

Oracle Access Manager Integration

Oracle Access Manager Integration  
Oracle FLEXCUBE Universal Banking  
Release 12.87.7.0.0

May 2021



# Table of Contents

<b>1. PREFACE .....</b>	<b>1-3</b>
1.1 INTRODUCTION .....	1-3
1.2 AUDIENCE .....	1-3
1.3 ABBREVIATIONS .....	1-3
1.4 DOCUMENTATION ACCESSIBILITY .....	1-3
1.5 ORGANIZATION .....	1-3
1.6 GLOSSARY OF ICONS .....	1-3
1.6.1 <i>Related Documents</i> .....	1-4
<b>2. ENABLING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER .....</b>	<b>2-1</b>
2.1 INTRODUCTION .....	2-1
2.2 BACKGROUND AND PREREQUISITES .....	2-1
2.2.1 <i>Software Requirements</i> .....	2-1
2.3 BACKGROUND OF SSO RELATED COMPONENTS .....	2-2
2.3.1 <i>Oracle Access Manager (OAM)</i> .....	2-2
2.3.2 <i>LDAP Directory Server</i> .....	2-2
2.3.3 <i>WebGate/AccessGate</i> .....	2-2
2.3.4 <i>Oracle Adaptive Access Manager</i> .....	2-3
2.4 CONFIGURATION .....	2-3
2.4.1 <i>Pre-requisites</i> .....	2-3
2.5 ENABLING SSL FOR WEBLOGIC AND OAM CONSOLE .....	2-3
2.5.1 <i>Self-signed Certificate Creation</i> .....	2-3
2.5.2 <i>Configuring Weblogic Console</i> .....	2-5
2.5.3 <i>Configuring SSL Mode in Oracle Internet Directory</i> .....	2-9
2.6 CONFIGURING SSO IN OAM CONSOLE .....	2-13
2.6.1 <i>Identity Store Creation</i> .....	2-14
2.6.2 <i>Creating Authentication Module</i> .....	2-18
2.6.3 <i>Creating Authentication Scheme</i> .....	2-19
2.6.4 <i>Creating OAM 11g Webgate</i> .....	2-23
2.6.5 <i>Post OAM Webgate 11g Creation</i> .....	2-30
2.7 FIRST LAUNCH OF FLEXCUBE AFTER INSTALLATION .....	2-40
2.7.1 <i>Parameter Maintenance</i> .....	2-40
2.7.2 <i>Maintaining LDAP DN for FLEXCUBE users</i> .....	2-41
2.7.3 <i>Launching FLEXCUBE</i> .....	2-43
2.7.4 <i>Signoff in a SSO Situation</i> .....	2-50

# 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 FLEXCUBE
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:

<b>Chapter 1</b>	<i>Preface</i> gives information on the intended audience. It also lists the various chapters covered in this User Manual.
<b>Chapter 2</b>	<i>Enabling Single Sign-on (SSO) with Oracle Access Manager</i> 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 .

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) in front 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
```

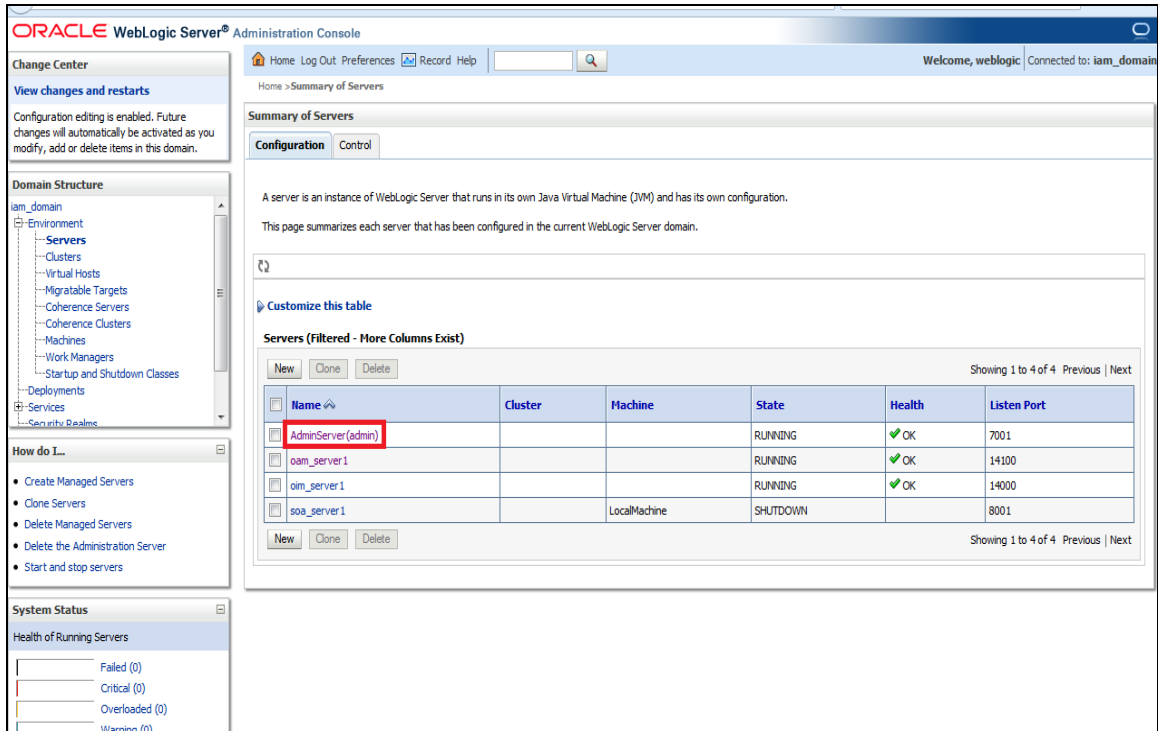
References: Oracle Support Articles (Article ID 1281035.1, Article ID 1218695.1), in case of Certificates issued by the Trusted Authorities



## 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



The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area displays the 'Summary of Servers' page, which includes a table of configured servers. The 'AdminServer(admin)' server is highlighted with a red box. The table columns are Name, Cluster, Machine, State, Health, and Listen Port. The 'AdminServer(admin)' server is in a RUNNING state with a Health of OK and a Listen Port of 7001. Other servers listed include oam\_server1, oim\_server1, and soa\_server1.

Name	Cluster	Machine	State	Health	Listen Port
AdminServer(admin)			RUNNING	OK	7001
oam_server1			RUNNING	OK	14100
oim_server1			RUNNING	OK	14000
soa_server1		LocalMachine	SHUTDOWN		8001

#### 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.

**General** Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload Health Monitoring Server Start Web Services

**Save**

Use this page to configure general features of this server such as default network communications.

View JNDI Tree

<b>Name:</b>	AdminServer	An alphanumeric name for this server instance. <a href="#">More Info...</a>
<b>Machine:</b>	(None)	The WebLogic Server host computer (machine) on which this server is meant to run. <a href="#">More Info...</a>
<b>Cluster:</b>	(Standalone)	The cluster, or group of WebLogic Server instances, to which this server belongs. <a href="#">More Info...</a>
<b>Listen Address:</b>	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>Listen Port Enabled</b>		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. <a href="#">More Info...</a>
<b>Listen Port:</b>	<input type="text" value="7001"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>SSL Listen Port Enabled</b>		Indicates whether the server can be reached through the default SSL listen port. <a href="#">More Info...</a>
<b>SSL Listen Port:</b>	<input type="text" value="7002"/>	The TCP/IP port at which this server listens for SSL connection requests. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>Client Cert Proxy Enabled</b>		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. <a href="#">More Info...</a>
<b>Java Compiler:</b>	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. <a href="#">More Info...</a>
<b>Diagnostic Volume:</b>	<input type="text" value="Low"/>	Specifies the volume of diagnostic data that is automatically produced by WebLogic Server at run time. Note that the WLDLF diagnostic volume setting does not affect explicitly configured diagnostic modules. For example, this controls the volume of events generated for JRockit Flight Recorder. <a href="#">More Info...</a>
<b>Advanced</b>		
<b>Virtual Machine Name:</b>	<input type="text" value="iam_domain_AdminSe"/>	When WLS is running on JRVSE, this specifies the name of the virtual machine running this server. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>WebLogic Plug-In Enabled</b>		Specifies whether this server uses the proprietary WL-Proxy-Client-IP header, which is recommended if the server instance will receive requests from a proxy plugin. <a href="#">More Info...</a>

### 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.

**ORACLE WebLogic Server** Administration Console

Home Log Out Preferences Record Help Welcome, weblogic Connected to: iam\_domain

Home > Summary of Servers > AdminServer

**Settings for AdminServer**

**Configuration** Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload Health Monitoring Server Start Web Services

**Save** Cancel

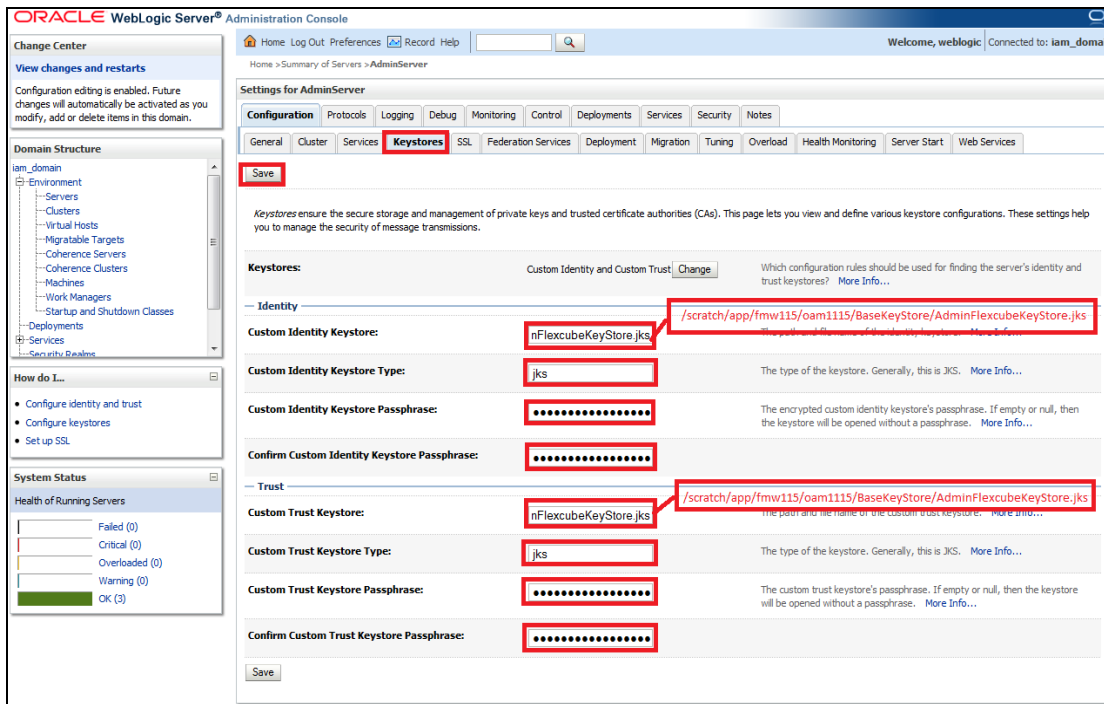
Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

**Keystores:**  Which configuration rules should be used for finding the server's identity and trust keystores? [More Info...](#)

- Custom Identity and Command Line Trust
- Custom Identity and Custom Trust**
- Custom Identity and Java Standard Trust
- Demo Identity and Demo Trust

### 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
```

**Change Center**  
View changes and restarts  
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

**Domain Structure**  
iam\_domain  
Environment  
Servers  
Clusters  
Virtual Hosts  
Migratable Targets  
Coherence Servers  
Coherence Clusters  
Machines  
Work Managers  
Startup and Shutdown Classes  
Deployments  
Services  
Security Realms

**How do I...**  
• Configure identity and trust  
• Set up SSL  
• Verify host name verification is enabled  
• Configure a custom host name verifier  
• Configure two-way SSL

**System Status**  
Health of Running Servers  
Failed (0)  
Critical (0)  
Overloaded (0)  
Warning (0)  
OK (2)

Home Log Out Preferences Record Help Welcome, weblogic Connected to: iam\_domain  
Home > Summary of Servers > AdminServer  
Settings for AdminServer  
Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes  
General Cluster Services Keystores **SSL** Federation Services Deployment Migration Tuning Overload Health Monitoring Server Start Web Services  
Save

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security of message transmissions.

**Identity and Trust Locations:** Keystores: [Change](#)  
Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CAs). [More Info...](#)

**Identity**

**Private Key Location:** from Custom Identity Keystore  
The keystore attribute that defines the location of the private key file. [More Info...](#)

**Private Key Alias:** FlexcubeCert  
The keystore attribute that defines the string alias used to store and retrieve the server's private key. [More Info...](#)

**Private Key Passphrase:** .....  
The keystore attribute that defines the passphrase used to retrieve the server's private key. [More Info...](#)

**Confirm Private Key Passphrase:** .....  
The keystore attribute that defines the passphrase used to retrieve the server's private key. [More Info...](#)

**Certificate Location:** from Custom Identity Keystore  
The keystore attribute that defines the location of the trusted certificate. [More Info...](#)

**Trust**

**Trusted Certificate Authorities:** from Custom Trust Keystore  
The keystore attribute that defines the location of the certificate authorities. [More Info...](#)

**Advanced**

**Hostname Verification:** None  
Specifies whether to ignore the installed implementation of the weblogic.security.SSL.HostnameVerifier interface (when this server is acting as a client to another application server). [More Info...](#)

**Custom Hostname Verifier:** BEA Hostname Verifier  
The name of the class that implements the weblogic.security.SSL.HostnameVerifier interface. [More Info...](#)

**Export Key Lifespan:** 500  
Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. [More Info...](#)

**Use Server Certs**  
Sets whether the client should use the server certificates/key as the client (client to another application server). [More Info...](#)

**Custom Hostname Verifier:** .....  
The name of the class that implements the weblogic.security.SSL.HostnameVerifier interface. [More Info...](#)

**Export Key Lifespan:** 500  
Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. [More Info...](#)

**Use Server Certs**  
Sets whether the client should use the server certificates/key as the client identity when initiating an outbound connection over https. [More Info...](#)

**Two Way Client Cert Behavior:** Client Certs Not Requested  
The form of SSL that should be used. [More Info...](#)

**Cert Authenticator:** .....  
The name of the Java class that implements the weblogic.security.acl.CertAuthenticator class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. [More Info...](#)

**SSLRejection Logging Enabled**  
Indicates whether warning messages are logged in the server log when SSL connections are rejected. [More Info...](#)

**Allow Unencrypted Null Cipher**  
Test if the AllowUnencryptedNullCipher is enabled. [More Info...](#)

**Inbound Certificate Validation:** Built-in SSL Validation Only  
Indicates the client certificate validation rules for inbound SSL. [More Info...](#)

**Outbound Certificate Validation:** Built-in SSL Validation Only  
Indicates the server certificate validation rules for outbound SSL. [More Info...](#)

**Use JSSE SSL**  
Select the JSSE SSL implementation to be used in Weblogic. [More Info...](#)

Save

Warning (0)  
OK (2)

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

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled "Summary of Servers" and contains a table of servers. The table has the following data:

Name	Cluster	Machine	State	Health	Listen Port
AdminServer (admin)			RUNNING	OK	7001
oam_server1			RUNNING	OK	14100
oim_server1			RUNNING	OK	14000
soa_server1		LocalMachine	SHUTDOWN		8001

The "System Status" section on the left shows the health of running servers:

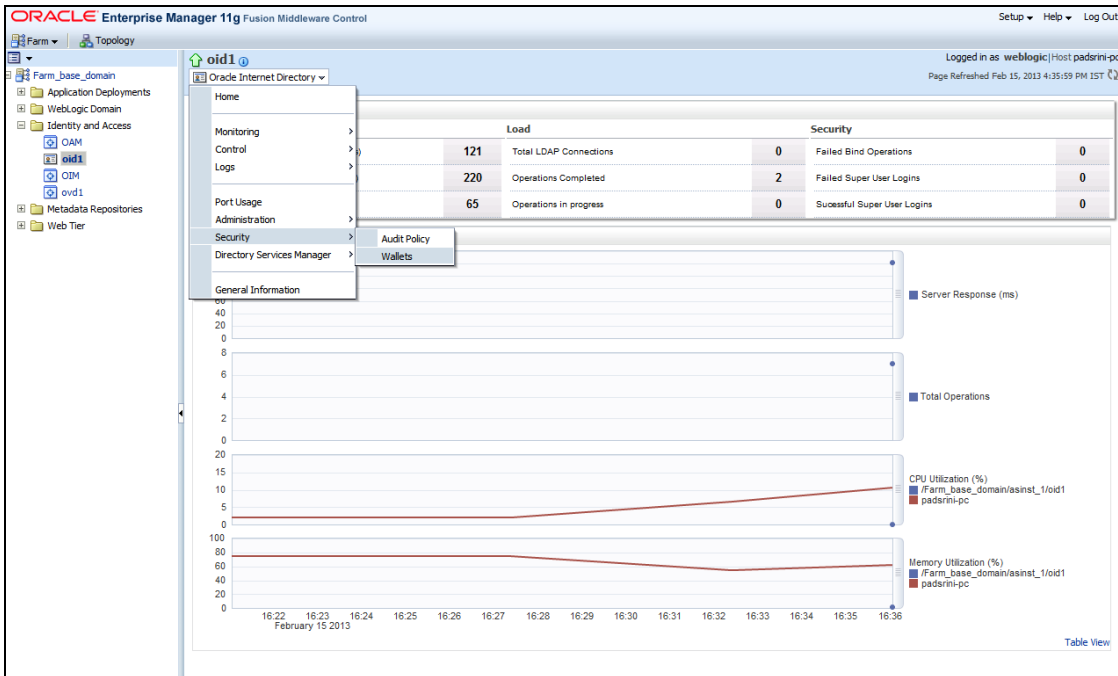
- Failed (0)
- Critical (0)
- Overloaded (0)
- Warning (0)
- OK (3)

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

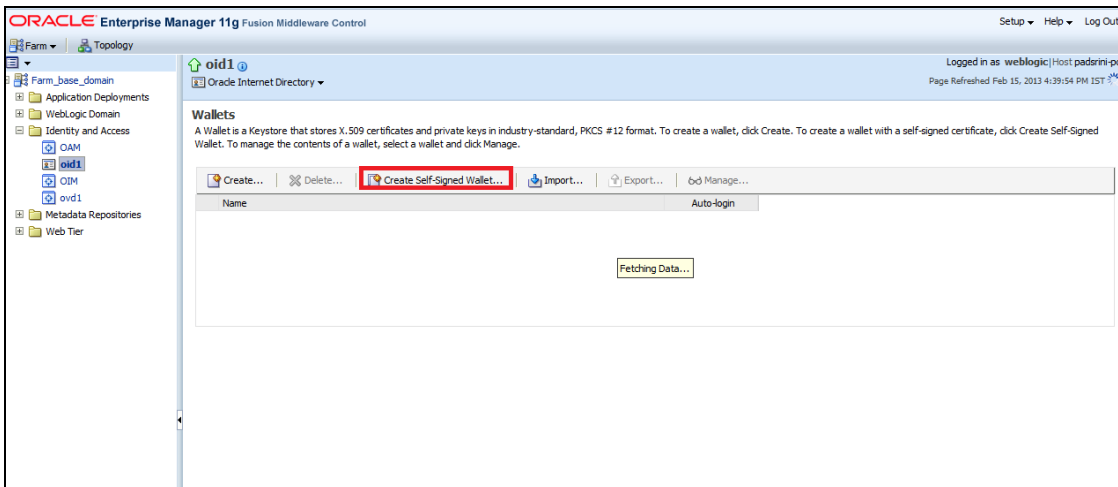
### 2.5.3 Configuring SSL Mode in Oracle Internet Directory

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

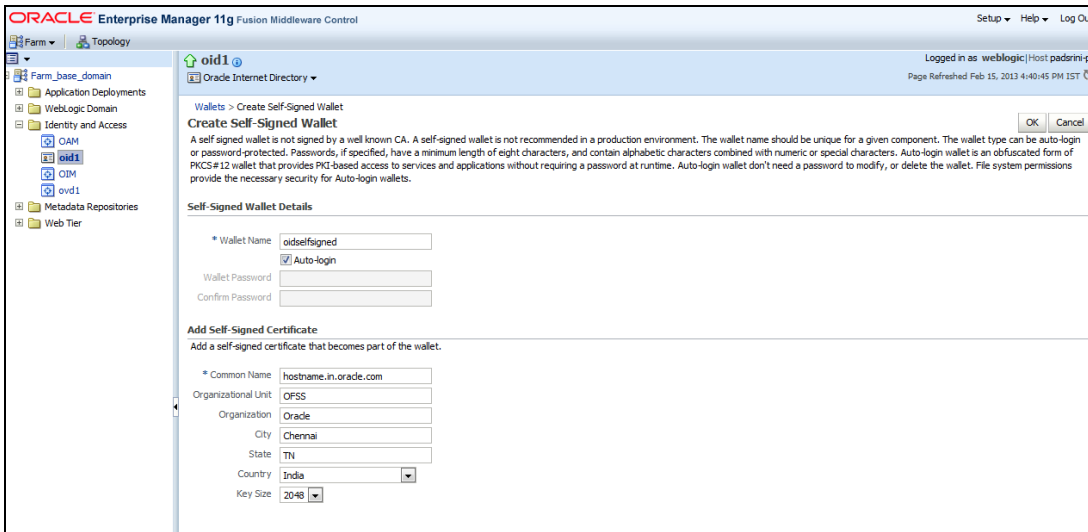
1. Login to the Enterprise Manager Console of the domain, in which Oracle Internet Directory is associated.



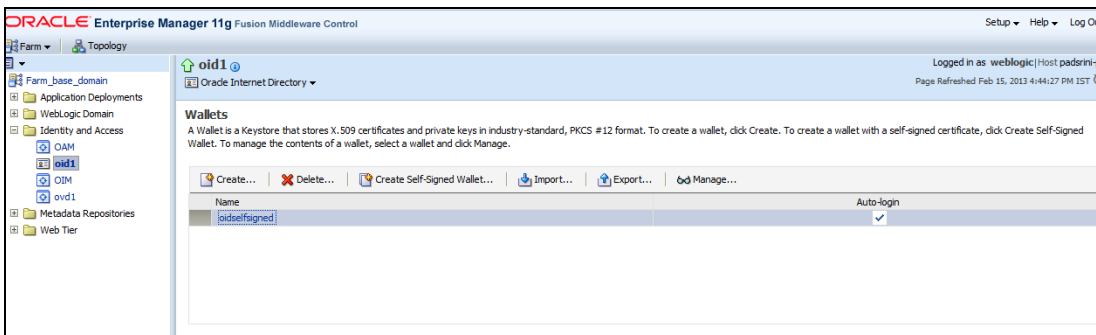
2. Click 'Create Self-Signed Wallet'.



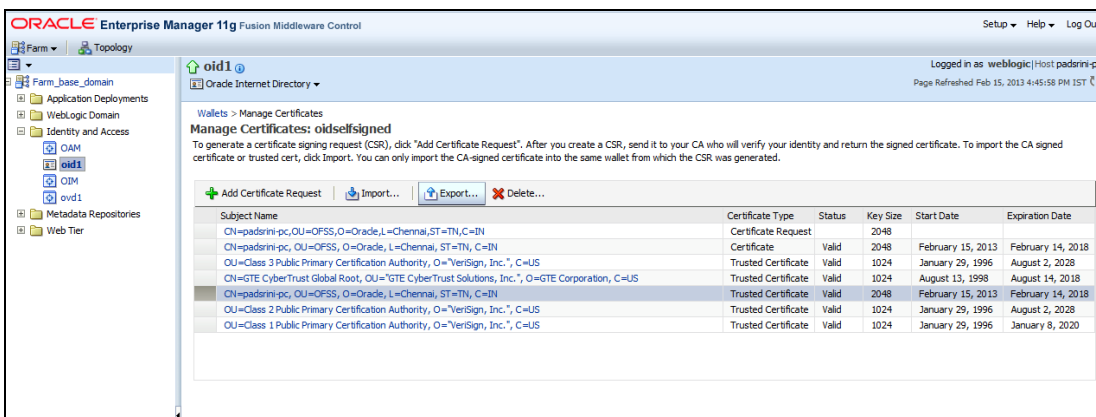
3. Enter the Details as below and Click 'OK'.



4. Click Manage...



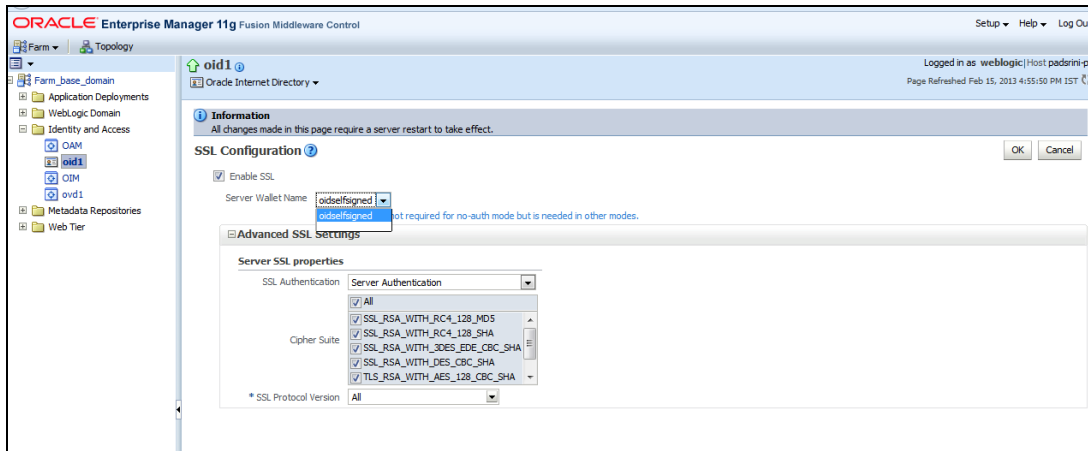
5. Select the Trusted Certificate and Click 'Export'.



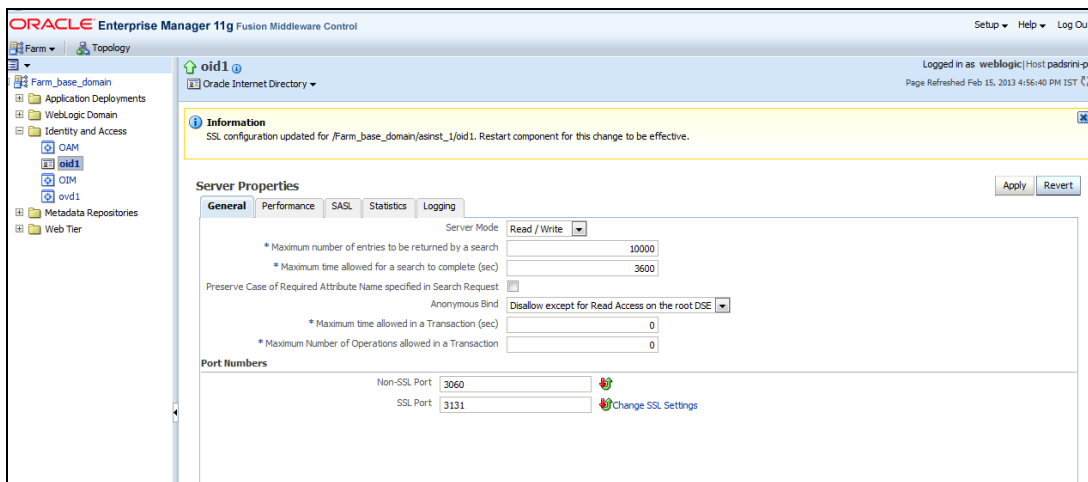
6. Click 'Export Trusted Certificate' and save the certificate file.







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 ldapcert -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

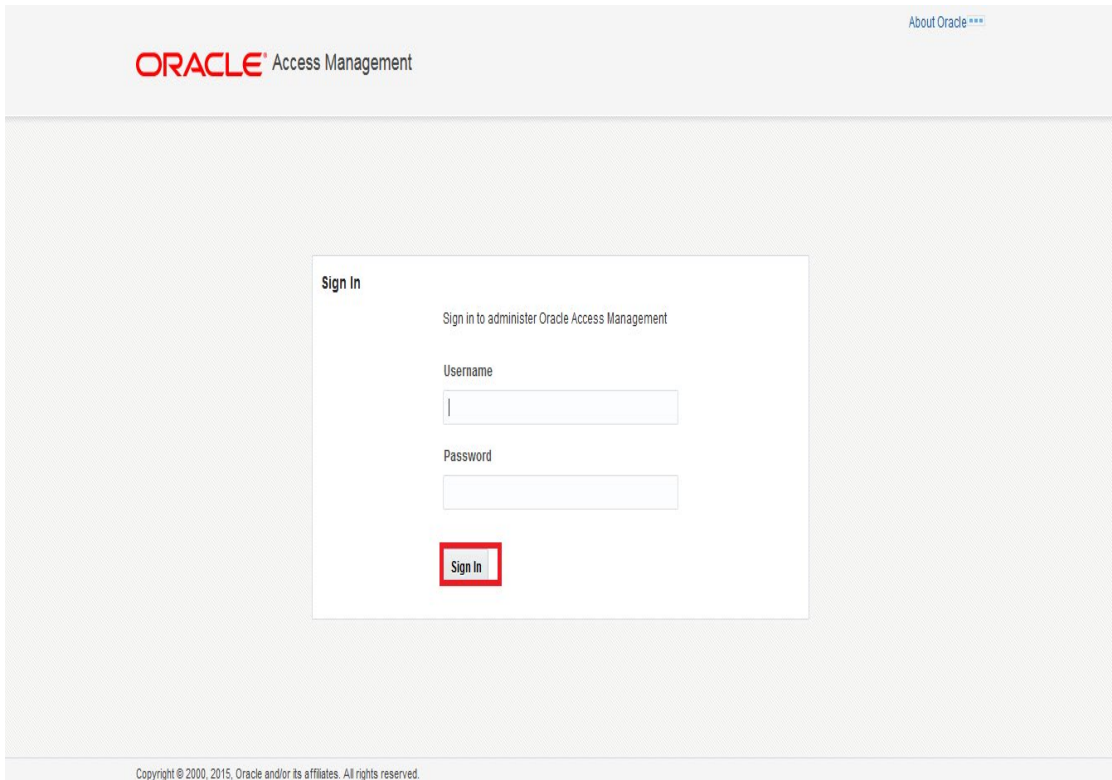
After installing OAM, Webtier Utilities and Webgate, extend the Weblogic domain to create OAM server.

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](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) in front 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.



ORACLE Access Management

About Oracle\*\*\*

**Sign In**

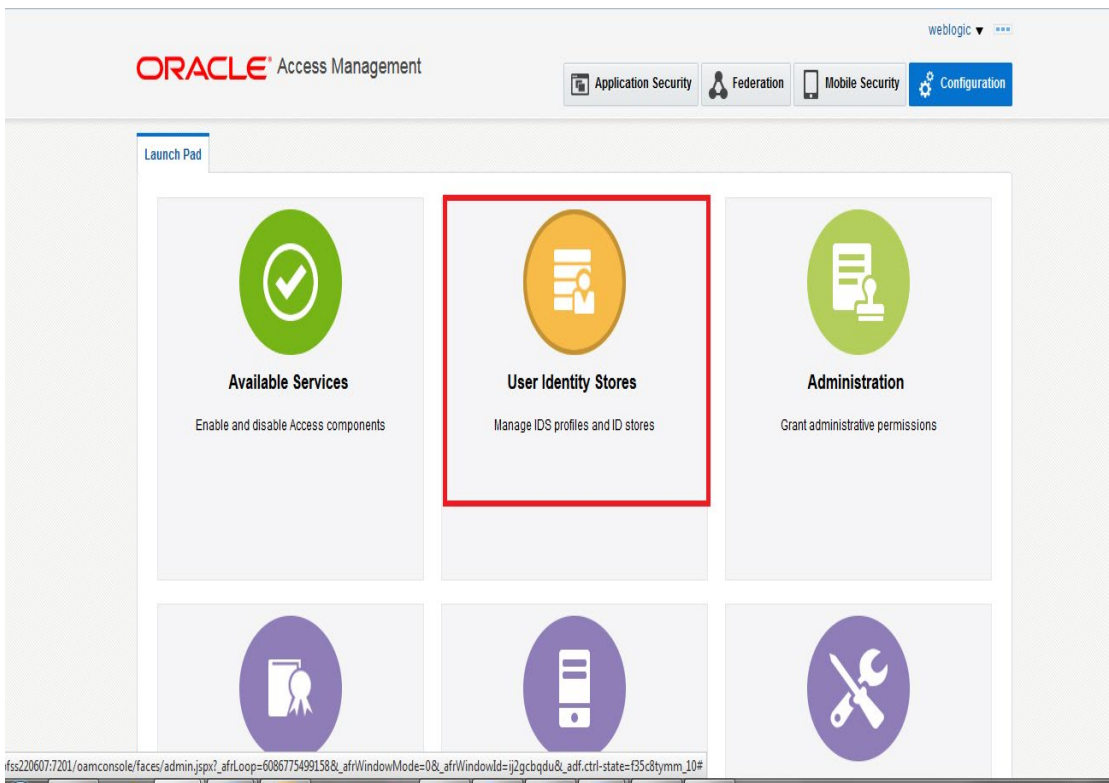
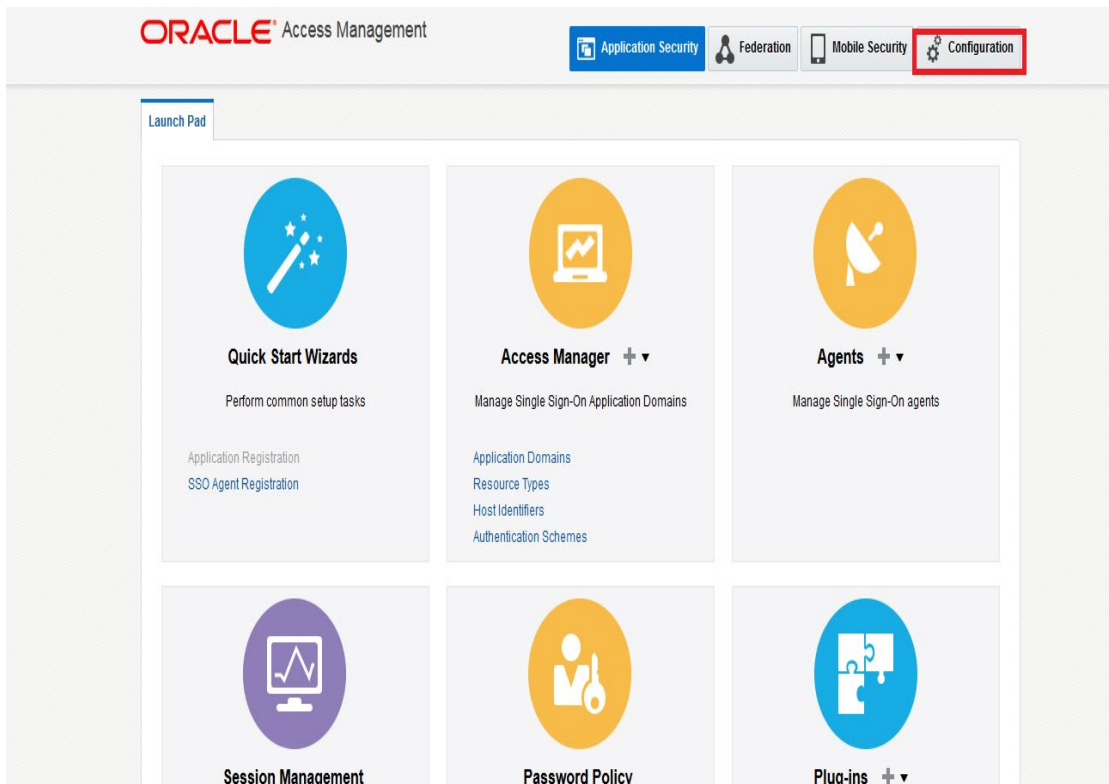
Sign in to administer Oracle Access Management

Username

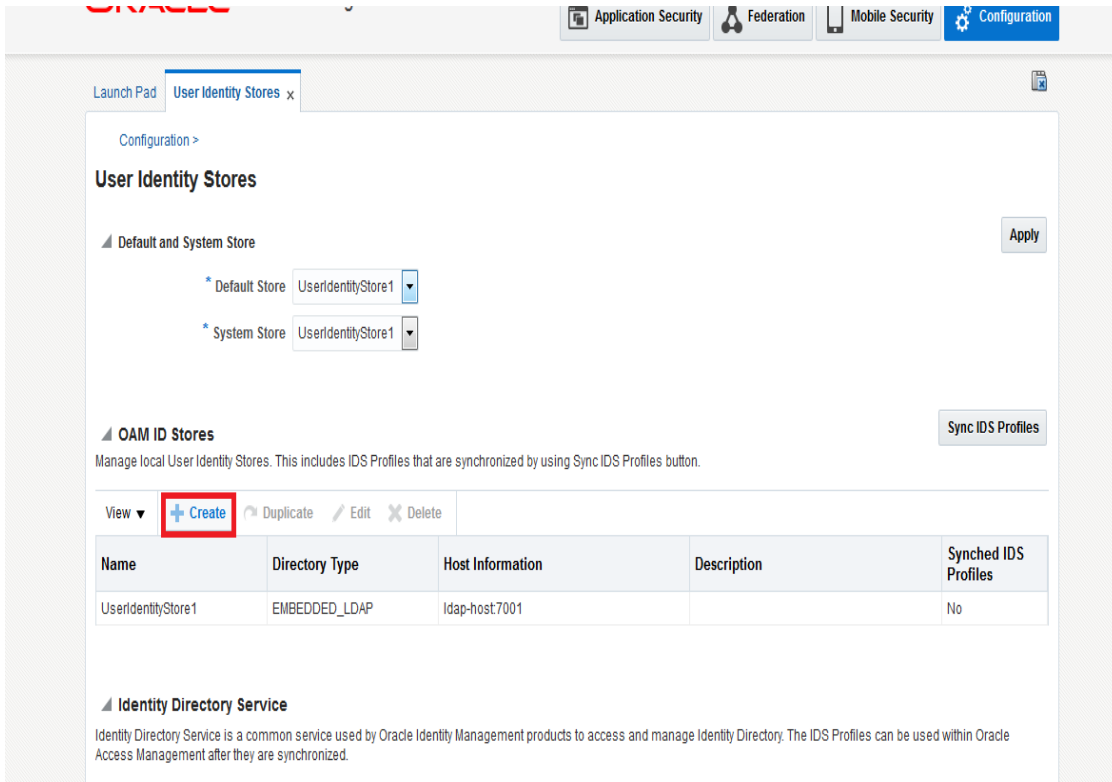
Password

**Sign In**

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.



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.

Launch Pad User Identity Stores x Create: User Identity Sto... x

Configuration >

### Create: User Identity Store

User Identity Store Service

**Store Name:** FLEXCUBESTore

**Store Type:** OID: Oracle Internet Directory

**Description:**

**Location and Credentials**

**Location:** ofss220607.in.oracle.com:3131

**Bind DN:** cn=orcladmin

**Enable SSL:**

**Use Native ID Store Settings:**

**Prefetched Attributes:**

**Password:** .....

**Users and Groups**

**Login ID Attribute:** cn

**User Password Attribute:** userPassword

**User Search Base:** cn=Users,dc=ofss,dc=in,dc=oracle,dc=c

**User Filter Object Classes:**

**Group Name Attribute:**

**Group Search Base:** cn=Groups,dc=ofss,dc=in,dc=oracle,dc=

**Test Connection** **Apply**

4. Click 'Test Connection' to validate the Credentials Passed.

Launch Pad User Identity Stores x Create: User Identity Sto... x

Configuration >

### Create: User Identity Store

User Identity Store Service

**Store Name:** FLEXCUBESTore

**Store Type:** OID: Oracle Internet Directory

**Description:**

**Location and Credentials**

**Location:** ofss220607.in.oracle.com:3131

**Bind DN:** cn=orcladmin

**Enable SSL:**

**Use Native ID Store Settings:**

**Prefetched Attributes:**

**Password:** .....

**Users and Groups**

**Login ID Attribute:** cn

**User Password Attribute:** userPassword

**User Search Base:** cn=Users,dc=ofss,dc=in,dc=oracle,dc=c

**User Filter Object Classes:**

**Group Name Attribute:**

**Group Search Base:** cn=Groups,dc=ofss,dc=in,dc=oracle,dc=

**Test Connection** **Apply**

**Connection Status** X

Connection to the User Identity Store successful!

**OK** **Cancel**


5. Click 'Apply' to Create the User Identity Store.

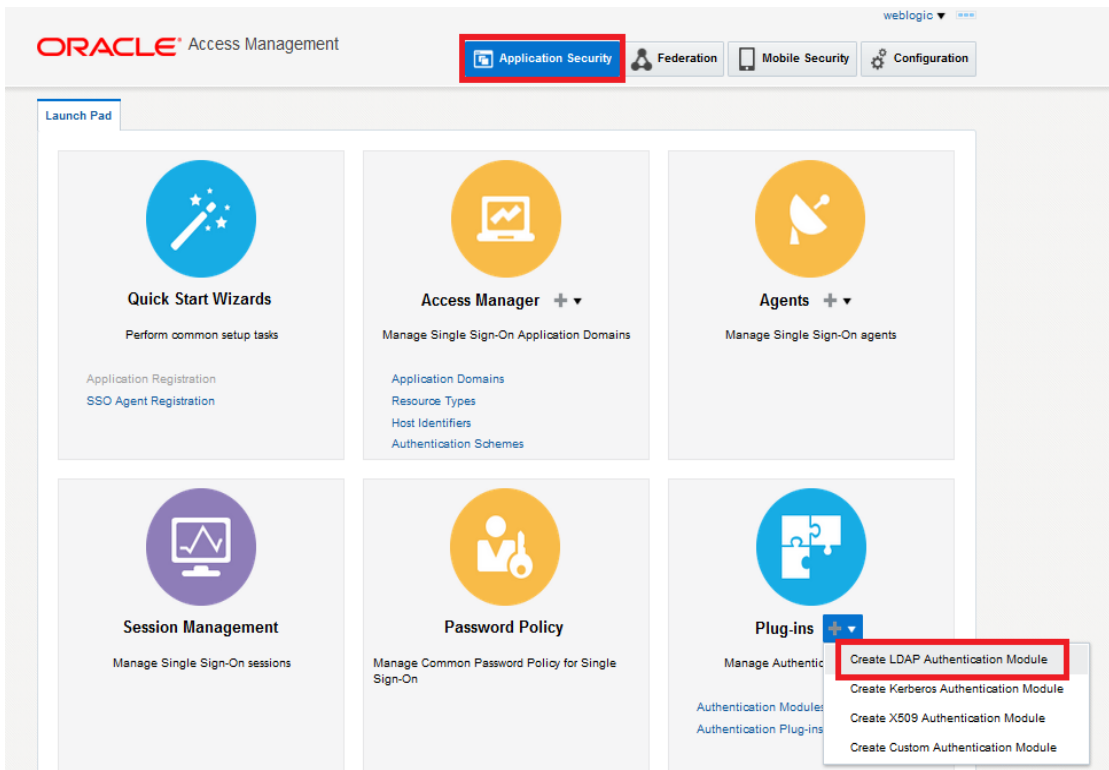
**Note:** User Identity Store will be created only if valid LDAP Parameters are passed.

The screenshot shows the configuration page for a User Identity Store Service named 'FLEXCUBEStore'. At the top, there are tabs for 'Launch Pad', 'User Identity Stores', and 'FLEXCUBEStore'. Below the tabs, there is a 'Configuration' link and buttons for 'Duplicate', 'Test Connection', and 'Apply' (highlighted with a red box). A green confirmation message states: 'User Identity Store FLEXCUBEStore created successfully.' The configuration fields are as follows:

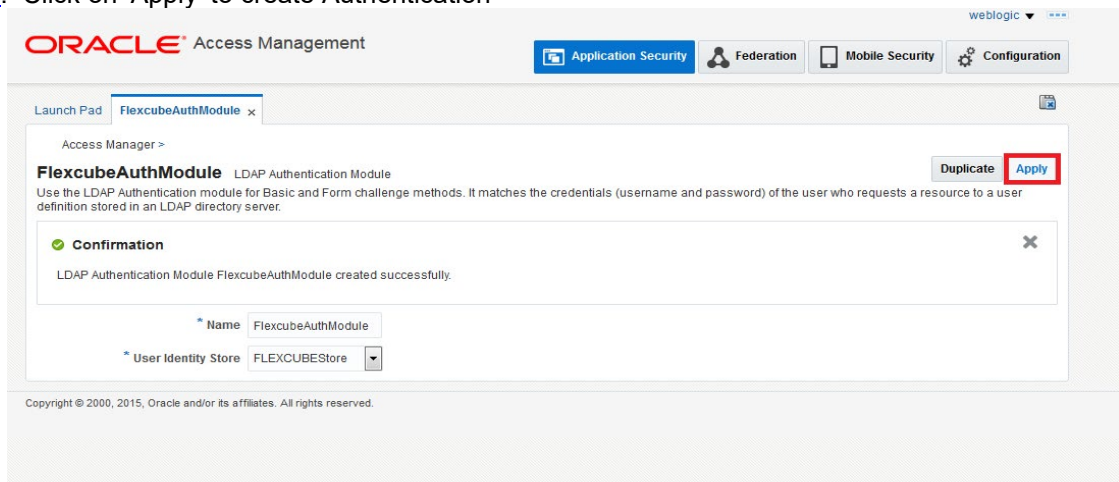
- Store Name: FLEXCUBEStore
- Store Type: OID: Oracle Internet Directory
- Description: (empty)
- Enable SSL:
- Use Native ID Store Settings:
- Prefetched Attributes: (empty)
- Location: ofss220607.in.oracle.com:3131
- Password: (masked with dots)
- Bind DN: cn=orcladmin
- Login ID Attribute: cn
- User Password Attribute: userPassword
- User Search Base: cn=Users,dc=ofss,dc=in,dc=oracle,dc=c
- User Filter Object Classes: (empty)

## 2.6.2 Creating Authentication Module

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



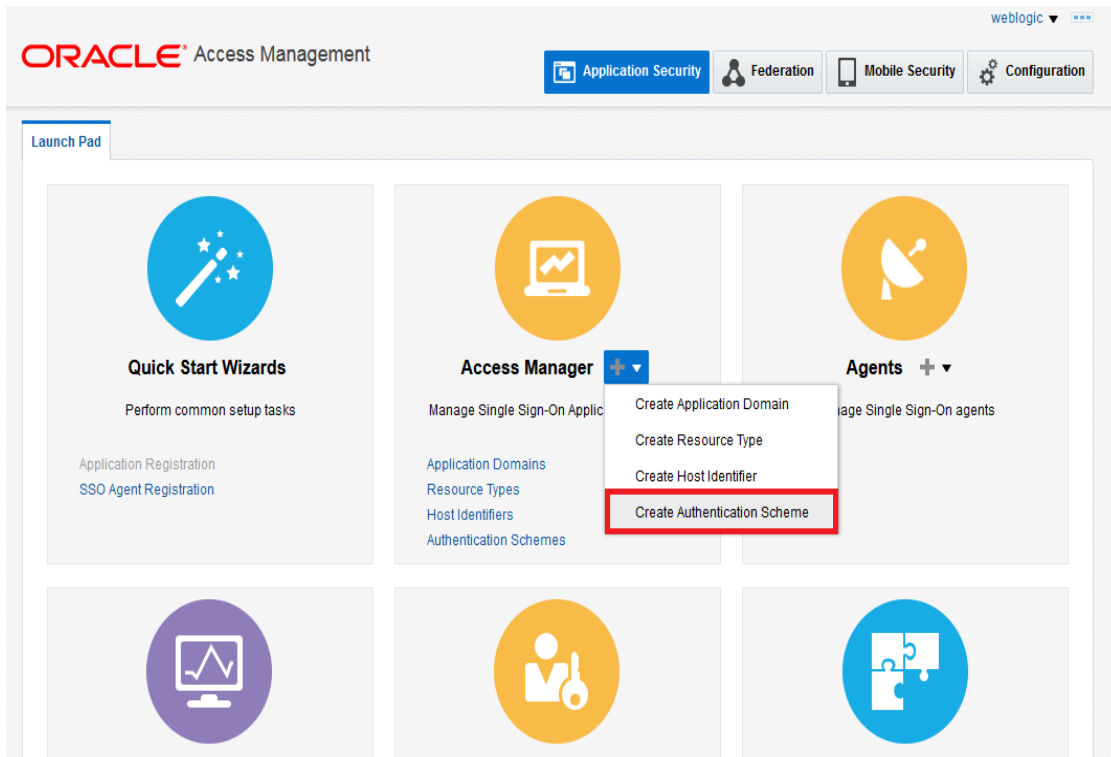
Enter the Name for the Authentication Module and choose the proper User Identification Store, ie created in [2.6.1](#). Click on 'Apply' to create Authentication



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](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

The screenshot shows the Oracle Access Manager console interface. At the top, there's a 'Launch Pad' with a tab for 'FlexcubeBasicOAMScheme'. Below that, the 'Access Manager >' navigation is visible. The main heading is 'Create Authentication Scheme' with a sub-heading 'Authentication Scheme'. To the right of the heading are three buttons: 'Set As Default', 'Duplicate', and 'Apply' (which is highlighted with a red box). Below the heading is a descriptive sentence: 'An Authentication Scheme defines the challenge mechanism required to authenticate a user. Each Authentication Scheme must also include a defined Authentication Module.' A green confirmation message box is displayed, stating 'Authentication Scheme, FlexcubeBasicOAMScheme, created successfully'. The main form contains the following fields: 'Name' (FlexcubeBasicOAMScheme), 'Description' (Basic login screen), 'Authentication Level' (1), 'Challenge Method' (BASIC), 'Challenge Redirect URL' (/oam/server), 'Authentication Module' (FlexcubeAuthModule), and '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

The screenshot shows the Oracle Access Manager console interface. At the top, there is a 'Launch Pad' and a tab for 'FlexcubeFormOAMScheme'. Below this, the 'Access Manager >' navigation is visible. The main heading is 'Create Authentication Scheme' with a sub-heading 'Authentication Scheme'. To the right of the heading are three buttons: 'Set As Default', 'Duplicate', and 'Apply' (which is highlighted with a red box). Below the heading is a descriptive sentence: 'An Authentication Scheme defines the challenge mechanism required to authenticate a user. Each Authentication Scheme must also include a defined Authentication Module.' A green confirmation message box is displayed, stating 'Confirmation: Authentication Scheme, FlexcubeFormOAMScheme, created successfully'. The main form area contains the following fields and controls:

- Name:** FlexcubeFormOAMScheme
- Description:** Form based login page
- Authentication Level:** 2 (with up and down arrows)
- Default:**
- Challenge Method:** FORM (dropdown menu)
- Challenge Redirect URL:** /oam/server
- Authentication Module:** FlexcubeAuthModule (dropdown menu)
- Challenge URL:** /pages/login.jsp
- Context Type:** default (dropdown menu)
- 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

**Create Authentication Scheme** Authentication Scheme Set As Default Duplicate **Apply**

An Authentication Scheme defines the challenge mechanism required to authenticate a user. Each Authentication Scheme must also include a defined Authentication Module.

**Confirmation** ✕  
Authentication Scheme, FlexcubeKBAOAMScheme, created successfully


\* Name FlexcubeKBAOAMScheme  
Description KBA Based login page  
\* Authentication Level 2  
Default   
\* Challenge Method FORM  
Challenge Redirect URL /oam/server  
\* Authentication Module FlexcubeAuthModule  
\* 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.


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'.

The screenshot shows the Oracle Access Management console interface. At the top, there are navigation tabs for 'Application Security', 'Federation', 'Mobile Security', and 'Configuration'. The main content area is titled 'Server Instances' and contains a 'Search OAM Servers' section. A search input field is present, and the 'Search' button is highlighted with a red box. Below the search section, there is a 'Search Results' table with a single row containing the text 'No data to display.'

3. Edit oam\_server1.

The screenshot shows the Oracle Access Management console interface. The 'Search OAM Servers' section is visible, and the search results table now contains one row with the name 'oam\_server1'. The name 'oam\_server1' in the table is highlighted with a red box.

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

The screenshot shows the Oracle Access Management console interface for editing the 'oam\_server1' instance. The 'Mode' dropdown menu is set to 'Simple' and is highlighted with a red box. The 'Apply' button is also highlighted with a red box. Other configuration fields include 'Server Name', 'Port', 'Host', 'Proxy Server Id', 'Coherence', 'Log Level', 'Local Port', and 'Log Limit'.

ORACLE Access Management weblogic ---

Application Security Federation Mobile Security Configuration

Launch Pad Server Instances x oam\_server1 x

Configuration >

**oam\_server1** OAM Server Instance Duplicate Apply

\* Server Name oam\_server1 \* Host ofss220607.in.oracle.  
\* Port 14101

**OAM Proxy**

\* Proxy Server Id AccessServerConfigP  
\* Port 5575  
\* Mode Simple

**Coherence Configuration**

\* Log Level 3  
\* Local Port 9095  
\* Log Limit 4096

**Confirm Edit** X

OAM Server instance oam\_server1 might be in use.  
Are you sure you want to edit it?

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Launch Pad Server Instances x oam\_server1 x

Configuration >

**oam\_server1** OAM Server Instance Duplicate Apply

**Confirmation** X

OAM Server instance oam\_server1 modified successfully.

\* Server Name oam\_server1 \* Host ofss220607.in.oracle.  
\* Port 14101

**OAM Proxy**

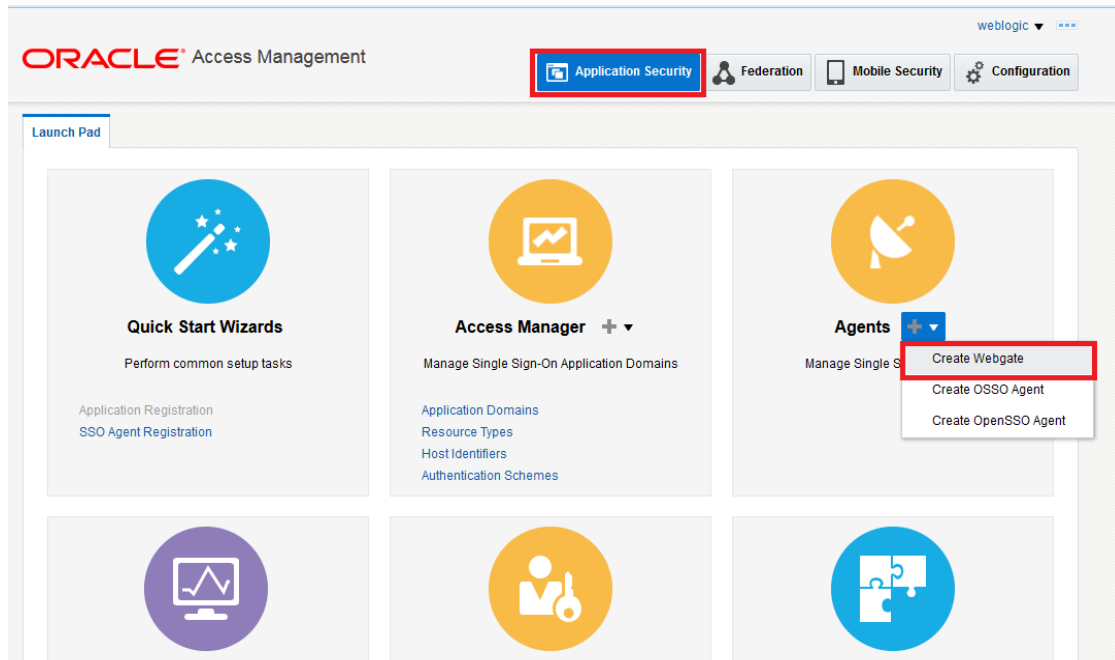
\* Proxy Server Id essServerConfigProxj  
\* Port 5575  
\* Mode Simple

**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

Launch Pad Create Webgate x

Access Manager >

### Create Webgate

Use the following screen to register an OAM Agent. Before you register, ensure that at least one OAM Server is running in the same mode as the Agent to be registered.

**Apply**

\* Version 11g

\* Name FlexcubeWebgate

Description Flexcube 11g Webgate

Base URL `https://ofss220807.in.oracle.com`

Access Client Password

Host Identifier FlexcubeWebgate

User Defined Parameters `filterOAMAuthnCookie=false`

\* Security  Open  Simple  Cert

Virtual host

Auto Create Policies

IP Validation

Enter the Base URLs for Agent

Resource Lists

Protected Resource List **Add Delete**

Relative URI
/FCJNeoWeb

Public Resource List **Add Delete**

Relative URI
--------------

FlexcubeWebgate Webgate **Apply Download**

**Confirmation**

OAM Webgate FlexcubeWebgate created successfully.

Version 11g

Name FlexcubeWebgate

Description Flexcube 11g Webgate

Access Client Password

\* Security  Open  Simple  Cert

\* State  Enable  Disable

\* Max Cache Elements 100000

\* Cache Timeout (Seconds) 1800

Logout Target URL

Deny On Not Protected

User Defined Parameters `proxySSLHeaderVar=IS_SSL  
URLInUTF8Format=true  
client_request_retry_atte  
mpts=1  
inactiveReconfigPeriod=`

\* Sleep for (Seconds) 60

Cache Pragma Header no-cache

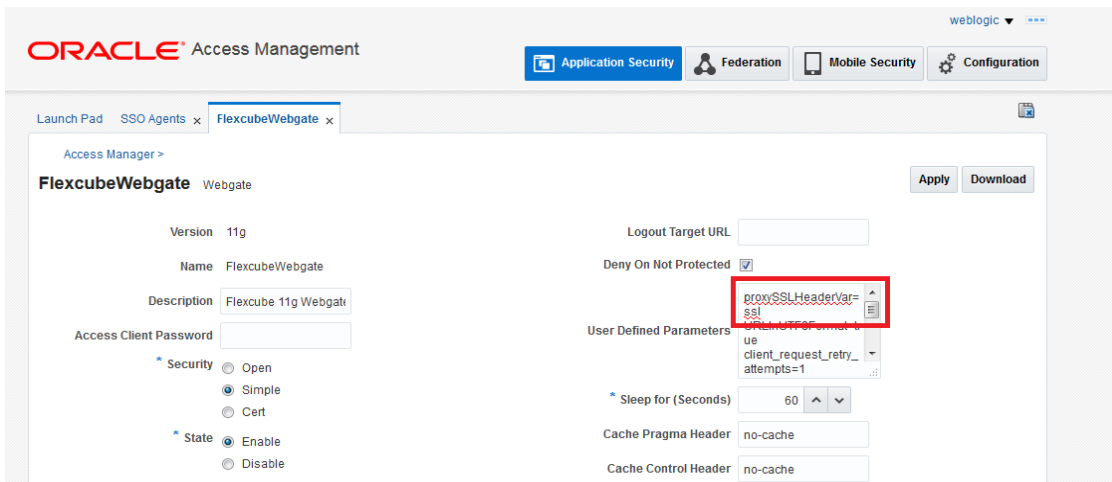
Cache Control Header no-cache

Debug

IP Validation

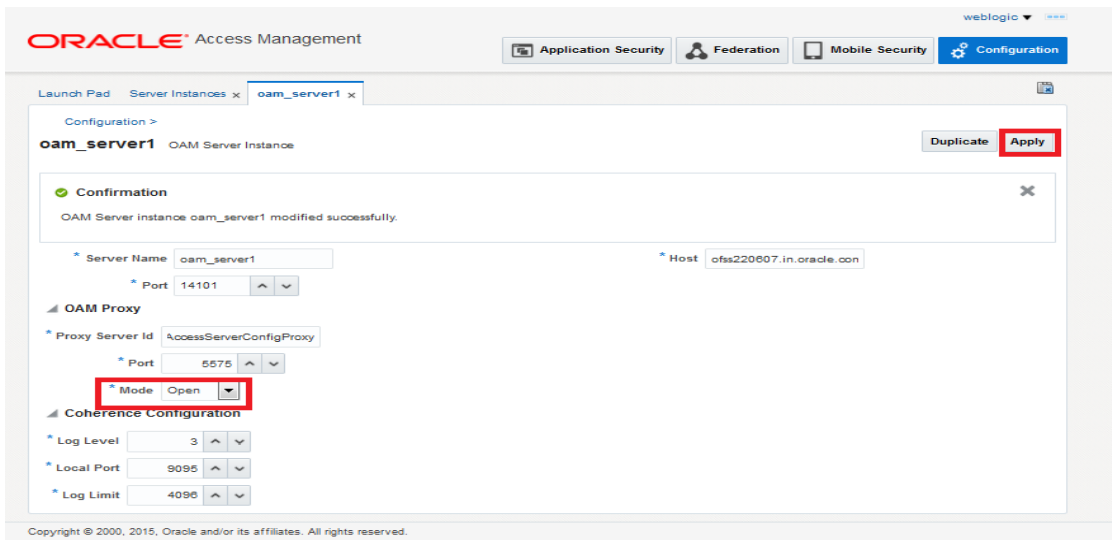
- Once the OAM 11g Webgate is created, Change the parameter from **proxySSLHeaderVar=IS\_SSL** to **proxySSLHeaderVar=ssl** along with other parameters in User Defined Parameters.
- Click on 'Apply'.





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.

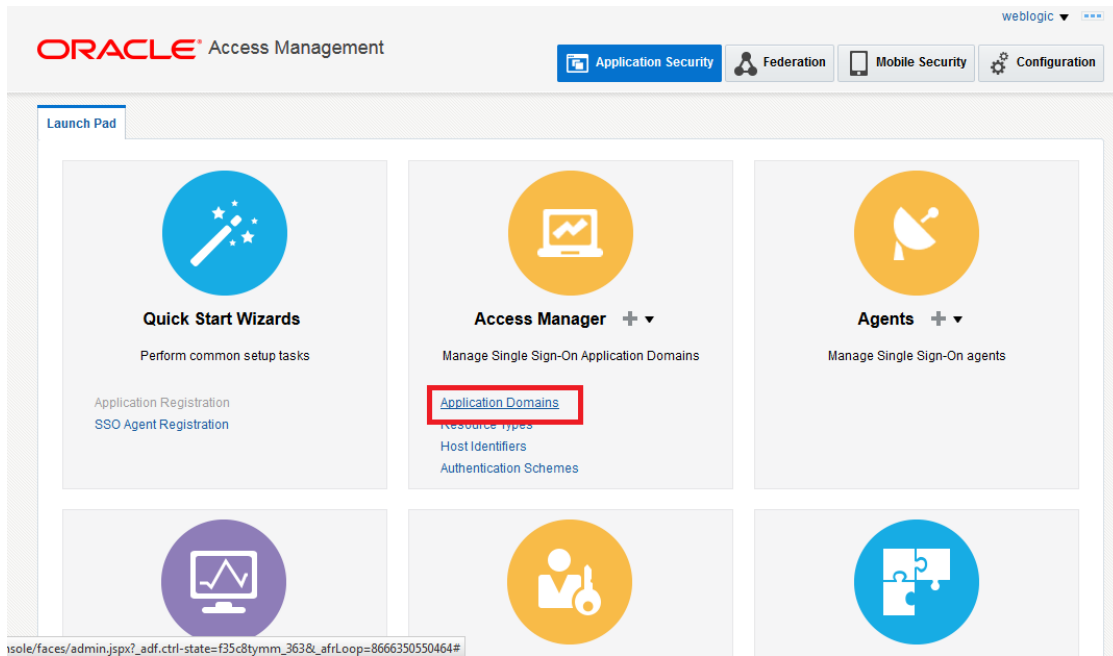


## 2.6.5 Post OAM Webgate 11g Creation

Follow the below steps to configure the webgate created .

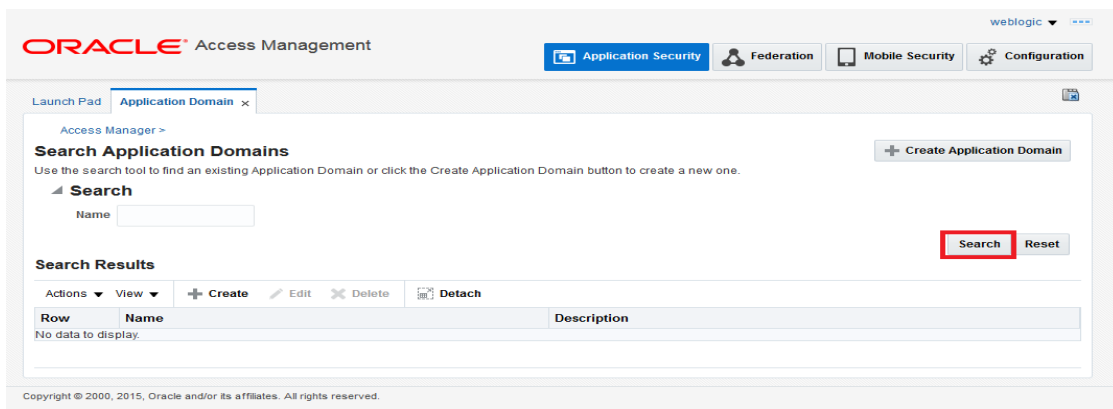
### 2.6.5.1 Application Domains Changes

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.



ORACLE Access Management weblogic ▾ ☰

Application Security
Federation
Mobile Security
Configuration

Launch Pad Application Domain x

Access Manager >

### Search Application Domains

Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one.

**Search**

Name

**Search Results**

▾
  ▾

Row	Name	Description
1	FlexcubeWebgate	Application Domain created through Remote Registration
2	Fusion Apps Integration	Policy objects enabling integration with Oracle Fusion Applications
3	IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications

3. Click on 'Authentication Polices'.

ORACLE Access Management weblogic ▾ ☰

Application Security
Federation
Mobile Security
Configuration

Launch Pad Application Domain x FlexcubeWebgate x

Access Manager >

### FlexcubeWebgate

Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

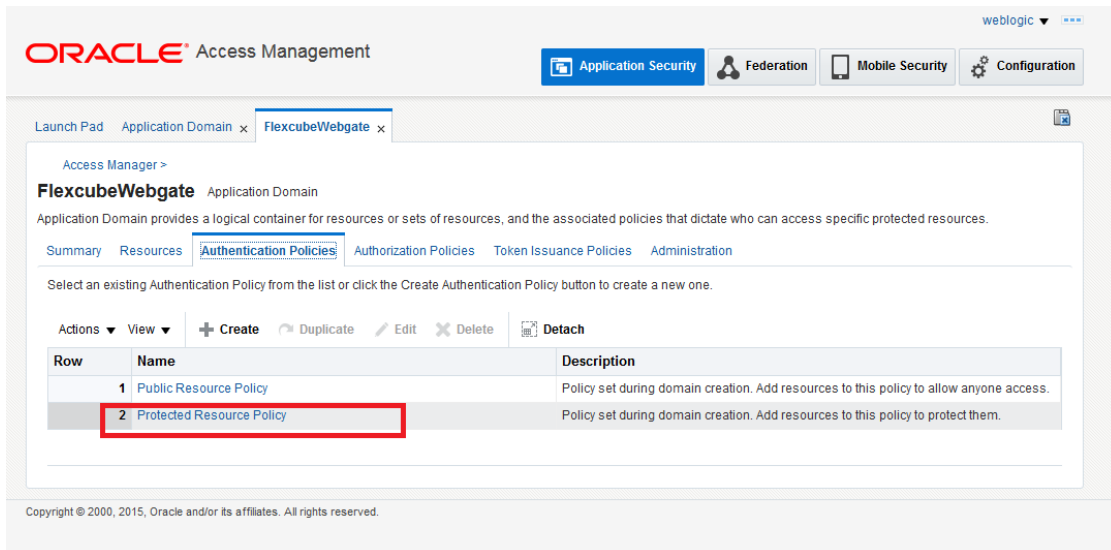
Name

Description

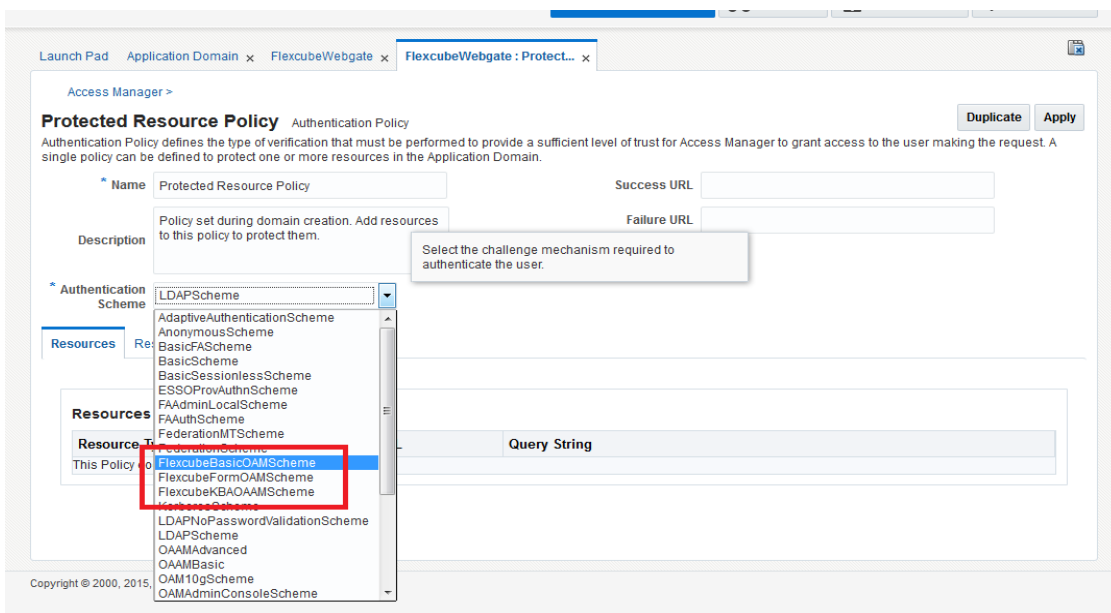
Session Idle Timeout (minutes)

Allow OAuth Token  
 Allow Session Impersonation  
 Enable Policy Ordering

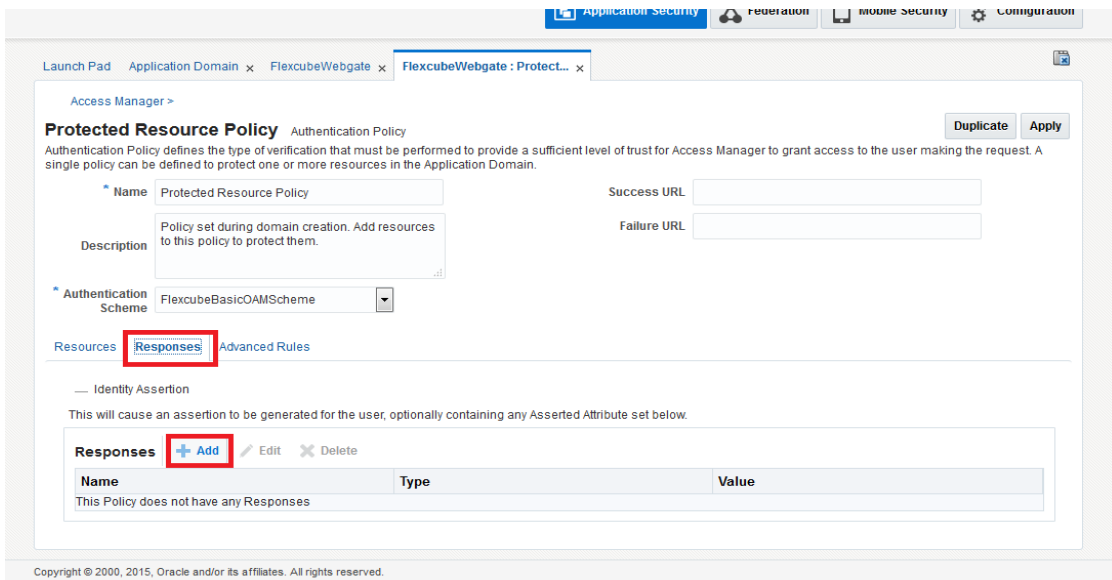
4. Click on 'Protected Resource Policy'.



- Choose the Authentication Scheme created earlier in 'Creating Authentication Scheme'. Refer the section '[Creating Authentication Scheme 2.6.3](#)' of this document.



- Click 'Responses' tab and click **+ Add** button to Add 'DN' variable to the Response Header.



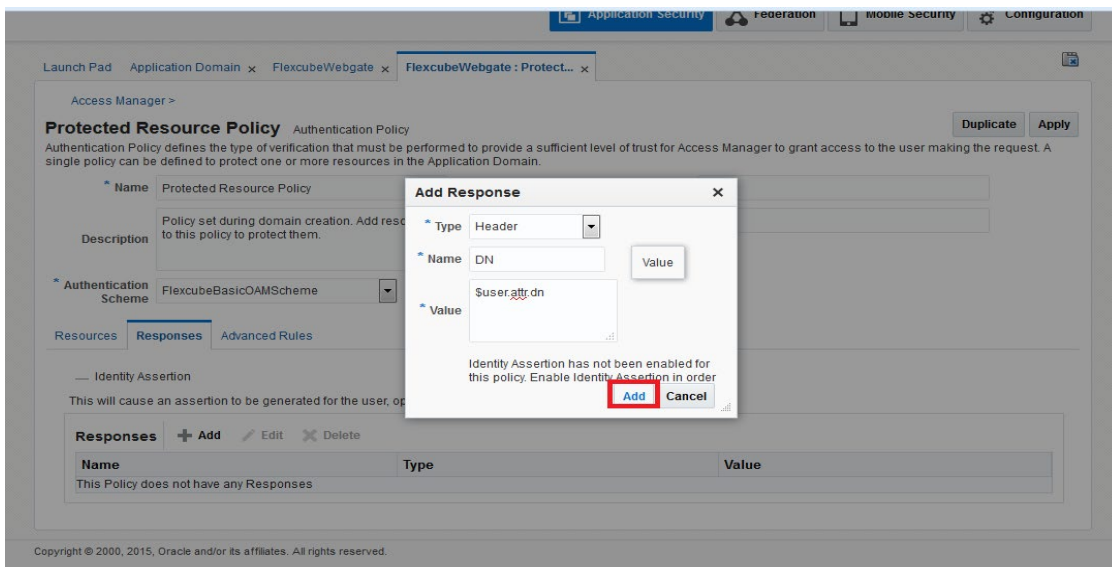
7. Enter the following values in the Add Response Window:

Type : Header

Name : DN

Value : \$user.attr.dn

Click on Add button



8. Click on Apply to Save the Changes

Launch Pad Application Domain x FlexcubeWebgate x FlexcubeWebgate : Protect...

Access Manager >

**Protected Resource Policy** Authentication Policy Duplicate **Apply**

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

**Confirmation** ✕

Authentication Policy, Protected Resource Policy, modified successfully

\* Name Protected Resource Policy Success URL

Description Policy set during domain creation. Add resources to this policy to protect them. Failure URL

\* Authentication Scheme FlexcubeBasicOAMScheme

Resources Responses Advanced Rules

Identity Assertion

This will cause an assertion to be generated for the user, optionally containing any Asserted Attribute set below.

**Responses** + Add Edit Delete

Name	Type	Value
DN	Header	Suser.attr.dn

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

ORACLE Access Management weblogic

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain x FlexcubeWebgate x

Access Manager >

**FlexcubeWebgate** Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Summary Resources Authentication Policies **Authorization Policies** Token Issuance Policies Administration

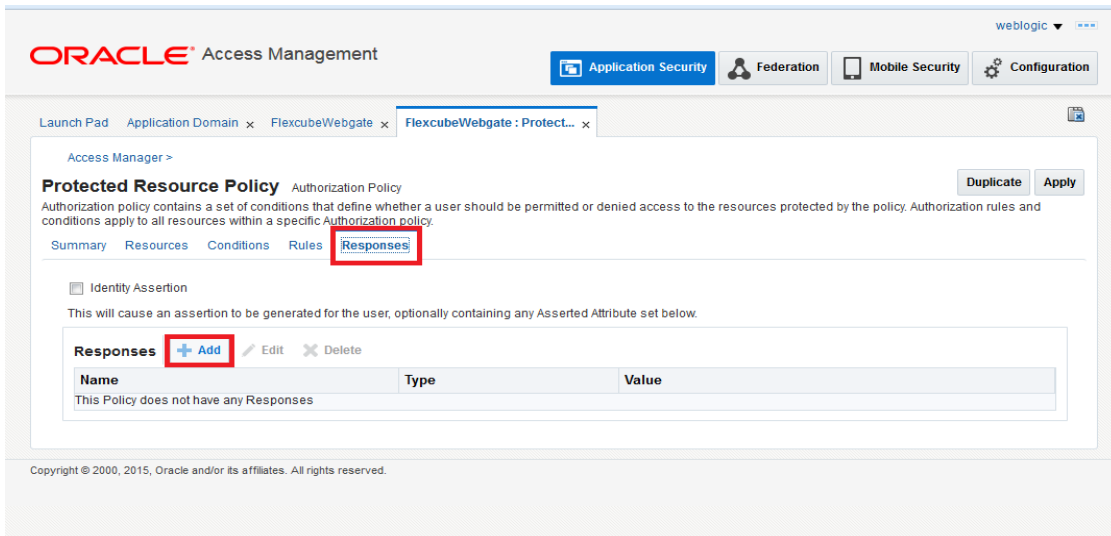
Select an existing Authorization Policy from the list or click the Create Authorization Policy button to create a new one.

Actions View + Create Duplicate Edit Delete Detach

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	<b>Protected Resource Policy</b>	Policy set during domain creation. Add resources to this policy to protect them.

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

10. Click on 'Response' tab and click on + Add button to Add 'DN' variable to the Response Header.



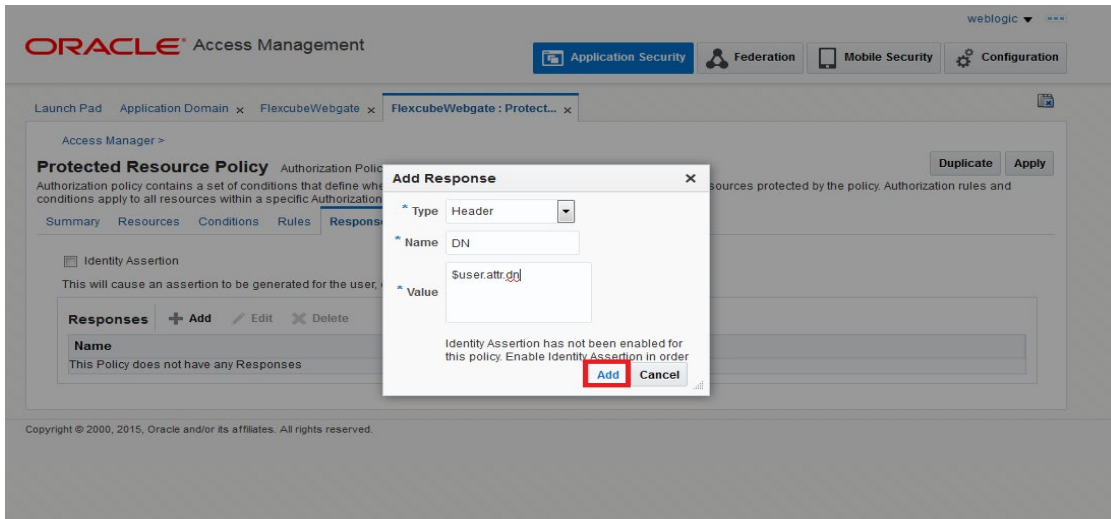
11. Enter the following values in the Add Response Window :

Type : Header

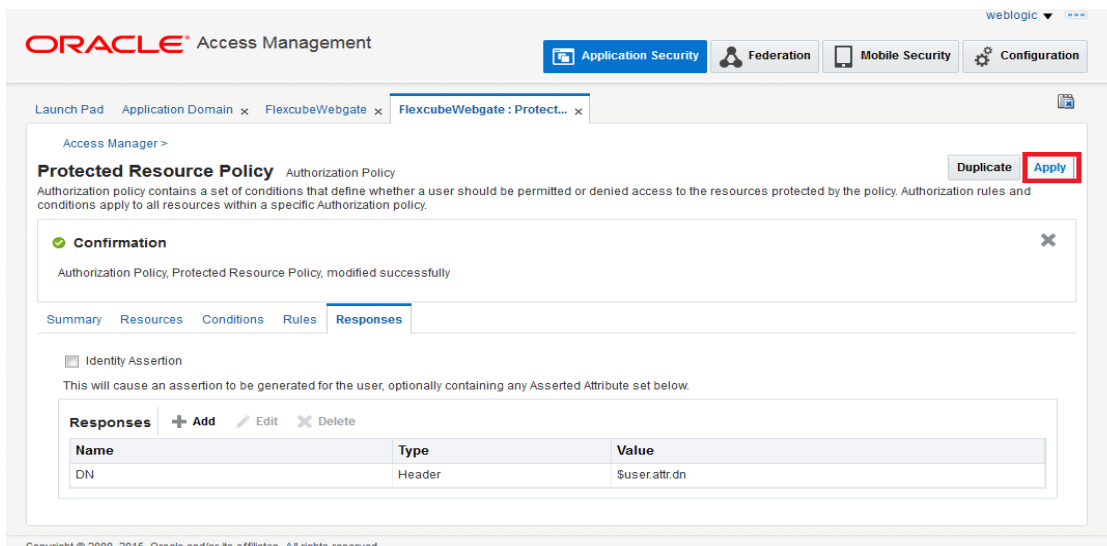
Name : DN

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
```

```
    WLSSSLWallet
```

```
    "<ORACLE_MIDDLEWARE>/<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1/kestores/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](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			

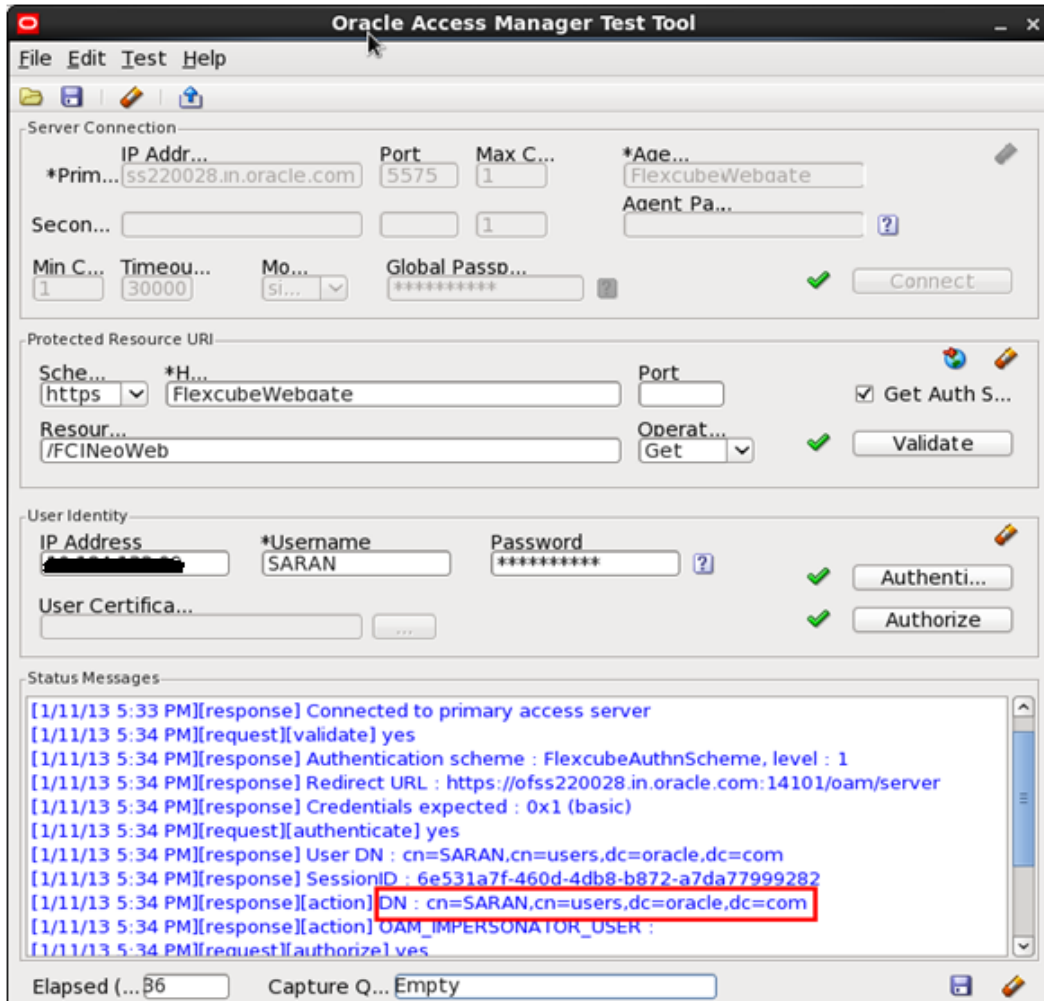
Cache Name	State	Max Elems	Curr Elems	Timeout (seconds)	Cache Stats (Hits:Misses:Expired:Flushed)	Memory Footprint (bytes)
Resource to Authentication Scheme	active	100000	100	1800	6451:273:61:0	59750
Authentication Scheme	active	25	1	1800	15012:34:33:0	802
Resource to Authorization Policy	active	100000	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 (\) in front 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.

The screenshot displays the 'Bank Parameters Maintenance' application window. The window title is 'Bank Parameters Maintenance'. The main area is divided into several sections: 'Bank Code' (000), 'Bank Name' (Bank Futura), 'Head Office Branch' (Branch Code: 000, Branch Description: Bank Futura), 'Financial Preferences' (General Preferences, FATCA), 'Format Mask' (Cif Mask: bbbnnnnn, General Ledger Mask: nnnnnnnn), 'Year End Profit and Loss' (General Ledger: 221000002, Transaction Code: YET), 'Spread' (Spread Application: Both Legs, Spoof Files Purge Days: 90, Inter Pay Lead Days: 3), 'Cheque Numbering Details' (Scheme: Automatic, Cheque Number Mask: NNNNNN), 'Checksum Algorithm' (dropdown menu), and 'IRS Details' (Suspense Account). The 'SSO Enabled' checkbox is checked and highlighted with a red box. The bottom status bar shows 'Maker', 'Checker', 'Mod No: 229', 'Date Time', 'Record Status Open', and 'Authorization Status'. A 'Cancel' button is visible in the bottom right corner.

### **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

**User Maintenance**

Save

**User Details**

User Identification \* FCUBSUSER  
 Name \* FCUBSUSER  
 User Reference  
 Language \* ENG  
 Home Branch \* 000  
 Customer No  
 Department Code  
 Department Description  
 Tax Identifier  
 LDAP DN **cn=FCUBSUSER,cn=Us**  
 Time Level \* 9  
 Amount Format  
 Date Format  
 Auto Authorization  
 Validate  
 Supervisor Identification  
 Supervisor Name

**User Status**  
 Enabled  
 Hold  
 Disabled  
 Locked  
**Classification**  
 Staff  
 Branch  
 Status Changed On 2011-01-04  
 Last Signed On  
 Staff Customer Restriction Required  
 ELCM User ID  
 Multi Branch Access  
 Other RM Customer Access Restricted  
 Show Dashboards  
 Alerts on Home  
 MFI User  
 F10 Access Required  
 F11 Access Required  
 F12 Access Required

**User Password**  
 Password  
 Password Changed On 2012-01-04  
 Email  
 Reference No

**Invalid Logins**  
 No of Cumulative Logins 17  
 No of Successive Logins 0

**Screen Saver Details**  
 Screensaver Interval (in seconds) 3600

Restricted Password | Roles | Rights | Functions | Tills | Account Classes | General Ledgers | Limits | Branches |

For FLEXCUBE - IS

**User Admin**

Save

**User Details**

User Identification \* FCISUSER  
 Name \* FCIS User  
 External Identifier  
 LDAP DN **cn=FCUSR,cn=Users,d**  
 Number Format  
 XXX,XXX,XXX,XXX  
 XX,XX,XX,XX,XX  
 Language \* ENG  
 Home Branch \* 000  
 Home Module \* FMG  
 Debug Window Enabled  
**Classification**  
 Staff  
 Auto End Of Day  
 Customer

**Modules**  
 Investments  
 Corporate

**Status Description**  
**User Status**  
 Enabled  
 Hold  
 Disabled  
 Locked  
 Time Level \* 9  
 Status Changed On  
 Last Signed On

**Invalid Logins**  
 Cumulative 0  
 Successive 0

**User Passwords**  
 Password  
 Password Changed On  
 Email  
 Start Date \* 07/26/2014  
 End Date

**Amount Limits**  
 Override Amount \*  
 Transaction Amount \*  
 Auth Amount \*  
 Date Format MM/DD/YYYY  
 Auto Auth No  
 Amount Format Dot Comma

Restricted Passwords | Roles | Functions | Branches | Module | Disallowed Functions

Input by  
 Authorized by  
 DateTime  
 DateTime  
 Mod No  
 Open  
 Authorized

OK Cancel

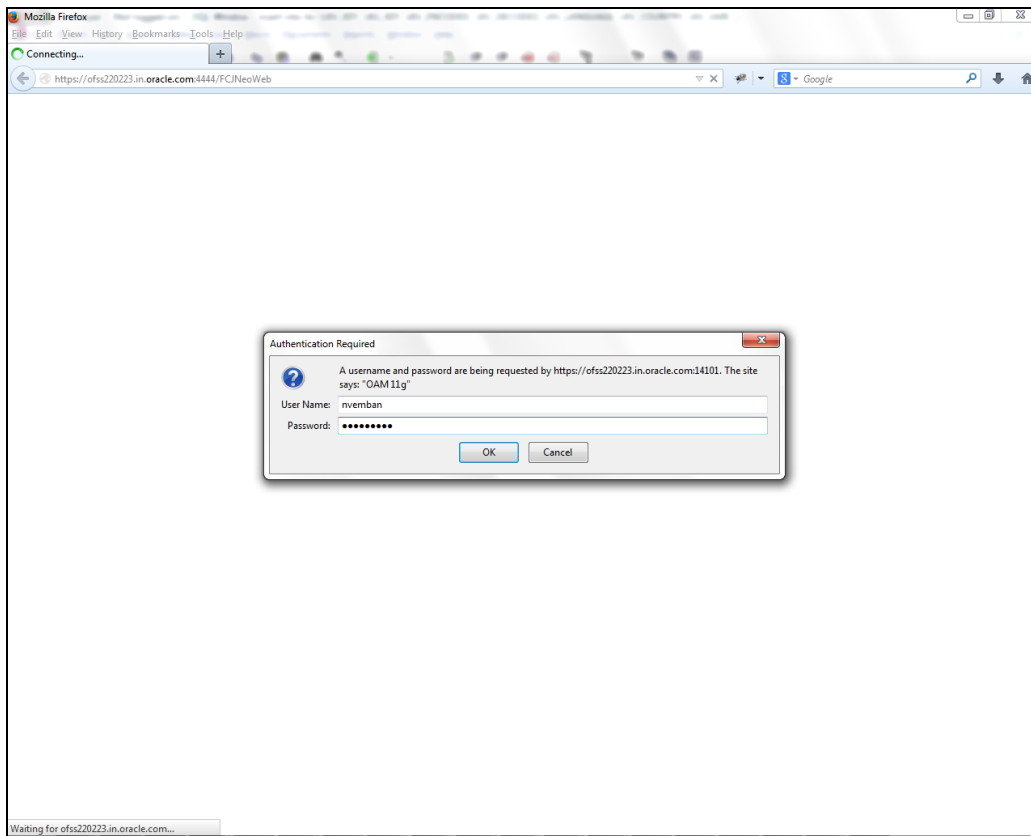
### 2.7.3 **Launching FLEXCUBE**

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>

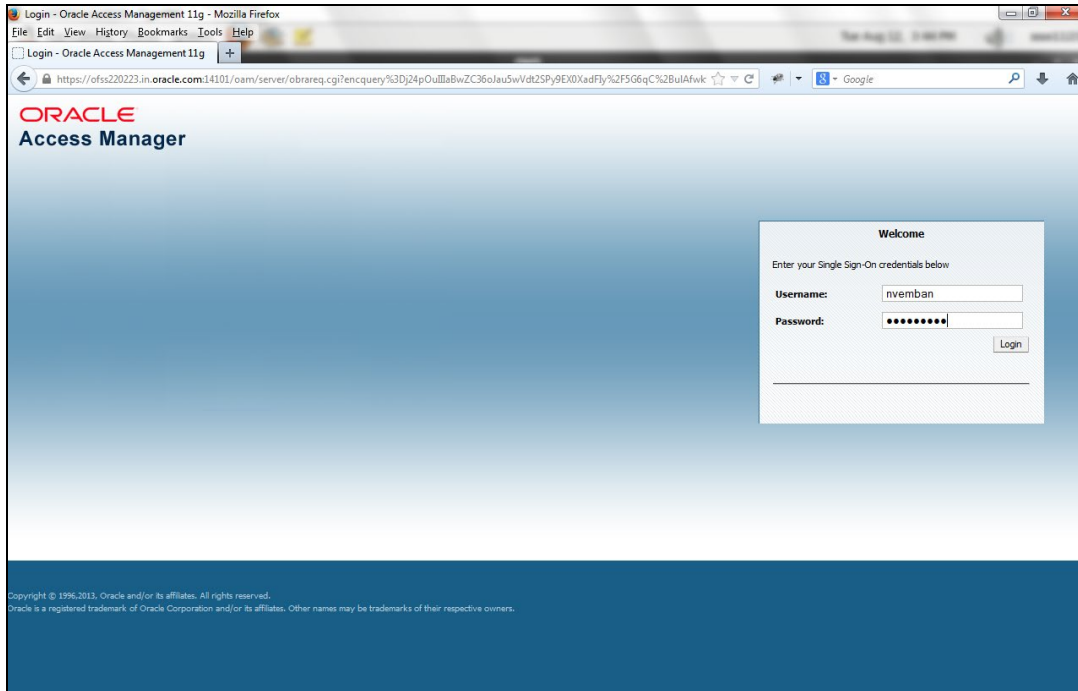
Since the resource is protected, the WebGate challenges the user for credentials as shown below.

### 2.7.3.1 Basic Style Challenge by Webgate

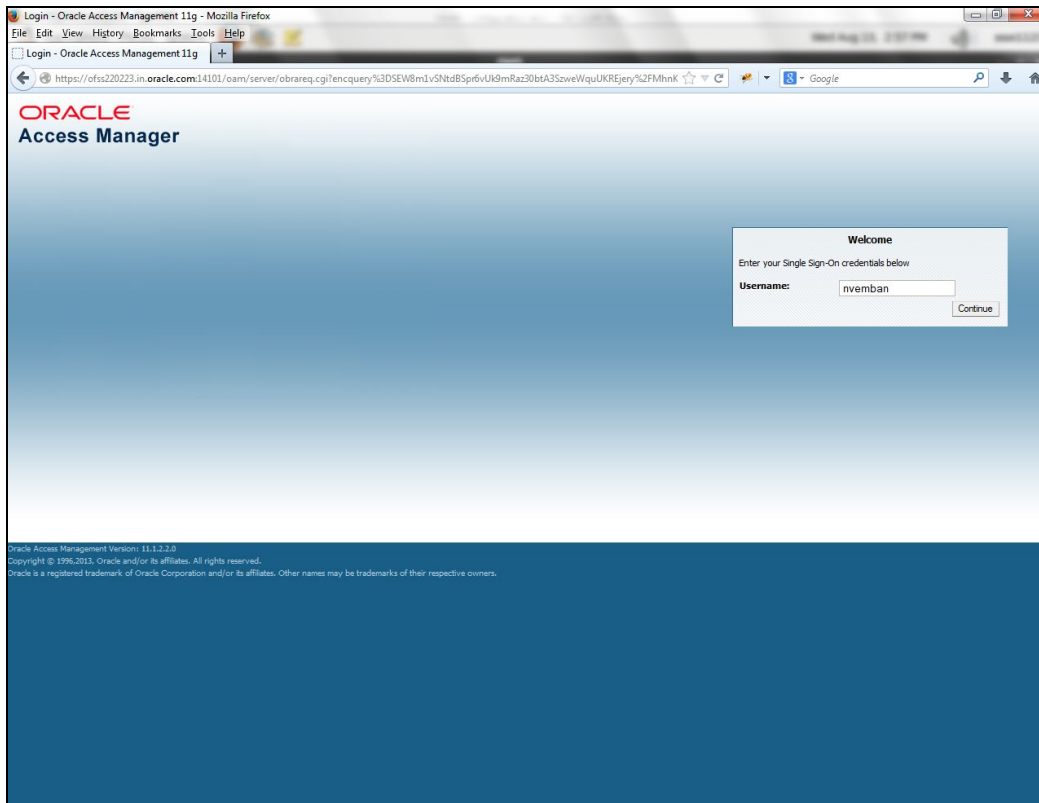




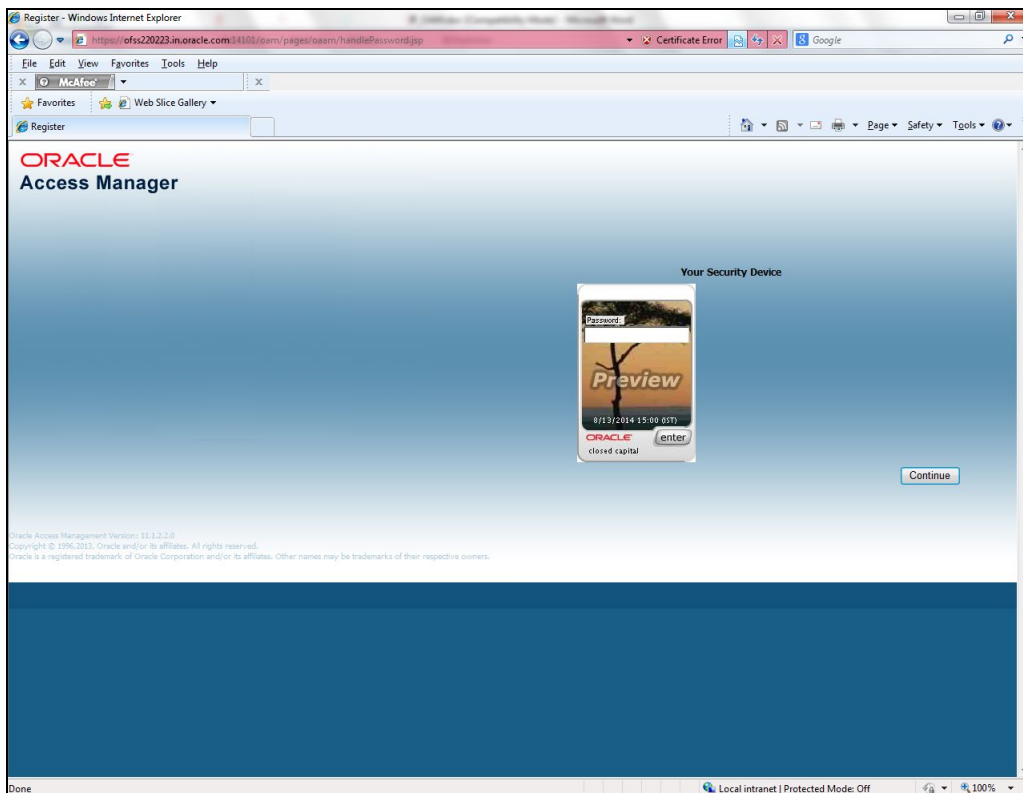
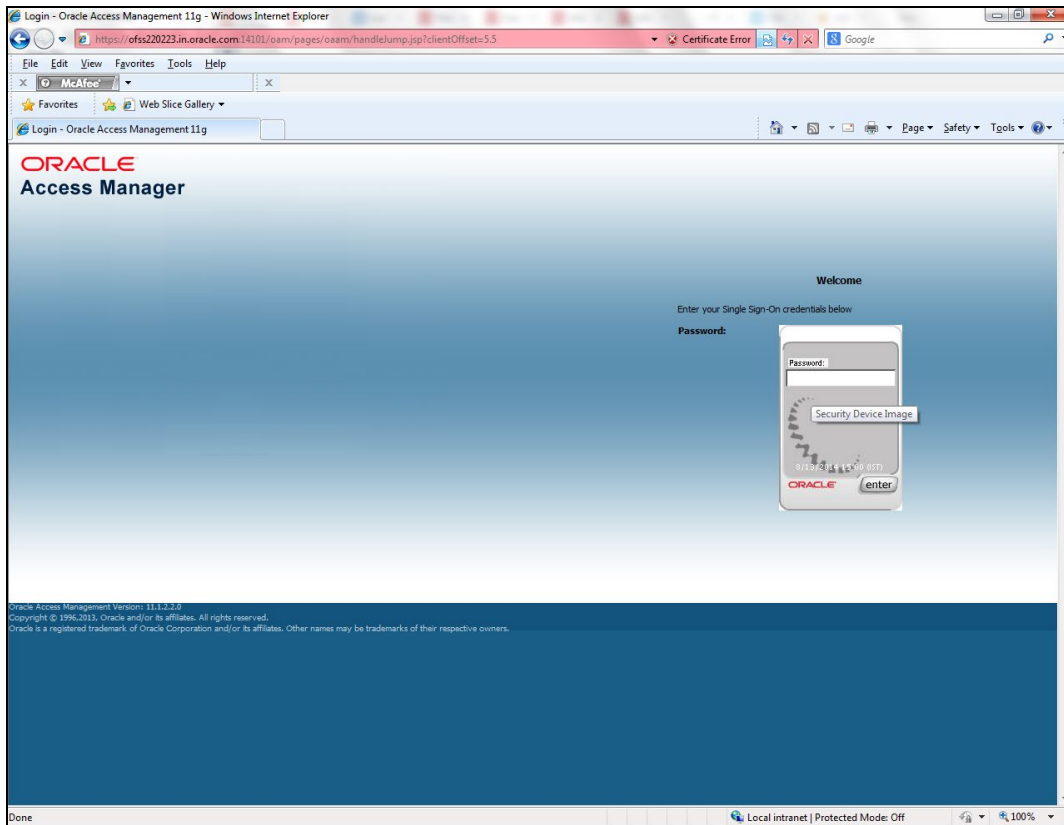
### 2.7.3.2 Form Style Challenge by Webgate

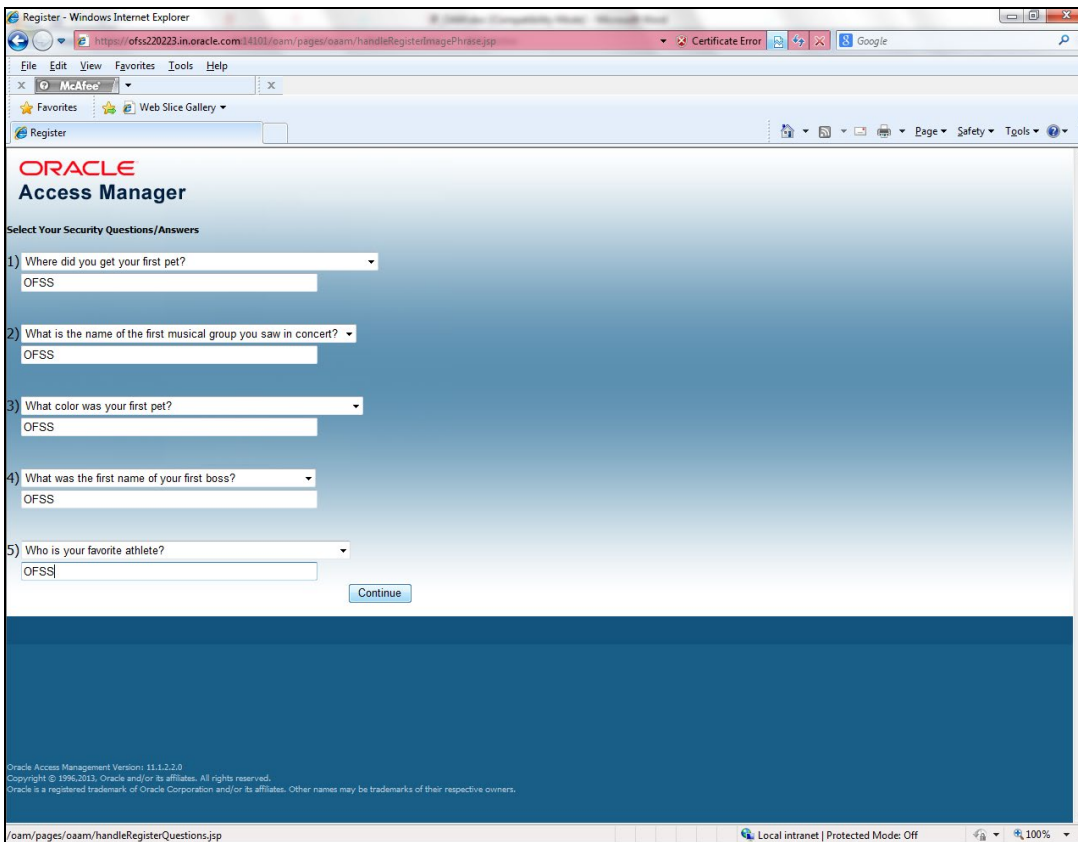
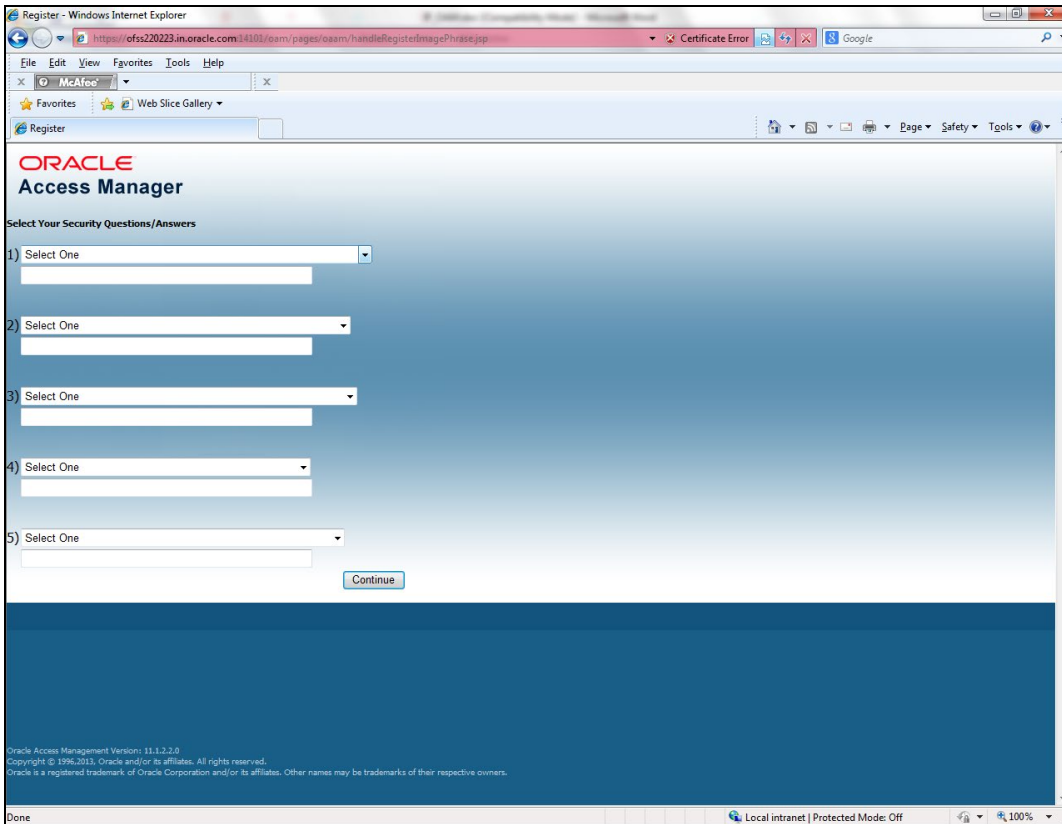


### 2.7.3.3 KBA Based Strong Authentication Challenge by Webgate( Only when OAM is used)

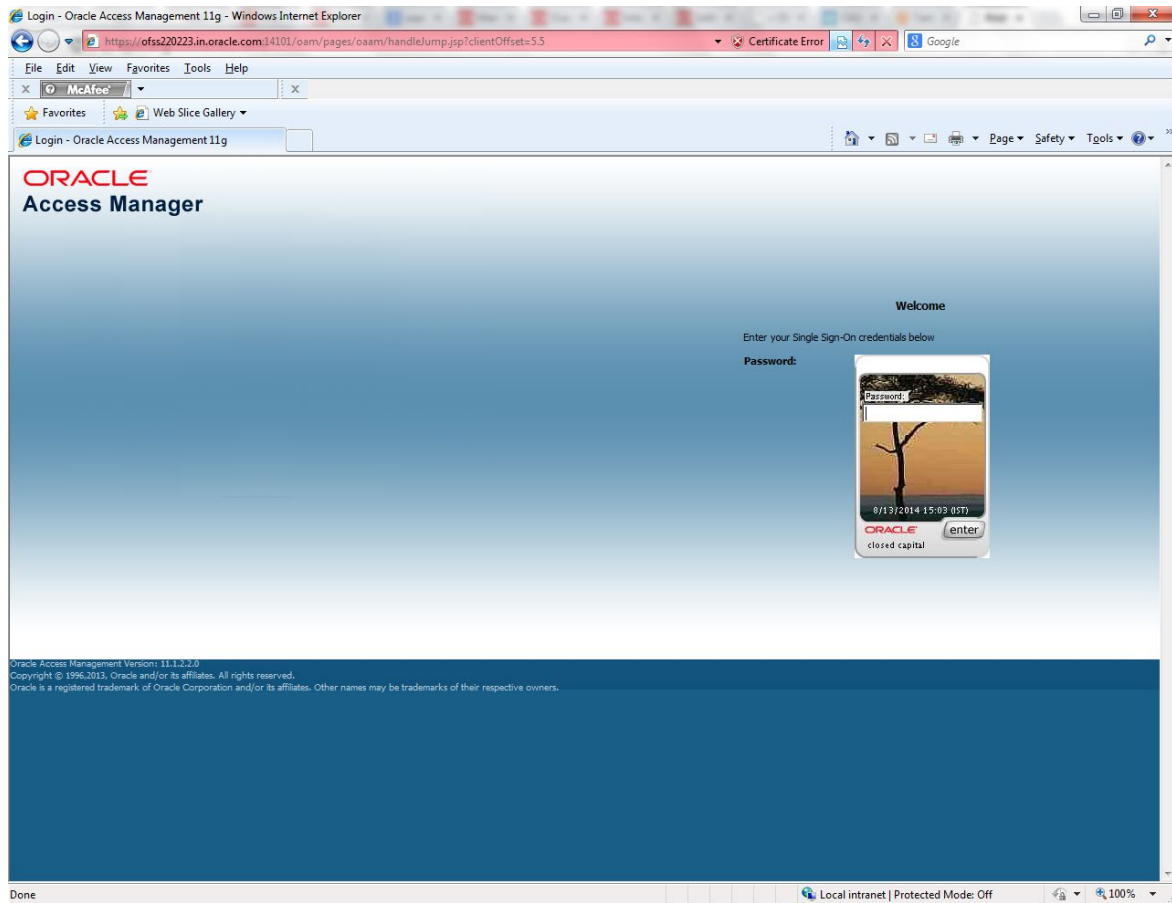


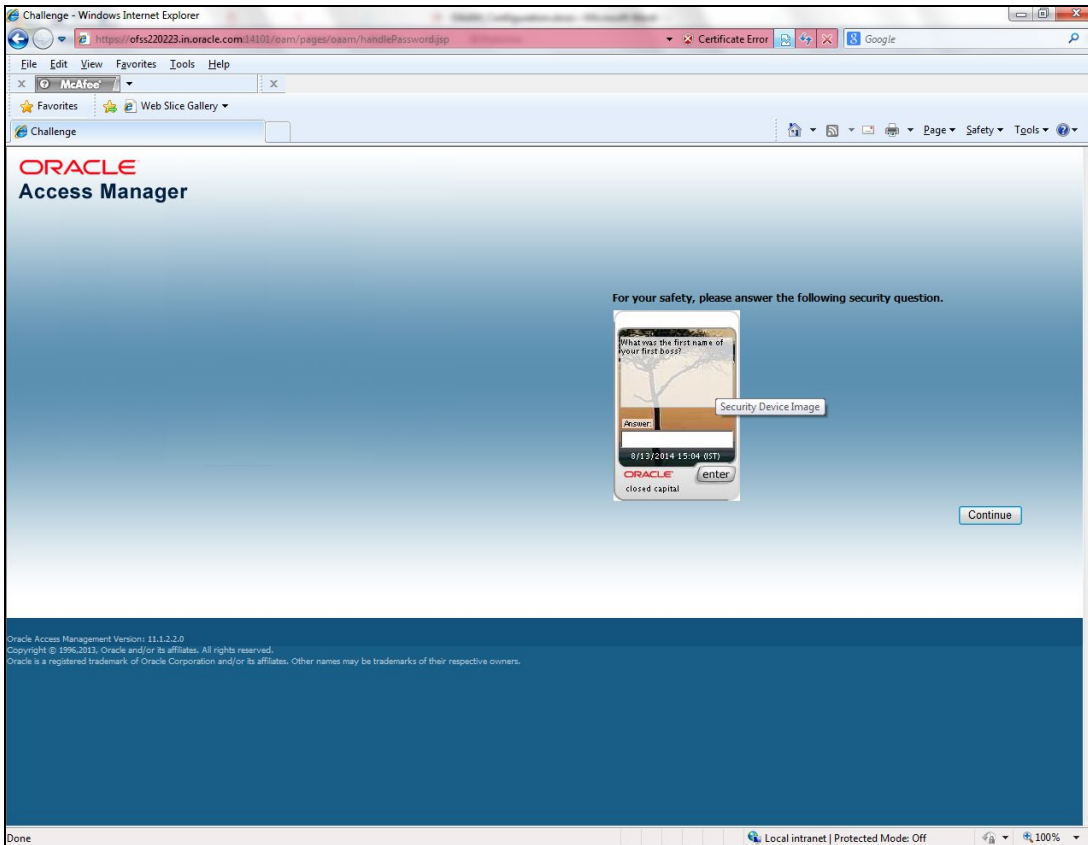
## First Time Login





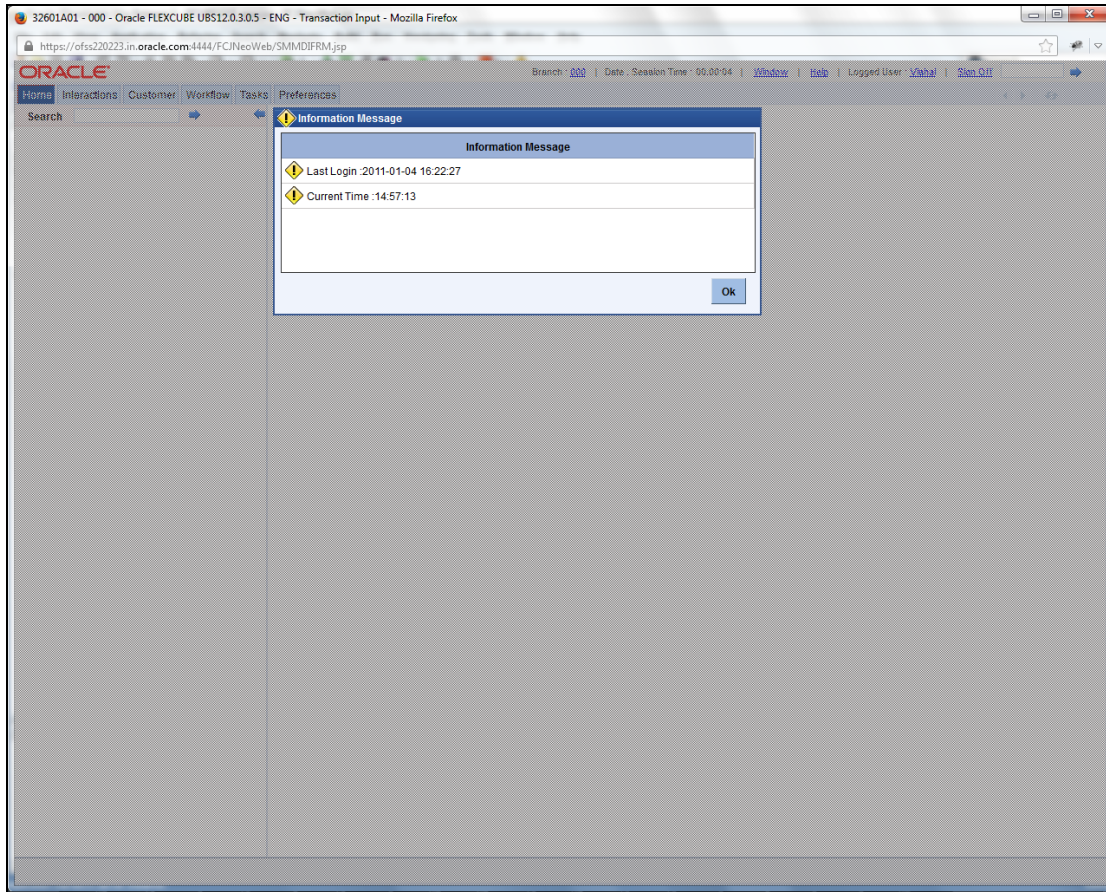
## Post First Login





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

Copyright © [2007], [2018], 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.