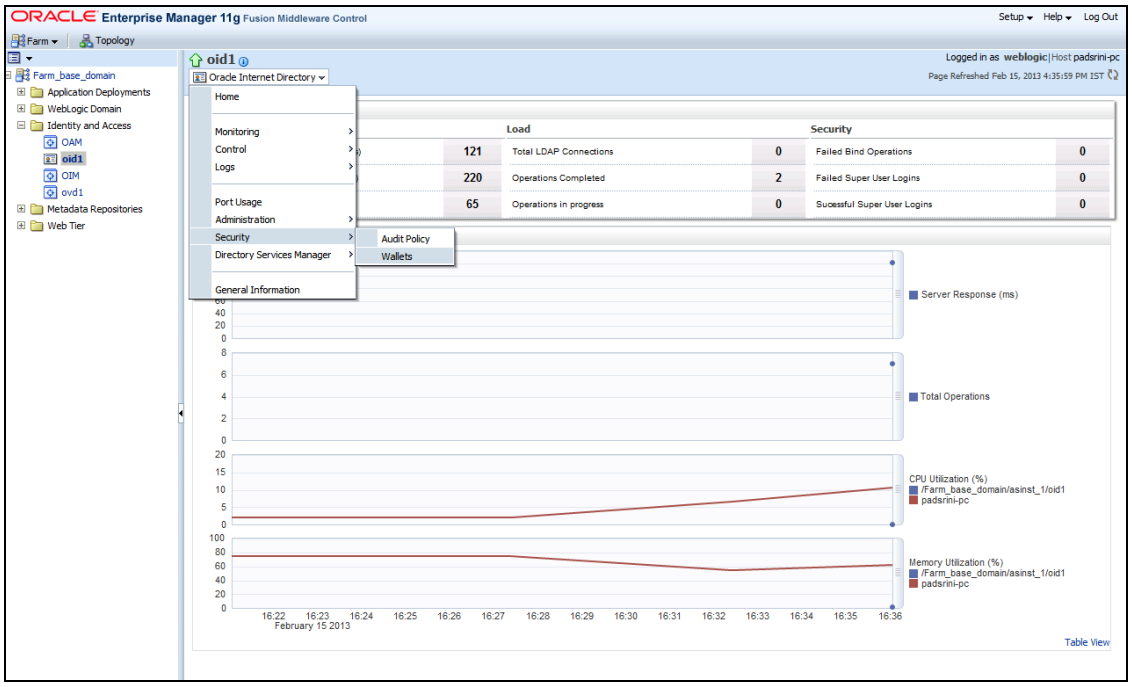


7. Now the admin server and OAM servers are SSL enabled. Restart both the servers.

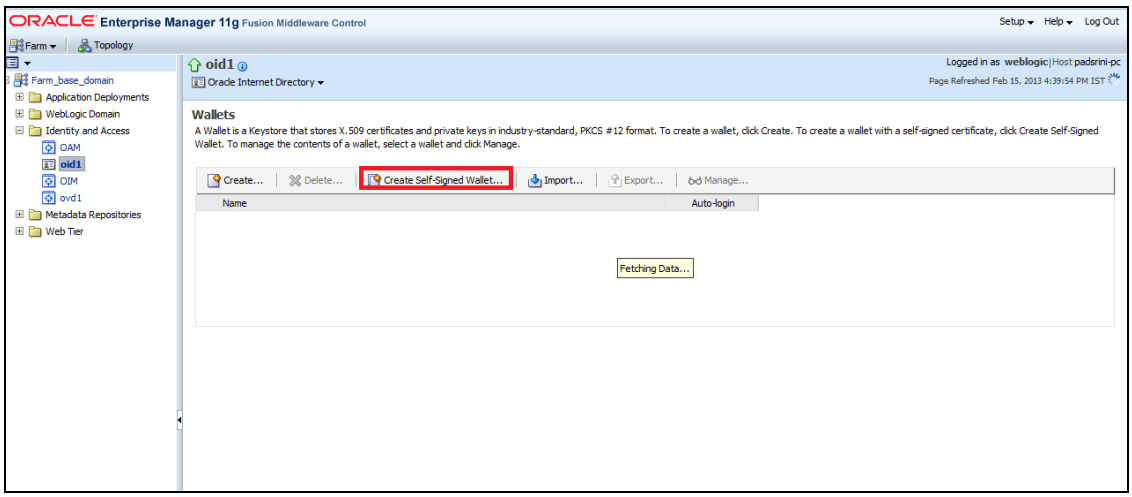
2.5.3 Configuring SSL Mode in Oracle Internet Directory

To enable SSL for OID LDAP Server refer, follow the below steps.

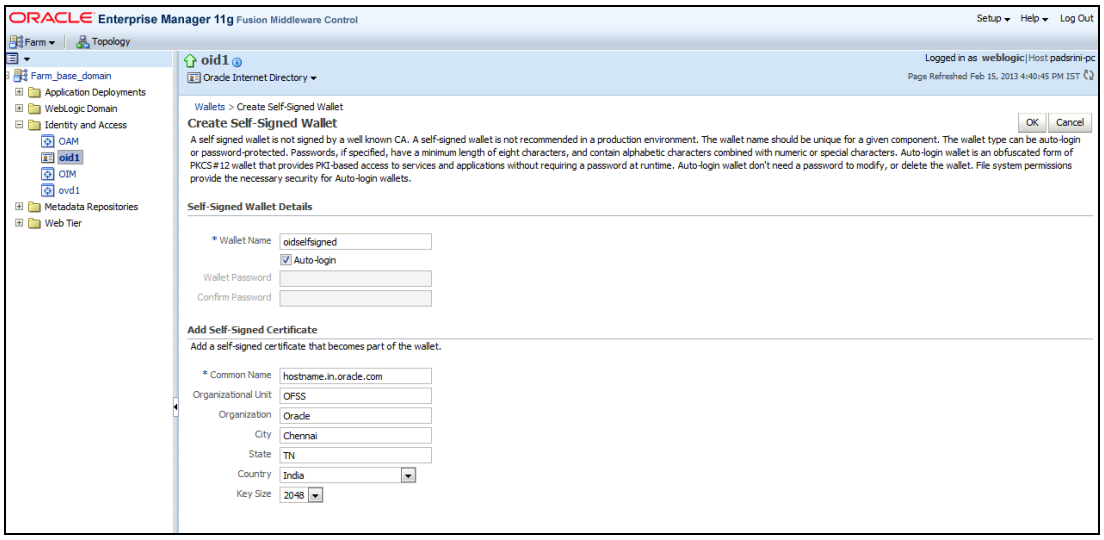
1. Login to the Enterprise Manager Console of the domain, in which Oracle Internet Directory is associated.

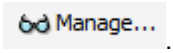


2. Click ‘Create Self-Signed Wallet’.

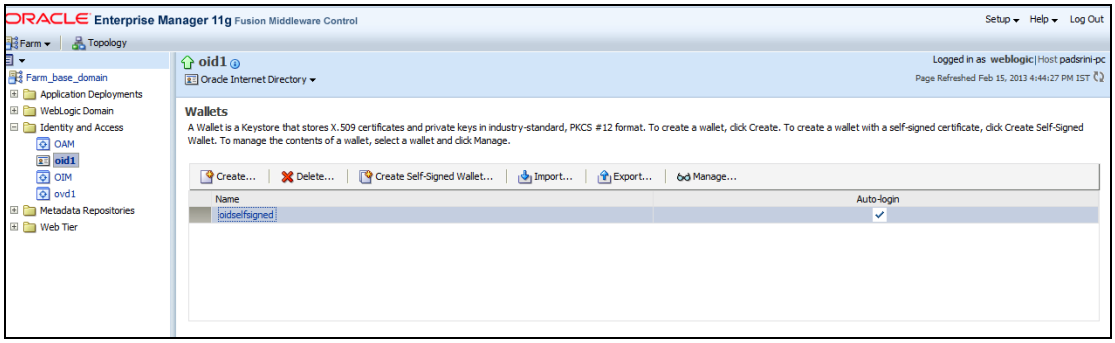


3. Enter the Details as below and Click ‘OK’.

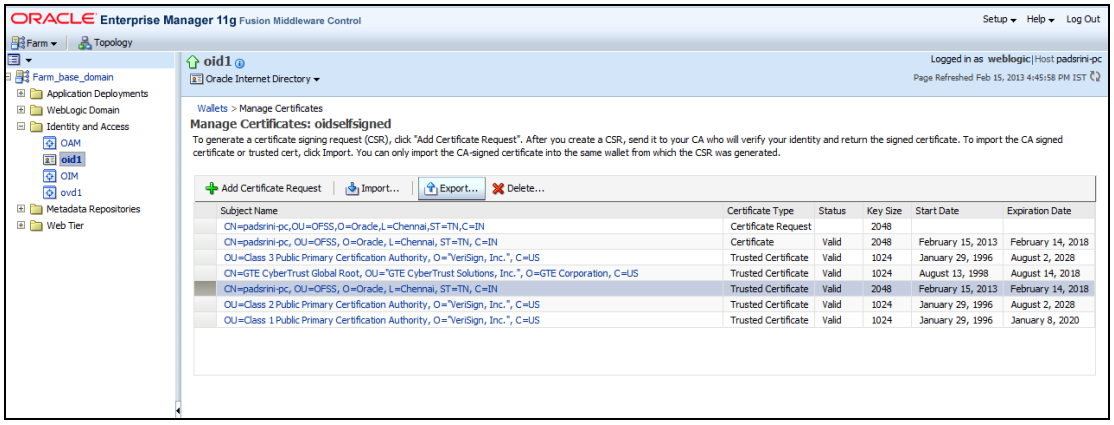


4. Click 

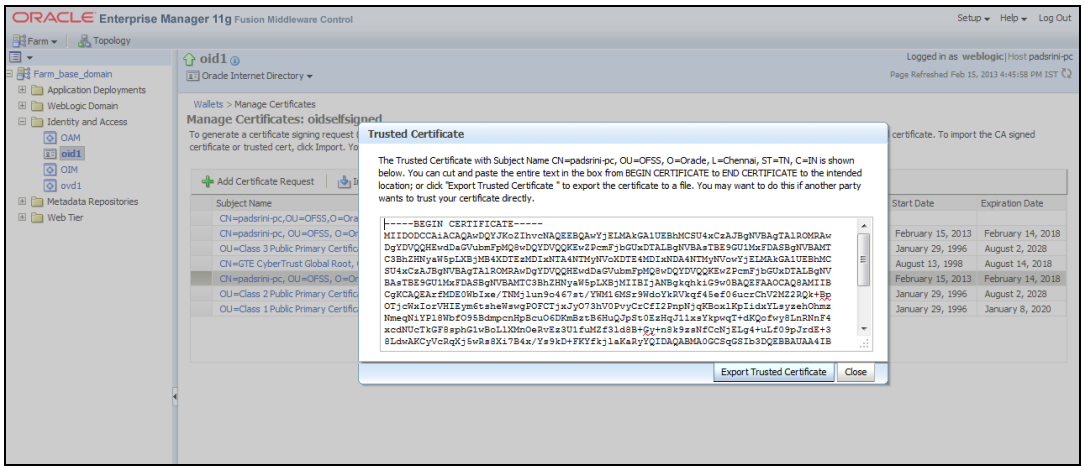
.



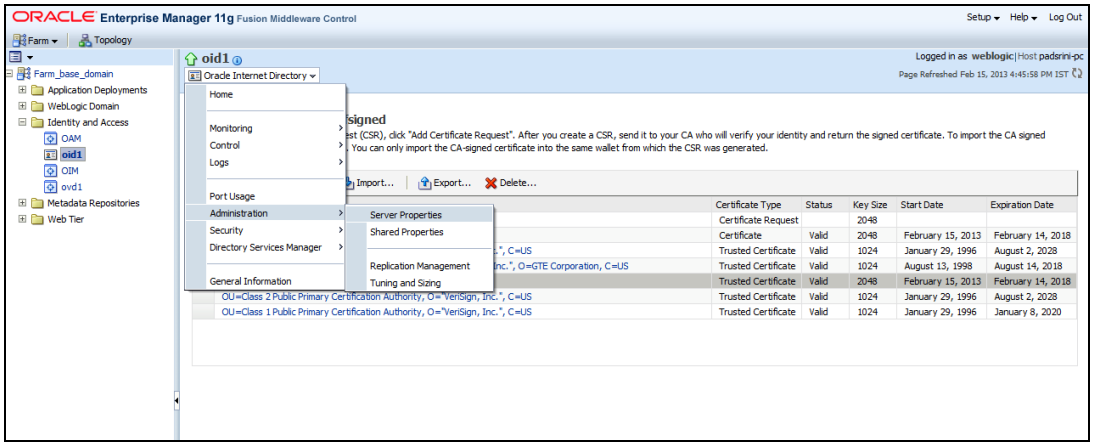
5. Select the Trusted Certificate and Click ‘Export’.



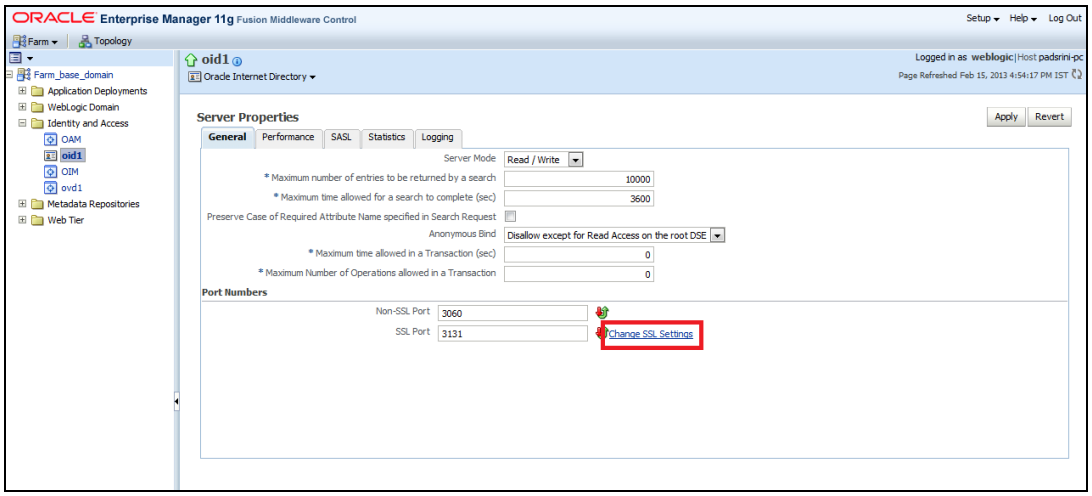
6. Click ‘Export Trusted Certificate’ and save the certificate file.



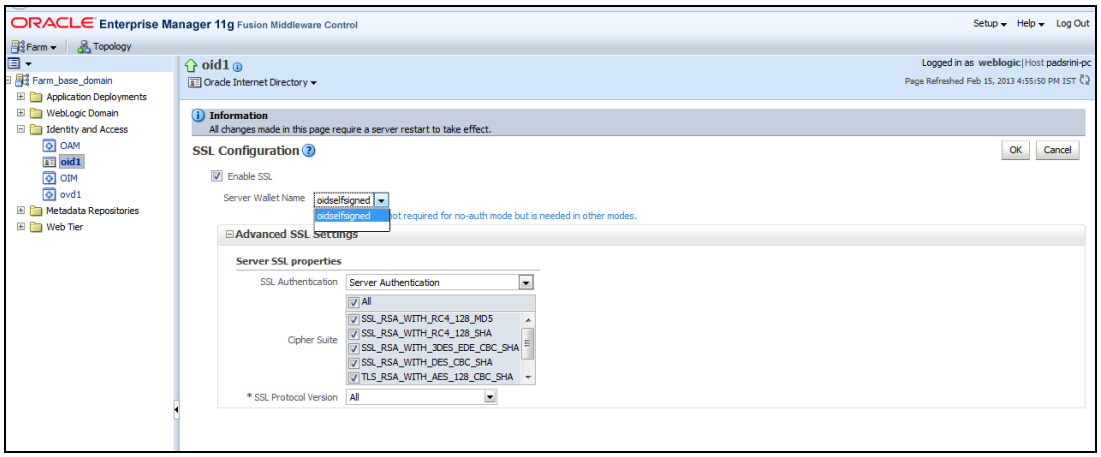
7. Click ‘Server Properties’.



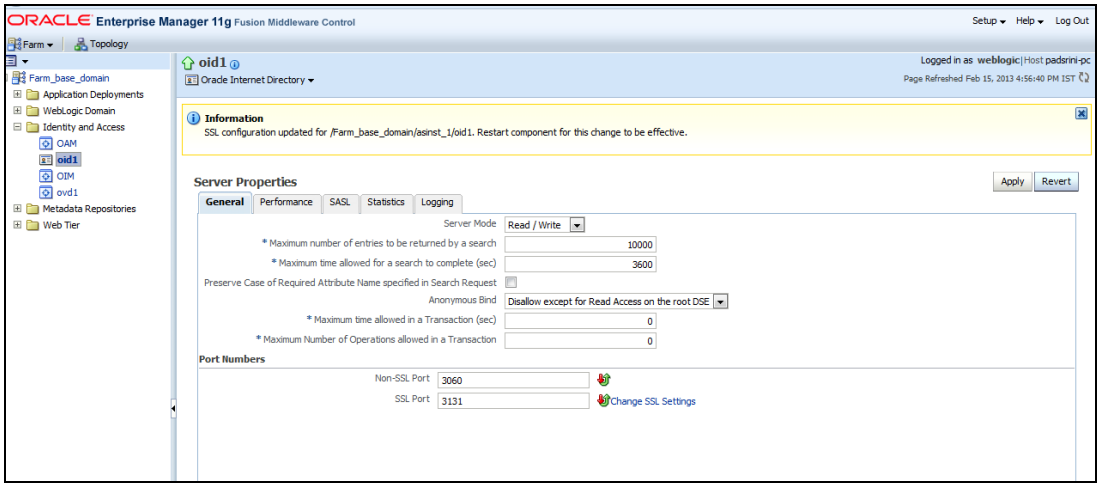
8. Click ‘Change SSL Settings’.



9. Select the Wallet, SSL Authentication as Server Authentication, Cipher Suite, SSL Protocal Version as below and click ‘OK’.



10. Click ‘Apply’.



2.5.3.1 Import LDAP Server SSL Certificate into OAM Server

We have to import the LDAP – Server certificatefile into OAM server’s JAVA_HOME/jre/lib/security/cacerts. Default Password is “**changeit**”.

For eg:

keytool -import -v -trustcacerts -alias ldapcacert –file ldap_server_certificate.cer -keystore JAVA_HOME/jre/lib/security/cacerts -storepass changeit

Restart Both OID & OAM Server.

2.6 Configuring SSO in OAM Console

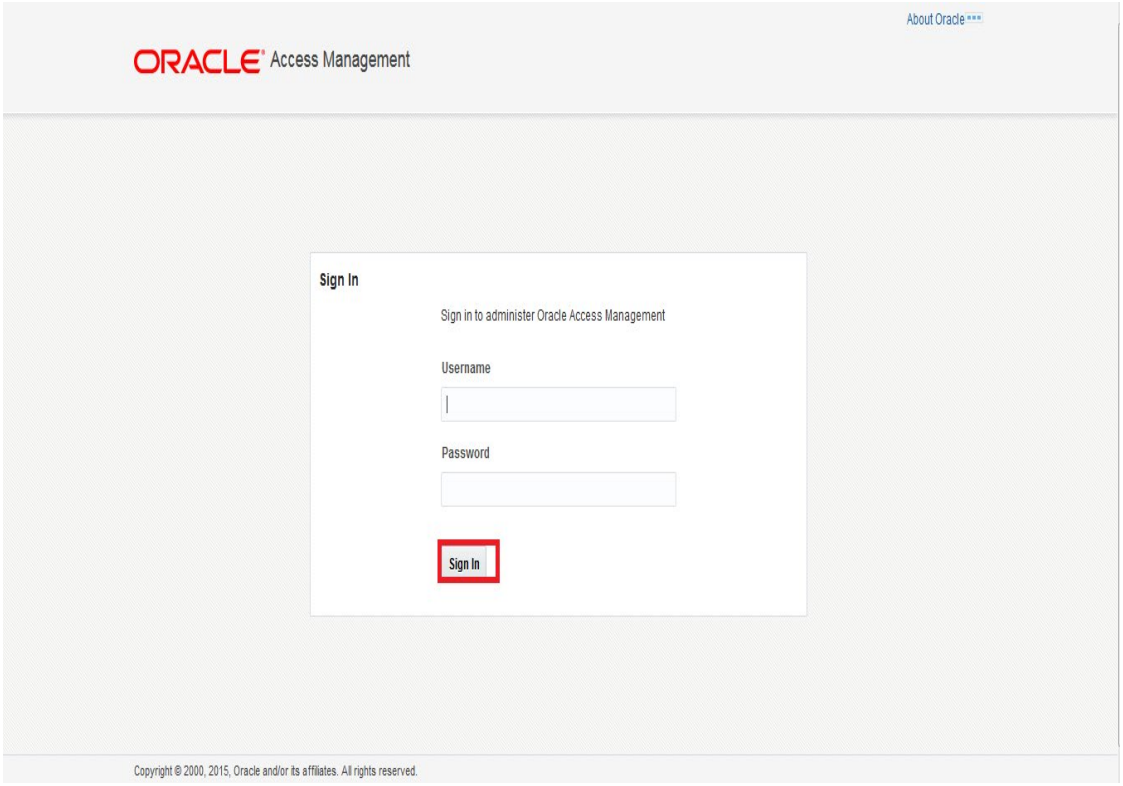
After installing OAM, Webtier Utilities and Webgate, extend the Weblogic domain to create OAM server.

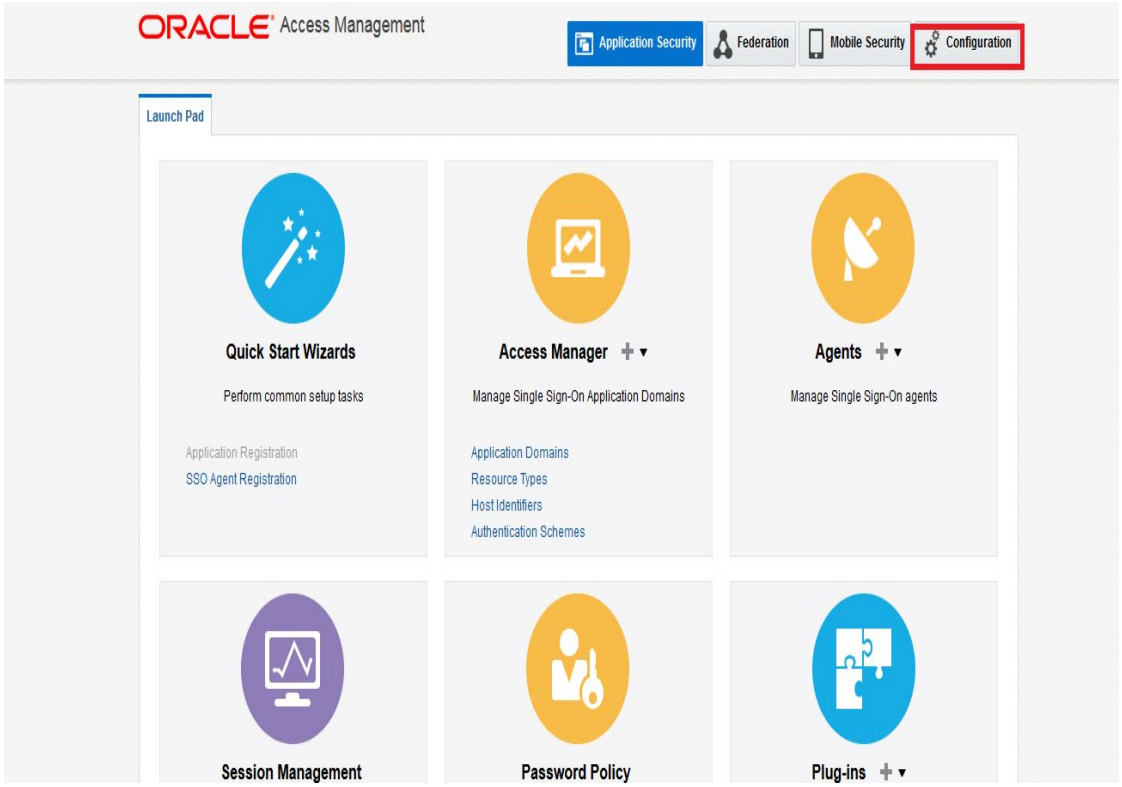
Follow the post installation scripts deployWebGate and EditHttpConf as provided in (http://docs.oracle.com/cd/E37115_01/install.1112/e38922/webgate_ohs.htm#CACDEJAD)

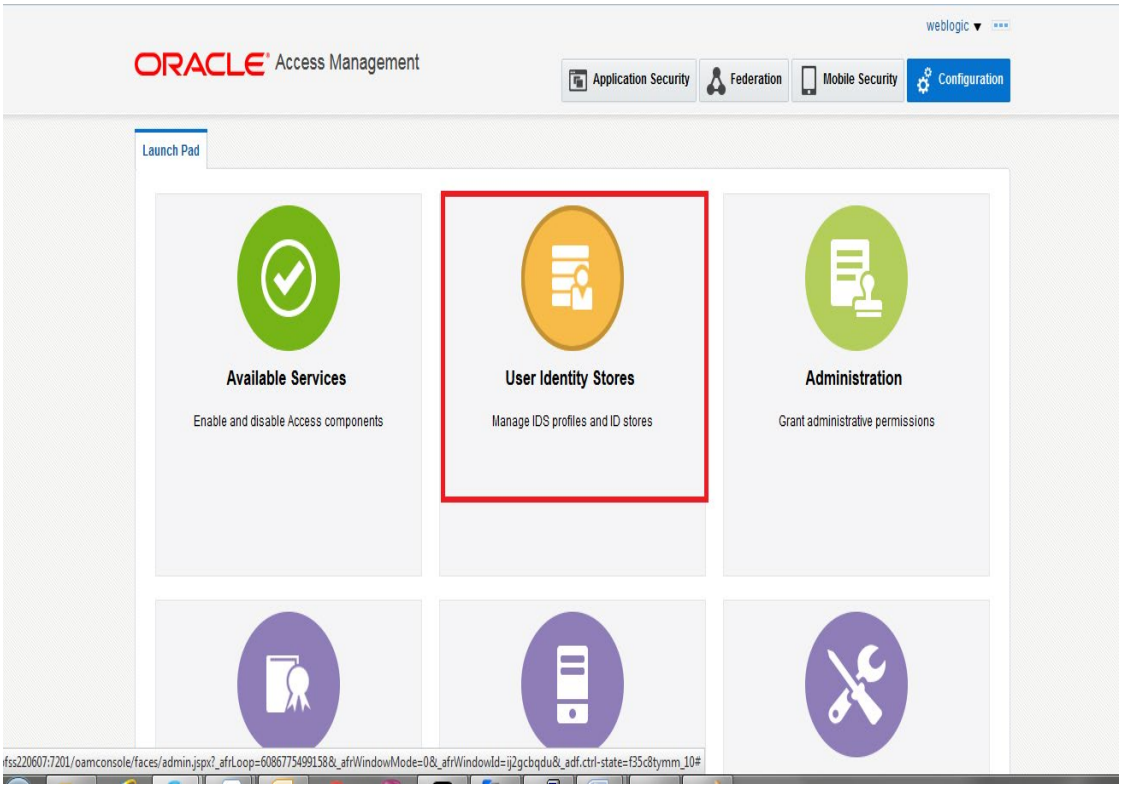
Note: Refer Oracle Support Document: **1935703.1**, to have skip the escape sequence \ (slash) infront of , (comma) in Oracle 11gR2 OAM request header values

2.6.1 Identity Store Creation

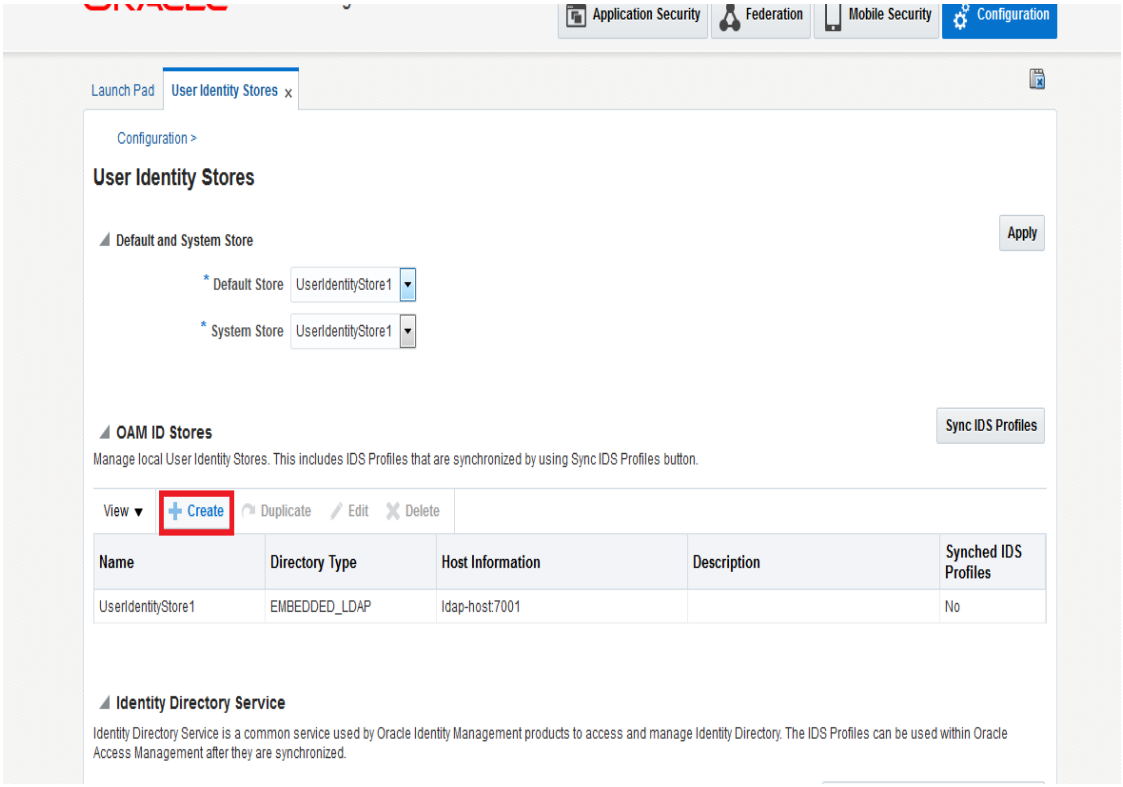
1. To create new User Identity Store, Login to OAM Console and Click 'User Identity Store' under Configuration.



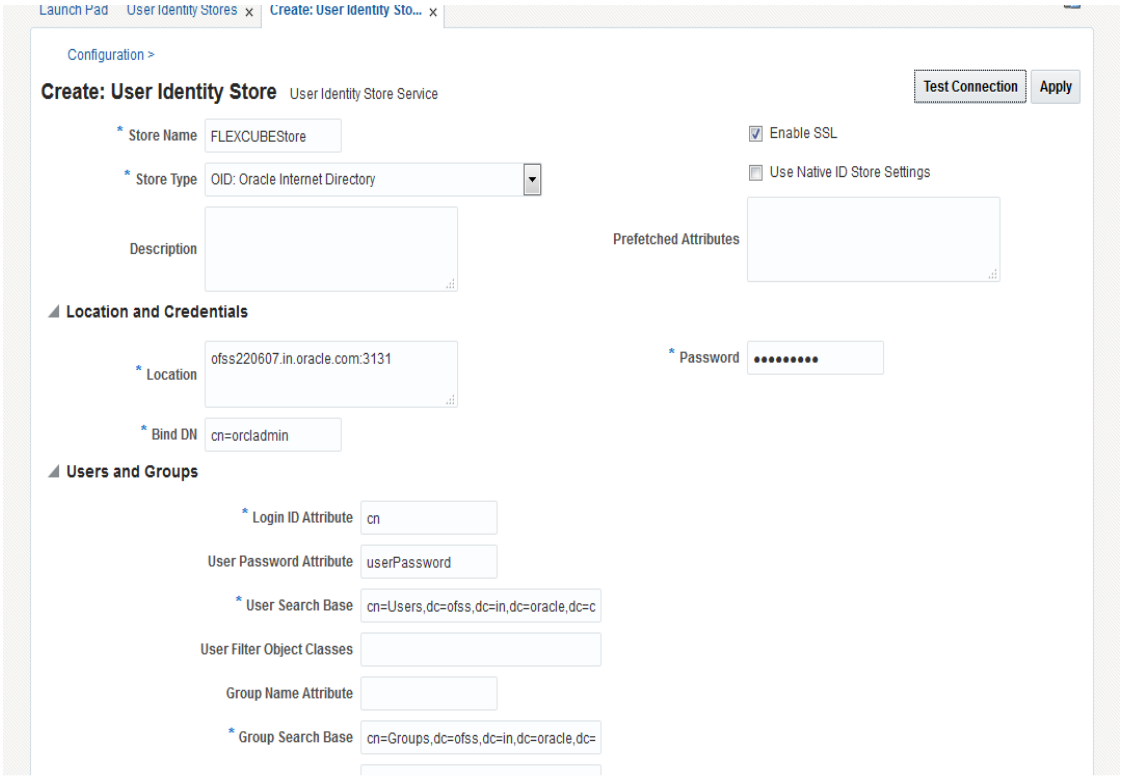




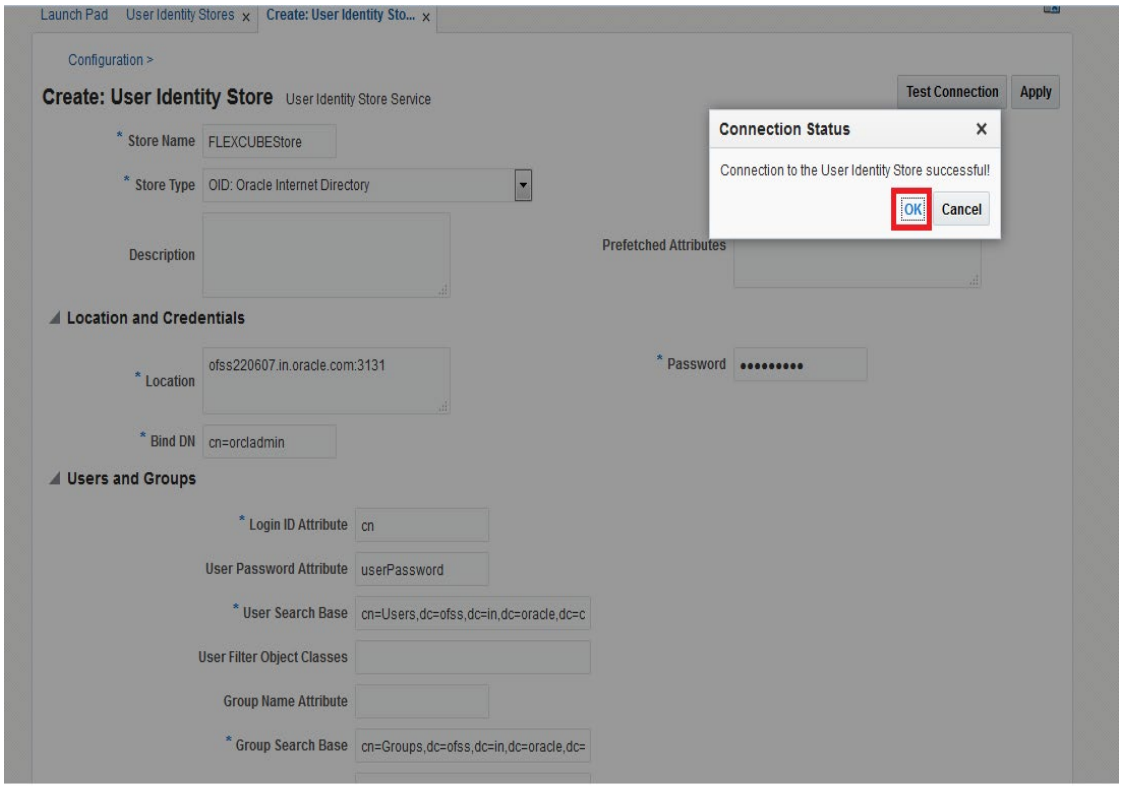
2. Click ‘Create’ under OAM ID Stores.



3. Enter the below details in the Create User Identity Store Form
   - Store Name : FLEXCUBEStore
   - Choose Store Type as OID: Oracle Internet Directory.
   - Location: LDAP server Host name and Port Number in <HOSTNAME>:SSL PORT format
   - Select Enable SSL check box
   - Bind DN: Admin User name to connect the LDAP Server
   - Password: Admin Password to connect the LDAP Server
   - Login ID Attribute: Specify the LDAP attribute from which the login ID specifying the User will be extracted (cn).
   - User Search Base: Full DN for the node at which enterprise users are stored in the directory; for example, cn=Users,realm_DN.
   - Group Search Base: Currently only static groups are supported, with the uniquemember attribute. The node in the directory information tree (DIT) under which group data is stored, and the highest possible base for all group data searches.

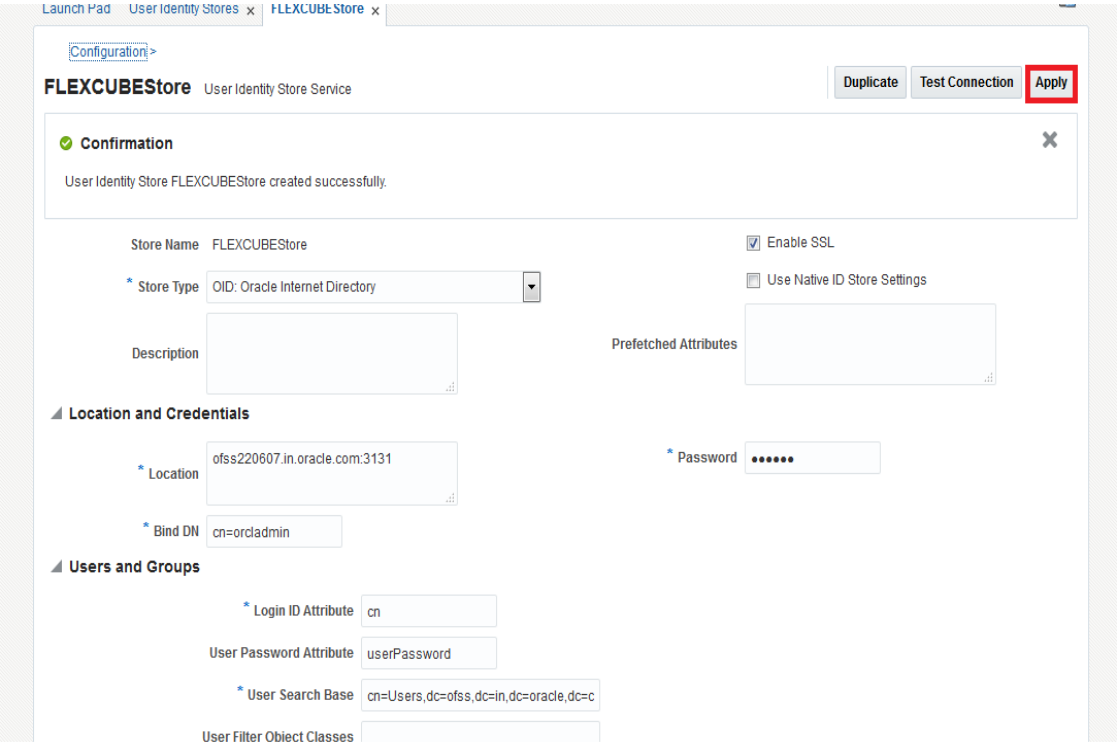


4. Click ‘Test Connection’ to validate the Credentials Passed.



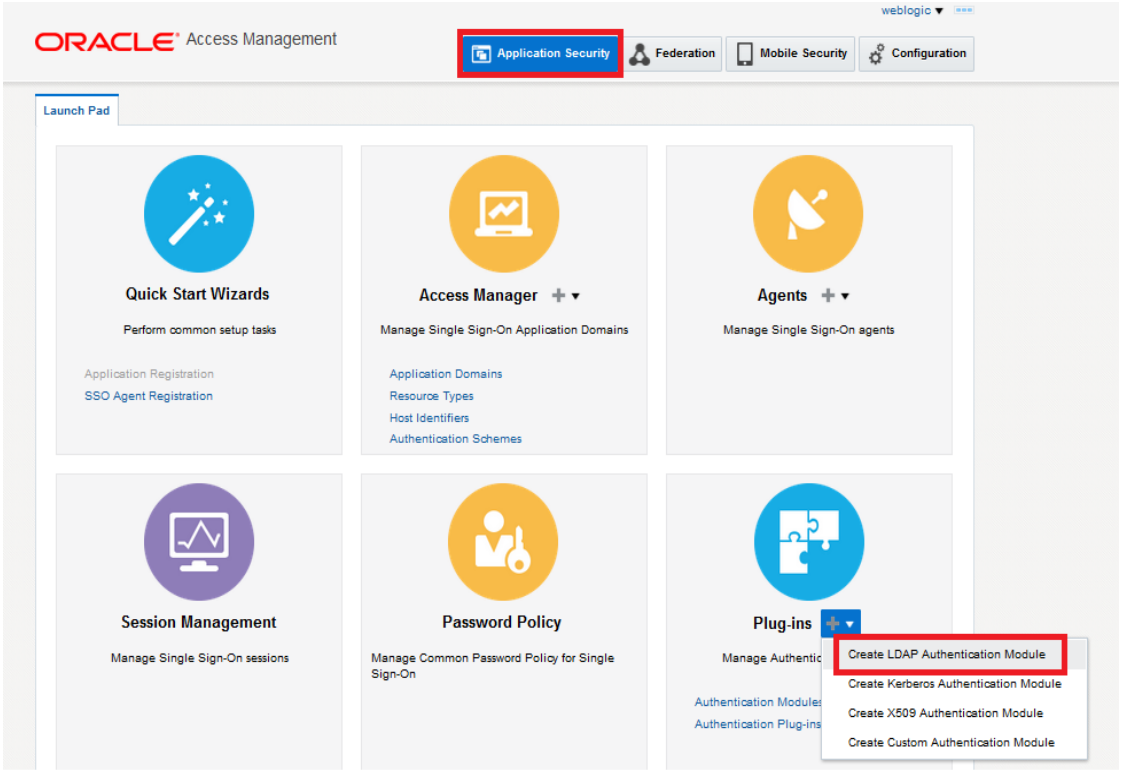
5. Click ‘Apply’ to Create the User Identity Store.

Note: User Identity Store will be created only if valid LDAP Parameters are passed.

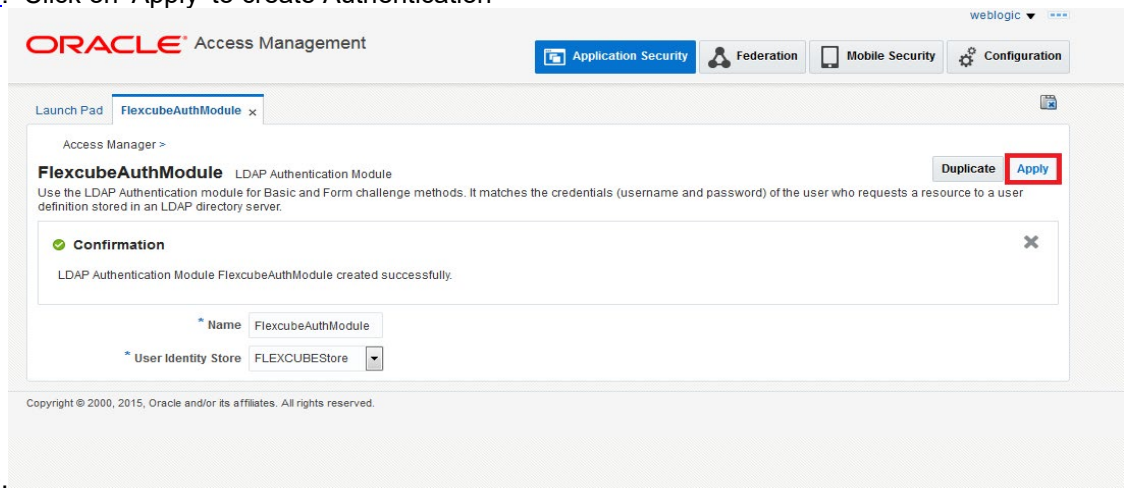


2.6.2 Creating Authentication Module

1. Click on  in Plug-ins under Application security to Create LDAP Authentication Modules.



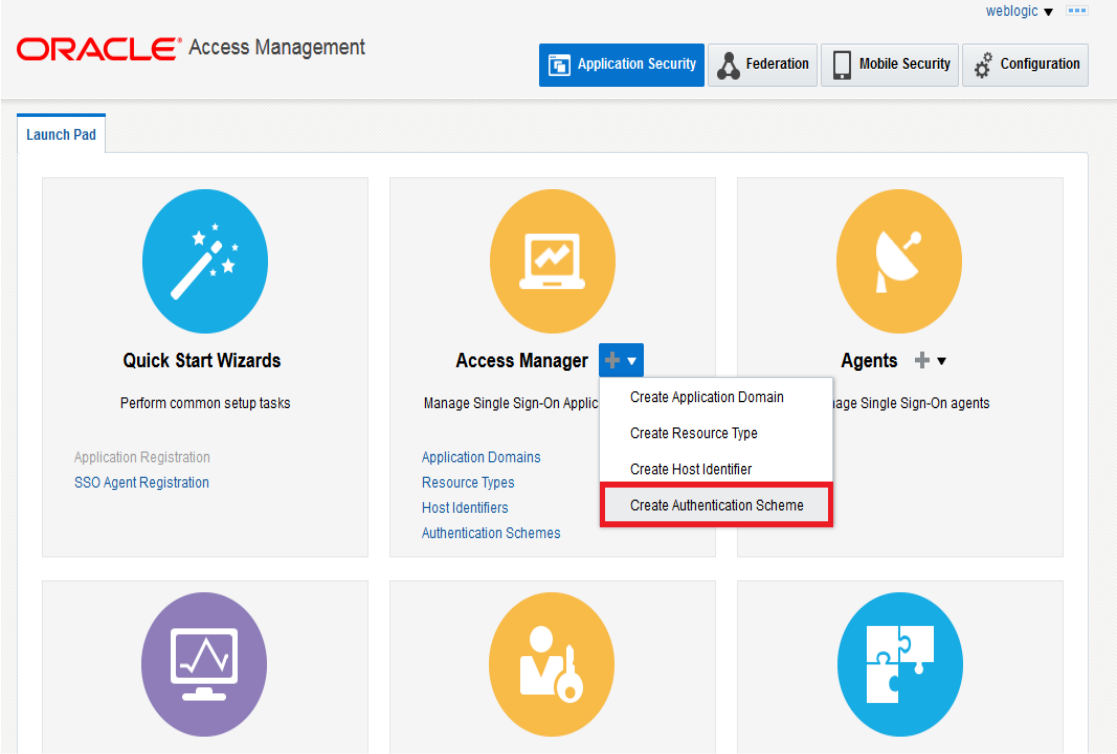
Enter the Name for the Authentication Module and choose the proper User Identification Store, ie created in 2.6.1. Click on 'Apply' to create Authentication



Module.

2.6.3 Creating Authentication Scheme

1. Click on  in Access Manager under Application Security to 'Create Authentication Scheme'.



Select any of the challenge method for creating an authentication Scheme as explained below and refer to OAM documentation for more details on the same.

2.6.3.1.1 https://docs.oracle.com/cd/E52734_01/oam/AIAAG/shared.htm#AIAAG488

Basic Style Authentication Scheme

Enter the below details and click ‘Apply’:

Name : Name of the Authentication Scheme

Authentication Level : 1

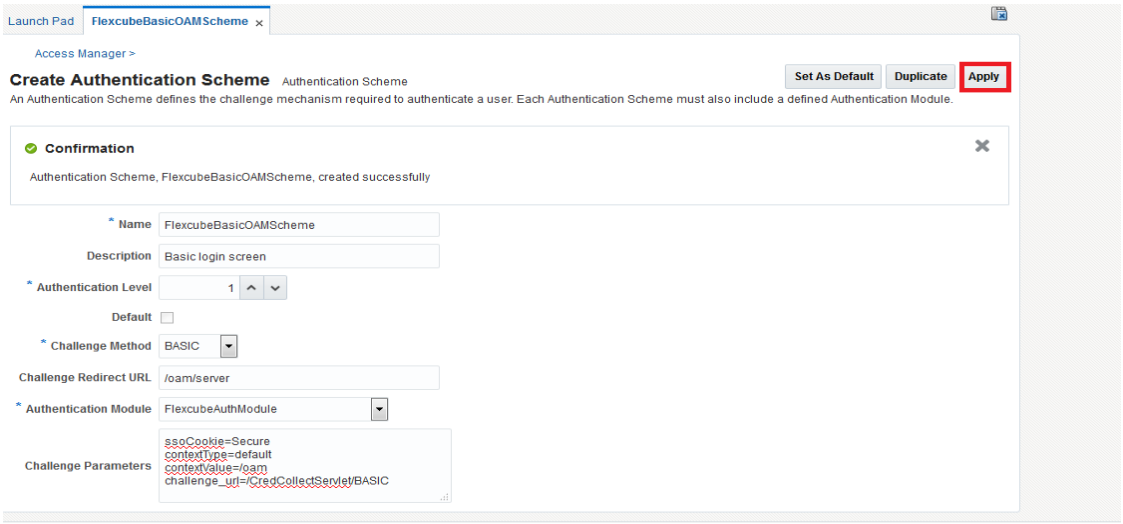
Challenge Method : BASIC

Challenge Redirect URL : /oam/server

Authentication Module : Authentication Module

Refer the section ‘Creating Authentication Module 2.6.2’ of this document.

Challenge Parameters : ssoCookie=Secure
contextType=default
contextValue=/oam
challenge_url=/CredCollectServlet/BASIC



We need to add the 'enforce-valid-basic-auth-credentials' tag to the config.xml file ,located under <weblogic deployment path>/user_projects/domains/<MyDomain>/config/.

The tag must be inserted within the <security-configuration> tag as follows: [Just above </security-configuration> tag]
<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>

2.6.3.2 Form Style Authentication Scheme

Enter the below details and click ‘Apply’:

Name : Name of the Authentication Scheme

Authentication Level : 2

Challenge Method : FORM

Challenge Redirect URL : /oam/server

Authentication Module : Authentication Module

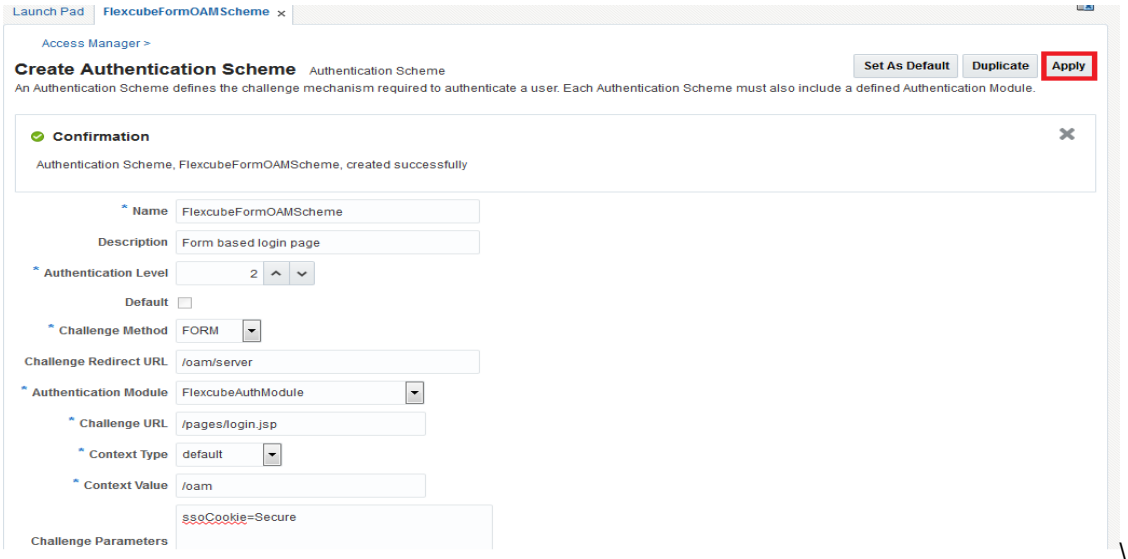
Refer the section ‘Creating Authentication Module 2.6.2’ of this document.

Challenge URL : /pages/login.jsp

Context Type : default

Context Value : /oam

Challenge Parameters : ssoCookie=Secure



2.6.3.3 KBA Based Strong Authentication Scheme (Only in case OAAM is used)

Enter the Below Details and click 'Apply':

Name : Name of the Authentication Scheme

Authentication Level : 2

Challenge Method : FORM

Challenge Redirect URL : /oam/server

Authentication Module : Authentication Module

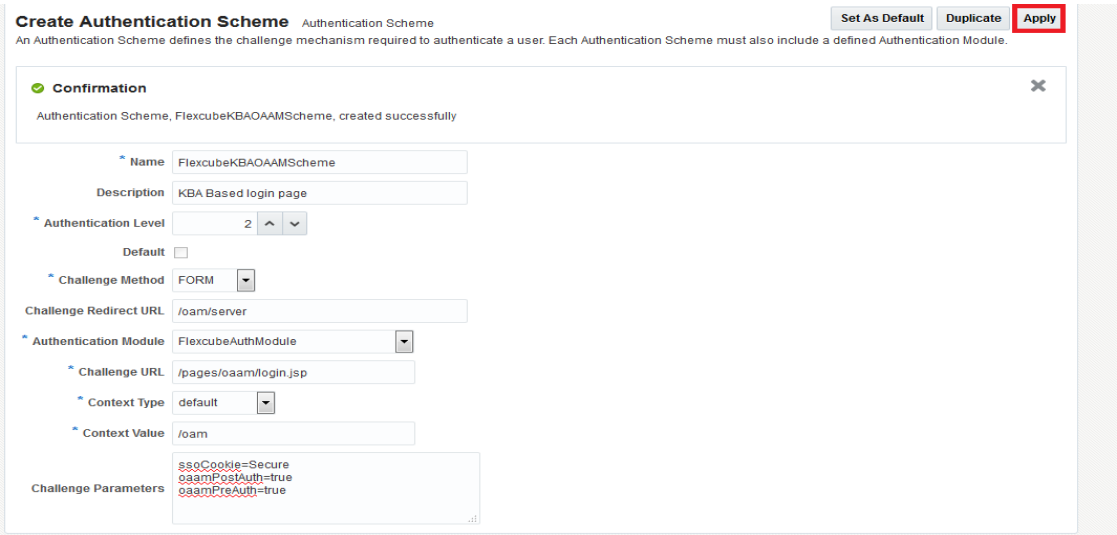
Refer the section 'Creating Authentication Module 2.6.2' of this document.

Challenge URL : /pages/oaam/login.jsp

Context Type : default

Context Value : /oam

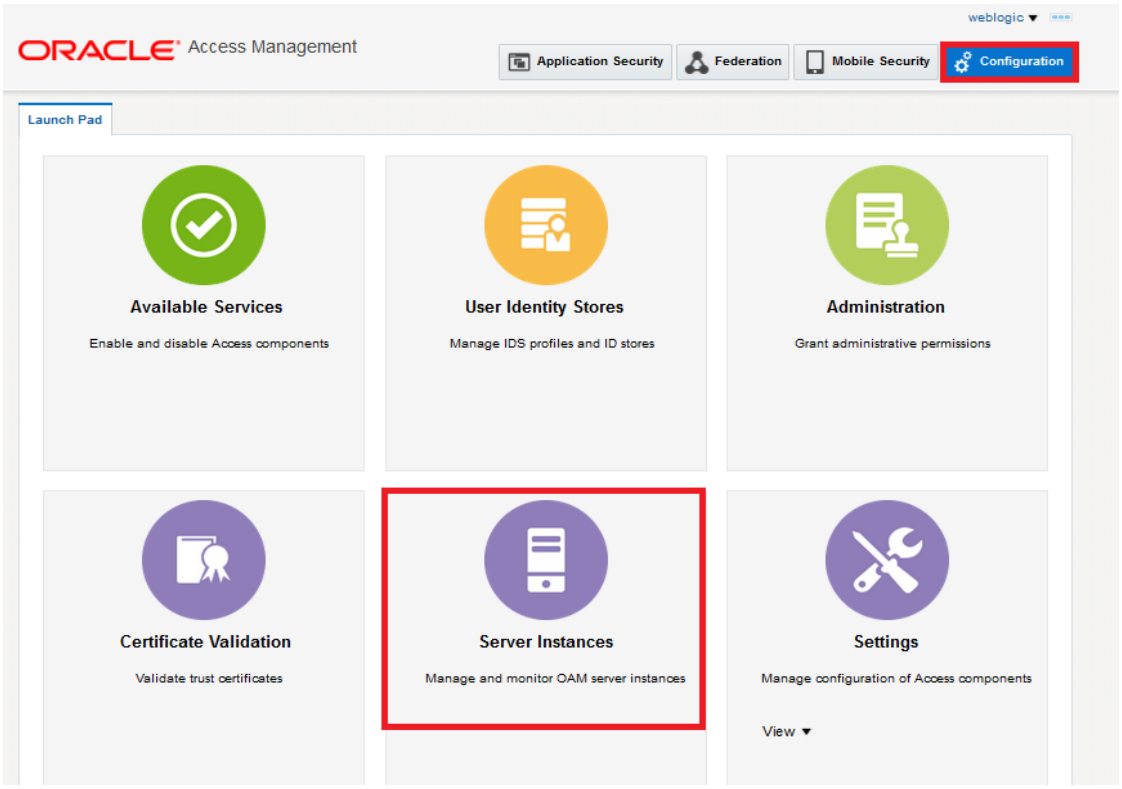
Challenge Parameters : ssoCookie=Secure
oaamPostAuth=true
oaamPreAuth=true



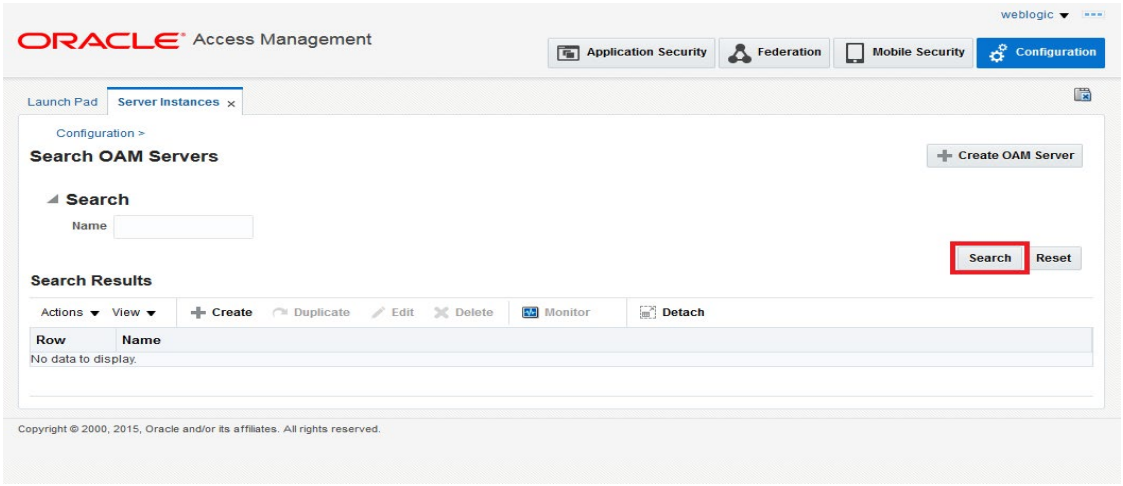
2.6.4 Creating OAM 11g Webgate

Follow the below steps to create a Webgate:

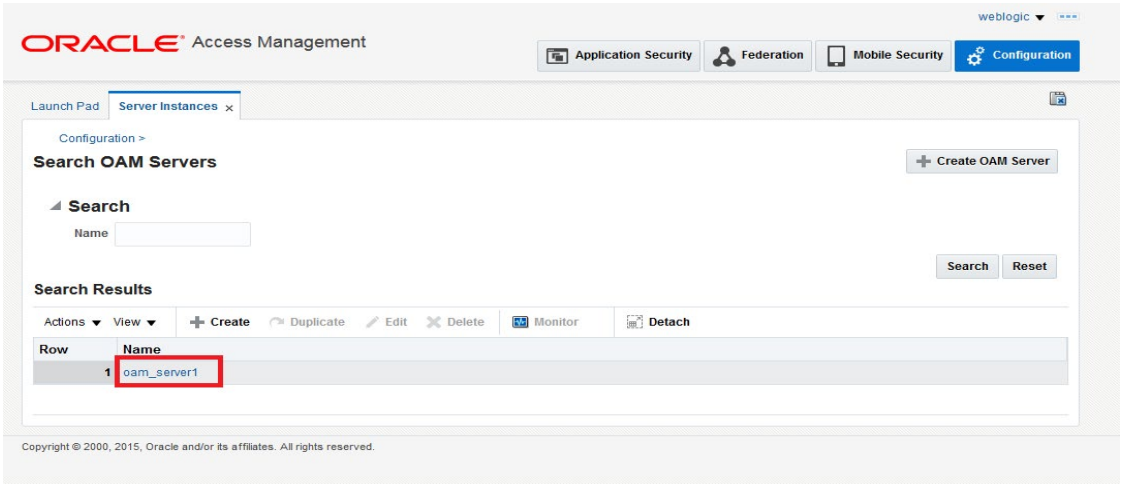
1. Click on 'Server Instances' under Configuration.


weblogic
ORACLE Access Management
Application Security
Federation
Mobile Security
Configuration
Launch Pad
Available Services
Enable and disable Access components
User Identity Stores
Manage IDS profiles and ID stores
Administration
Grant administrative permissions
Certificate Validation
Validate trust certificates
Server Instances
Manage and monitor OAM server instances
Settings
Manage configuration of Access components
View

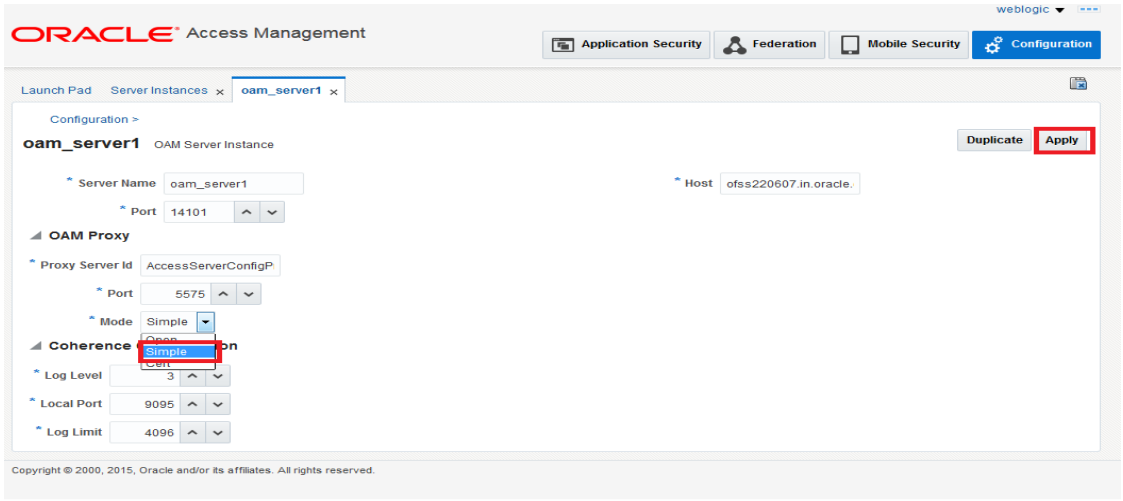
2. Click on ‘Search’.

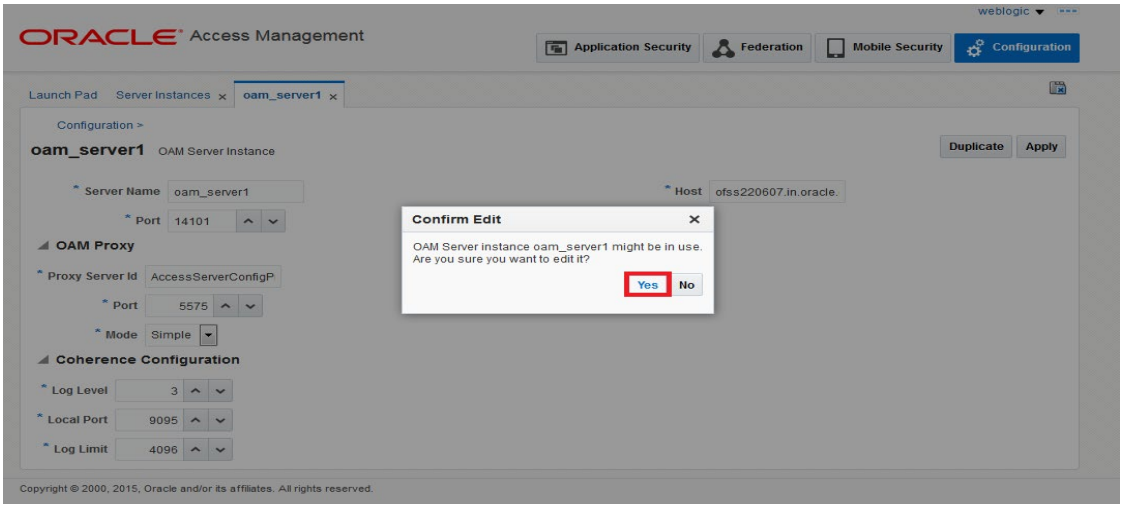


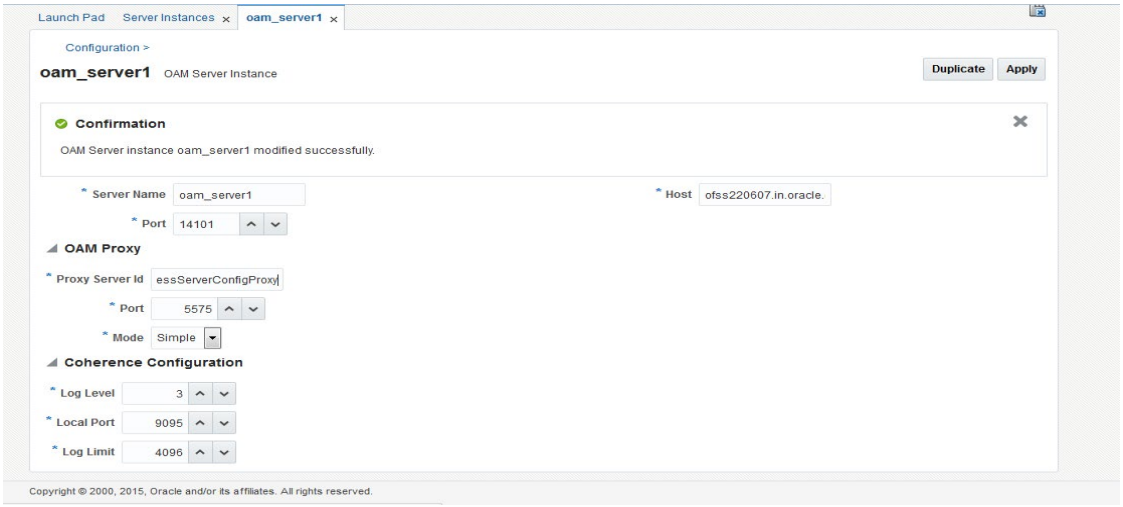
3. Edit oam_server1.



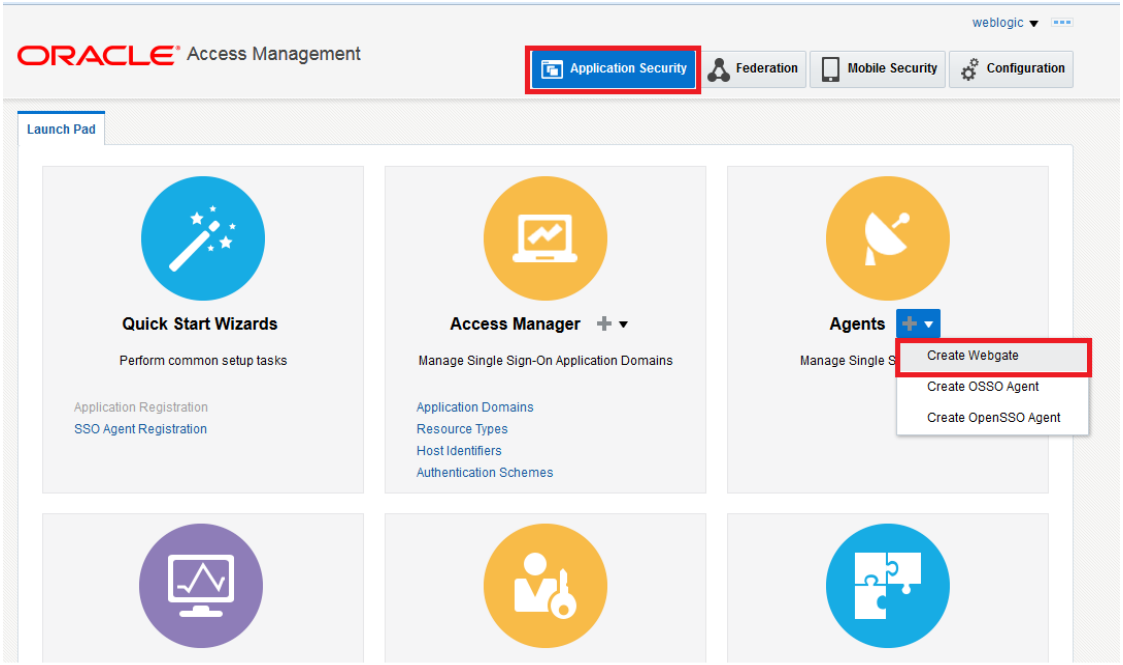
4. Modify the Mode from Open to Simple and click on ‘Apply’.




ORACLE Access Management
weblogic
Application Security
Federation
Mobile Security
Configuration
Launch Pad
Server Instances
oam_server1
Configuration >
oam_server1
OAM Server Instance
Duplicate
Apply
* Server Name
oam_server1
* Host
ofss220607.in.oracle.
* Port
14101
Confirm Edit
OAM Server instance oam_server1 might be in use.
Are you sure you want to edit it?
Yes
No
OAM Proxy
* Proxy Server Id
AccessServerConfigP
* Port
5575
* Mode
Simple
Coherence Configuration
* Log Level
3
* Local Port
9095
* Log Limit
4096
Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

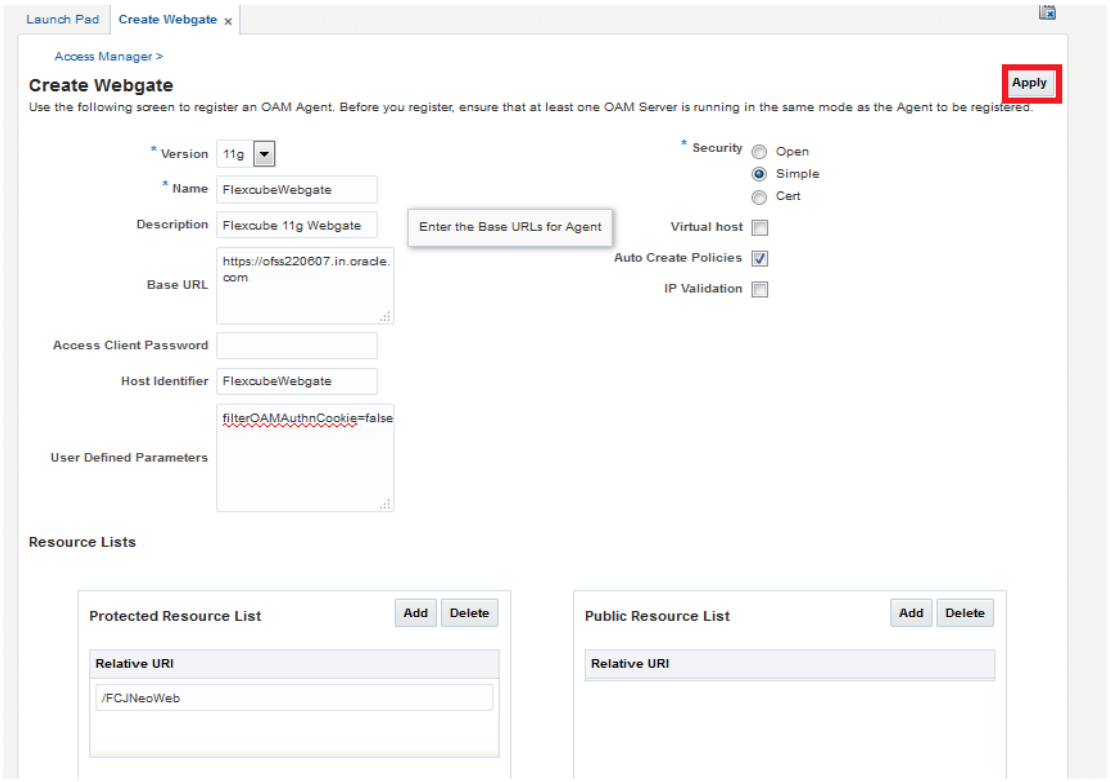

Launch Pad
Server Instances
oam_server1
Configuration >
oam_server1
OAM Server Instance
Duplicate
Apply
Confirmation
OAM Server instance oam_server1 modified successfully.
* Server Name
oam_server1
* Host
ofss220607.in.oracle.
* Port
14101
OAM Proxy
* Proxy Server Id
essServerConfigProxy
* Port
5575
* Mode
Simple
Coherence Configuration
* Log Level
3
* Local Port
9095
* Log Limit
4096
Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

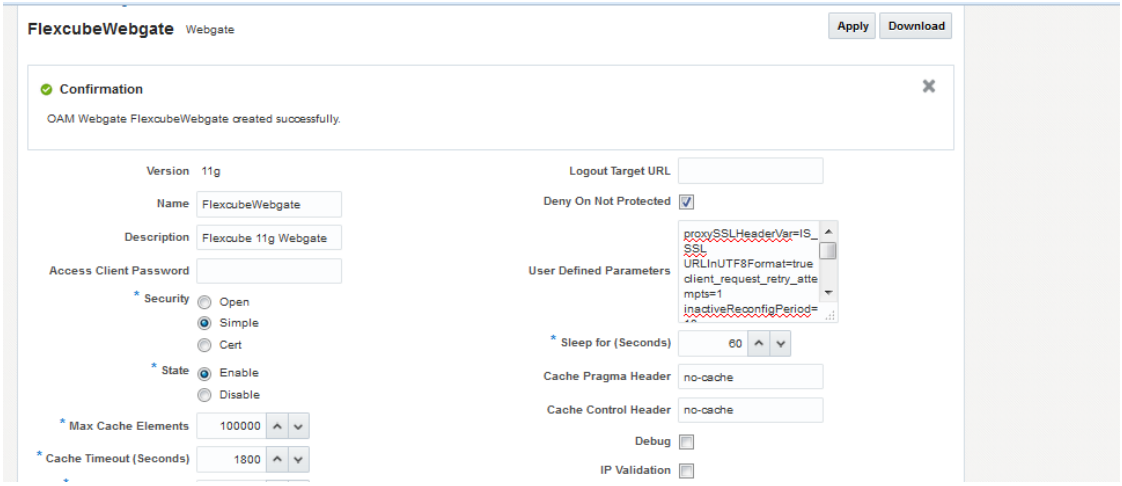
5. Click on  in Agents under Application Security to Create Webgate.



6. Enter the below and Click 'Apply':

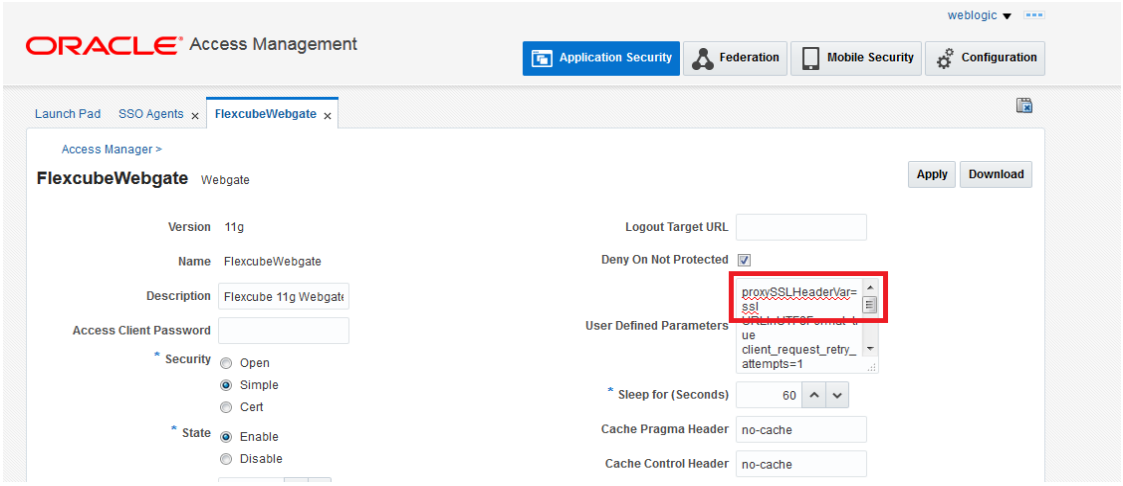
Version	: 11g
Name	: Custom Webgate Name
Base URL	: The host and port of the computer on which the Web server for the Webgate is installed. For example, http://example_host:port or https://example_host:port. The port number is optional.
Security	: Simple
Protected Resource List	: for FCUBS : /FCJNeoWeb For FCIS : /FCISNeoWeb
User Defined Parameters	: filterOAMAuthnCookie=false





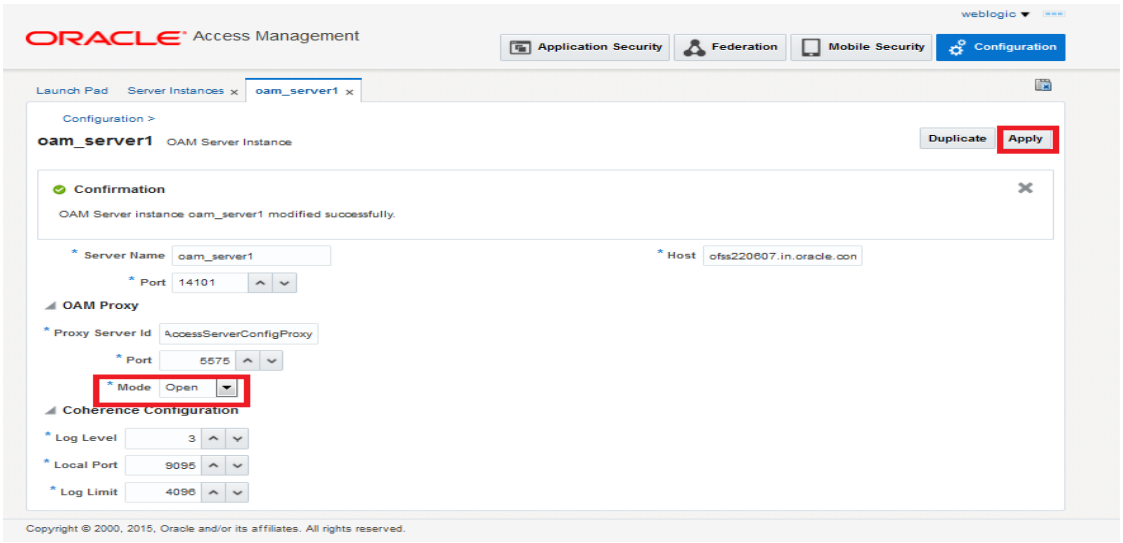
7. Once the OAM 11g Webgate is created, Change the parameter from **proxySSLHeaderVar=IS_SSL** to **proxySSLHeaderVar=ssl** along with other parameters in User Defined Parameters.

8. Click on ‘Apply’.



9. Change the value of Mode back to Open in oam_server1 on Server Instance and click 'Apply'.

   Refer 'Creating OAM 11g Webgate 2.6.3' section of this document.

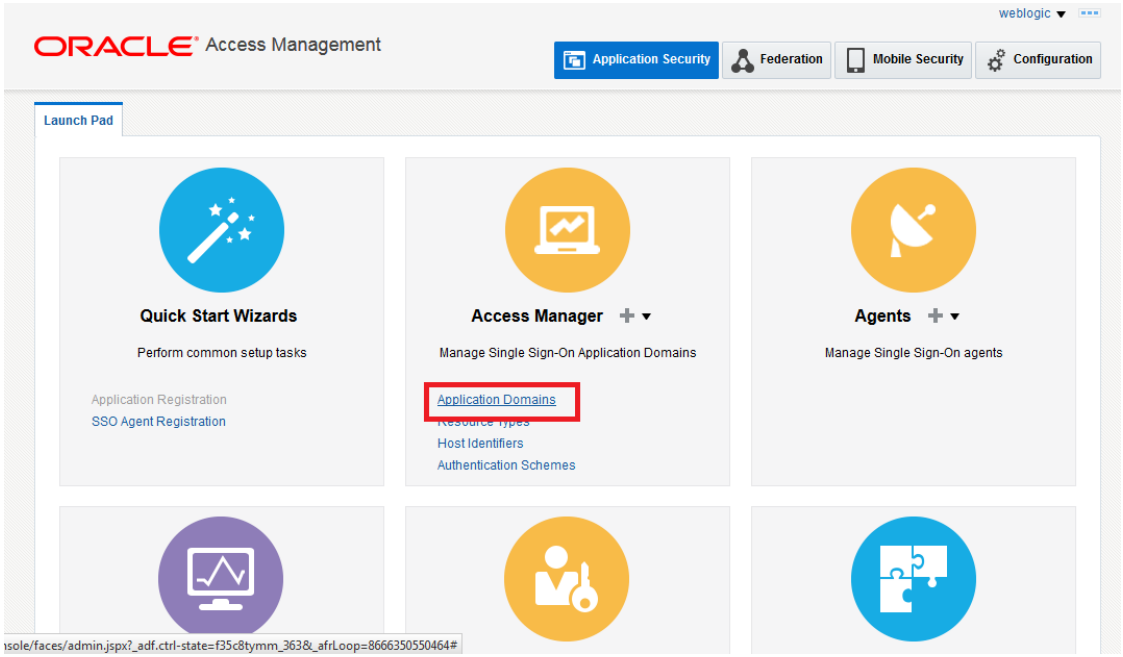


2.6.5 Post OAM Webgate 11g Creation

Follow the below steps to configure the webgate created .

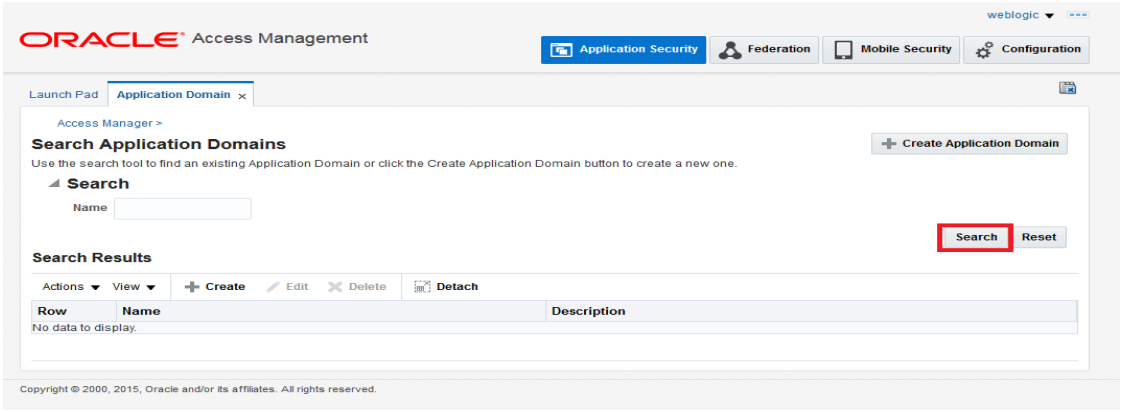
2.6.5.1 Application Domains Changes

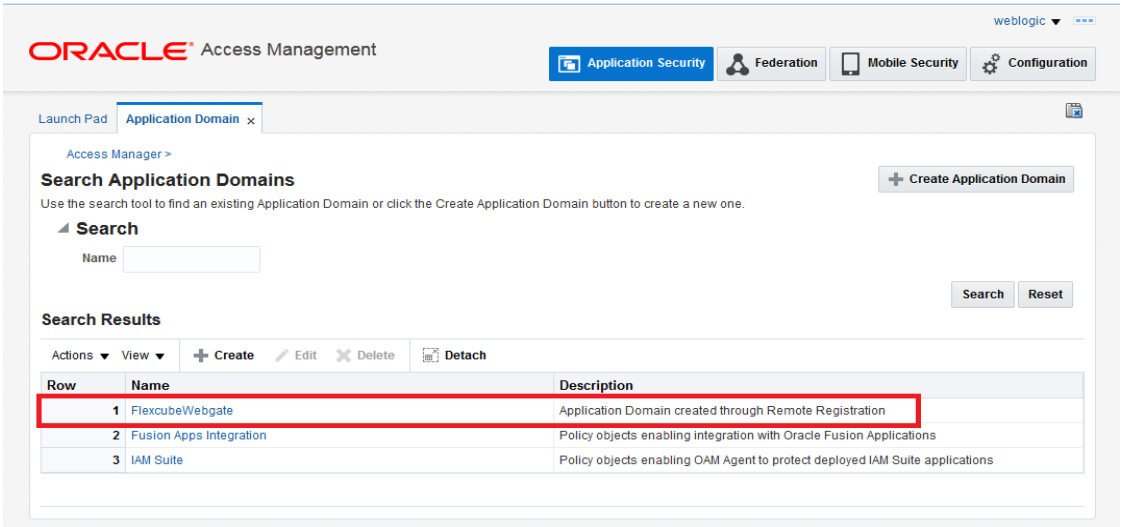
1. Click on ‘Application Domains’ in Access Manager under Application Security



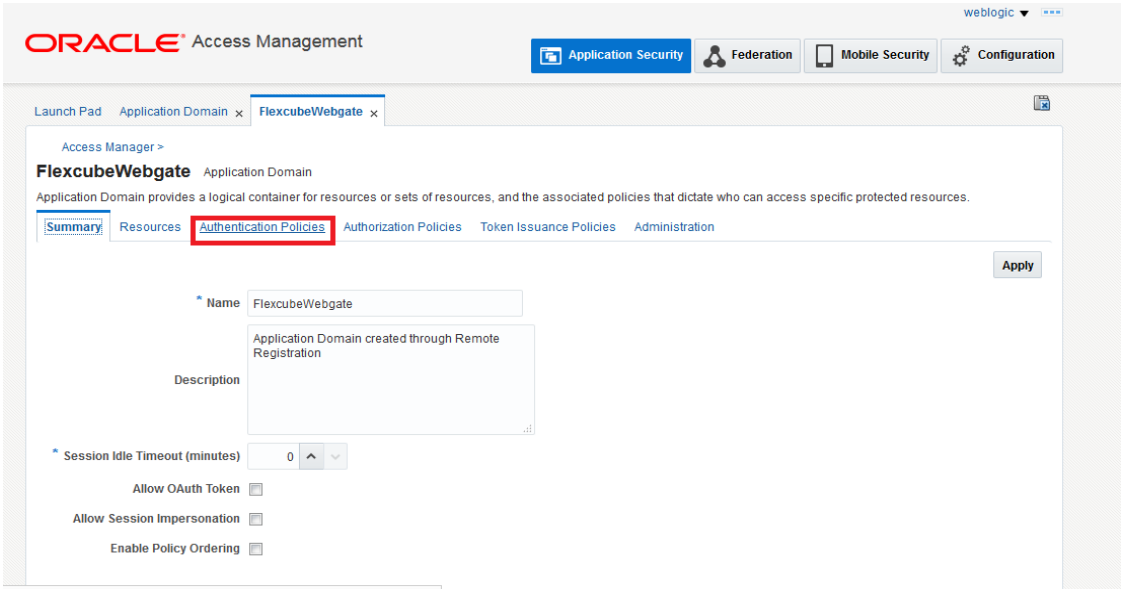
2. Click on ‘Search’ to find the 11g Webgate.

   Refer the section ‘Creating OAM 11g webgate 2.6.4’ of this document.

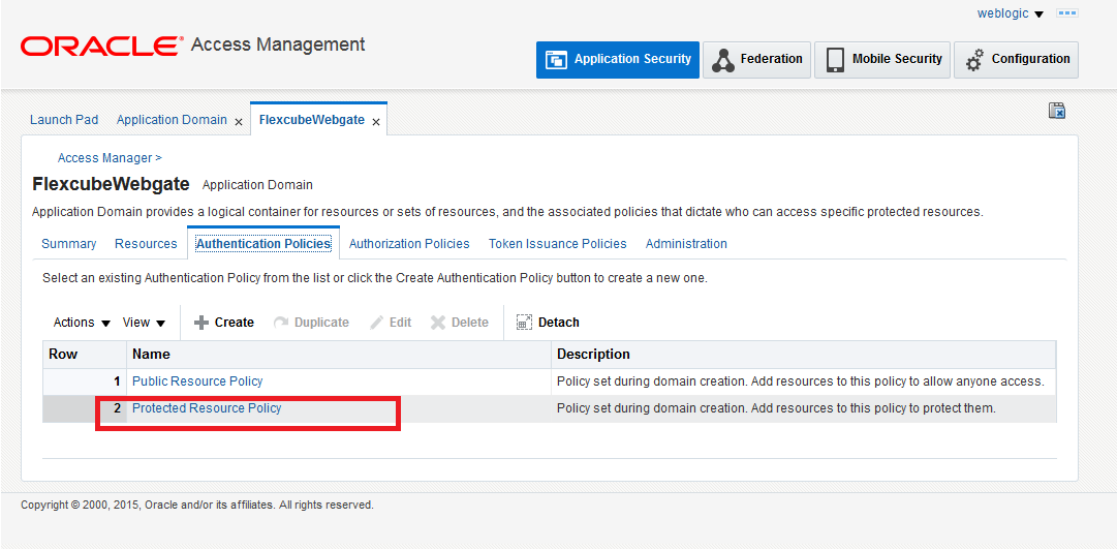




3. Click on ‘Authentication Polices’.

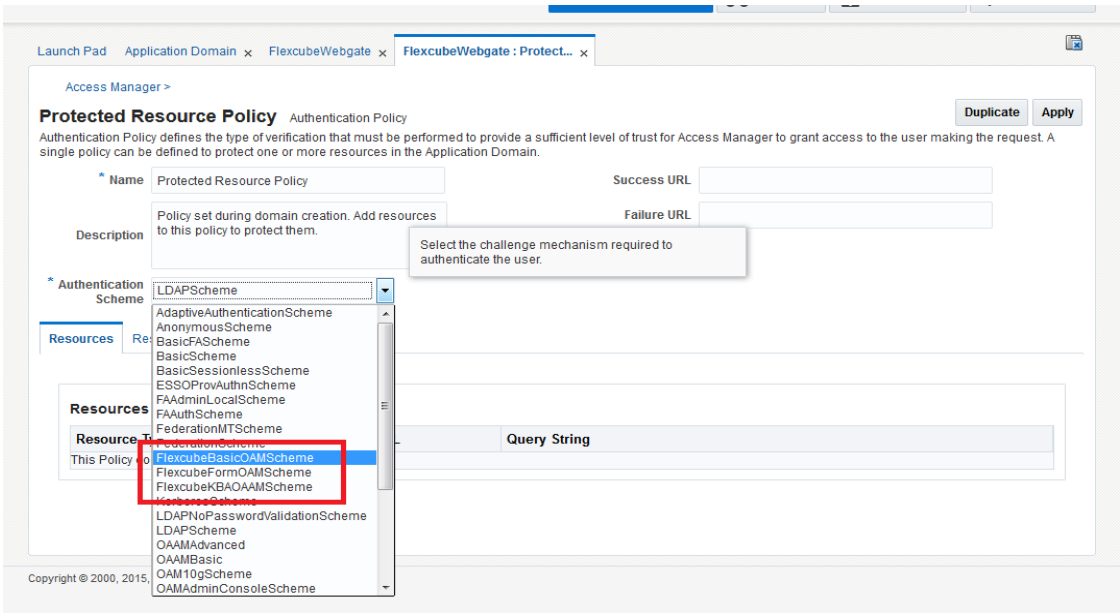


4. Click on ‘Protected Resource Policy’.

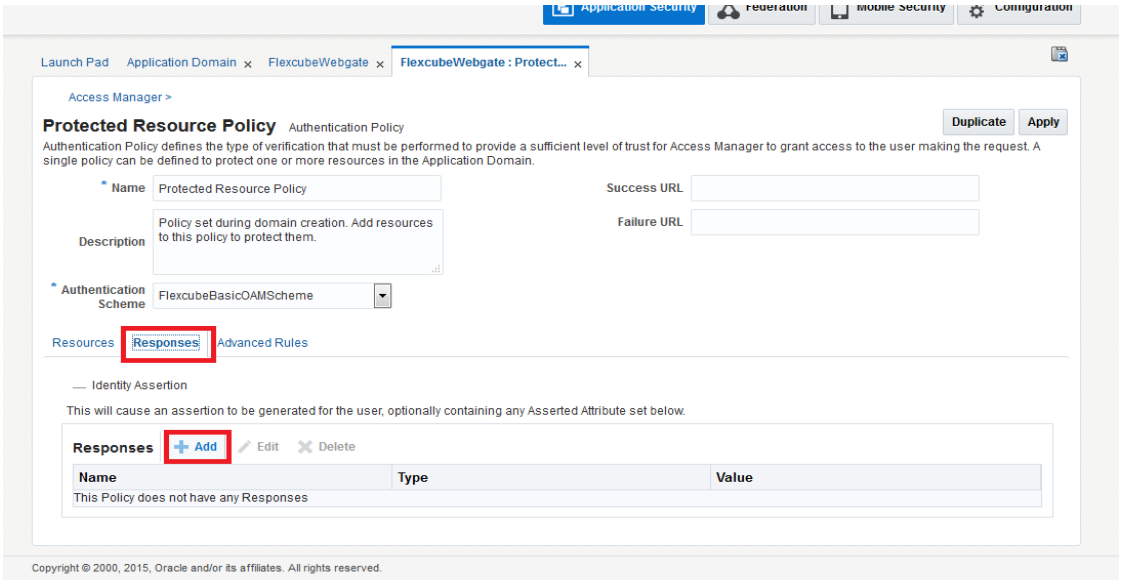


5. Choose the Authentication Scheme created earlier in ‘Creating Authentication Scheme’.

   Refer the section ‘Creating Authentication Scheme 2.6.3’ of this document.



6. Click ‘Responses’ tab and click + Add button to Add ‘DN’ variable to the Response Header.



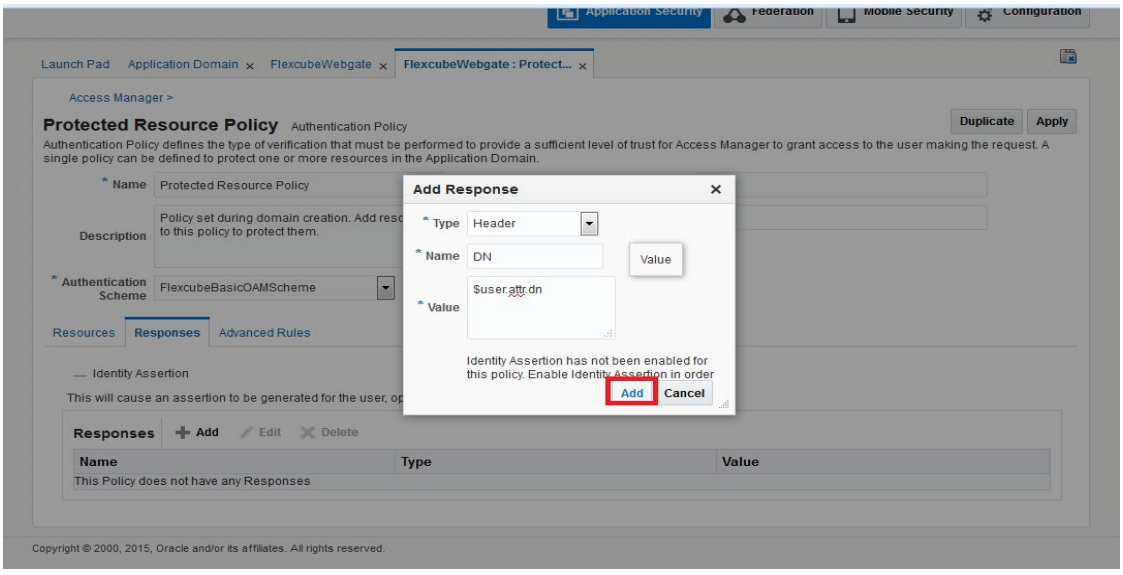
7. Enter the following values in the Add Response Window:

   Type : Header

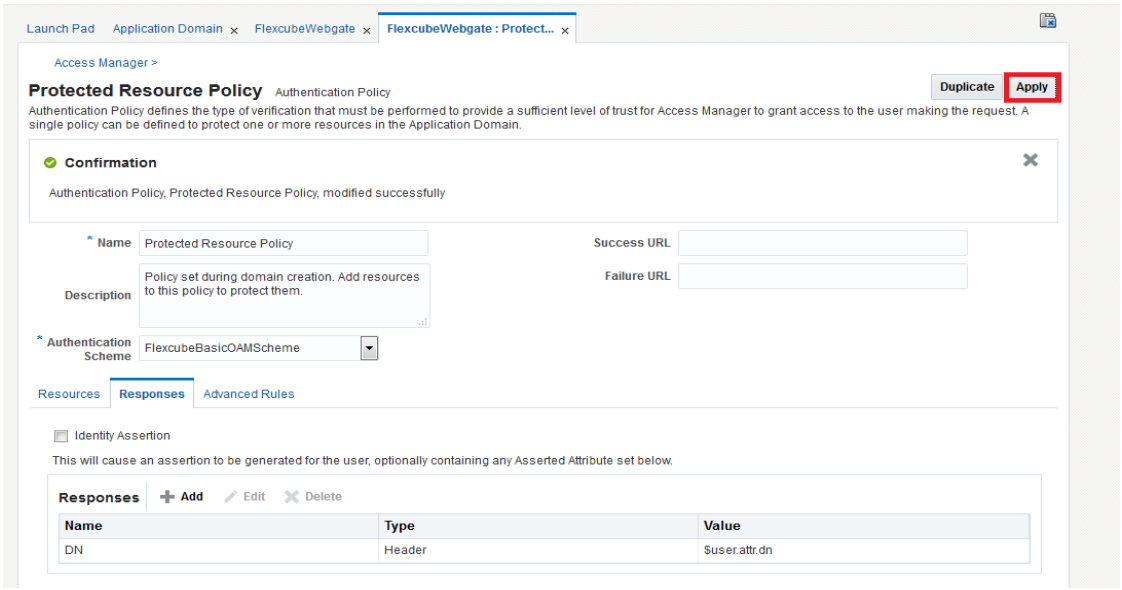
   Name : DN

   Value : $user.attr.dn

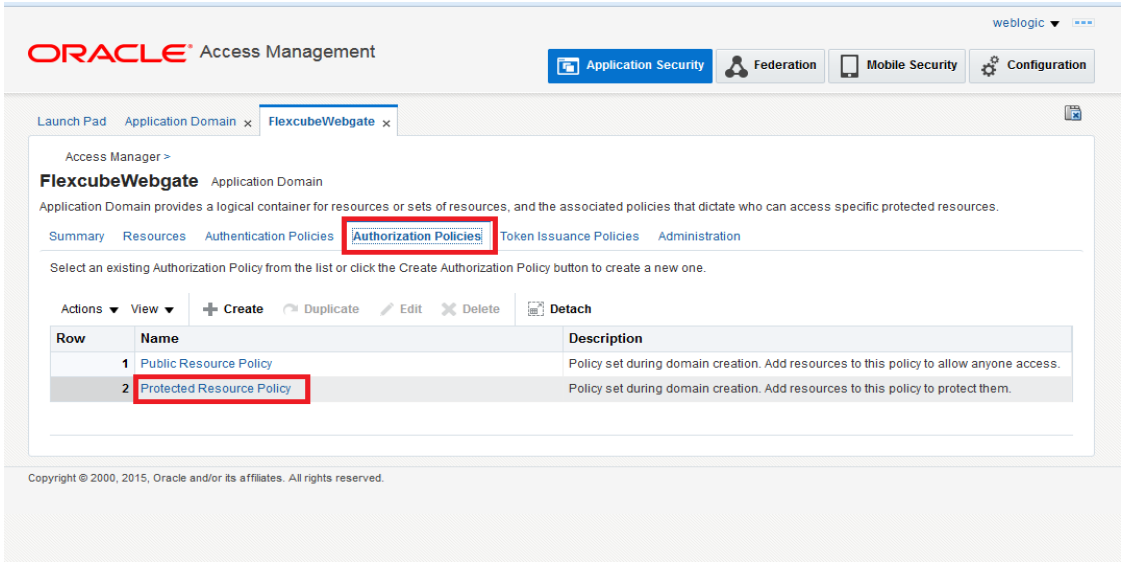
   Click on Add button



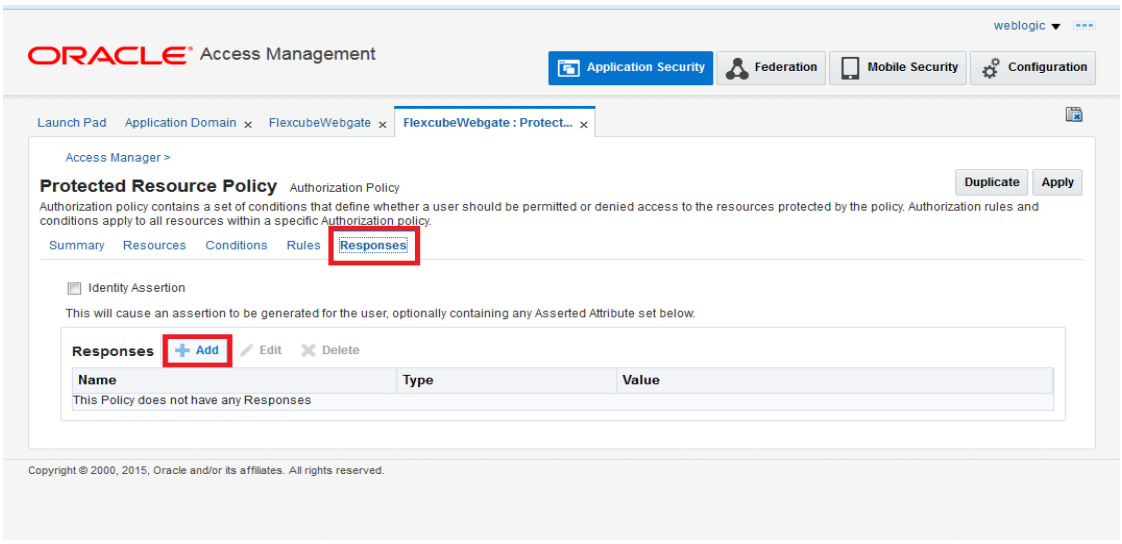
8. Click on Apply to Save the Changes



9. Click on ‘Authorization Policies’ and then click on ‘Protected Resource Policy’.



10. Click on ‘Response’ tab and click on Add button to Add ‘DN’ variable to the Response Header.



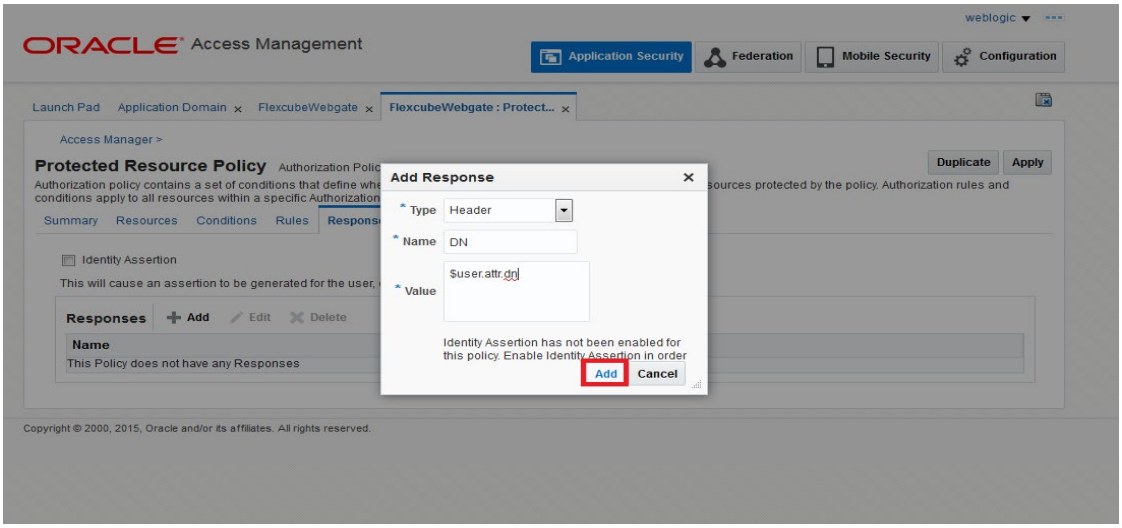
11. Enter the following values in the Add Response Window :

    Type : Header

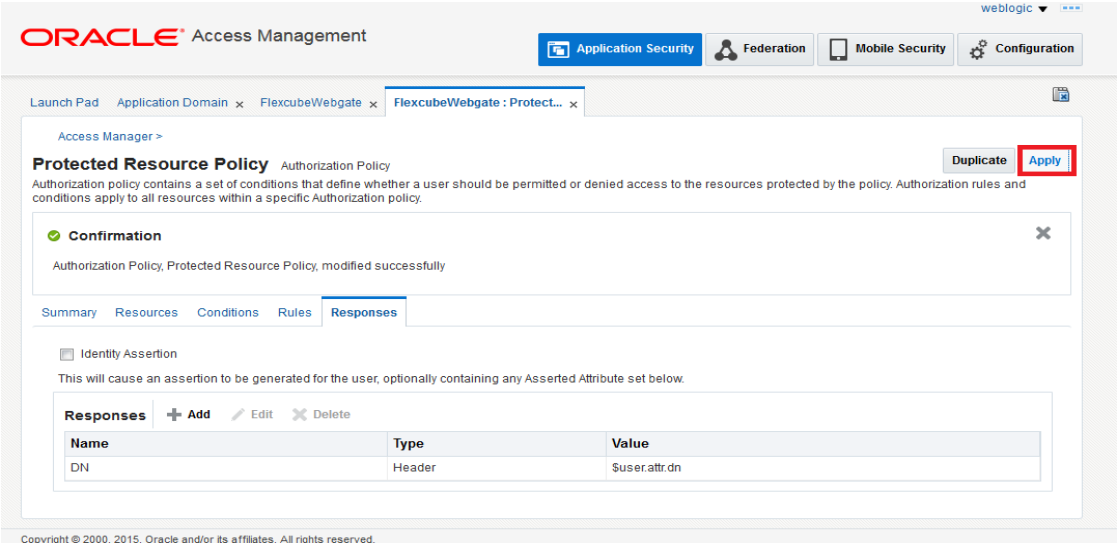
    Name : DN

    Value : $user.attr.dn

    Click on Add button



12. Click on ‘Apply’ to Save the changes.



2.6.5.2 Copying Generated Files and Artifacts to the Oracle HTTP Server WebGate Instance

Perform the following steps to copy the artifacts generated while creating the Oracle 11g Webgate to the Webgate installation directory:

- Navigate to <DOMAIN_HOME>/output/$WebgateAgentName
- Select the following files

  ObAccessClient.xml

  password.xml

- cwallet.sso

  cwallet.sso.lck

Copy the files to <ORACLE_MIDDLEWARE>/<ORACLE_WIBTIER_HOME> /instances/instance1/ config/OHS/ohs1/webgate/config/

- Select the remaining 2 files

  aaa_key.pem

  aaa_cert.pem

- Copy the files to <ORACLE_MIDDLEWARE>/<ORACLE_WIBTIER_HOME> /instances/instance1/ config/OHS/ohs1/webgate/config/simple

2.6.5.3 Add the Application Certificates to Oracle HTTP Server to work in SSL mode.

Use the ORAPKI tool to import the Flexcube and OAM Server certificates to Oracle HTTP Server. Add <Oracle_MIDDLEWARE>/oracle_common/bin to PATH environment variable and also set JAVA_HOME environment variable. Execute the below command in the command line.

orapki wallet add -wallet
<Oracle_MIDDLEWARE>/<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1/keystore
s/default -trusted_cert -cert <export_certificate_file_name_with_location.cer> -auto_login_only

Note: Certificate has to be imported into OHS Wallet.

2.6.5.4 Configuring mod_wl_ohs for Oracle HTTP server Routing

To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server, add the directive shown below to the mod_wl_ohs.conf file available in <ORACLE_MIDDLEWARE> /<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1.

<Location /FCJNeoWeb>

SetHandler weblogic-handler

WebLogicHost ofss00002.in.oracle.com

WeblogicPort 7002

WLProxySSL ON

SecureProxy ON

WLSSLWallet
"<ORACLE_MIDDLEWARE>/<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1/keystores/default"

</Location>

Note: In the above example, ofss00002.in.oracle.com is the server name where the Flexcube Application is deployed, 7002 is the SSL port and FCJNeoWeb is the context root of the FLEXCUBE application

2.6.5.5 Verify the Webgate 11g Agent Created

After configuring webgate 11g agent , launch the URL https://<hostname>:<ohs_Port>/ohs/modules/webgate.cgi?progid=1 to verify whether the webgate configuration is working fine. If the URL launches a screen as below then the webgate configuration is working fine.

Note *: To enable this option refer Oracle Doc ID: 1624131.1

Access Server	Connection State	Created	Installation Directory	Num Of Threads	Directory Information
ofss220028.in.oracle.com:5575, 1	Up	Friday, January 11, 2013 16:18:27			

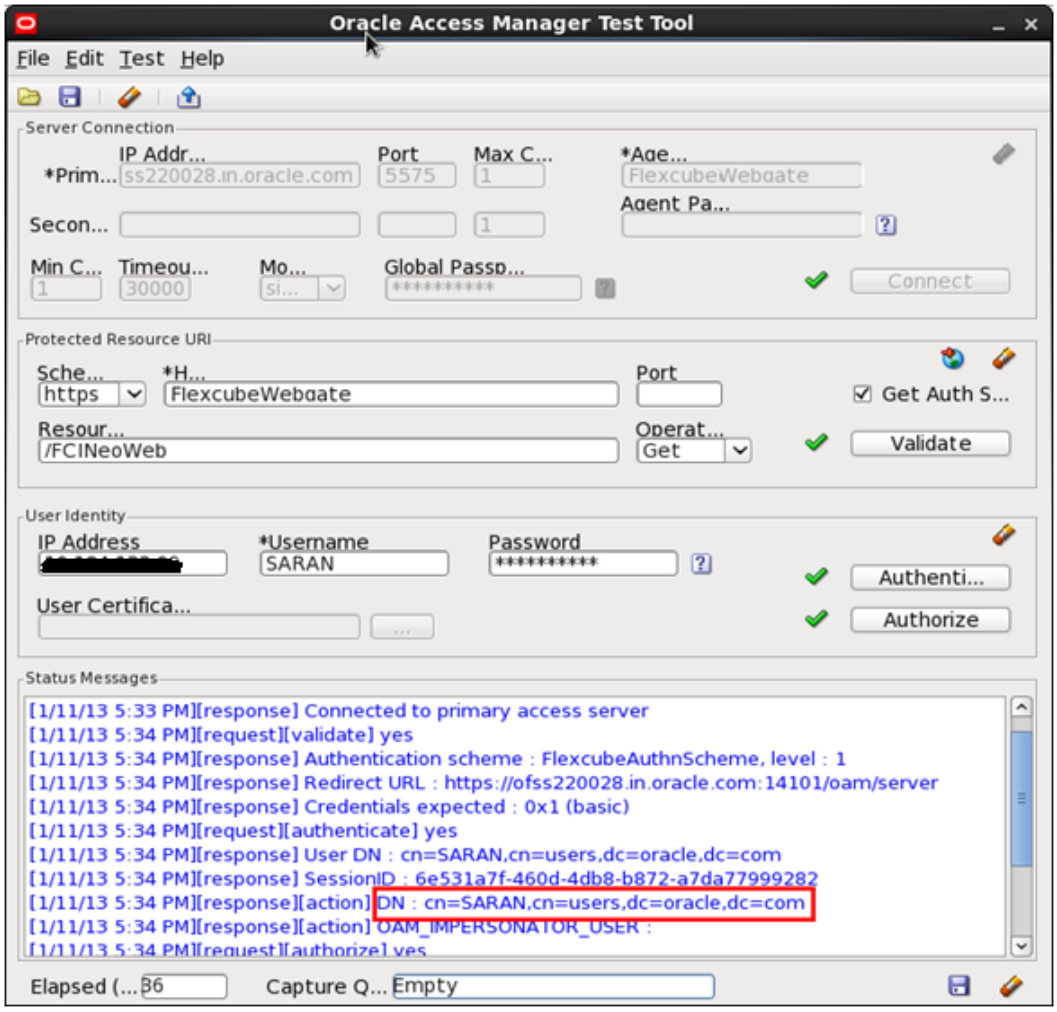
Cache Name	State	Max Elems	Curr Elems	Timeout (seconds)	Cache Stats (Hits:Misses: Expired:Flushed)	Memory Footprint (bytes)
Resource to Authentication Scheme	active	100000	100	1800	6451:273:61:0	59750
Authentication Scheme	active	25	1	1800	15012:34:33:0	802
Resource to Authorization Policy	active	100000	100	1800	381:127:27:0	43200
Authorization Result	active	1000	5	15	372:9:3:0	10845

2.6.5.6 Using OAM Test Tool (This step is not mandatory)

There is a test tool provided in OAM software which helps us to check the response parameter values. The test tool is available in <OAM Install Dir>\ oam\server\tester.

For eg. D:\weblogic\Middleware\Oracle_IDM1\oam\server\tester

Use ***java -jar oamtest.jar*** to launch the OAM test tool.



2.6.5.7 Fix for Escape sequence character back slash (\) infront of comma (,) in OAM Header Variable

cd <Oracle_IDM>/common/bin

./wlst.sh or **wlst.cmd**

wls:/offline> **connect()**

Please enter your username :Weblogic

Please enter your password :

Please enter your server URL [t3://localhost:7001] :t3://localhost:7201

Connecting to t3://vm34.sg.oracle.com:8001 with userid weblogic ...

Successfully connected to Admin Server 'AdminServer' that belongs to domain 'iam_domain'.

Warning: An insecure protocol was used to connect to the server. To ensure on-the-wire security, the SSL port or Admin port should be used instead.

wls:/base_domain/serverConfig> **domainRuntime()**

Location changed to domainRuntime tree. This is a read-only tree with DomainMBean as the root.

For more help, use help(domainRuntime)

wls:/base_domain/domainRuntime> **configurePolicyResponses(responseSeparator=",", responseEscapeChar="")**

Policy Responses configuration is updated.

wls:/base_domain/domainRuntime>

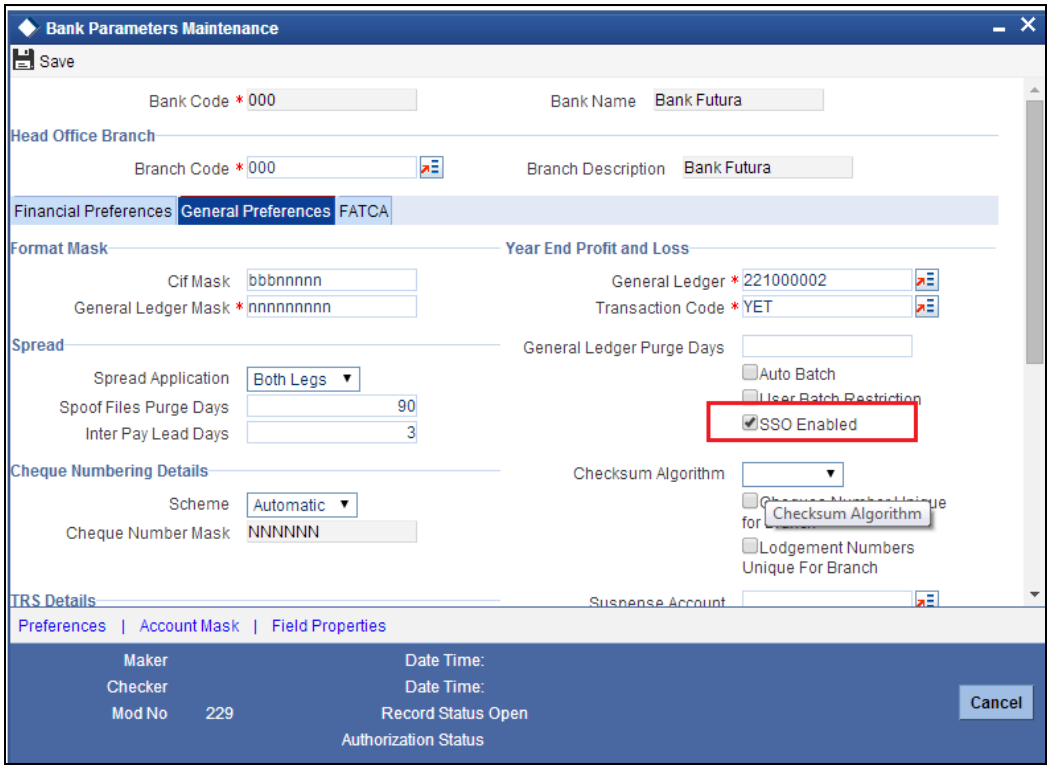
2.7 First launch of FLEXCUBE after installation

After installing FLEXCUBE and while launching it for first time, the normal login screen with userid and password will appear. This is because the bank parameter maintenance will have the value for sso_intalled set to 'N' by default during installation.

2.7.1 Parameter Maintenance

2.7.1.1 Bank Parameter maintenance - UBS

To enable SSO in FLEXCUBE UBS, login into the application and enable "SSO Enabled" Check box in "Bank Maintenance [SMDBANKP]" screen.



2.7.1.2 Parameters Maintenance – IS

There is no such a screen to maintain the SSO Enabled Parameter in FLEXCUBE Investor Servicing.

2.7.2 Maintaining LDAP DN for FLEXCUBE users

For each user id in FLEXCUBE a user has to be created in the LDAP.

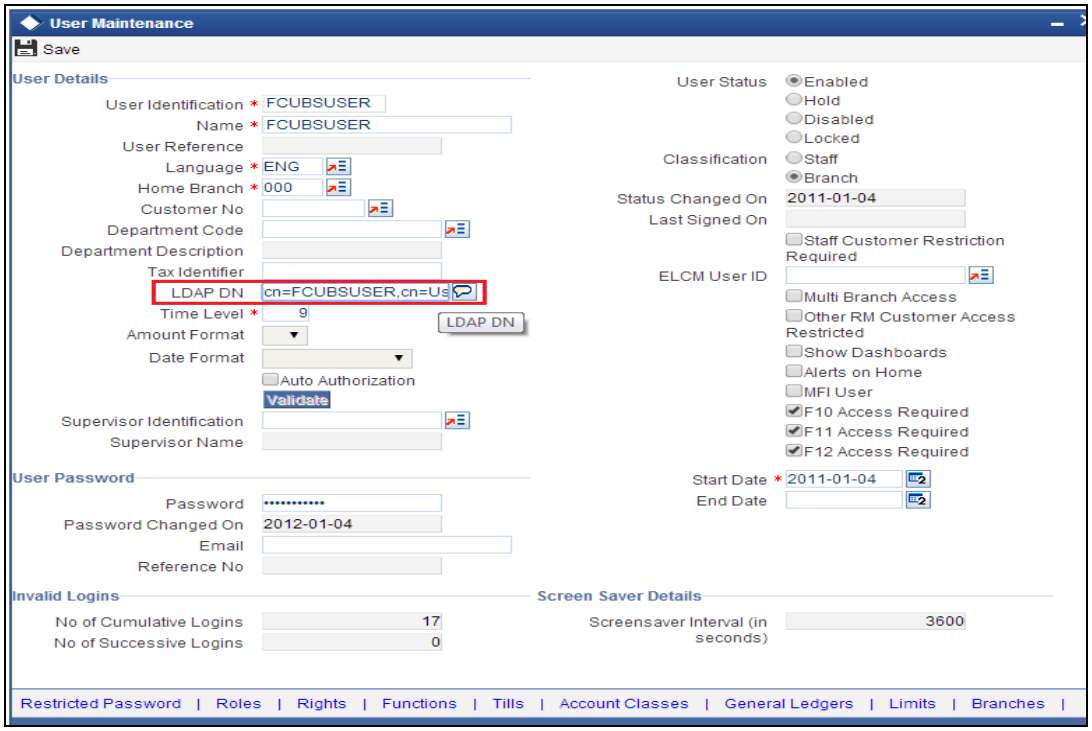
When creating the user in LDAP, ensure that the DN used is same as the LDAP DN value that will be updated in user maintenance form. Once the user is created in LDAP go to the user maintenance form in FCUBS. If the FCUBS user already exists then unlock the user and update the LDAP DN value which was set when creating the user in LDAP. Click on Validate button to check whether any other user is having the same LDAP DN value.

LDAP DN value should be entered as complete DN value.

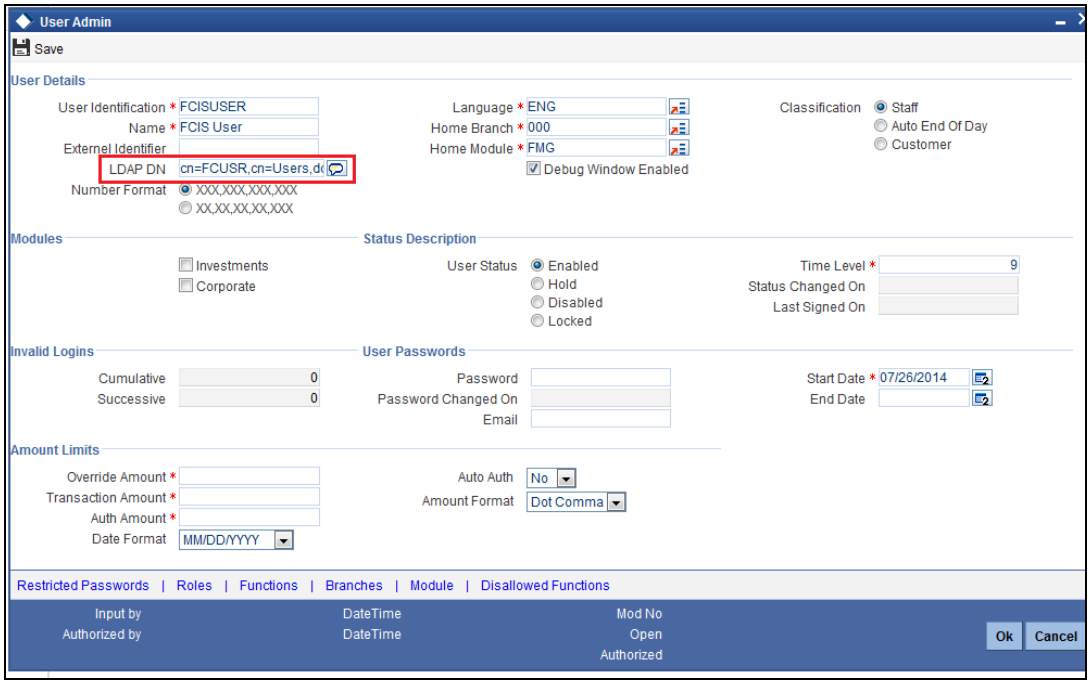
eg.

cn=FCUSR,cn=Users,dc=oracle,dc=com

For FLEXCUBE – UBS



For FLEXCUBE - IS



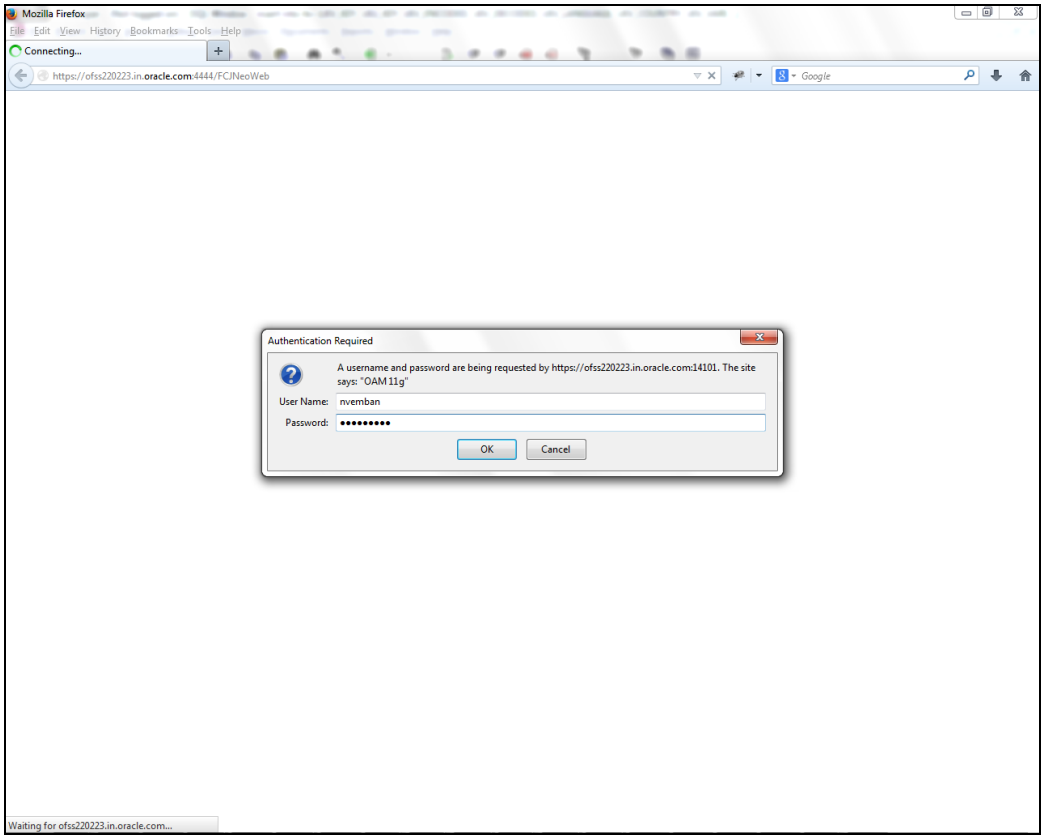
2.7.3 Launching FLEXCUBE

After setting up FLEXCUBE to work on Single Sign on mode, navigate to the URL https://<hostname>:<OHS SSL Port>/<Context Root> from your browser

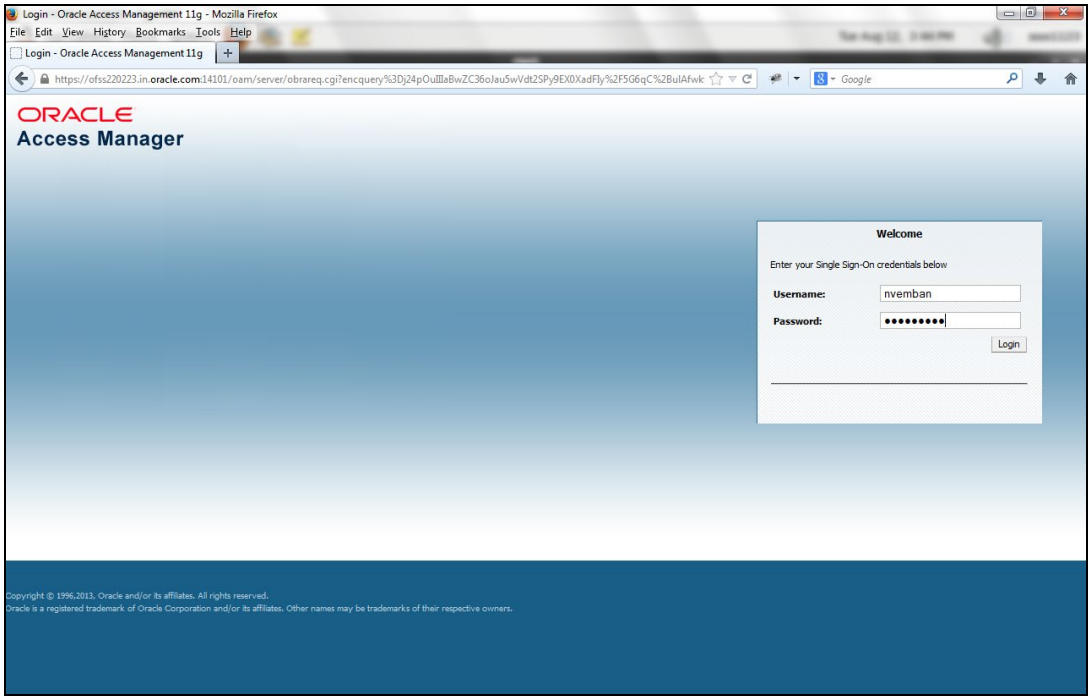
eg: https://ofss00001.in.oracle.com:4443/FCJNeoWeb

Since the resource is protected, the WebGate challenges the user for credentials as shown below.

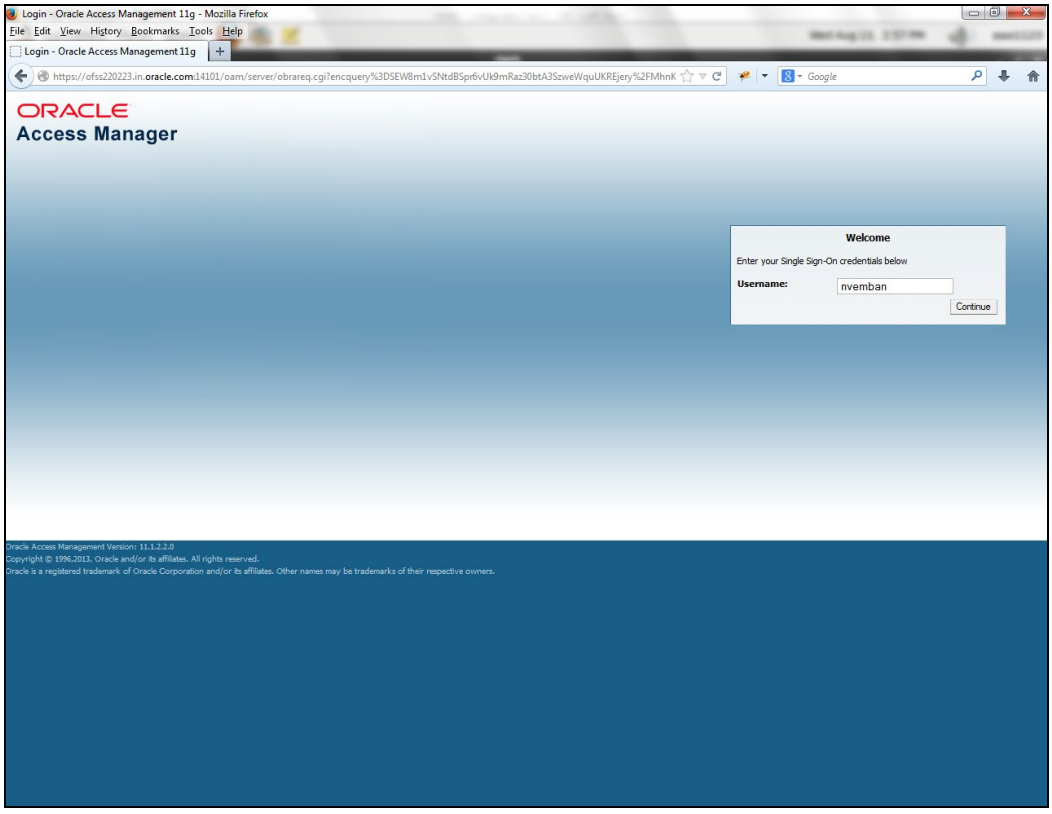
2.7.3.1 Basic Style Challenge by Webgate



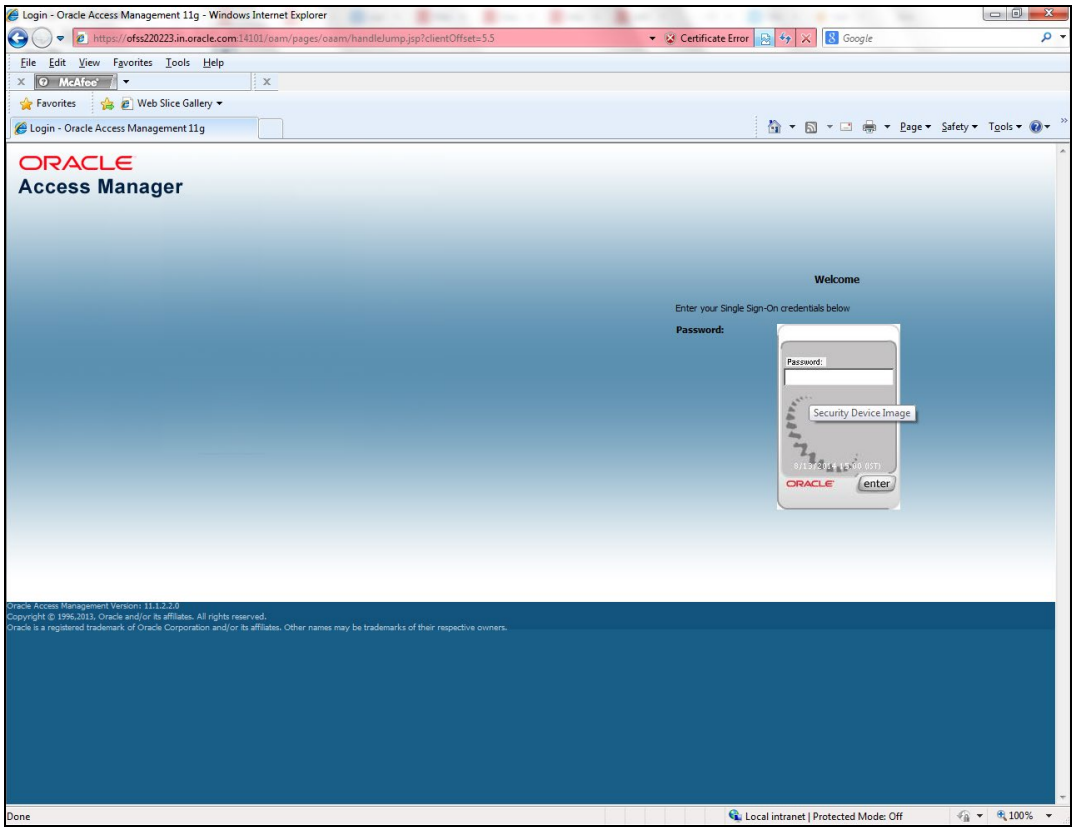
2.7.3.2 Form Style Challenge by Webgate

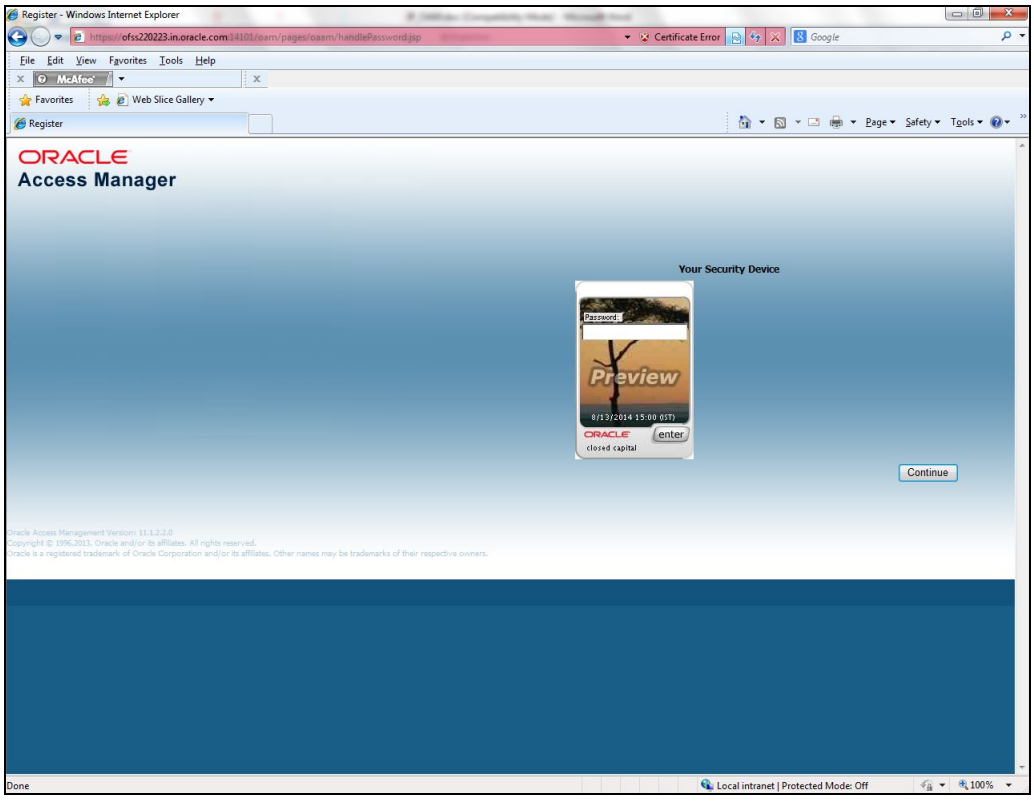


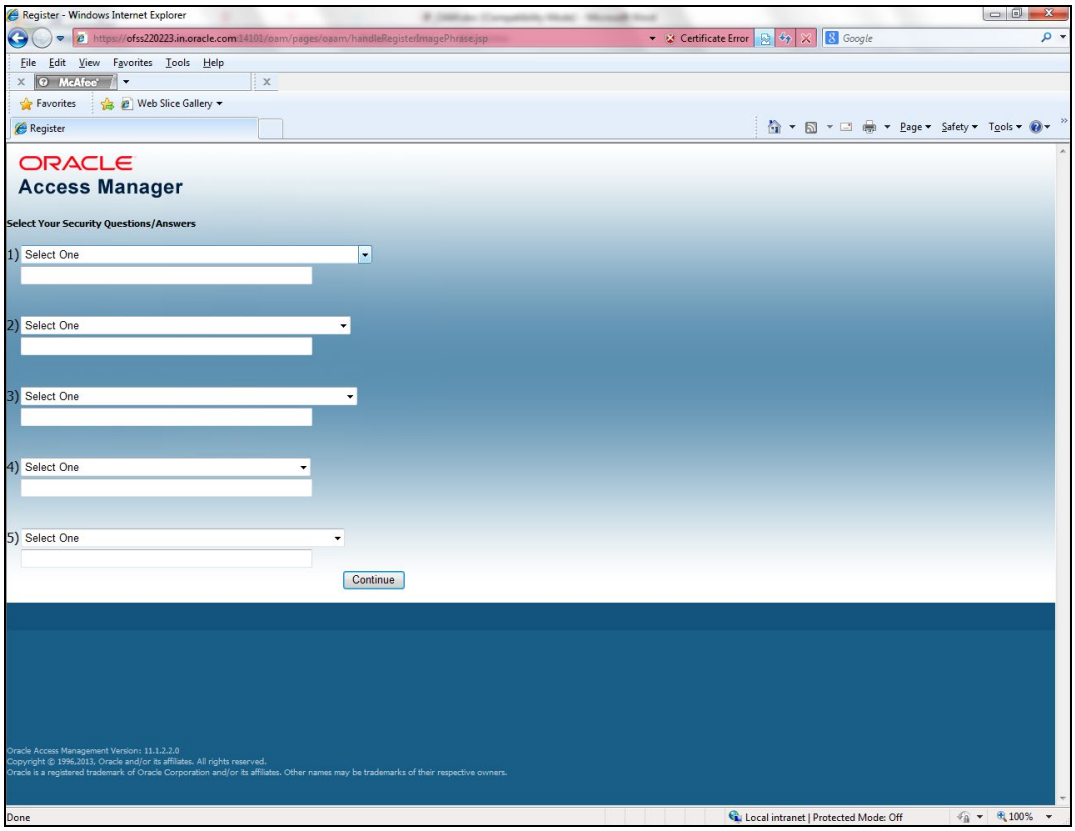
2.7.3.3 KBA Based Strong Authentication Challenge by Webgate(Only when OAAM is used)

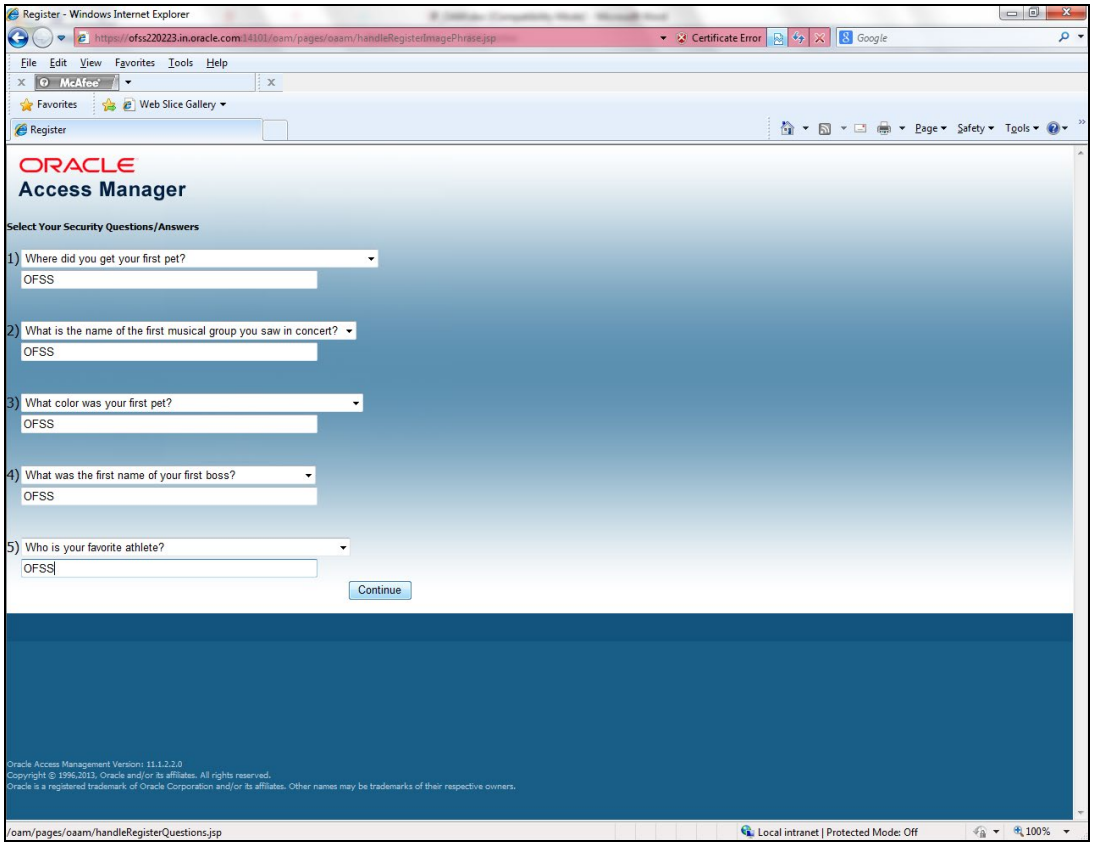


First Time Login

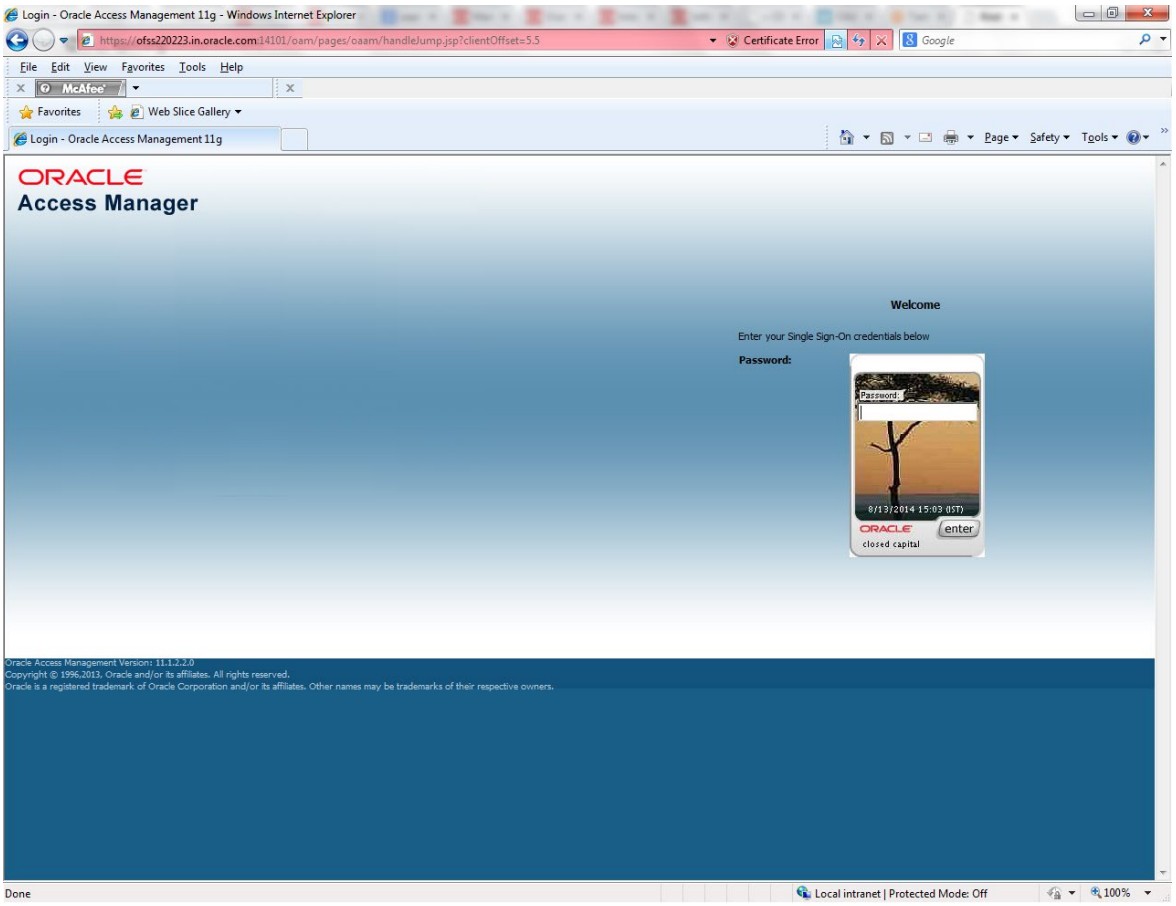


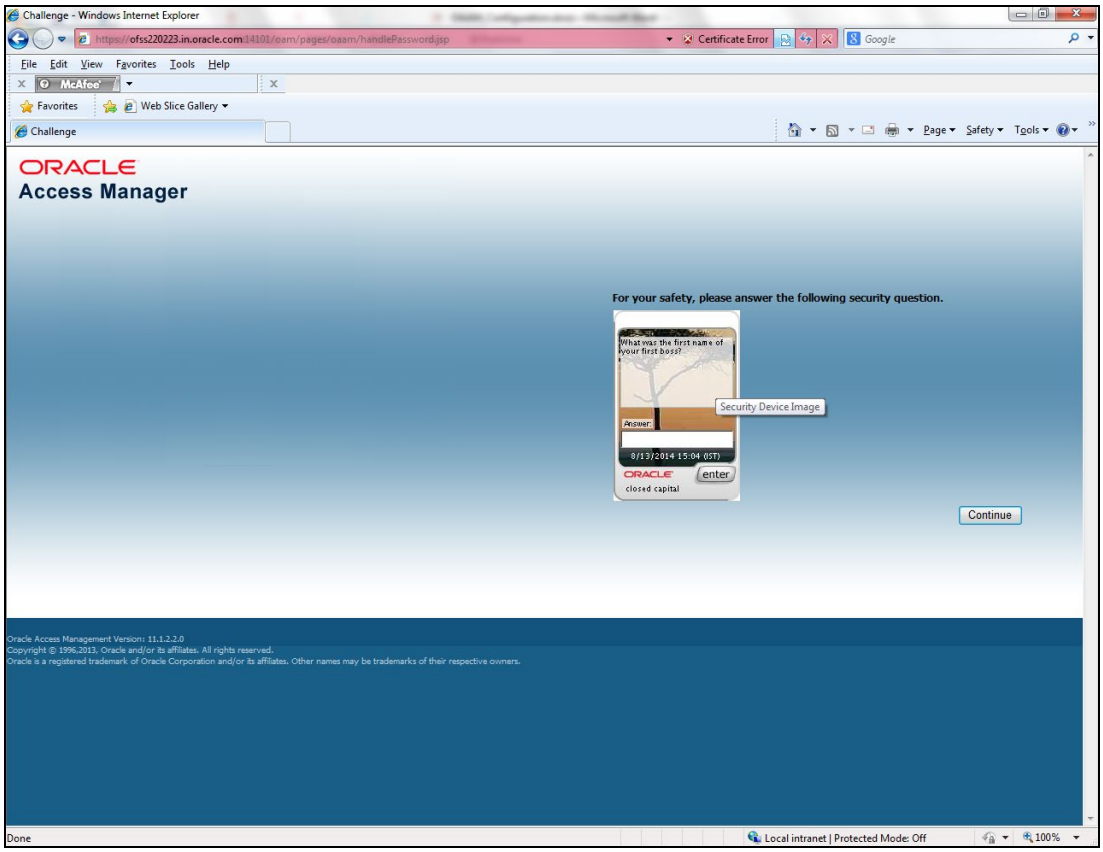



Register - Windows Internet Explorer
Certificate Error
Google
File Edit View Favorites Tools Help
Favorites
Web Slice Gallery
Register
Page Safety Tools
ORACLE
Access Manager
Select Your Security Questions/Answers
1) Select One
2) Select One
3) Select One
4) Select One
5) Select One
Continue
Oracle Access Management Version: 11.1.2.2.0
Copyright © 1996,2013, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Done
Local intranet | Protected Mode: Off
100%


Register - Windows Internet Explorer
Certificate Error
Google
File Edit View Favorites Tools Help
Favorites
Web Slice Gallery
Register
Page Safety Tools
ORACLE
Access Manager
Select Your Security Questions/Answers
1) Where did you get your first pet?
OFSS
2) What is the name of the first musical group you saw in concert?
OFSS
3) What color was your first pet?
OFSS
4) What was the first name of your first boss?
OFSS
5) Who is your favorite athlete?
OFSS
Continue
Oracle Access Management Version: 11.1.2.2.0
Copyright © 1996,2013, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
/oam/pages/oaam/handleRegisterQuestions.jsp
Local intranet | Protected Mode: Off
100%

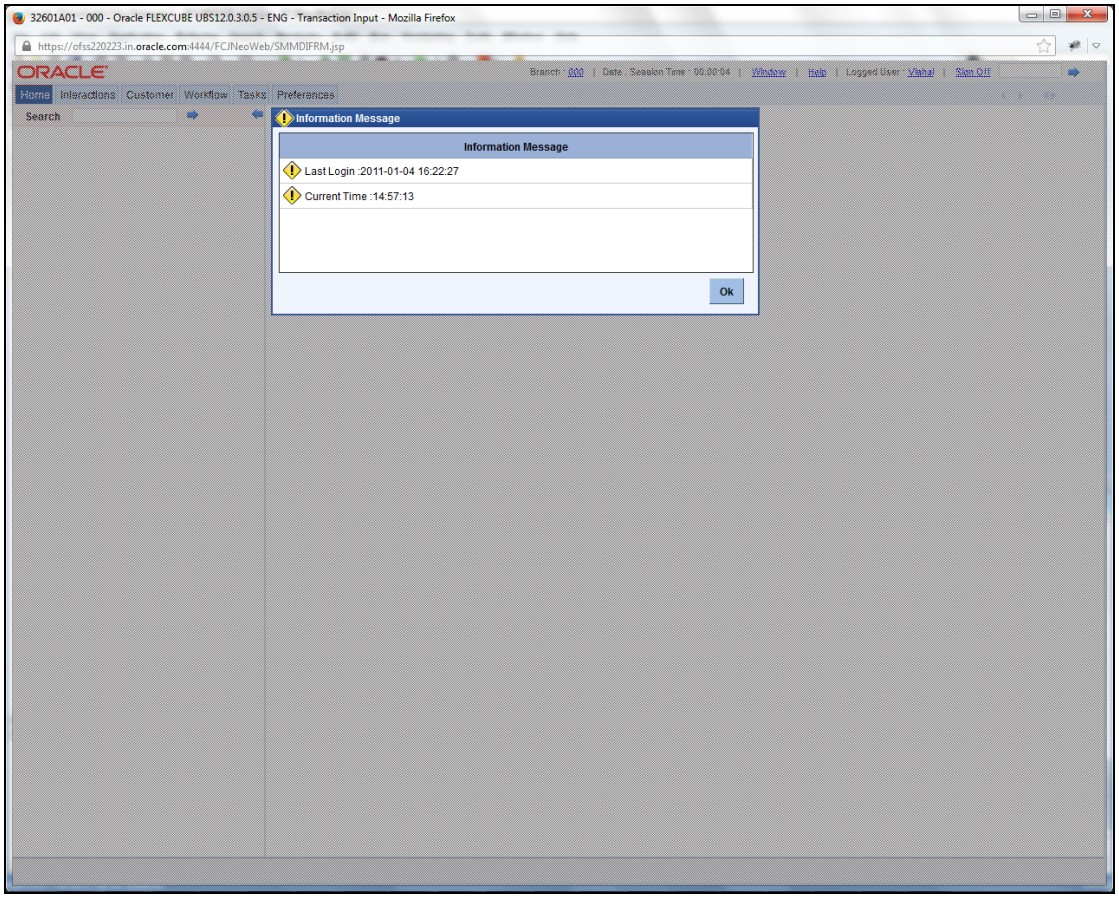
Post First Login





Once the user is authenticated and authorized to access the resource, the request gets redirected to normal FLEXCUBE application and it will take the user to Home Branch.

2.7.3.4 After SSO Login FLEXCUBE Application launch - Home Branch / Module



2.7.4 Signoff in a SSO Situation

FLEXCUBE does not provide for single signoff currently, i.e., when a user signs off in FLEXCUBE, the session established with Oracle Access Manager by the user will not be modified in any manner.

In a SSO situation the “Exit” and “Logoff” actions in FLEXCUBE will function as “Exit”, i.e., on clicking these, the user will “exit” FLEXCUBE and will need to re-launch FLEXCUBE using the FLEXCUBE launch URL.

Oracle Access Manager Integration
May 2021
Version 12.87.7.0.0

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/