Oracle Access Manager Integration

Oracle FLEXCUBE Investor Servicing

Release 14.5.3.0.0

Part Number F53508-01

February 2022

Oracle Access Manager Integration
[February] [2022]
Version 14.5.3.0.0

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/

Table of Contents

1. Preface

1.1 Introduction

This manual discusses the integration of Oracle FLEXCUBE Investor Servicing 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
IS	Investor Servicing
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 IS 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.

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 "SHA256withRSA" -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:

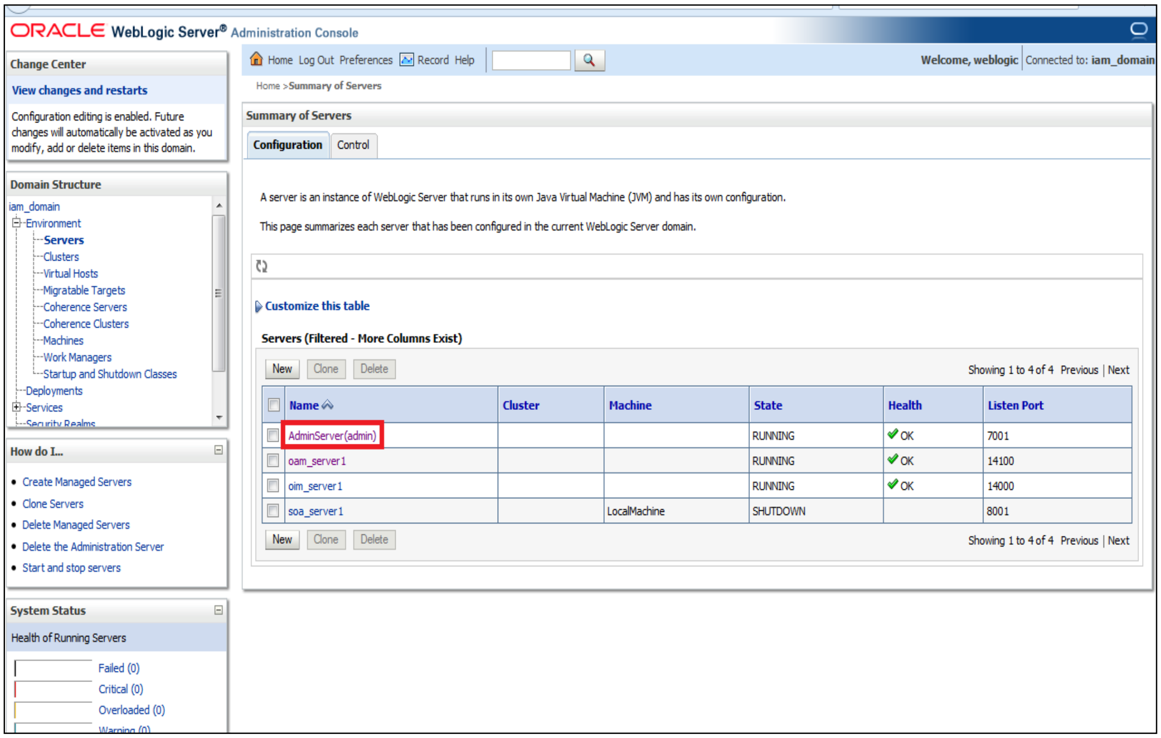
```
keytool -import -v -trustcacerts -alias rootcacert -file AdminFlexcubeCert.cer -keystore
AdminFlexcubeKeyStore.jks -keypass Password@123 -storepass Password@123
```

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



ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Welcome, weblogic | Connected to: iam_domain

Home >Summary of Servers

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...

- Create Managed Servers
- Clone Servers
- Delete Managed Servers
- Delete the Administration Server
- Start and stop servers

System Status

Health of Running Servers

Failed (0)
Critical (0)
Overloaded (0)
Warning (0)

Summary of Servers

Configuration | Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.

This page summarizes each server that has been configured in the current WebLogic Server domain.

Customize this table

Servers (Filtered - More Columns Exist)

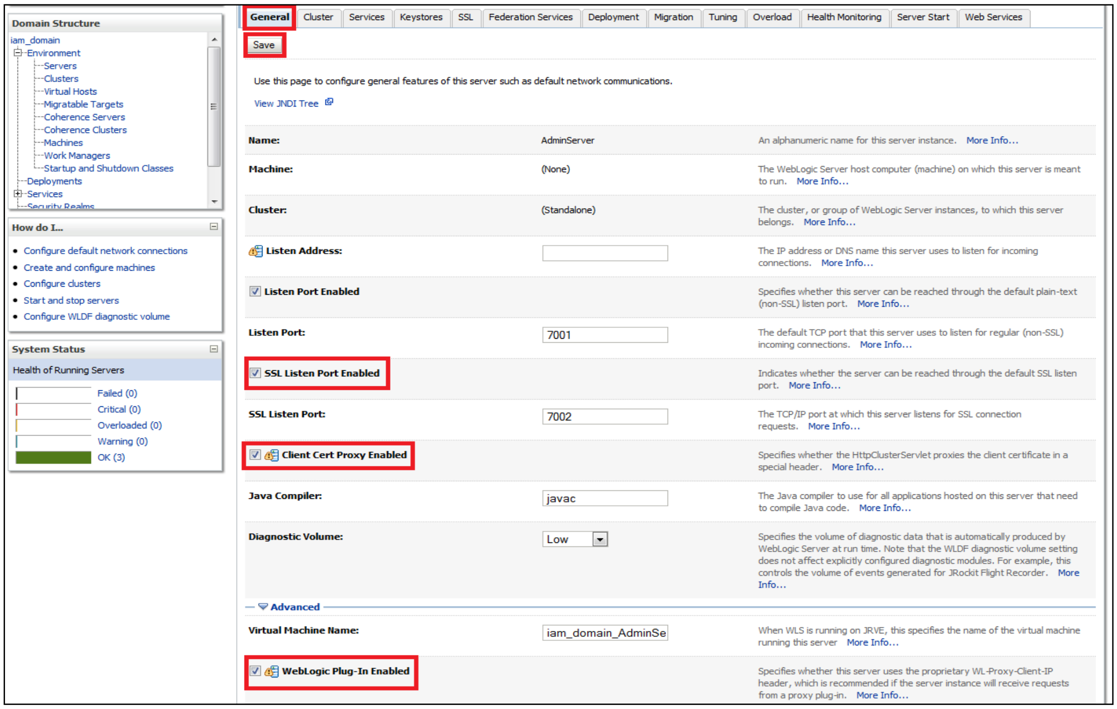
New Clone Delete — Showing 1 to 4 of 4 Previous | Next

	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

New Clone Delete — Showing 1 to 4 of 4 Previous | Next

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.



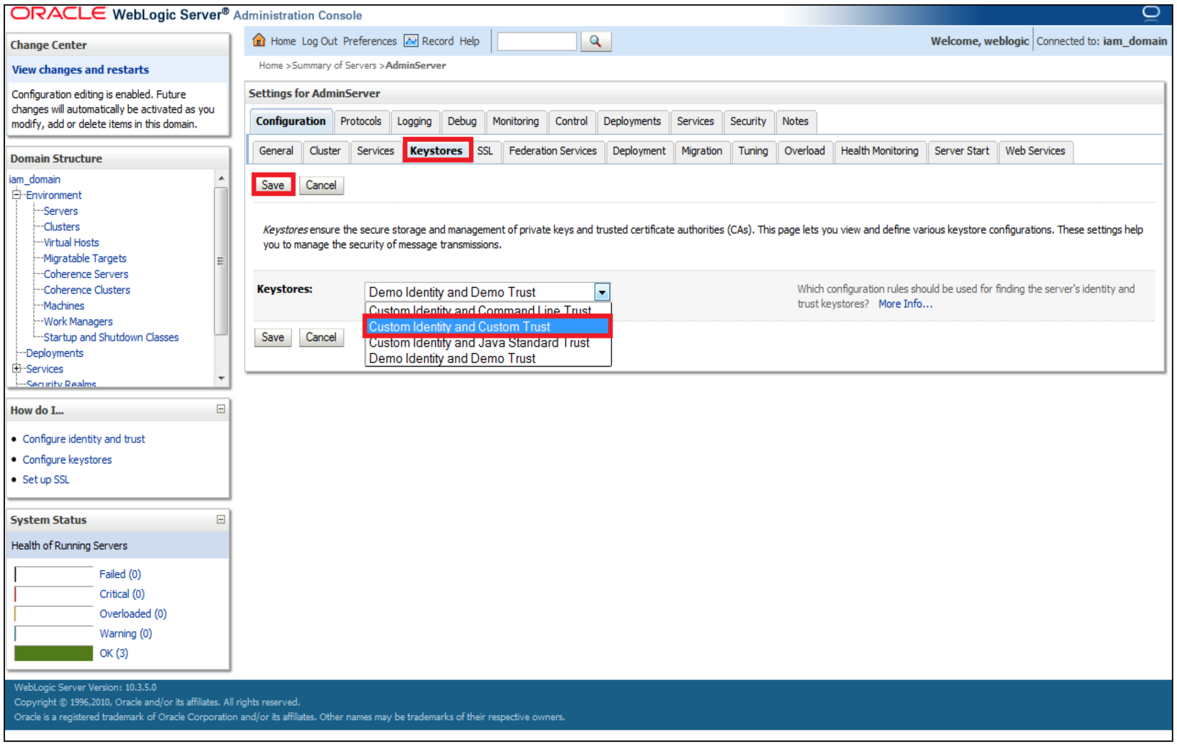
Use this page to configure general features of this server such as default network communications.

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

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.



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

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: Demo Identity and Demo Trust

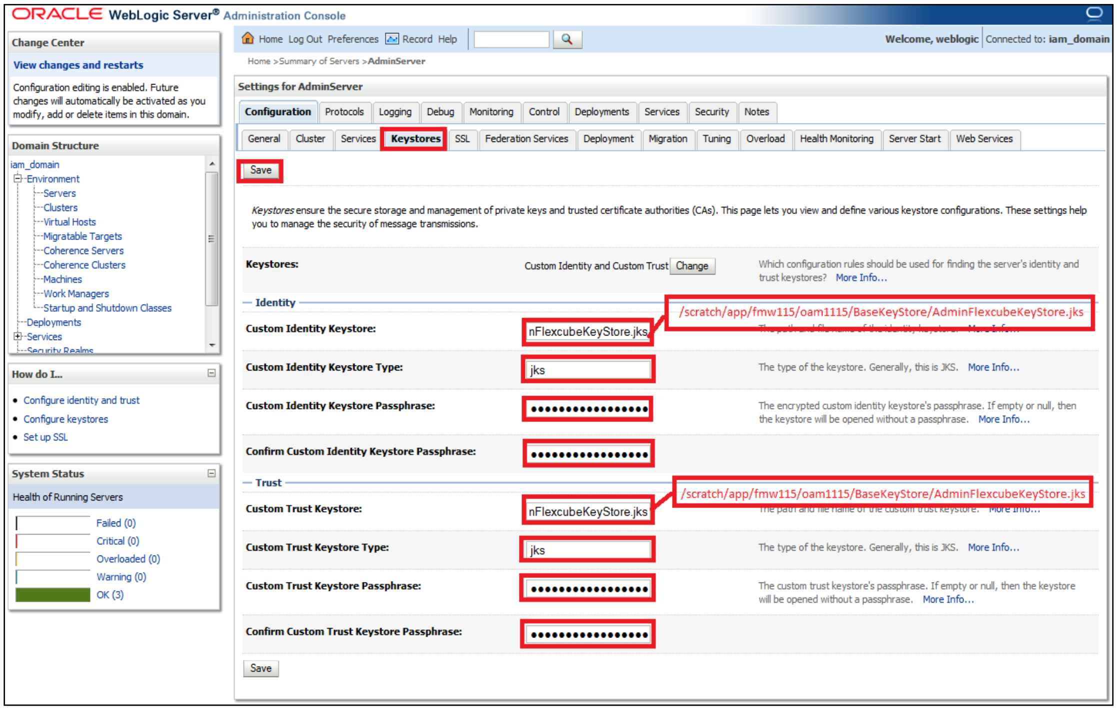
- Custom Identity and Command Line Trust
- Custom Identity and Custom Trust
- Custom Identity and Java Standard Trust
- Demo Identity and Demo Trust

Which configuration rules should be used for finding the server's identity and trust keystores? More Info...

WebLogic Server Version: 10.3.5.0
Copyright © 1996,2010, 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.

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.



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Settings for AdminServer

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: Custom Identity and Custom Trust — Which configuration rules should be used for finding the server's identity and trust keystores? More Info...

Identity

Custom Identity Keystore: nFlexcubeKeyStore.jks — /scratch/app/fmw115/oam1115/BaseKeyStore/AdminFlexcubeKeyStore.jks

Custom Identity Keystore Type: jks — The type of the keystore. Generally, this is JKS. More Info...

Custom Identity Keystore Passphrase: ••••••••••••••••• — The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info...

Confirm Custom Identity Keystore Passphrase: •••••••••••••••••

Trust

Custom Trust Keystore: nFlexcubeKeyStore.jks — /scratch/app/fmw115/oam1115/BaseKeyStore/AdminFlexcubeKeyStore.jks

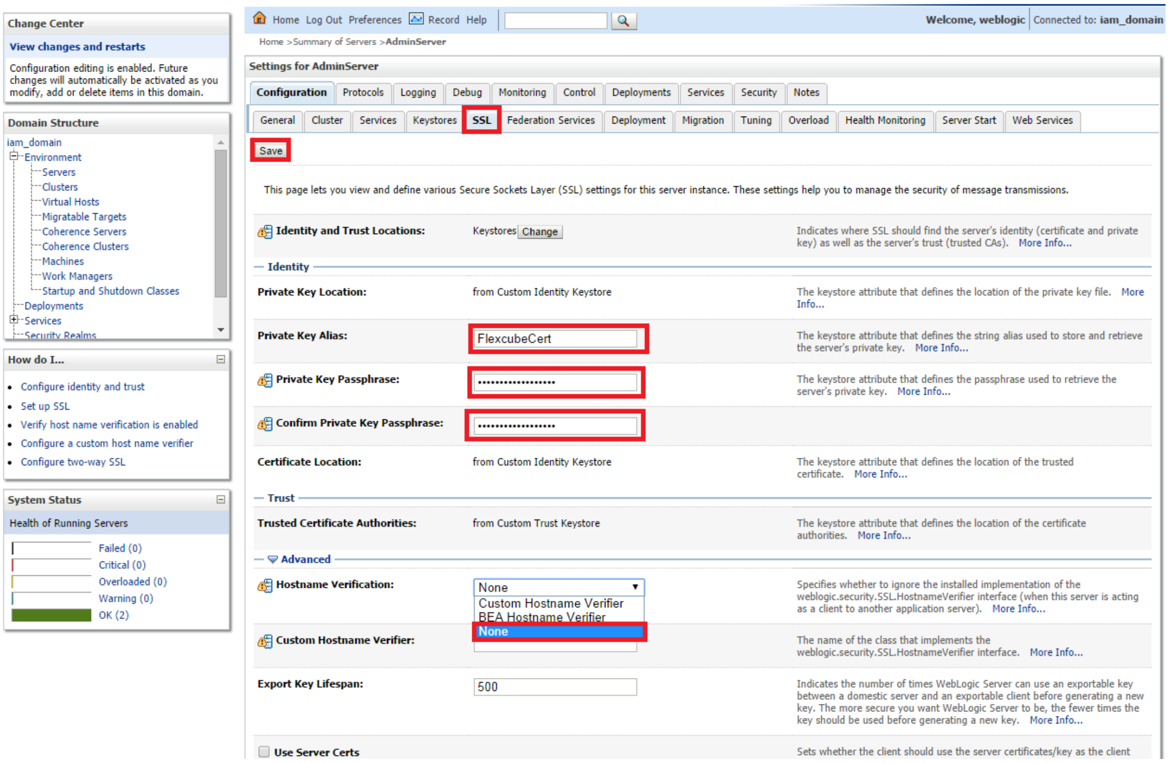
Custom Trust Keystore Type: jks — The type of the keystore. Generally, this is JKS. More Info...

Custom Trust Keystore Passphrase: ••••••••••••••••• — The custom trust keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info...

Confirm Custom Trust Keystore Passphrase: •••••••••••••••••

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 during Key Store Creation.
2. Enter Private Key Passphrase and Confirm Private Key Passphrase as same as the Private Key Password entered during Key Store Creation.
3. Change the Hostname Verification to None.
4. Select Use JSSE SSL option
5. Click on Save.



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: ••••••••••••••••••

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...

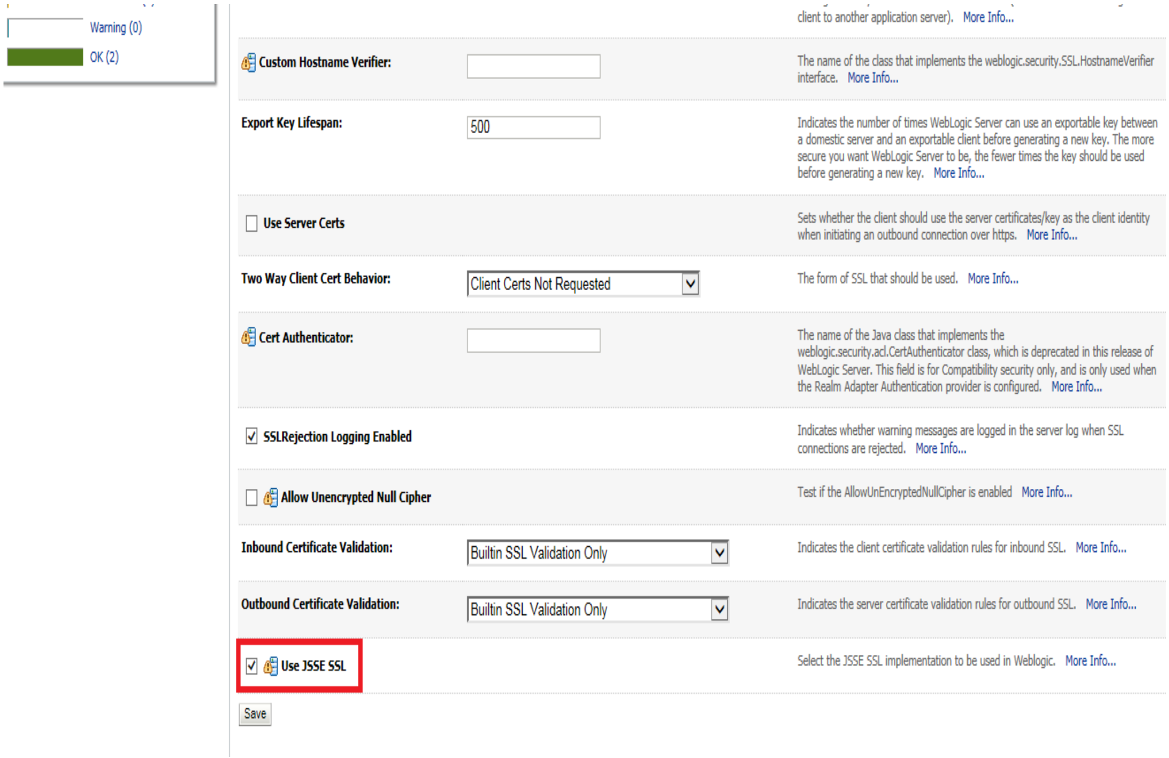
— Advanced

Hostname Verification: None (Custom Hostname Verifier / BEA Hostname Verifier / 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: — 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...

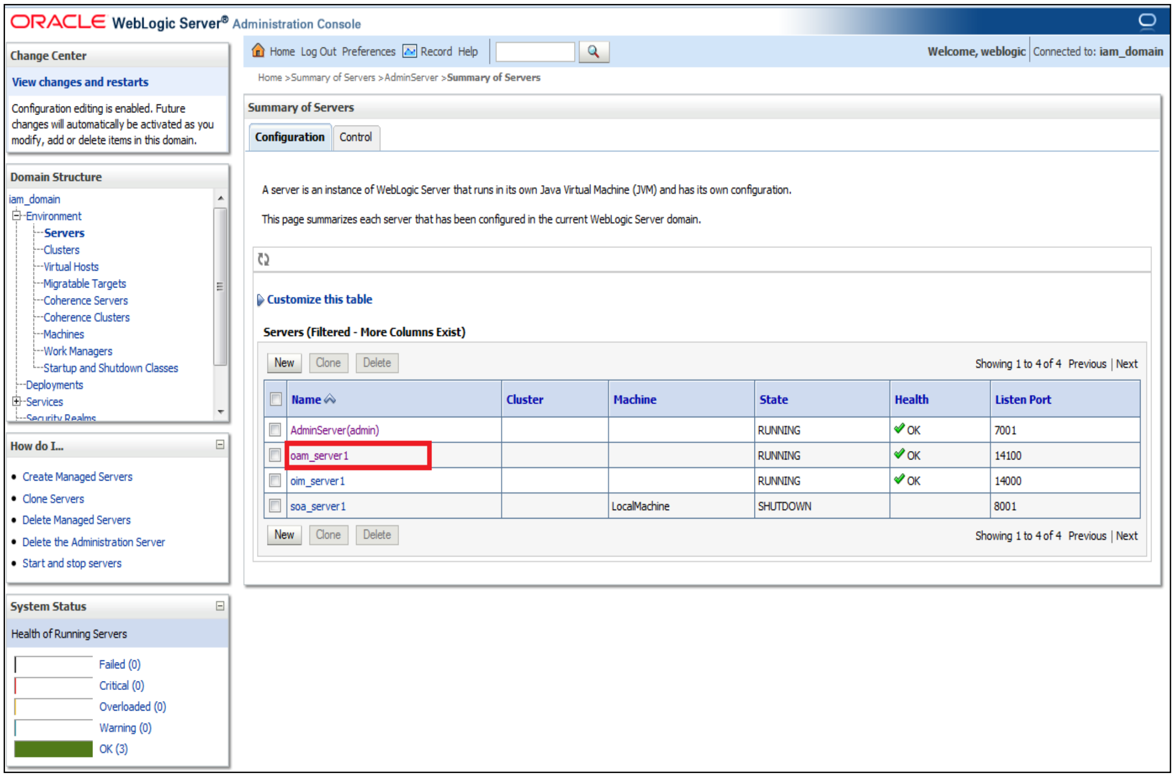
□ Allow Unencrypted Null Cipher — Test if the AllowUnEncryptedNullCipher is enabled More Info...

Inbound Certificate Validation: Builtin SSL Validation Only — Indicates the client certificate validation rules for inbound SSL. More Info...

Outbound Certificate Validation: Builtin 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...

6. Select OAM Server to enable SSL options and Repeat the steps performed for admin server



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.

This page summarizes each server that has been configured in the current WebLogic Server domain.

Servers (Filtered - More Columns Exist)

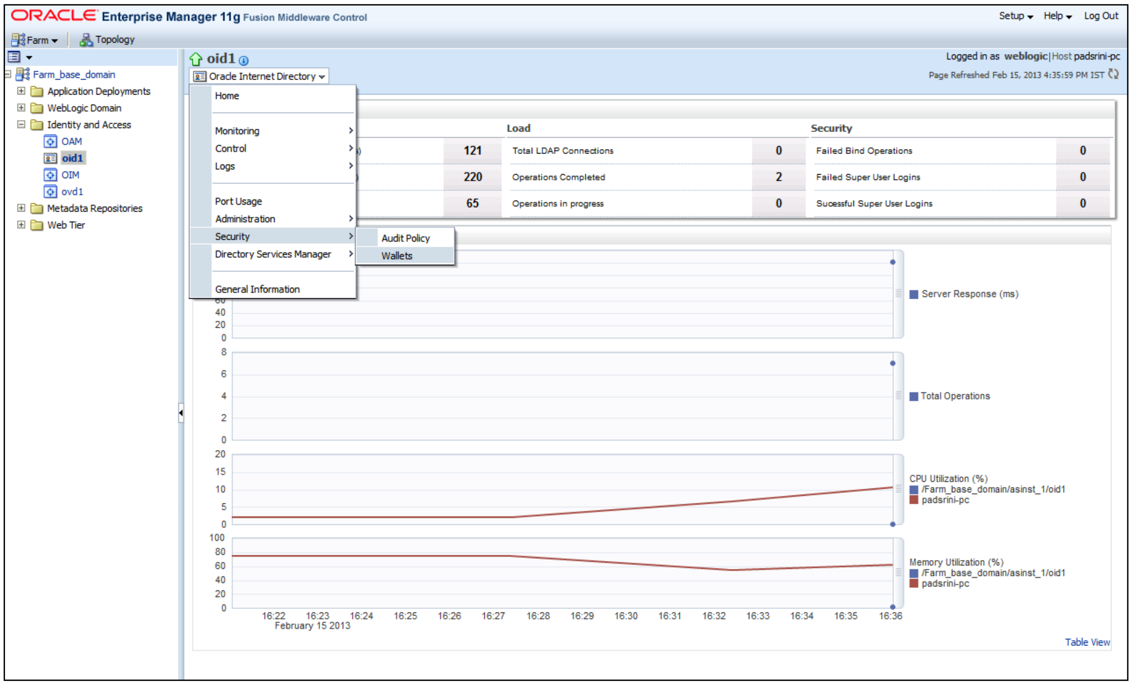
□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	7001
□	oam_server1			RUNNING	✓ OK	14100
□	oim_server1			RUNNING	✓ OK	14000
□	soa_server1		LocalMachine	SHUTDOWN		8001

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

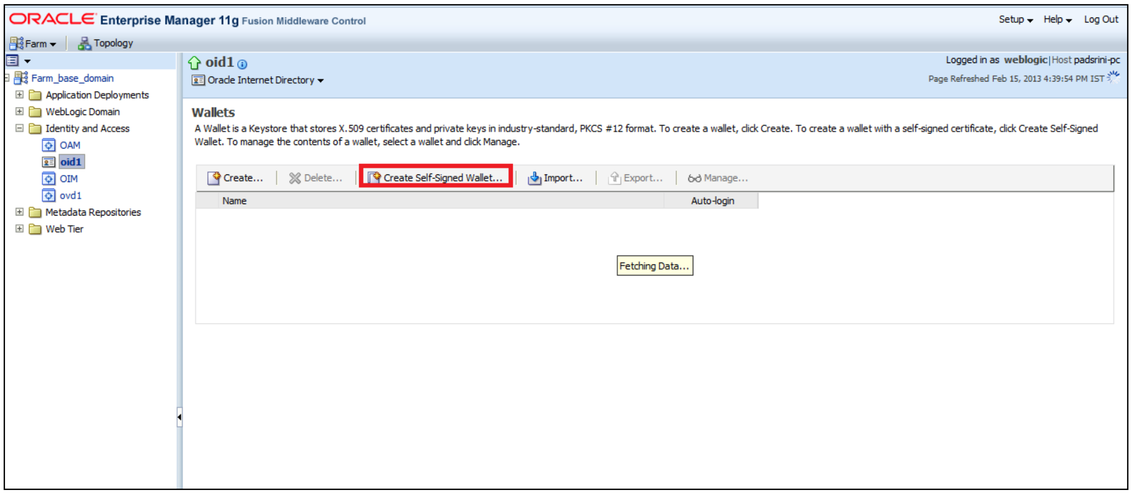
2.5.3 Configuring SSL Mode in Oracle Internet Directory

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.



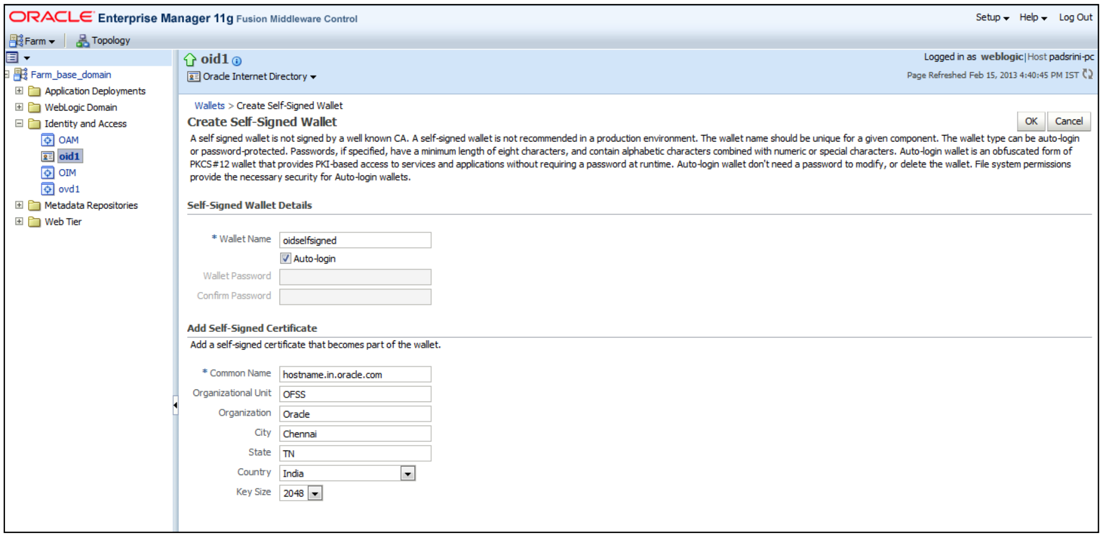
2. Click 'Create Self-Signed Wallet'.



Wallets

A Wallet is a Keystore that stores X.509 certificates and private keys in industry-standard, PKCS #12 format. To create a wallet, click Create. To create a wallet with a self-signed certificate, click Create Self-Signed Wallet. To manage the contents of a wallet, select a wallet and click Manage.

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


ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup
Help
Log Out
Farm
Topology
Farm_base_domain
Application Deployments
WebLogic Domain
Identity and Access
OAM
oid1
OIM
ovd1
Metadata Repositories
Web Tier
oid1
Oracle Internet Directory
Logged in as weblogic|Host padsrini-pc
Page Refreshed Feb 15, 2013 4:40:45 PM IST
OK
Cancel

Wallets > Create Self-Signed Wallet

Create Self-Signed Wallet

A self signed wallet is not signed by a well known CA. A self-signed wallet is not recommended in a production environment. The wallet name should be unique for a given component. The wallet type can be auto-login or password-protected. Passwords, if specified, have a minimum length of eight characters, and contain alphabetic characters combined with numeric or special characters. Auto-login wallet is an obfuscated form of PKCS#12 wallet that provides PKI-based access to services and applications without requiring a password at runtime. Auto-login wallet don't need a password to modify, or delete the wallet. File system permissions provide the necessary security for Auto-login wallets.

Self-Signed Wallet Details

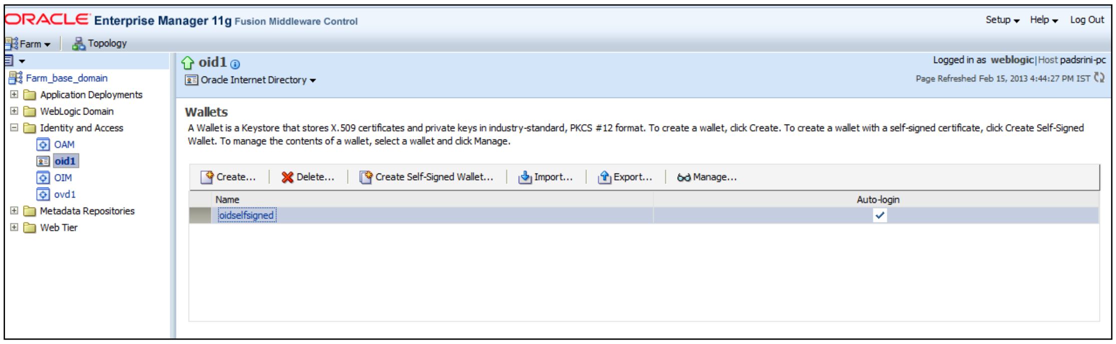
* Wallet Name	oidselfsigned
	☑ Auto-login
Wallet Password	
Confirm Password	

Add Self-Signed Certificate

Add a self-signed certificate that becomes part of the wallet.

* Common Name	hostname.in.oracle.com
Organizational Unit	OFSS
Organization	Oracle
City	Chennai
State	TN
Country	India
Key Size	2048

4. Click Manage… .

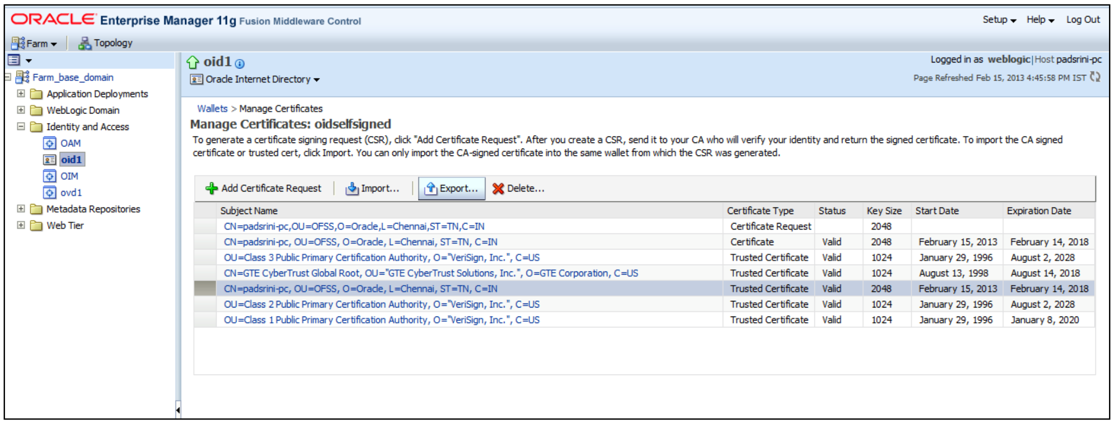

ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup
Help
Log Out
Farm
Topology
Farm_base_domain
Application Deployments
WebLogic Domain
Identity and Access
OAM
oid1
OIM
ovd1
Metadata Repositories
Web Tier
oid1
Oracle Internet Directory
Logged in as weblogic|Host padsrini-pc
Page Refreshed Feb 15, 2013 4:44:27 PM IST
Create…
Delete…
Create Self-Signed Wallet…
Import…
Export…
Manage…

Wallets

A Wallet is a Keystore that stores X.509 certificates and private keys in industry-standard, PKCS #12 format. To create a wallet, click Create. To create a wallet with a self-signed certificate, click Create Self-Signed Wallet. To manage the contents of a wallet, select a wallet and click Manage.

Name	Auto-login
oidselfsigned	✓

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



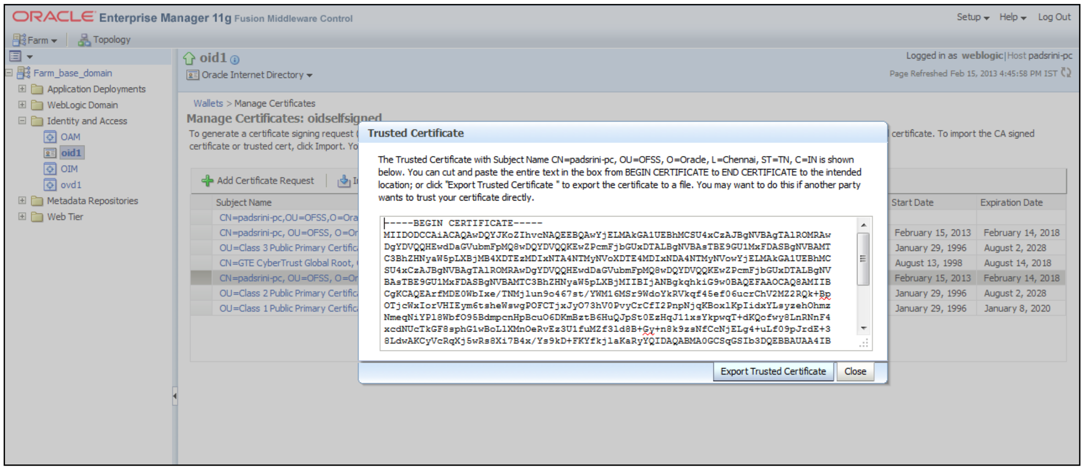
Wallets > Manage Certificates

Manage Certificates: oidselfsigned

To generate a certificate signing request (CSR), click "Add Certificate Request". After you create a CSR, send it to your CA who will verify your identity and return the signed certificate. To import the CA signed certificate or trusted cert, click Import. You can only import the CA-signed certificate into the same wallet from which the CSR was generated.

Subject Name	Certificate Type	Status	Key Size	Start Date	Expiration Date
CN=padsrini-pc,OU=OFSS,O=Oracle,L=Chennai,ST=TN,C=IN	Certificate Request		2048		
CN=padsrini-pc, OU=OFSS, O=Oracle, L=Chennai, ST=TN, C=IN	Certificate	Valid	2048	February 15, 2013	February 14, 2018
OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
CN=GTE CyberTrust Global Root, OU="GTE CyberTrust Solutions, Inc.", O=GTE Corporation, C=US	Trusted Certificate	Valid	1024	August 13, 1998	August 14, 2018
CN=padsrini-pc, OU=OFSS, O=Oracle, L=Chennai, ST=TN, C=IN	Trusted Certificate	Valid	2048	February 15, 2013	February 14, 2018
OU=Class 2 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
OU=Class 1 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	January 8, 2020

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



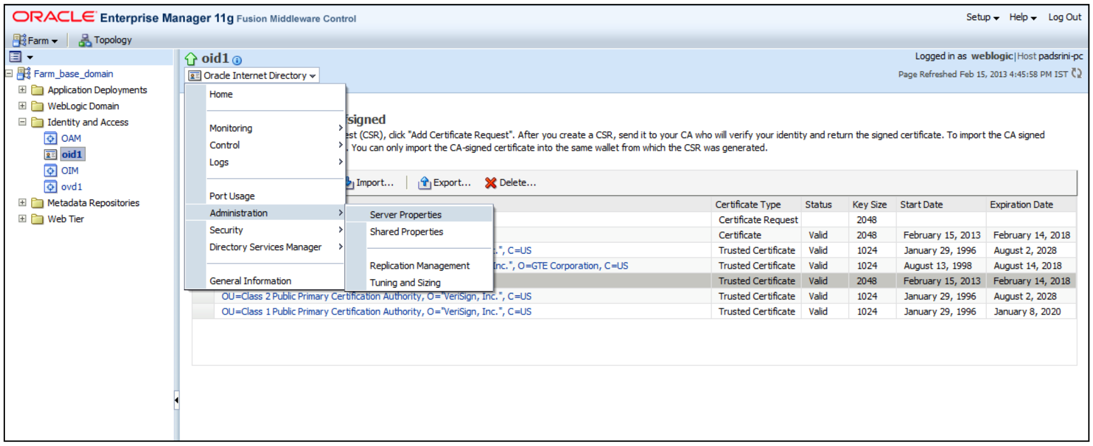
ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup
Help
Log Out
Farm
Topology
Farm_base_domain
Application Deployments
WebLogic Domain
Identity and Access
OAM
oid1
OIM
ovd1
Metadata Repositories
Web Tier
oid1
Oracle Internet Directory
Logged in as weblogic|Host padsrini-pc
Page Refreshed Feb 15, 2013 4:45:58 PM IST
Wallets > Manage Certificates
Manage Certificates: oidselfsigned
Add Certificate Request
Subject Name
Start Date
Expiration Date
Export Trusted Certificate
Close

Trusted Certificate

The Trusted Certificate with Subject Name CN=padsrini-pc, OU=OFSS, O=Oracle, L=Chennai, ST=TN, C=IN is shown below. You can cut and paste the entire text in the box from BEGIN CERTIFICATE to END CERTIFICATE to the intended location; or click "Export Trusted Certificate " to export the certificate to a file. You may want to do this if another party wants to trust your certificate directly.

```
-----BEGIN CERTIFICATE-----
MIIDODCCAiACAQAwDQYJKoZIhvcNAQEEBQAwYjELMAkGA1UEBhMCSU4xCzAJBgNVBAgTA1ROMRAw
DgYDVQQHEwdDaGVubmFpMQ8wDQYDVQQKEwZPcmFjbGUxDTALBgNVBAsTBE9GU1MxFDASBgNVBAMT
C3BhZHNyaW5pLXBjMB4XDTEzMDIxNTA4NTMyNVoXDTE4MDIxNDA4NTMyNVowYjELMAkGA1UEBhMC
SU4xCzAJBgNVBAgTA1ROMRAwDgYDVQQHEwdDaGVubmFpMQ8wDQYDVQQKEwZPcmFjbGUxDTALBgNV
BAsTBE9GU1MxFDASBgNVBAMTC3BhZHNyaW5pLXBjMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArfMDE0WbIxe/TNMjlun9o467st/YWM16MSr9WdoYkRVkqf45ef06ucrChV2MZ2RQk+Bp
OTjcWxIorVHIEym6tsheWswgPOFCTjxJyO73hV0PvyCrCfI2PnpNjqKBoxlKpIidxYLsyzehOhmz
NmeqNiYPl8WbfO95BdmpcnHpBcuO6DKmBztB6HuQJpSt0EzHqJ11xsYkpwqT+dKQofwy8LnRNnF4
xcdNUcTkGF8sphG1wBoLlXMnOeRvEz3U1fuMZf31d8B+Gy+n8k9zsNfCcNjELg4+uLf09pJrdE+3
8LdwAKCyVcRqXj5wRs8Xi7B4x/Ys9kD+FKYfkjlaKaRyYQIDAQABMA0GCSqGSIb3DQEBBAUAA4IB
```

7. Click ‘Server Properties’.

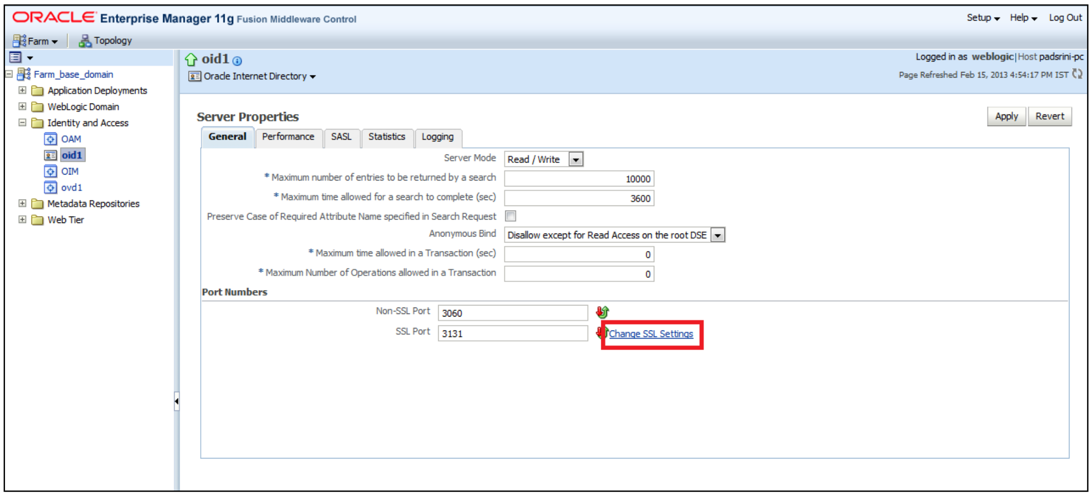


signed

st (CSR), click "Add Certificate Request". After you create a CSR, send it to your CA who will verify your identity and return the signed certificate. To import the CA signed . You can only import the CA-signed certificate into the same wallet from which the CSR was generated.

	Certificate Type	Status	Key Size	Start Date	Expiration Date
	Certificate Request		2048		
	Certificate	Valid	2048	February 15, 2013	February 14, 2018
.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
Inc.", O=GTE Corporation, C=US	Trusted Certificate	Valid	1024	August 13, 1998	August 14, 2018
	Trusted Certificate	Valid	2048	February 15, 2013	February 14, 2018
OU=Class 2 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
OU=Class 1 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	January 8, 2020

8. Click ‘Change SSL Settings’.



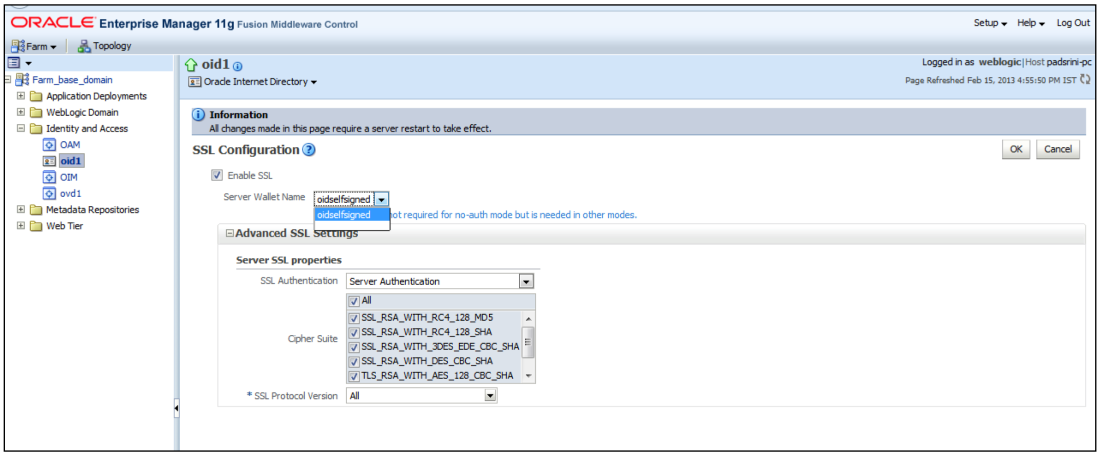
Server Properties

Server Mode	Read / Write
* Maximum number of entries to be returned by a search	10000
* Maximum time allowed for a search to complete (sec)	3600
Preserve Case of Required Attribute Name specified in Search Request	□
Anonymous Bind	Disallow except for Read Access on the root DSE
* Maximum time allowed in a Transaction (sec)	0
* Maximum Number of Operations allowed in a Transaction	0

Port Numbers

Non-SSL Port	3060
SSL Port	3131

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



Logged in as weblogic|Host padsrini-pc
Page Refreshed Feb 15, 2013 4:55:50 PM IST

Information
All changes made in this page require a server restart to take effect.

SSL Configuration

☑ Enable SSL

Server Wallet Name: oidselfsigned (oidselfsigned) …not required for no-auth mode but is needed in other modes.

Advanced SSL Settings

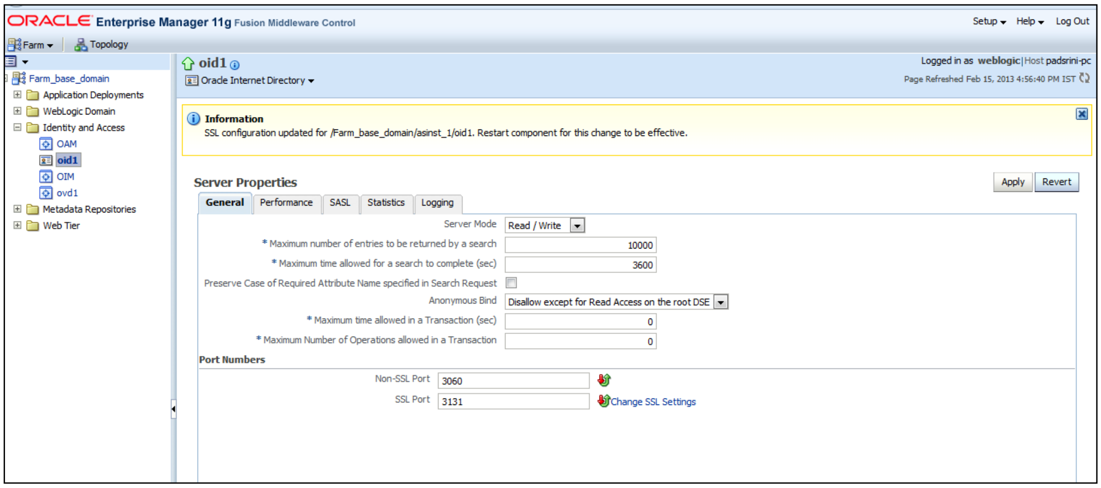
Server SSL properties

SSL Authentication: Server Authentication

Cipher Suite:
☑ All
☑ SSL_RSA_WITH_RC4_128_MD5
☑ SSL_RSA_WITH_RC4_128_SHA
☑ SSL_RSA_WITH_3DES_EDE_CBC_SHA
☑ SSL_RSA_WITH_DES_CBC_SHA
☑ TLS_RSA_WITH_AES_128_CBC_SHA

* SSL Protocol Version: All

10. Click ‘Apply’.



Logged in as weblogic|Host padsrini-pc
Page Refreshed Feb 15, 2013 4:56:40 PM IST

Information
SSL configuration updated for /Farm_base_domain/asinst_1/oid1. Restart component for this change to be effective.

Server Properties

Server Mode: Read / Write
* Maximum number of entries to be returned by a search: 10000
* Maximum time allowed for a search to complete (sec): 3600
Preserve Case of Required Attribute Name specified in Search Request: ☐
Anonymous Bind: Disallow except for Read Access on the root DSE
* Maximum time allowed in a Transaction (sec): 0
* Maximum Number of Operations allowed in a Transaction: 0

Port Numbers

Non-SSL Port: 3060
SSL Port: 3131

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.

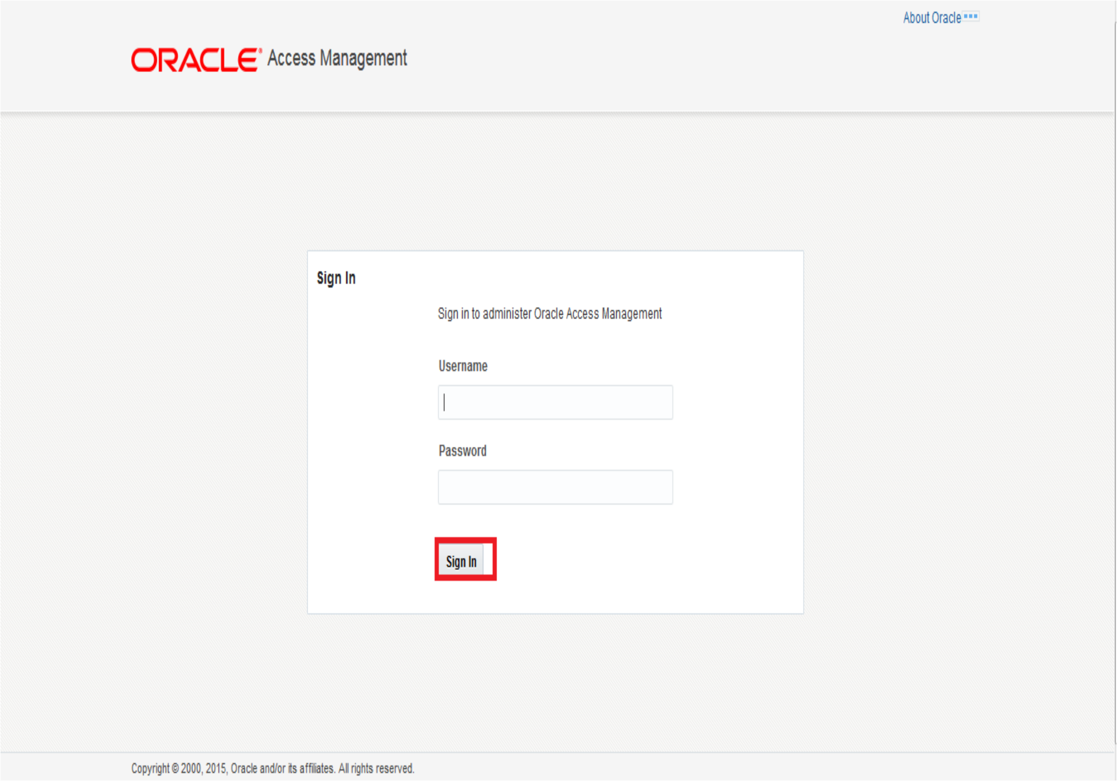
2.6 Configuring SSO in OAM Console

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)

2.6.1 Identity Store Creation

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



About Oracle

ORACLE Access Management

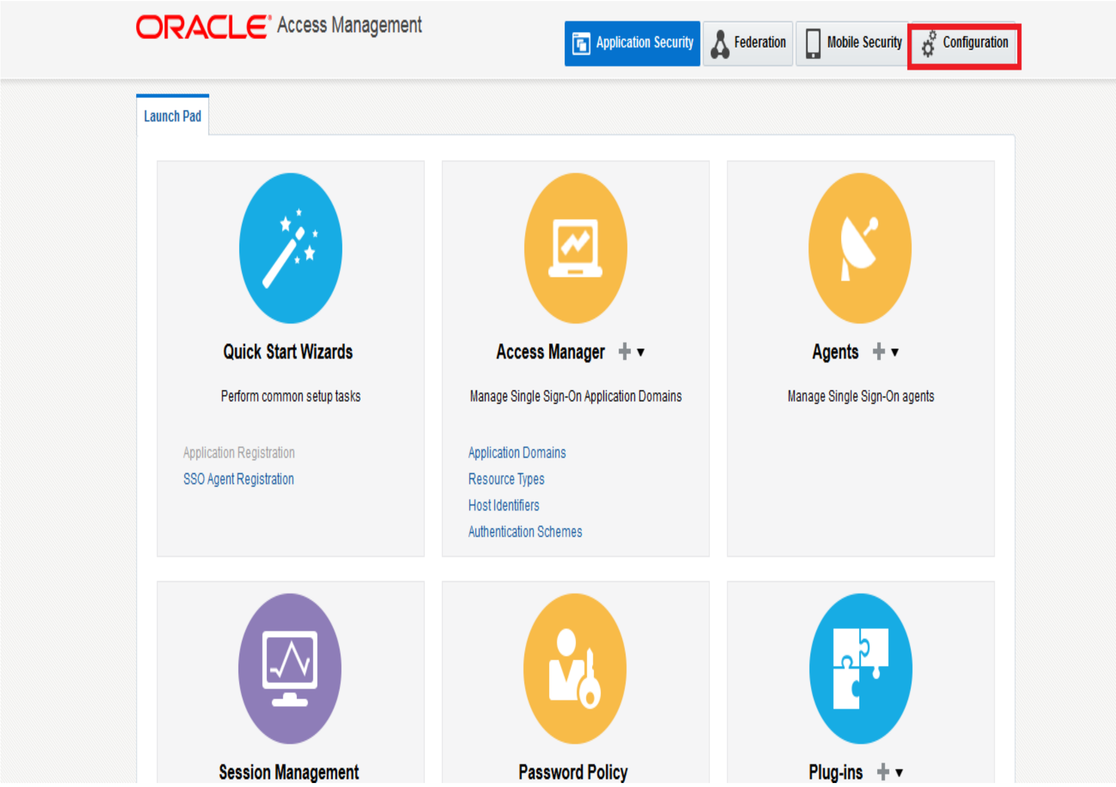
Sign In

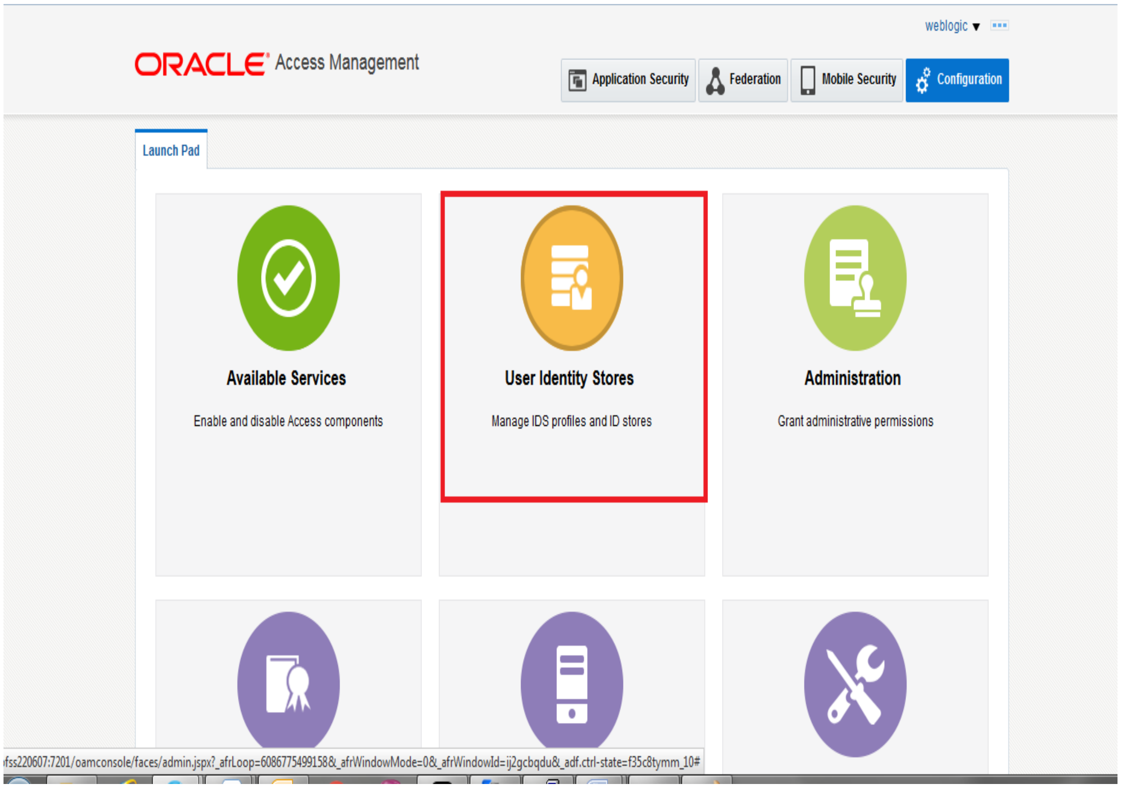
Sign in to administer Oracle Access Management

Username

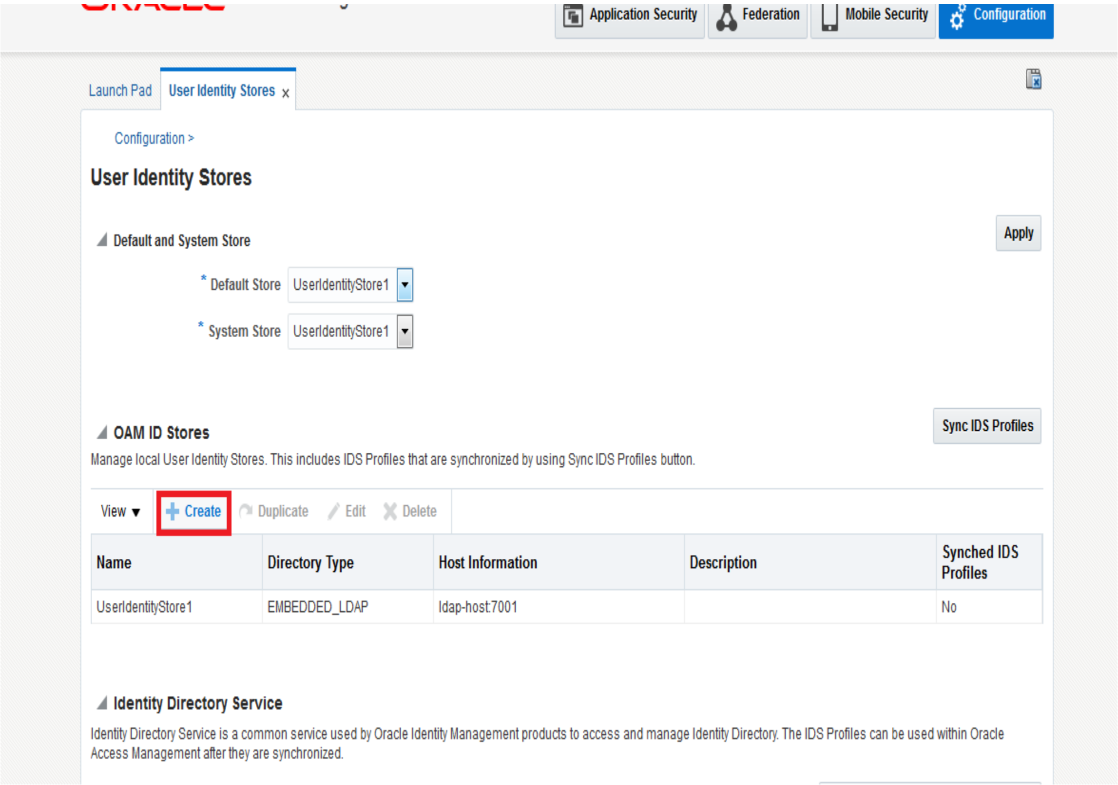
Password

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




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
ifss220607:7201/oamconsole/faces/admin.jspx?_afrLoop=60867754991588&_afrWindowMode=0&_afrWindowId=ij2gcbqdu&_adf.ctrl-state=f35c8tymm_10#

2. Click ‘Create’ under OAM ID Stores.



User Identity Stores

Default and System Store

* Default Store UserIdentityStore1

* System Store UserIdentityStore1

OAM ID Stores

Manage local User Identity Stores. This includes IDS Profiles that are synchronized by using Sync IDS Profiles button.

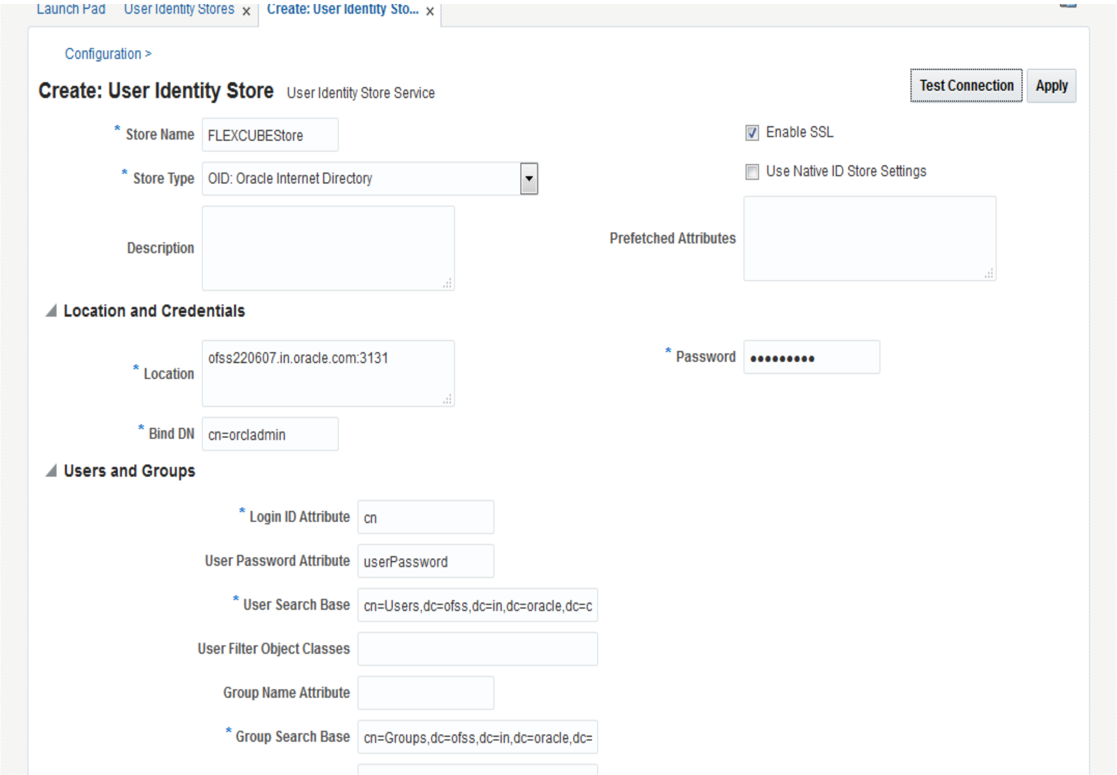
Name	Directory Type	Host Information	Description	Synched IDS Profiles
UserIdentityStore1	EMBEDDED_LDAP	ldap-host:7001		No

Identity Directory Service

Identity Directory Service is a common service used by Oracle Identity Management products to access and manage Identity Directory. The IDS Profiles can be used within Oracle Access Management after they are synchronized.

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.



Create: User Identity Store User Identity Store Service

* Store Name: FLEXCUBEStore
* Store Type: OID: Oracle Internet Directory
Description:

☑ Enable SSL
□ Use Native ID Store Settings
Prefetched Attributes:

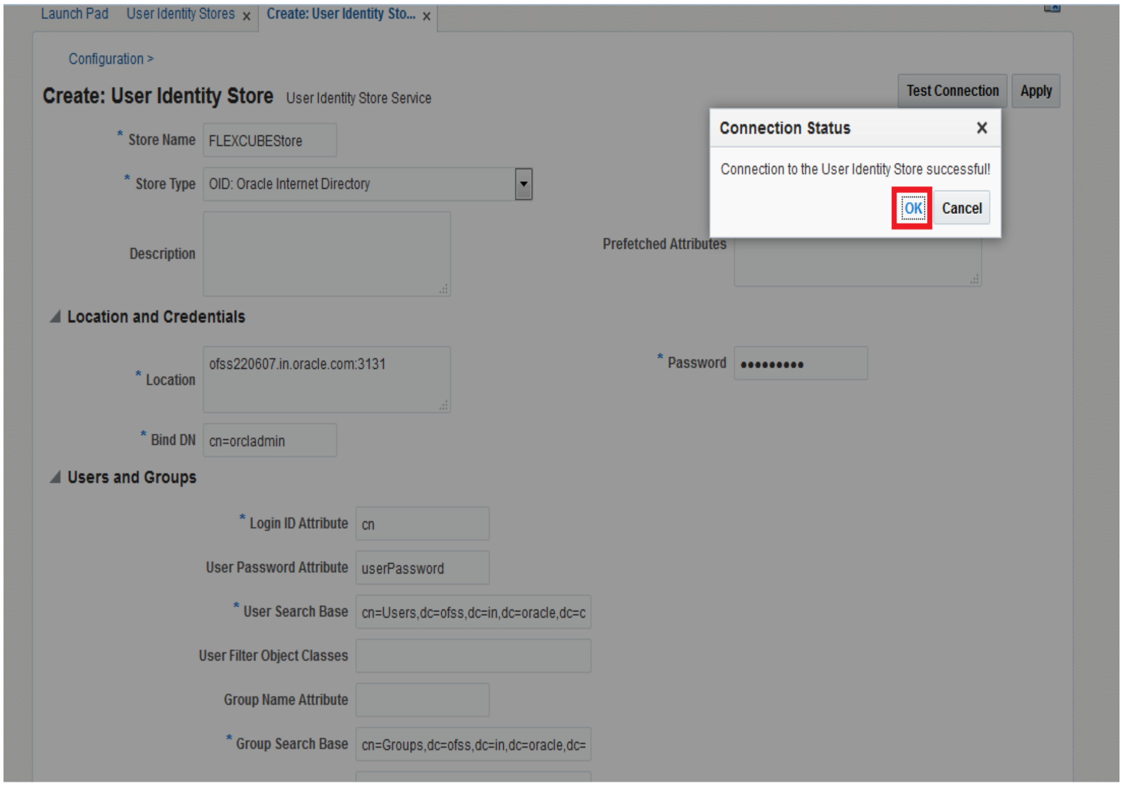
Location and Credentials

* Location: ofss220607.in.oracle.com:3131
* Bind DN: cn=orcladmin
* 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=

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



Connection Status

Connection to the User Identity Store successful!

Create: User Identity Store User Identity Store Service

* Store Name: FLEXCUBEStore
* Store Type: OID: Oracle Internet Directory
Description:
Prefetched Attributes:

Location and Credentials

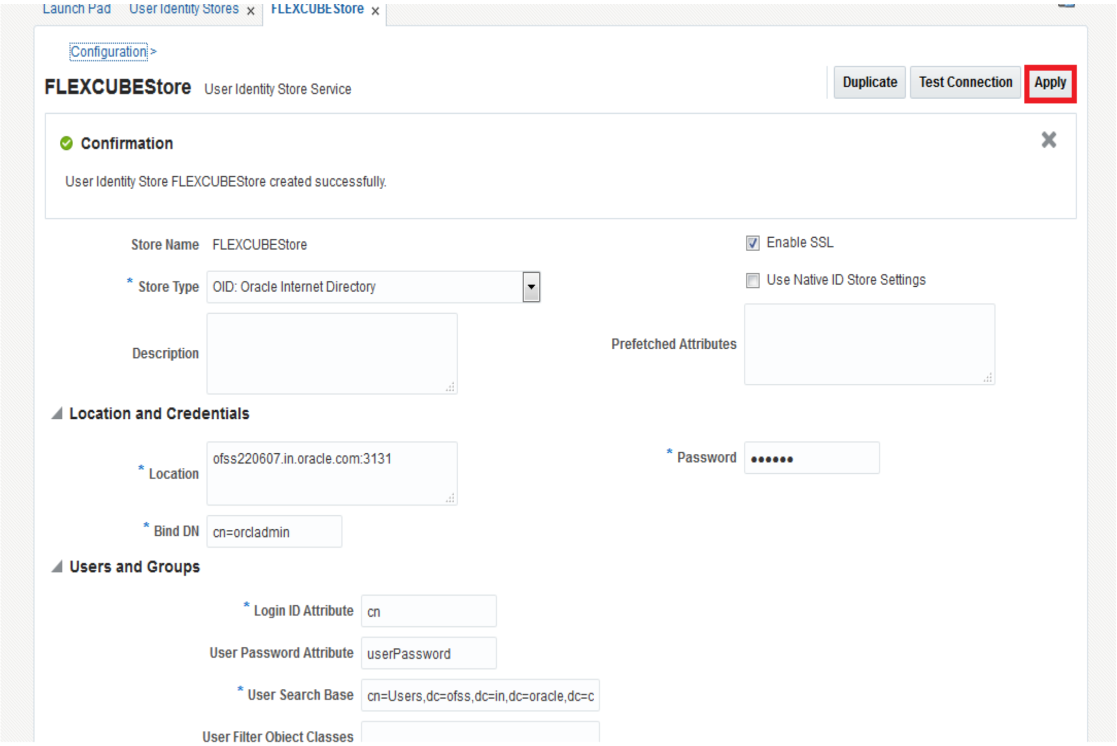
* Location: ofss220607.in.oracle.com:3131
* Bind DN: cn=orcladmin
* Password: •••••••••

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=

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

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



FLEXCUBEStore User Identity Store Service

Confirmation

User Identity Store FLEXCUBEStore created successfully.

Store Name	FLEXCUBEStore	☑ Enable SSL	
* Store Type	OID: Oracle Internet Directory	☐ Use Native ID Store Settings	
Description		Prefetched Attributes	

Location and Credentials

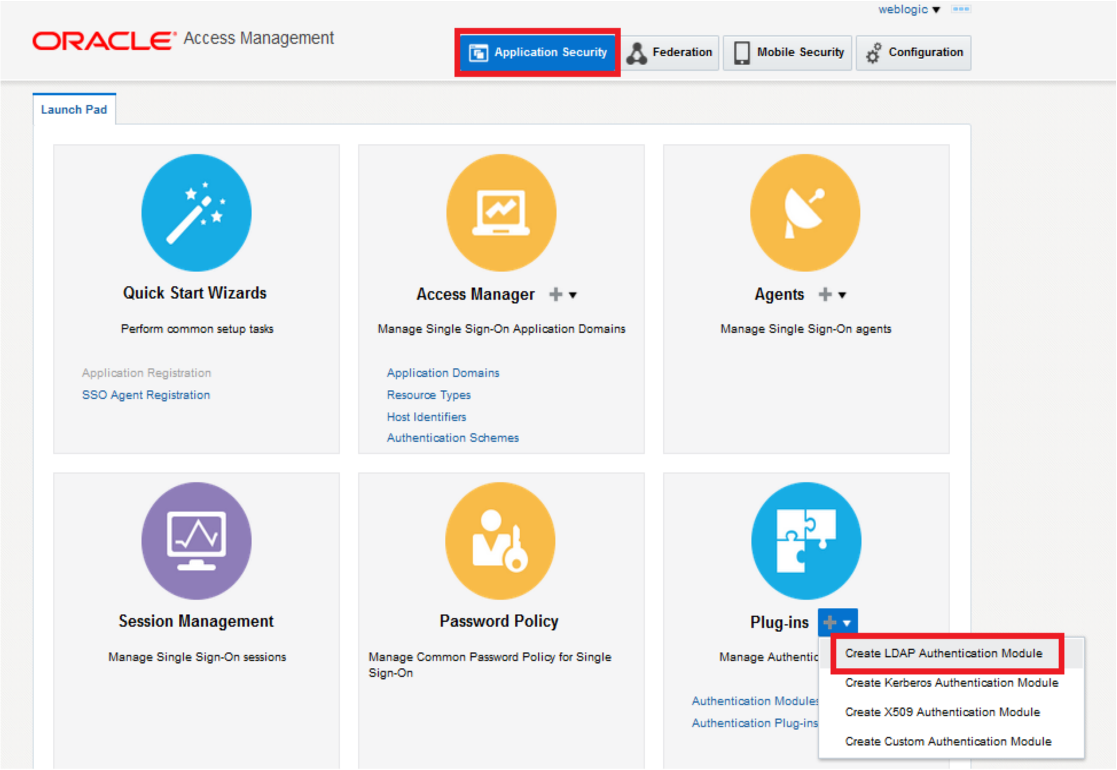
* Location	ofss220607.in.oracle.com:3131	* Password	••••••
* Bind DN	cn=orcladmin		

Users and Groups

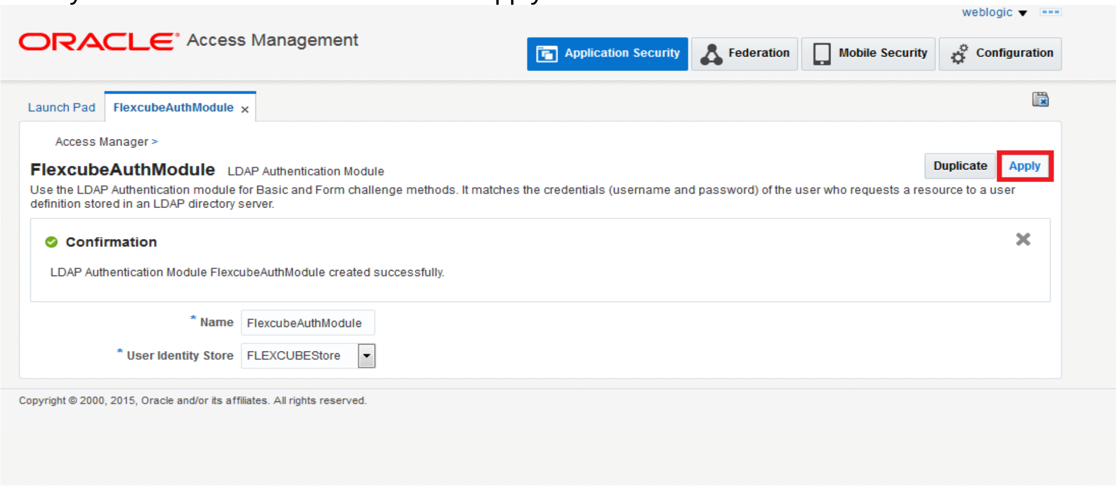
* Login ID Attribute	cn
User Password Attribute	userPassword
* User Search Base	cn=Users,dc=ofss,dc=in,dc=oracle,dc=c
User Filter Object Classes	

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 User Identification Store, created in Identity Store Creation section. Click on ‘Apply’ to create Authentication Module.



FlexcubeAuthModule LDAP Authentication Module

Use the LDAP Authentication module for Basic and Form challenge methods. It matches the credentials (username and password) of the user who requests a resource to a user definition stored in an LDAP directory server.

Confirmation

LDAP Authentication Module FlexcubeAuthModule created successfully.

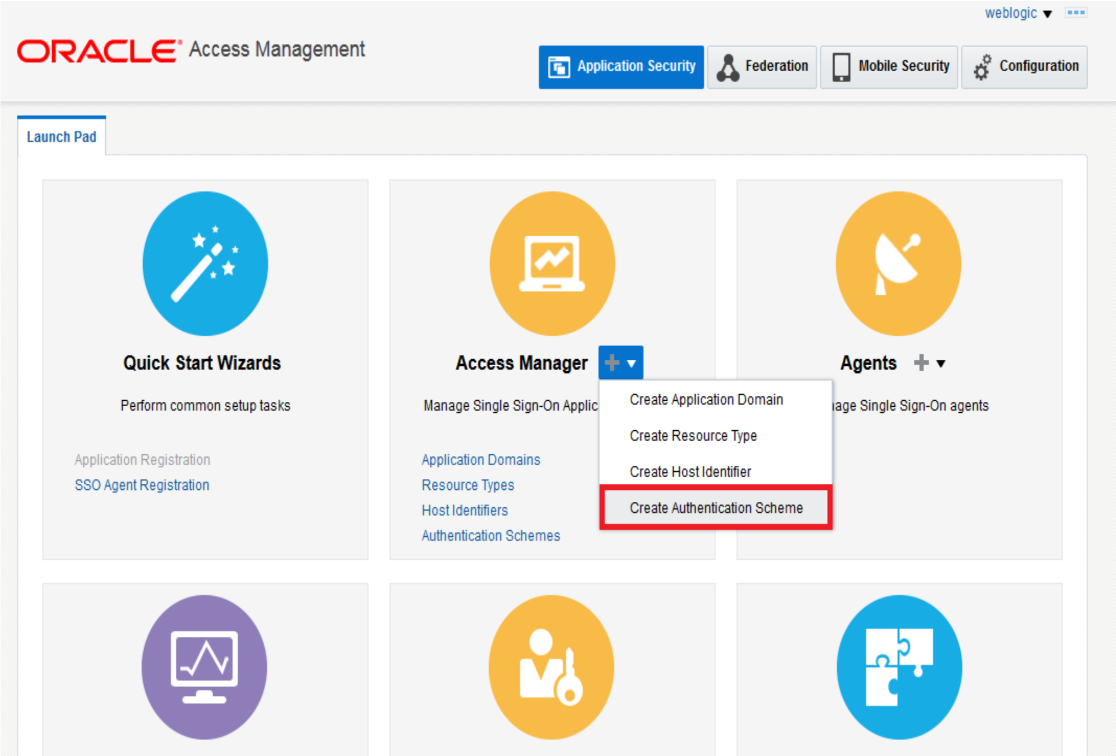
* Name: FlexcubeAuthModule

* User Identity Store: FLEXCUBEStore

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

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

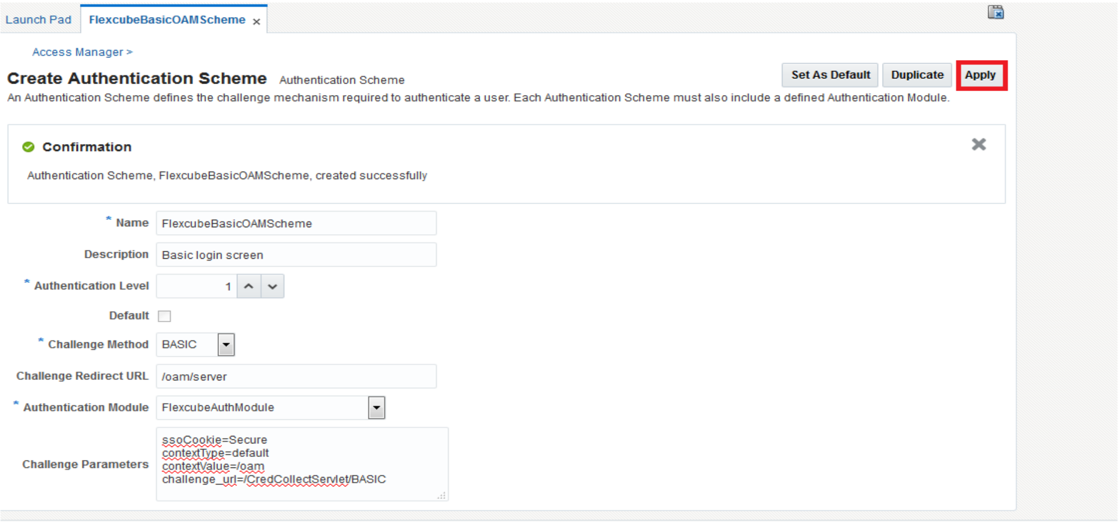
2.6.3.1 Basic Style Authentication Scheme

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



Create Authentication Scheme Authentication Scheme

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, FlexcubeBasicOAMScheme, created successfully

* Name	FlexcubeBasicOAMScheme
Description	Basic login screen
* Authentication Level	1
Default	□
* Challenge Method	BASIC
Challenge Redirect URL	/oam/server
* Authentication Module	FlexcubeAuthModule

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>

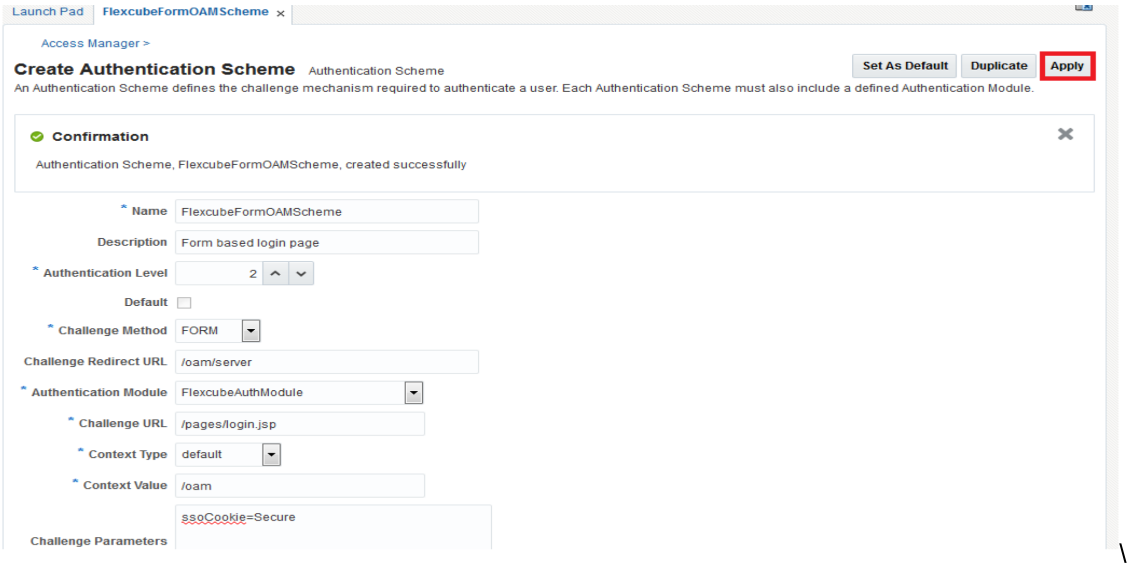
2.6.3.2 Form Style Authentication Scheme

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



Create Authentication Scheme Authentication Scheme

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, FlexcubeFormOAMScheme, created successfully

* Name	FlexcubeFormOAMScheme
Description	Form based login page
* Authentication Level	2
Default	□
* Challenge Method	FORM
Challenge Redirect URL	/oam/server
* Authentication Module	FlexcubeAuthModule
* 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

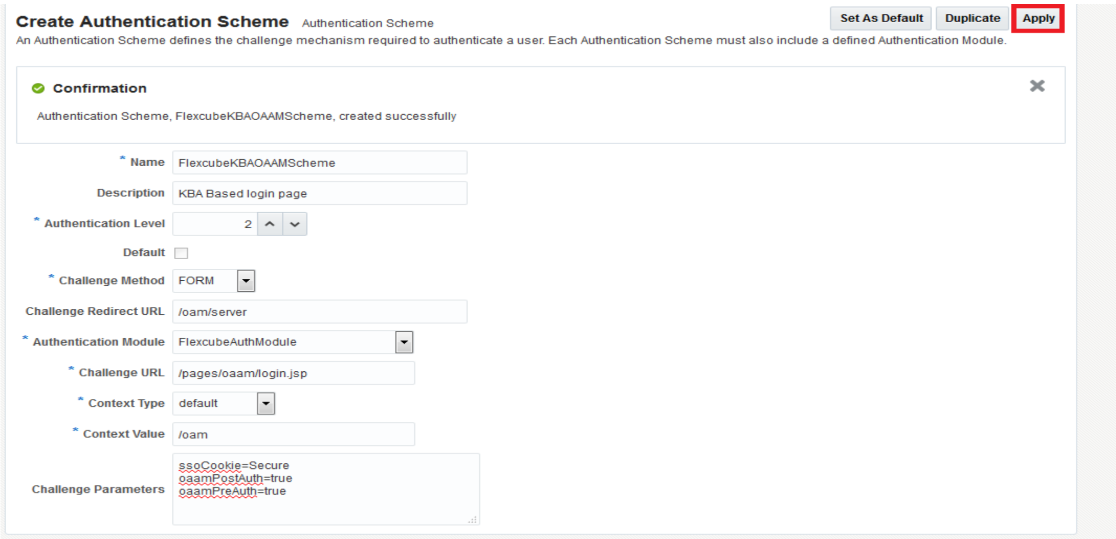
Refer the section ‘Creating Authentication Module 2.6.2’ of this document.

Challenge URL : /pages/oaam/login.jsp

Context Type : default

Context Value : /oam

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



Create Authentication Scheme Authentication Scheme

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

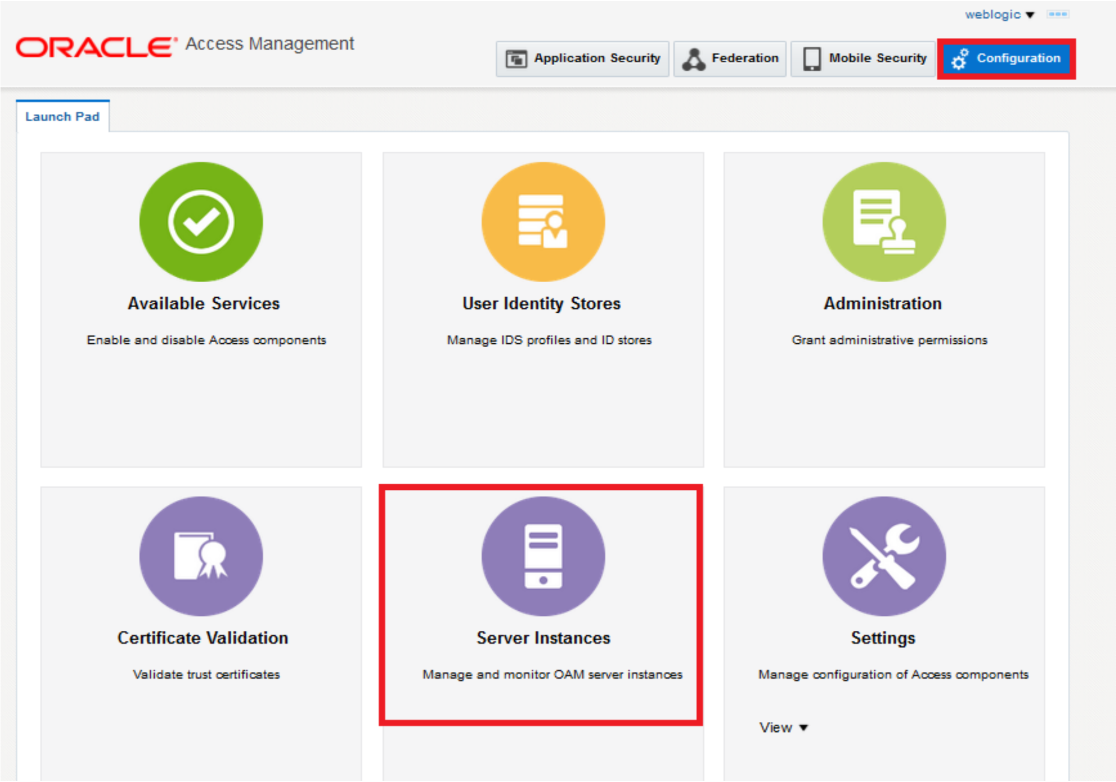
* Name	FlexcubeKBAOAMScheme
Description	KBA Based login page
* Authentication Level	2
Default	□
* Challenge Method	FORM
Challenge Redirect URL	/oam/server
* Authentication Module	FlexcubeAuthModule
* Challenge URL	/pages/oaam/login.jsp
* Context Type	default
* Context Value	/oam

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.



Available Services
Enable and disable Access components

User Identity Stores
Manage IDS profiles and ID stores

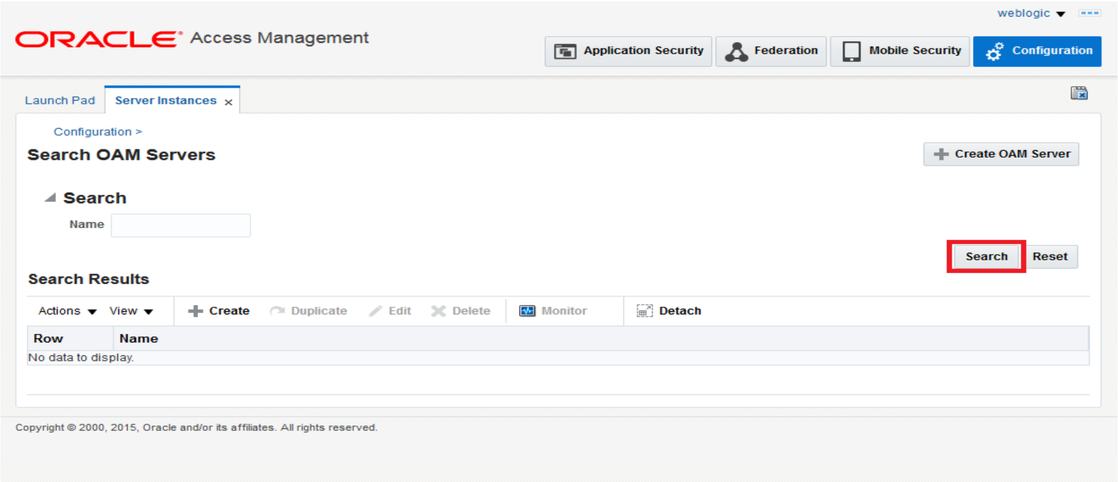
Administration
Grant administrative permissions

Certificate Validation
Validate trust certificates

Server Instances
Manage and monitor OAM server instances

Settings
Manage configuration of Access components

2. Click on ‘Search’.



Search OAM Servers

Search

Name

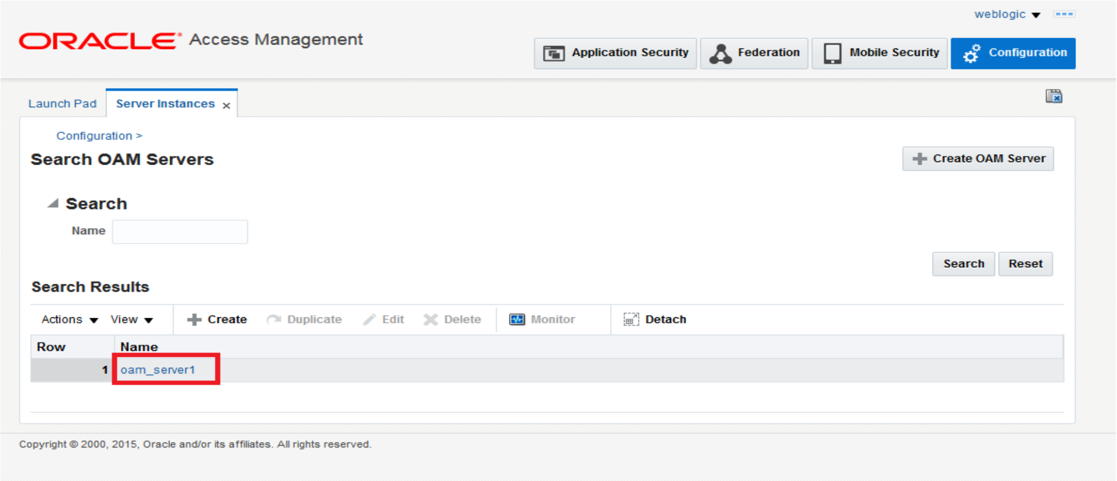
Search Results

Row	Name

No data to display.

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

3. Edit oam_server1.



Search OAM Servers

Search

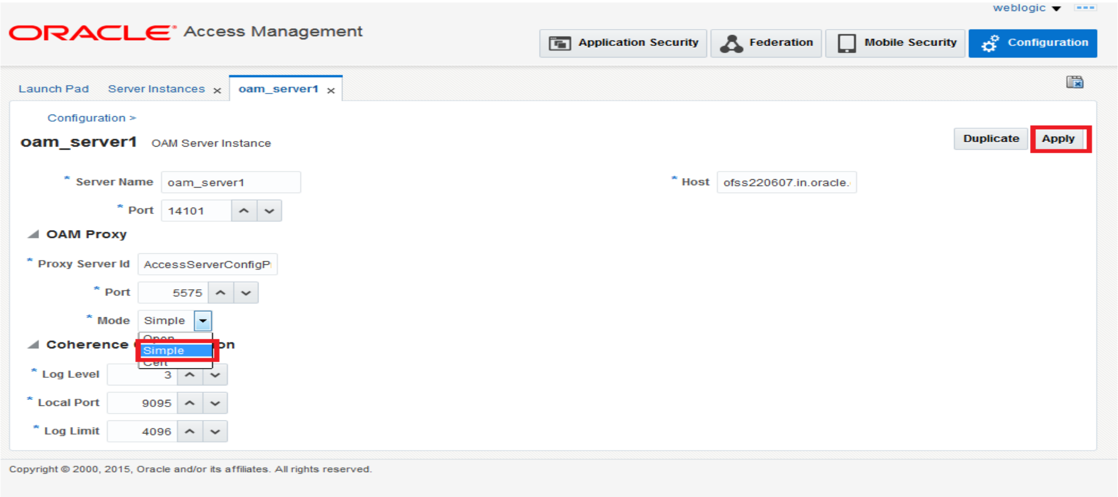
Name

Search Results

Row	Name
1	oam_server1

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

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



oam_server1 OAM Server Instance

* Server Name oam_server1

* Host ofss220607.in.oracle.

* Port 14101

OAM Proxy

* Proxy Server Id AccessServerConfigP

* Port 5575

* Mode Simple

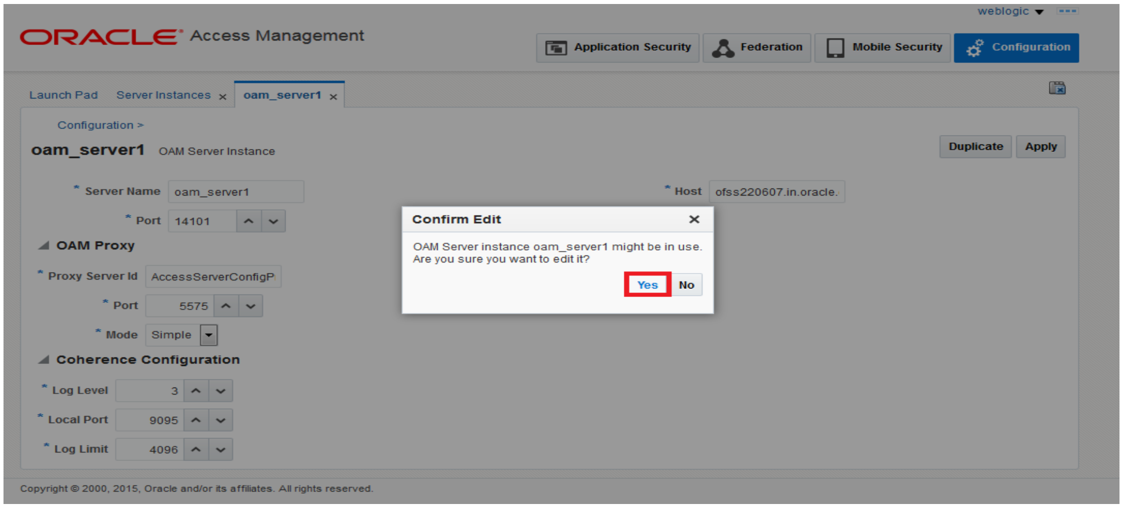
Coherence

* Log Level 3

* Local Port 9095

* Log Limit 4096

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



oam_server1 OAM Server Instance

* 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

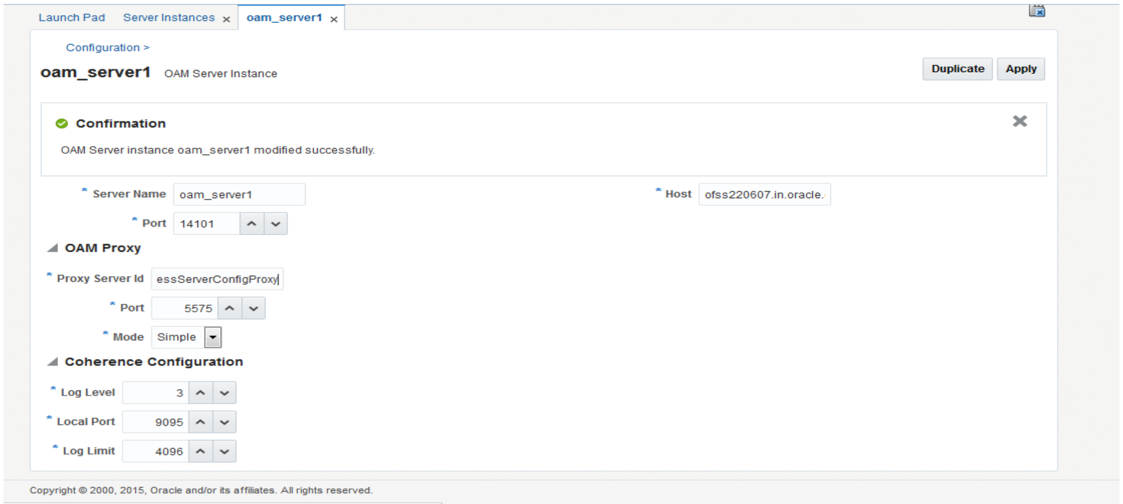
* Local Port: 9095

* Log Limit: 4096

Confirm Edit

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.



oam_server1 OAM Server Instance

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

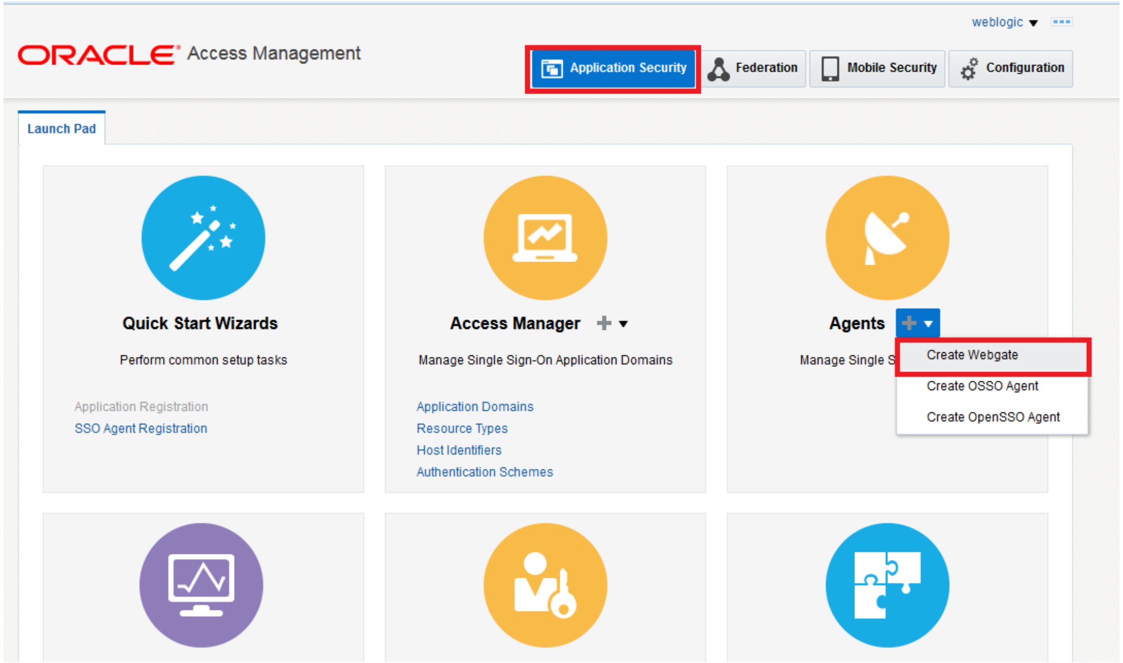
* Log Level: 3

* Local Port: 9095

* Log Limit: 4096

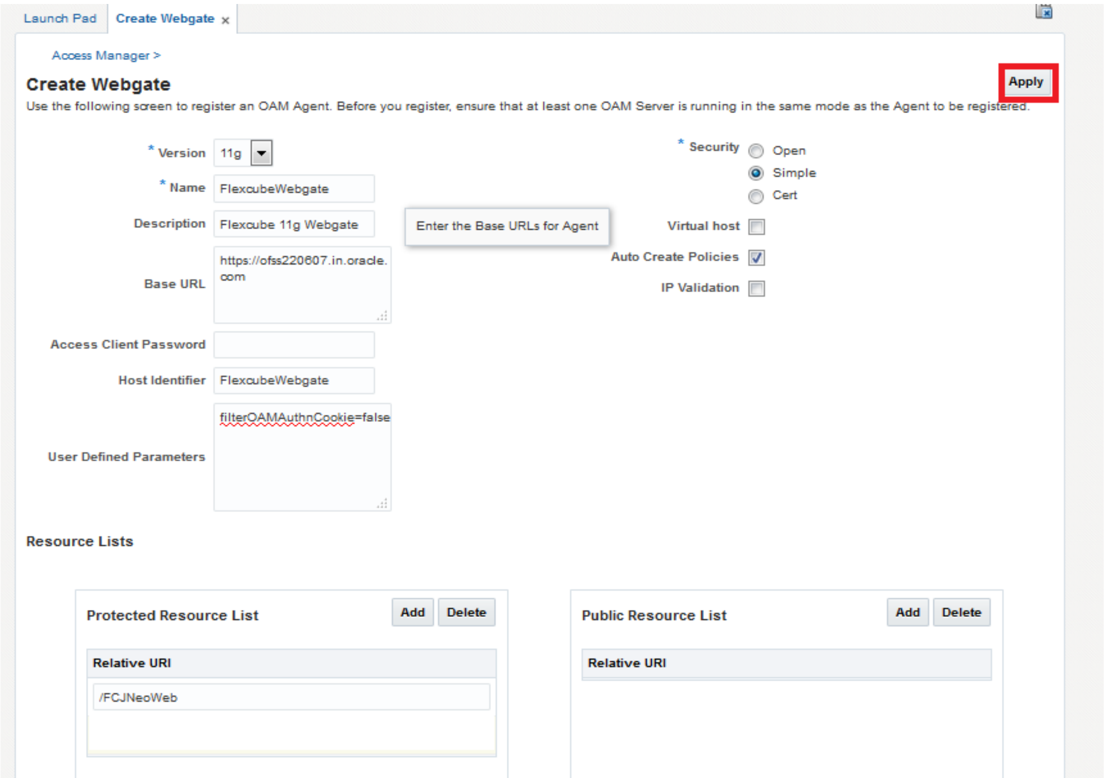
Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

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



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.

* Version	11g	* Security	○ Open ● Simple ○ Cert
* Name	FlexcubeWebgate		
Description	Flexcube 11g Webgate	Virtual host	□
Base URL	https://ofss220607.in.oracle.com	Auto Create Policies	☑
		IP Validation	□
Access Client Password			
Host Identifier	FlexcubeWebgate		
User Defined Parameters	filterOAMAuthnCookie=false		

Enter the Base URLs for Agent

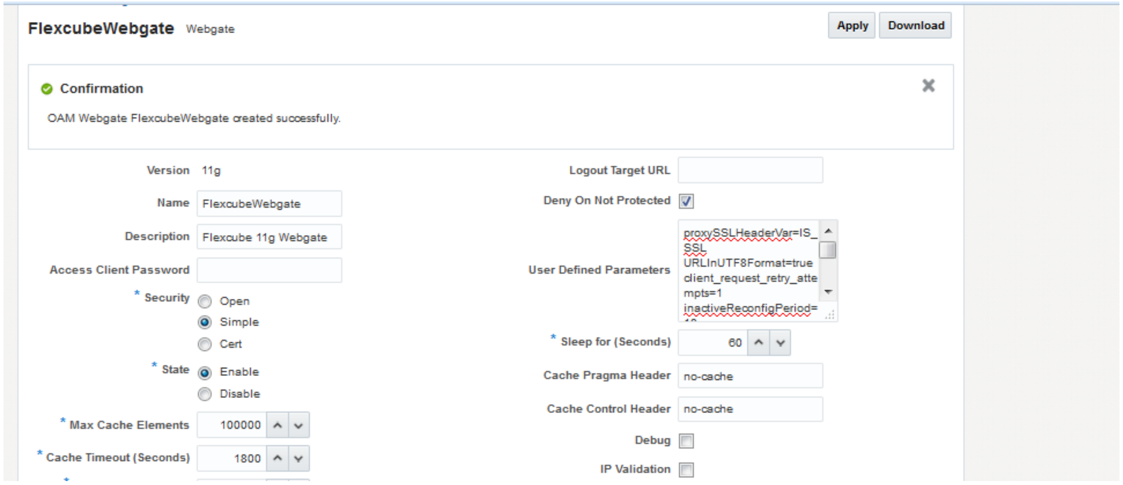
Resource Lists

Protected Resource List

Relative URI
/FCJNeoWeb

Public Resource List

Relative URI



FlexcubeWebgate Webgate

Confirmation

OAM Webgate FlexcubeWebgate created successfully.

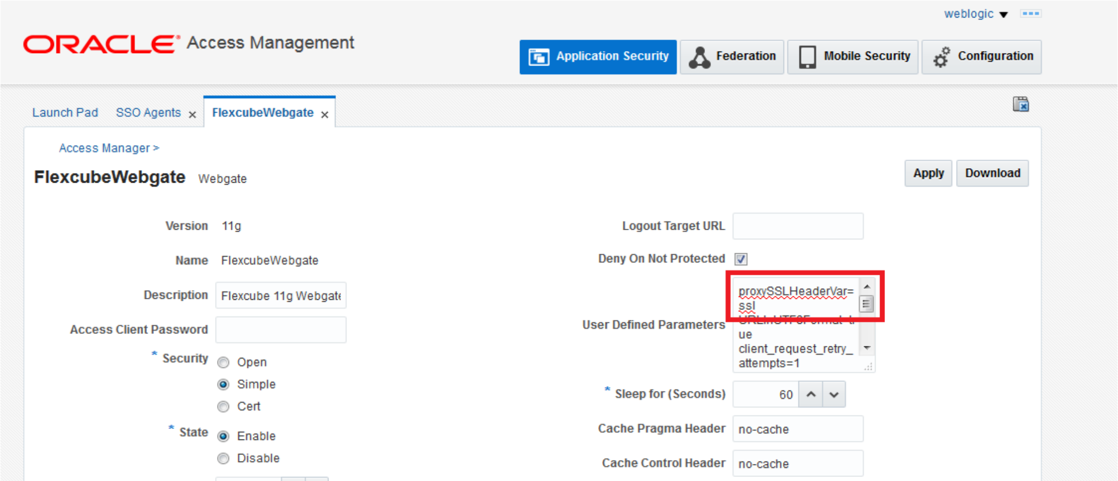
Version	11g	Logout Target URL	
Name	FlexcubeWebgate	Deny On Not Protected	☑

Description	Flexcube 11g Webgate	User Defined Parameters	proxySSLHeaderVar=IS_SSL
			URLInUTF8Format=true
			client_request_retry_attempts=1
			inactiveReconfigPeriod=

Access Client Password			
* Security	○ Open ● Simple ○ Cert	* Sleep for (Seconds)	60
* State	● Enable ○ Disable	Cache Pragma Header	no-cache
		Cache Control Header	no-cache
* Max Cache Elements	100000	Debug	□
* Cache Timeout (Seconds)	1800	IP Validation	□

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’.



FlexcubeWebgate Webgate

Version 11g

Name FlexcubeWebgate

Description Flexcube 11g Webgate

Access Client Password

* Security ○ Open ● Simple ○ Cert

* State ● Enable ○ Disable

Logout Target URL

Deny On Not Protected ☑

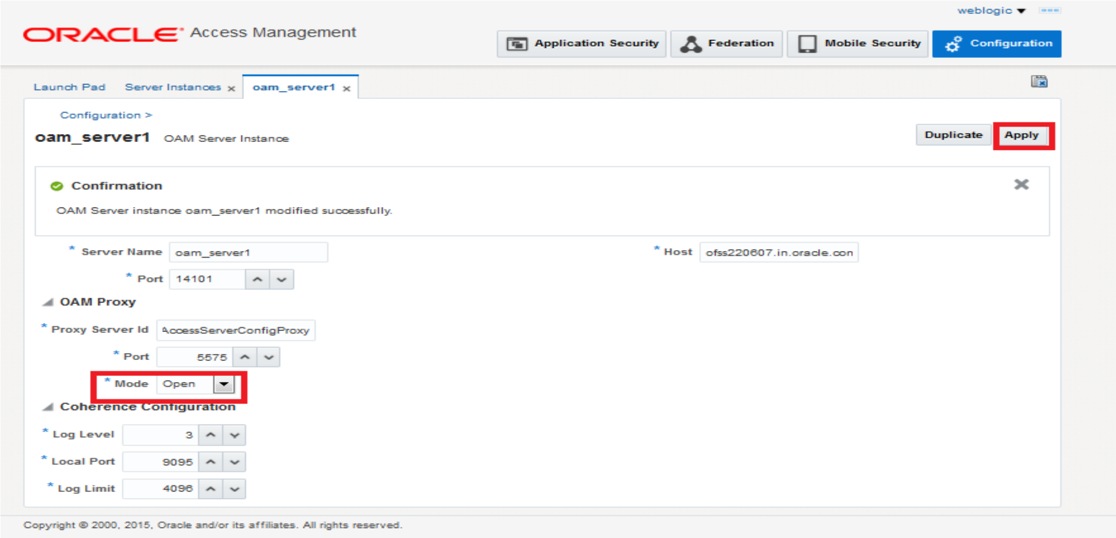
User Defined Parameters
proxySSLHeaderVar=ssl
ue
client_request_retry_attempts=1

* Sleep for (Seconds) 60

Cache Pragma Header no-cache

Cache Control Header no-cache

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



oam_server1 OAM Server Instance

Confirmation

OAM Server instance oam_server1 modified successfully.

* Server Name oam_server1

* Host ofss220607.in.oracle.con

* Port 14101

OAM Proxy

* Proxy Server Id AccessServerConfigProxy

* Port 5575

* Mode Open

Coherence Configuration

* Log Level 3

* Local Port 9095

* Log Limit 4096

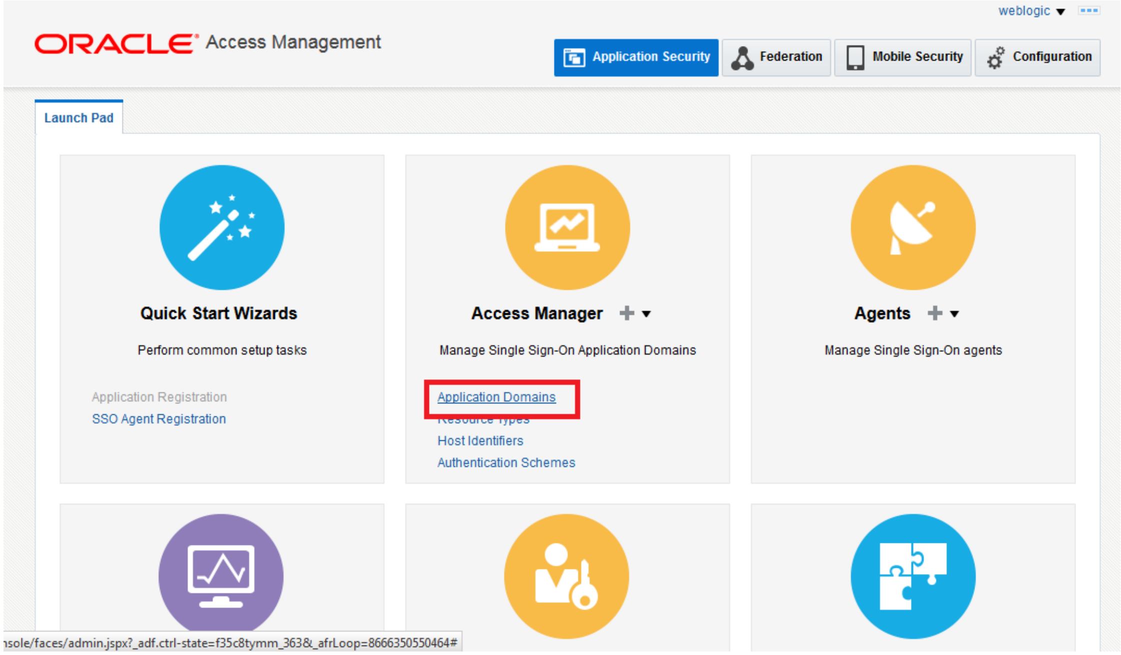
Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

2.6.5 Post OAM Webgate 11g Creation

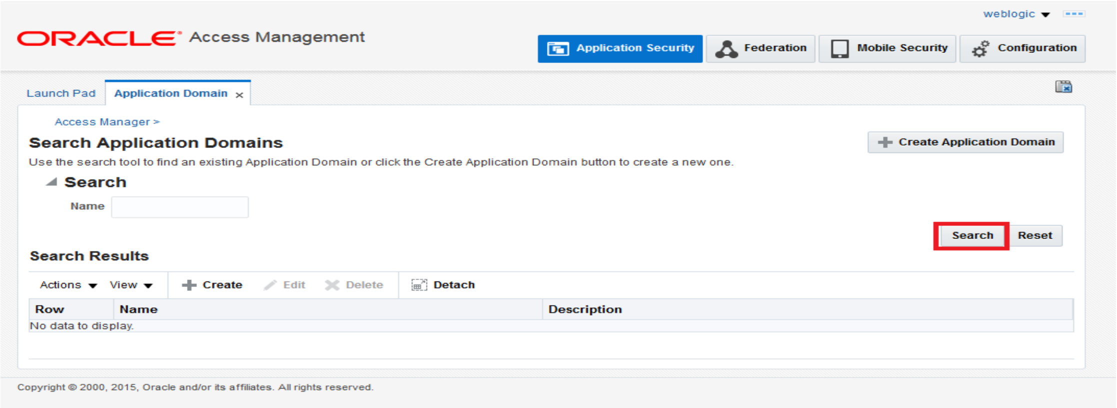
Follow the below steps to configure the webgate created.

2.6.5.1 Application Domains Changes

1. Click on 'Application Domains' in Access Manager under Application Security

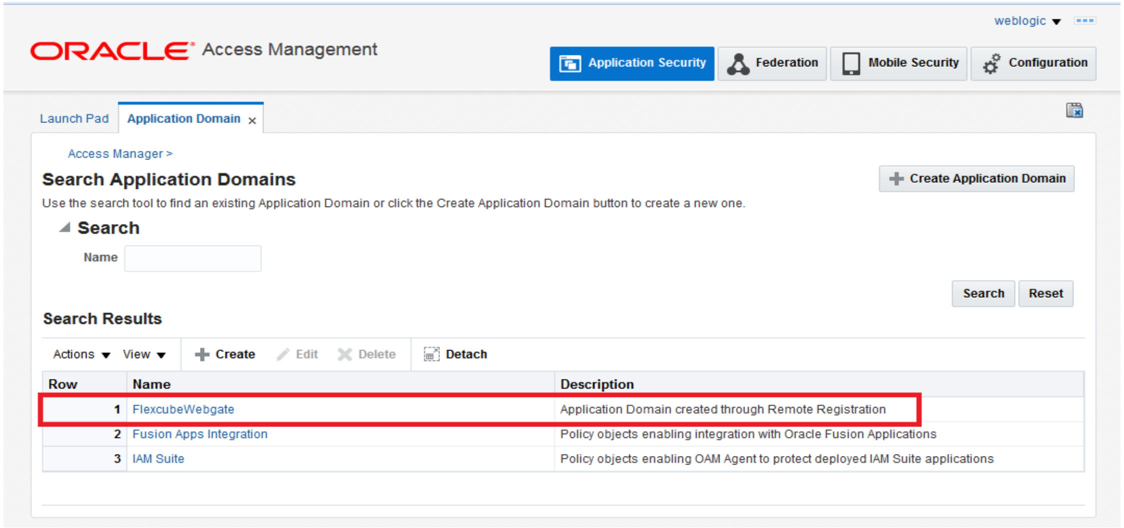


2. Click on 'Search' to find the 11g Webgate.



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

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



Search Application Domains

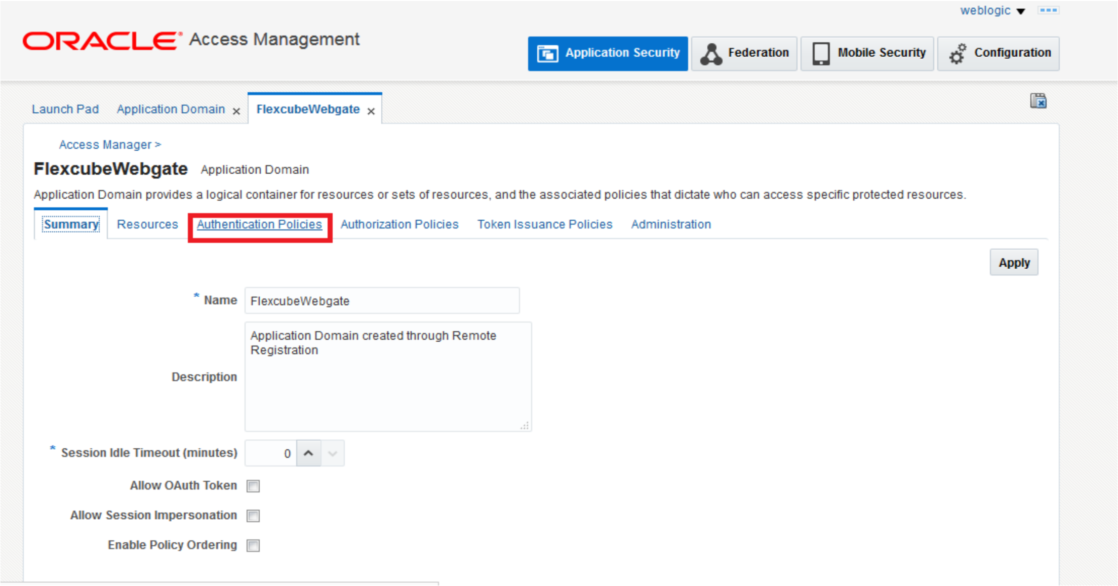
Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one.

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’.



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: FlexcubeWebgate

Description: Application Domain created through Remote Registration

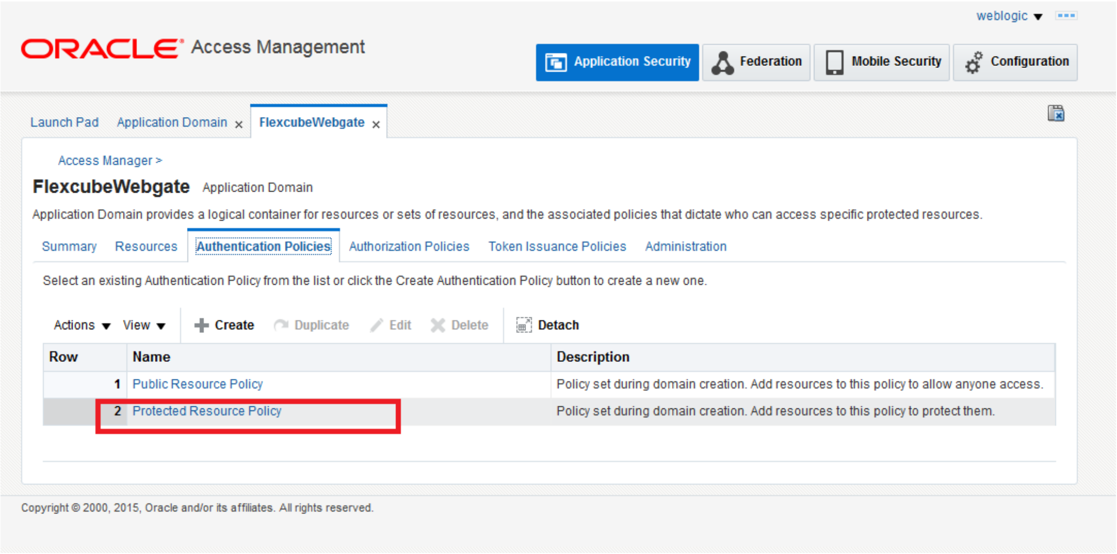
* Session Idle Timeout (minutes): 0

Allow OAuth Token □

Allow Session Impersonation □

Enable Policy Ordering □

4. Click on ‘Protected Resource Policy’.



FlexcubeWebgate Application Domain

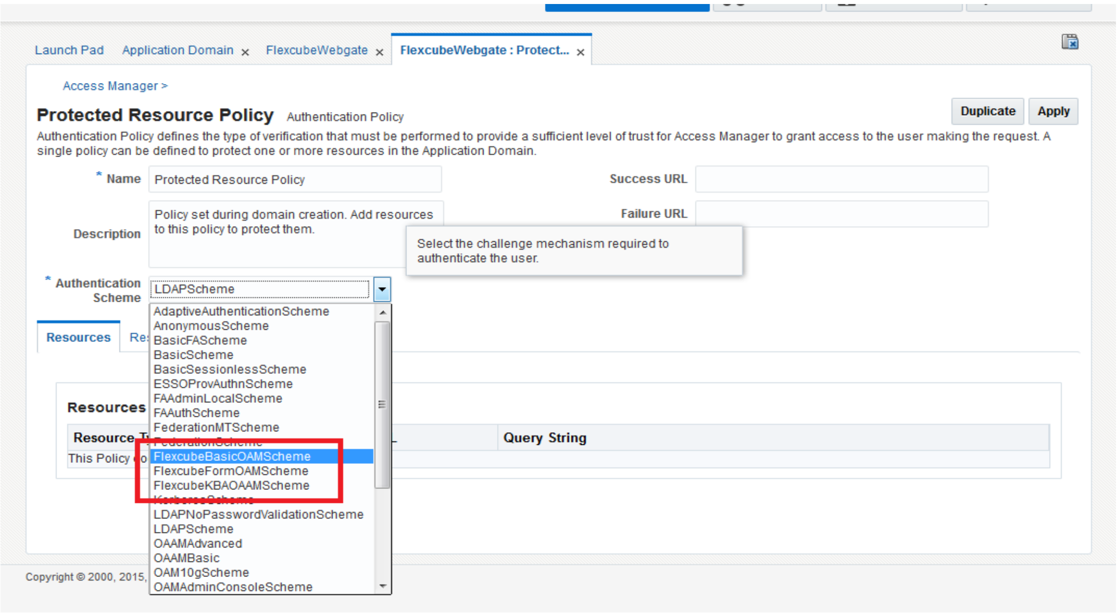
Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

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

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

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

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



Protected Resource Policy Authentication Policy

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.

* Name: Protected Resource Policy

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

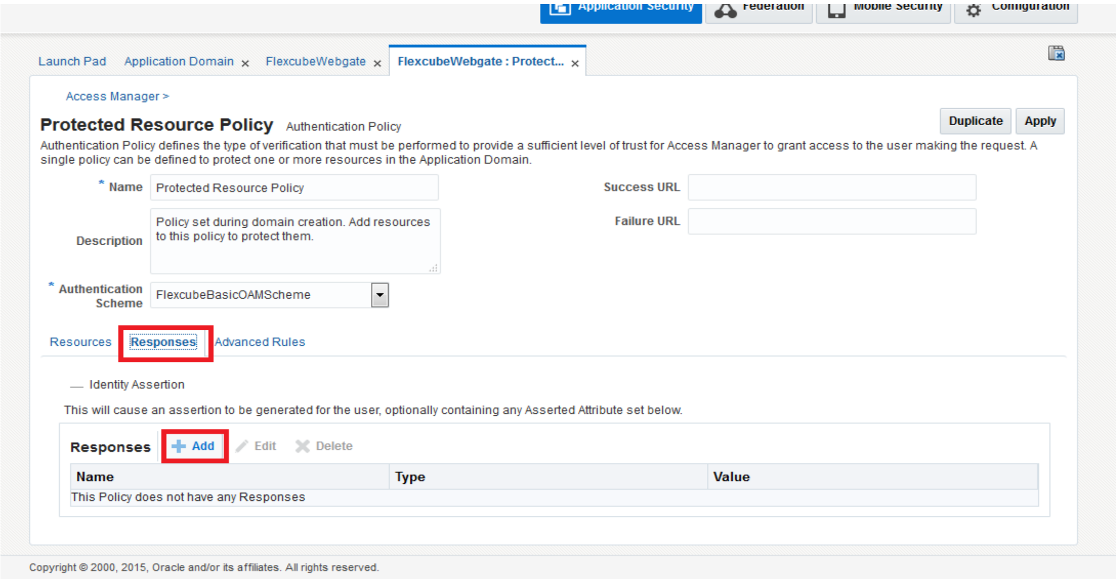
* Authentication Scheme: LDAPScheme

Success URL:

Failure URL:

Select the challenge mechanism required to authenticate the user.

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



Protected Resource Policy Authentication Policy

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.

* Name: Protected Resource Policy

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

* Authentication Scheme: FlexcubeBasicOAMScheme

Success URL:

Failure URL:

Identity Assertion

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

Responses

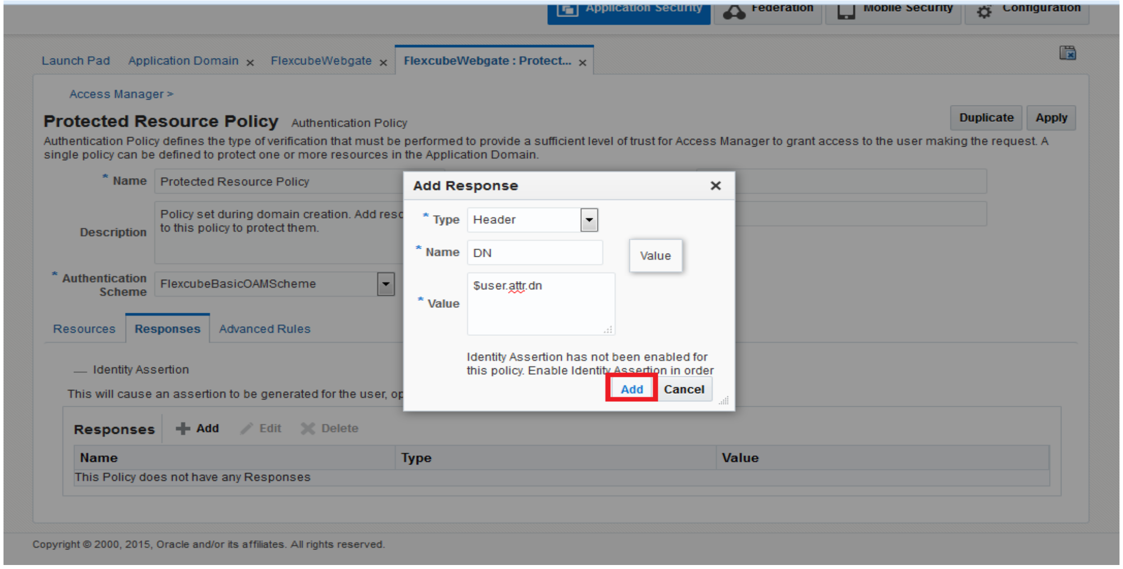
Name	Type	Value
This Policy does not have any Responses		

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

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

Type	: Header
Name	: DN
Value	: $user.attr.dn

Click on Add button



Protected Resource Policy Authentication Policy

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.

* Name: Protected Resource Policy

Description: Policy set during domain creation. Add reso… to this policy to protect them.

* Authentication Scheme: FlexcubeBasicOAMScheme

Identity Assertion

This will cause an assertion to be generated for the user, op

Add Response

* Type: Header

* Name: DN

* Value: $user.attr.dn

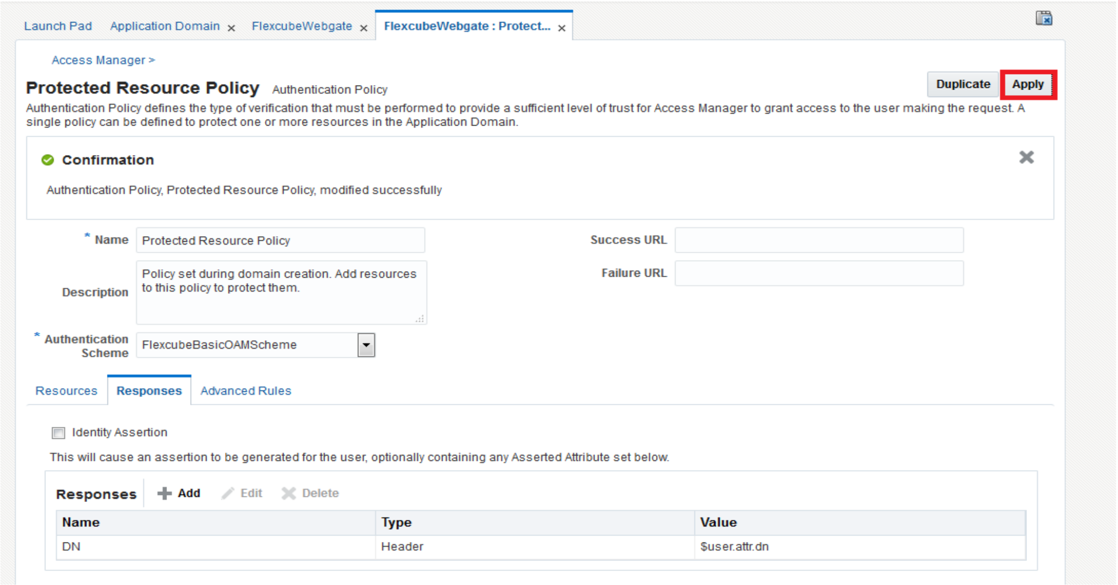
Identity Assertion has not been enabled for this policy. Enable Identity Assertion in order

Responses

Name	Type	Value
This Policy does not have any Responses		

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

8. Click on Apply to Save the Changes



Protected Resource Policy Authentication Policy

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

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

* Authentication Scheme: FlexcubeBasicOAMScheme

Success URL:

Failure URL:

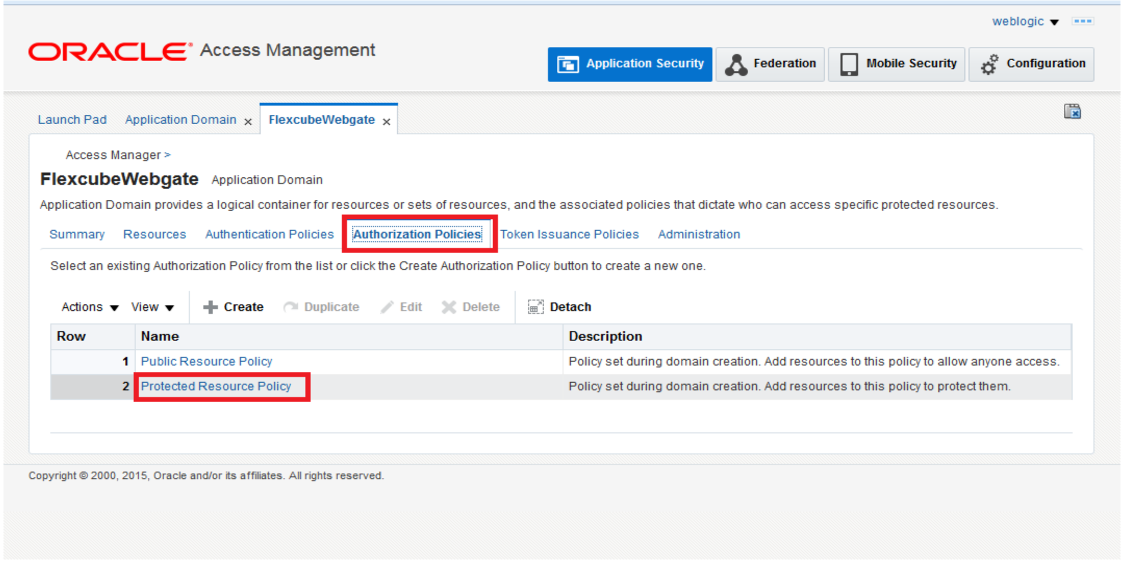
☐ Identity Assertion

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

Responses

Name	Type	Value
DN	Header	$user.attr.dn

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



FlexcubeWebgate Application Domain

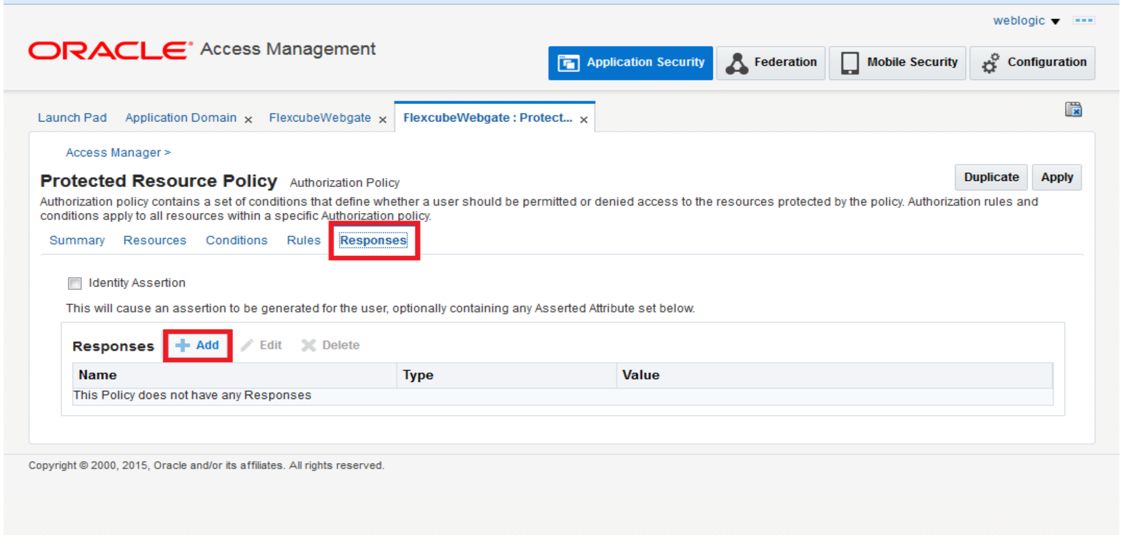
Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

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

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	Protected Resource Policy	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.



Protected Resource Policy Authorization Policy

Authorization policy contains a set of conditions that define whether a user should be permitted or denied access to the resources protected by the policy. Authorization rules and conditions apply to all resources within a specific Authorization policy.

□ Identity Assertion

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

Responses

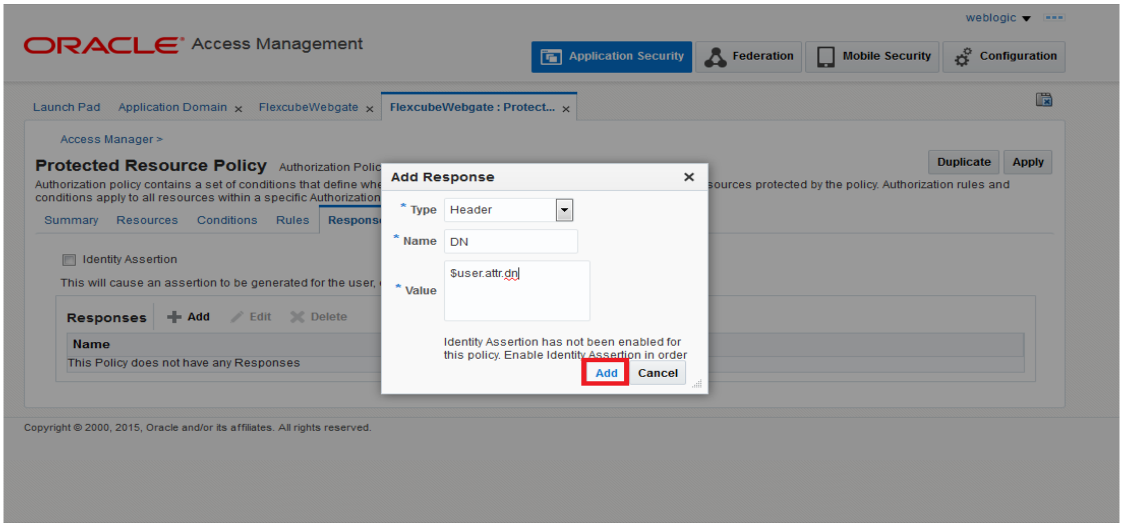
Name	Type	Value
This Policy does not have any Responses		

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

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

Type	: Header
Name	: DN
Value	: $user.attr.dn

Click on Add button



Add Response

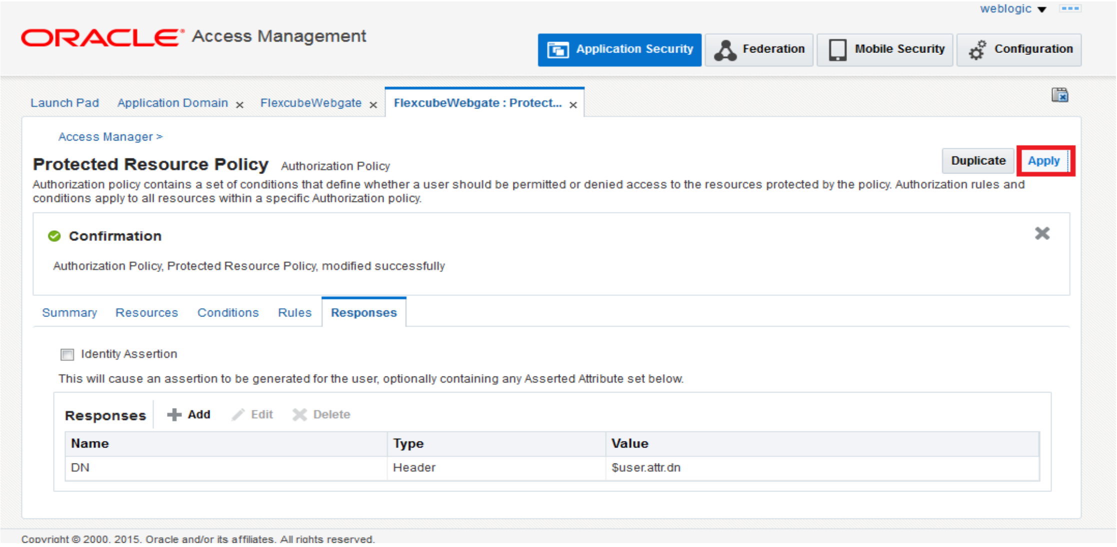
* Type: Header

* Name: DN

* Value: $user.attr.dn

Identity Assertion has not been enabled for this policy. Enable Identity Assertion in order

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



Protected Resource Policy Authorization Policy

Authorization policy contains a set of conditions that define whether a user should be permitted or denied access to the resources protected by the policy. Authorization rules and conditions apply to all resources within a specific Authorization policy.

Confirmation

Authorization Policy, Protected Resource Policy, modified successfully

□ Identity Assertion

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

Responses

Name	Type	Value
DN	Header	$user.attr.dn

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

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/keystores/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.

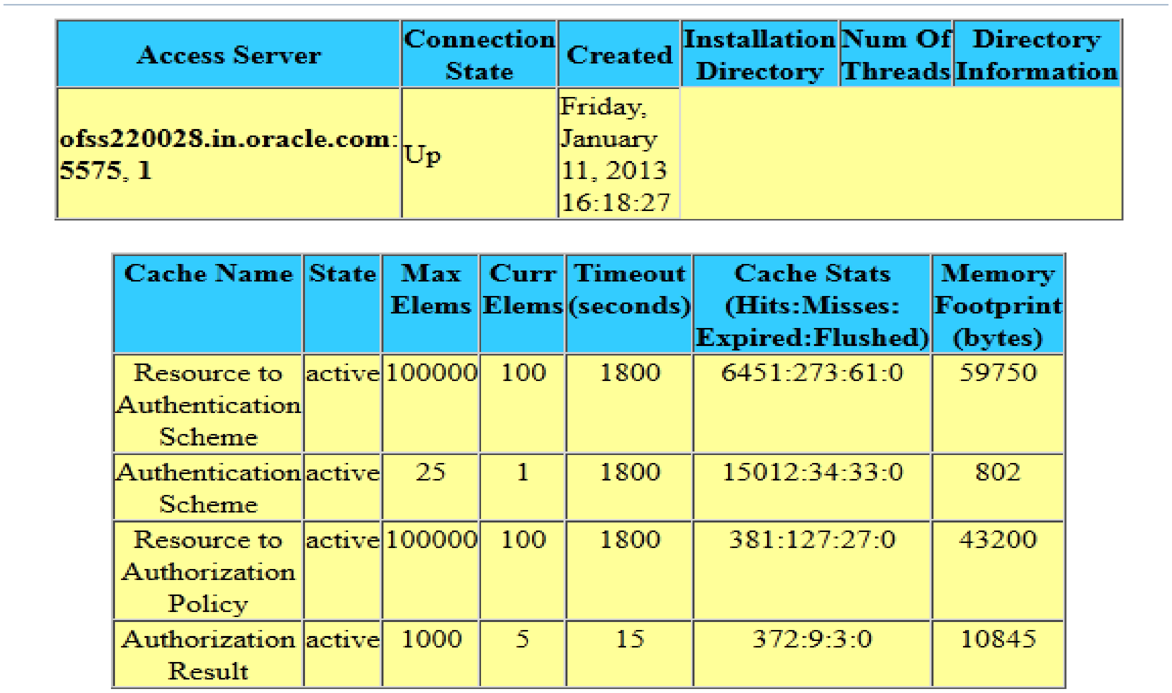
```
<Location /FCJNeoWeb>

        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			

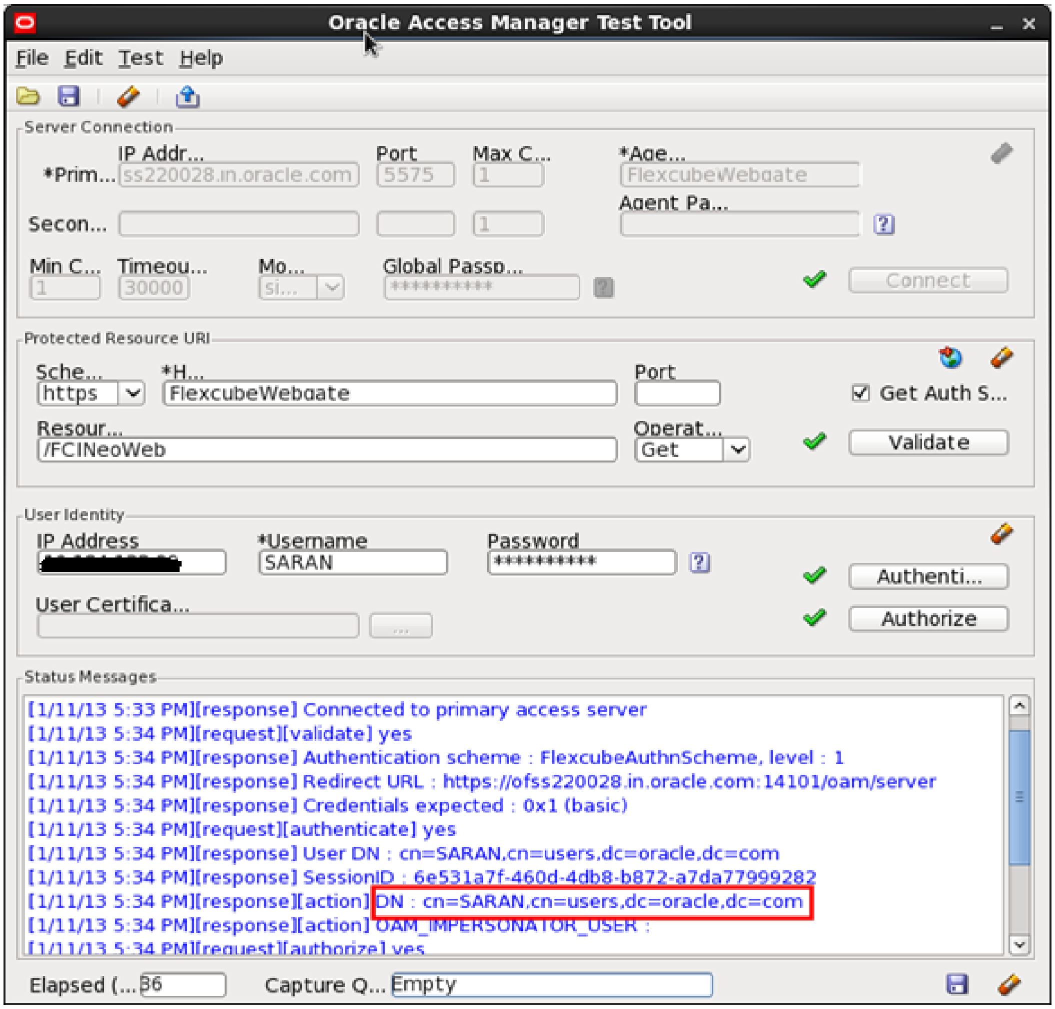
Cache Name	State	Max Elems	Curr Elems	Timeout (seconds)	Cache Stats (Hits:Misses: Expired:Flushed)	Memory Footprint (bytes)
Resource to Authentication Scheme	active	100000	100	1800	6451:273:61:0	59750
Authentication Scheme	active	25	1	1800	15012:34:33:0	802
Resource to Authorization Policy	active	100000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



*Prim... IP Addr... ss220028.in.oracle.com Port 5575 Max C... 1 *Age... FlexcubeWebgate

Secon... 1 Agent Pa...

Min C... 1 Timeou... 30000 Mo... si... Global Passp... **********

Sche... https *H... FlexcubeWebgate Port ☑ Get Auth S...

Resour... /FCINeoWeb Operat... Get

IP Address [redacted] *Username SARAN Password **********

User Certifica...

```
[1/11/13 5:33 PM][response] Connected to primary access server
[1/11/13 5:34 PM][request][validate] yes
[1/11/13 5:34 PM][response] Authentication scheme : FlexcubeAuthnScheme, level : 1
[1/11/13 5:34 PM][response] Redirect URL : https://ofss220028.in.oracle.com:14101/oam/server
[1/11/13 5:34 PM][response] Credentials expected : 0x1 (basic)
[1/11/13 5:34 PM][request][authenticate] yes
[1/11/13 5:34 PM][response] User DN : cn=SARAN,cn=users,dc=oracle,dc=com
[1/11/13 5:34 PM][response] SessionID : 6e531a7f-460d-4db8-b872-a7da77999282
[1/11/13 5:34 PM][response][action] DN : cn=SARAN,cn=users,dc=oracle,dc=com
[1/11/13 5:34 PM][response][action] OAM_IMPERSONATOR_USER :
[1/11/13 5:34 PM][request][authorize] yes
```

Elapsed (... 36 Capture Q... Empty

If there is any escape character available in DN address, then refer ‘1935703.1’ Oracle Document ID to remove the escape character.

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

In STTM_BANK table update SSO_INSTALLED to 'Y' to enable Single Sign On.

During property file creation for FCIS application, select ‘SSO Required’ option as YES.

Refer FCIS_Property_File_Creation.pdf in FLEXCUBE_IS_Installation/FCIS Components/FCIS in Installation manual

2.7.2 Maintaining LDAP DN for FLEXCUBE users

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

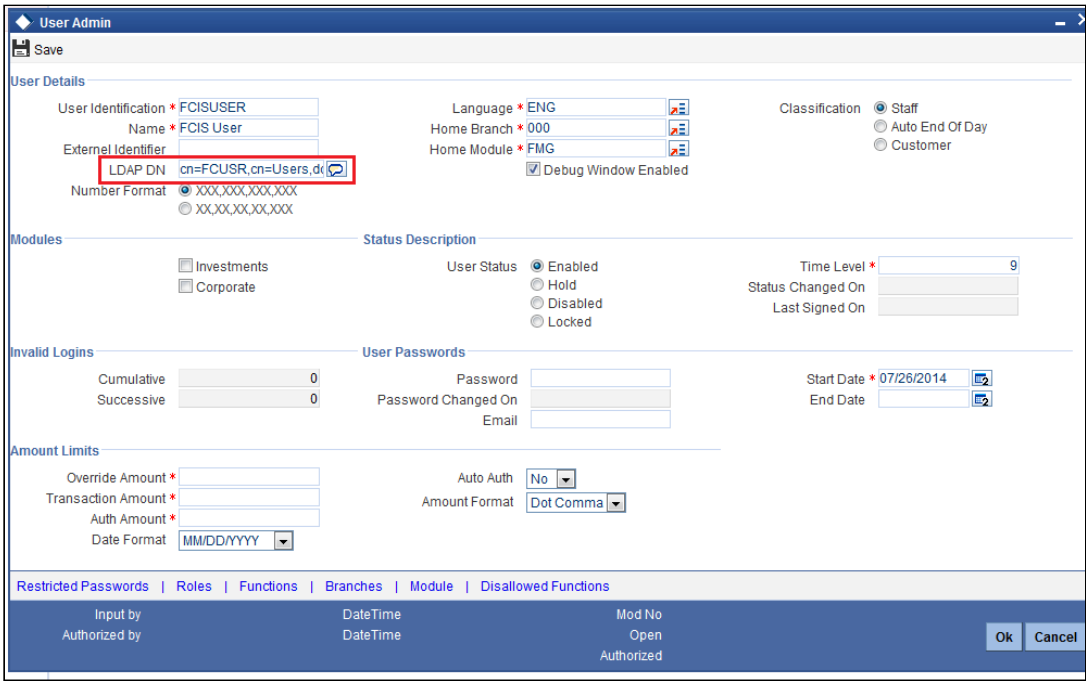
When creating the user in LDAP, ensure that the DN used is same as the LDAP DN value that will be updated in user maintenance form. Once the user is created in LDAP go to the user maintenance form in FCUBS. If the FCUBS user already exists then unlock the user and update the LDAP DN value which was set 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 - IS



User Details

User Identification * FCISUSER
Name * FCIS User
External Identifier
LDAP DN cn=FCUSR,cn=Users,dc
Number Format ● XXX,XXX,XXX,XXX ○ XX,XX,XX,XX,XXX

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

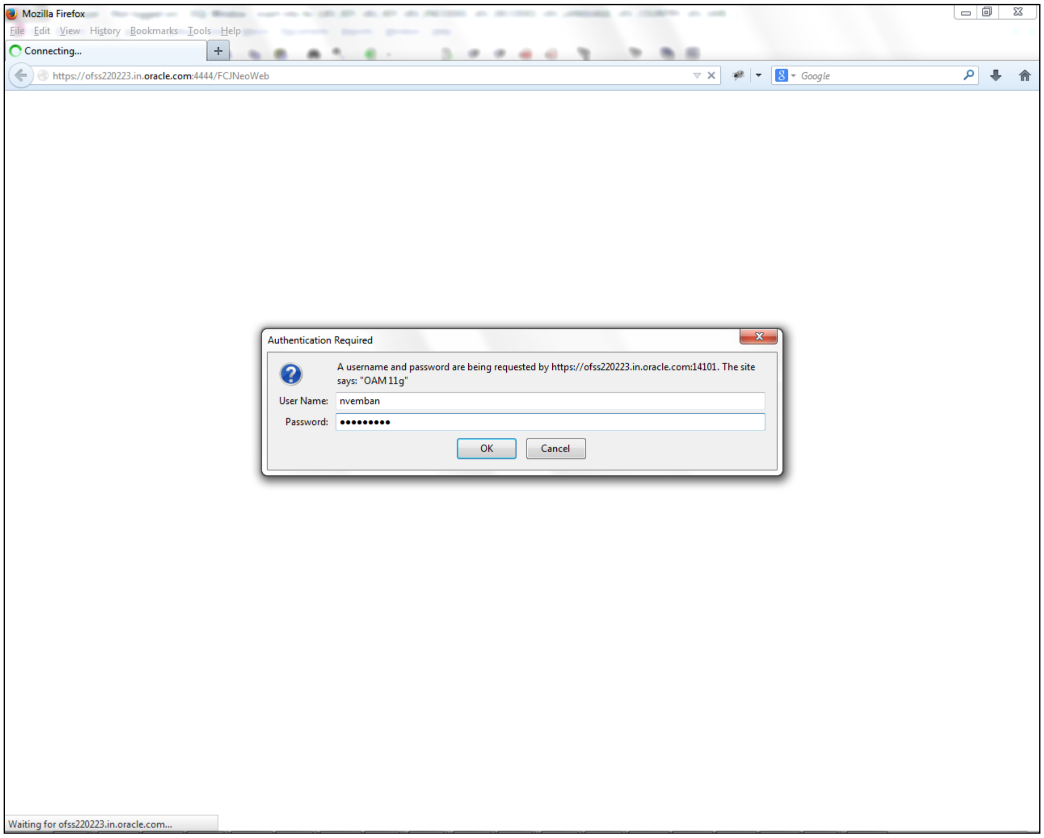
2.7.3 Launching FLEXCUBE

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



Mozilla Firefox
File Edit View History Bookmarks Tools Help
Connecting...
https://ofss220223.in.oracle.com:4444/FCJNeoWeb
Google
Waiting for ofss220223.in.oracle.com...

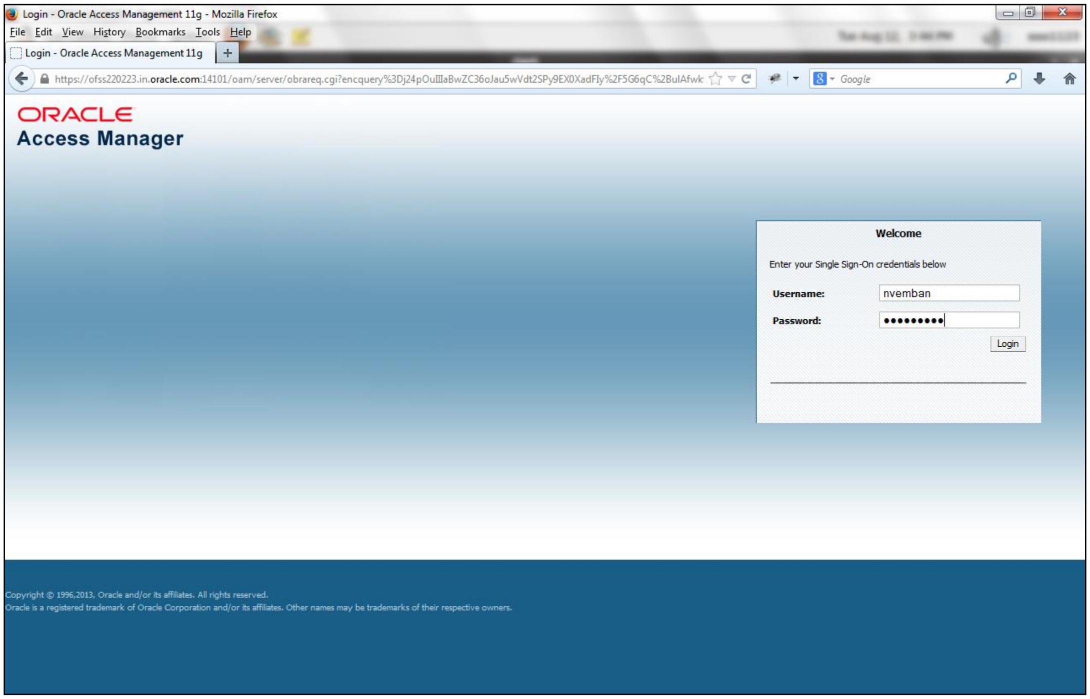
Authentication Required

A username and password are being requested by https://ofss220223.in.oracle.com:14101. The site says: "OAM 11g"

User Name: nvemban

Password: ••••••••••

2.7.3.2 Form Style Challenge by Webgate


Login - Oracle Access Management 11g - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Login - Oracle Access Management 11g
Google
ORACLE
Access Manager
Login

https://ofss220223.in.oracle.com:14101/oam/server/obrareq.cgi?encquery%3Dj24pOuIIIaBwZC36oJau5wVdt2SPy9EX0XadFly%2F5G6qC%2BuIAfwk

Welcome

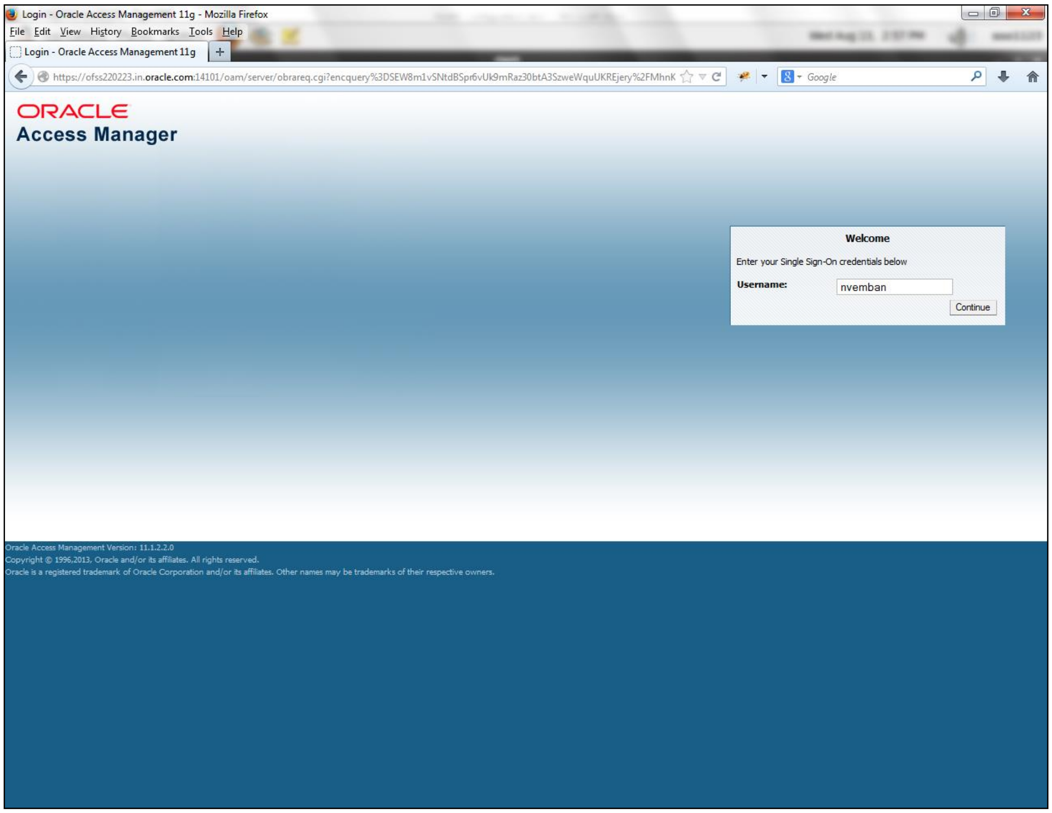
Enter your Single Sign-On credentials below

Username: nvemban

Password: •••••••••

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.

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


Login - Oracle Access Management 11g - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Login - Oracle Access Management 11g
Google
ORACLE
Access Manager
Continue

https://ofss220223.in.oracle.com:14101/oam/server/obrareq.cgi?encquery%3DSEW8m1vSNtdBSpr6vUk9mRaz30btA3SzweWquUKREjery%2FMhnK

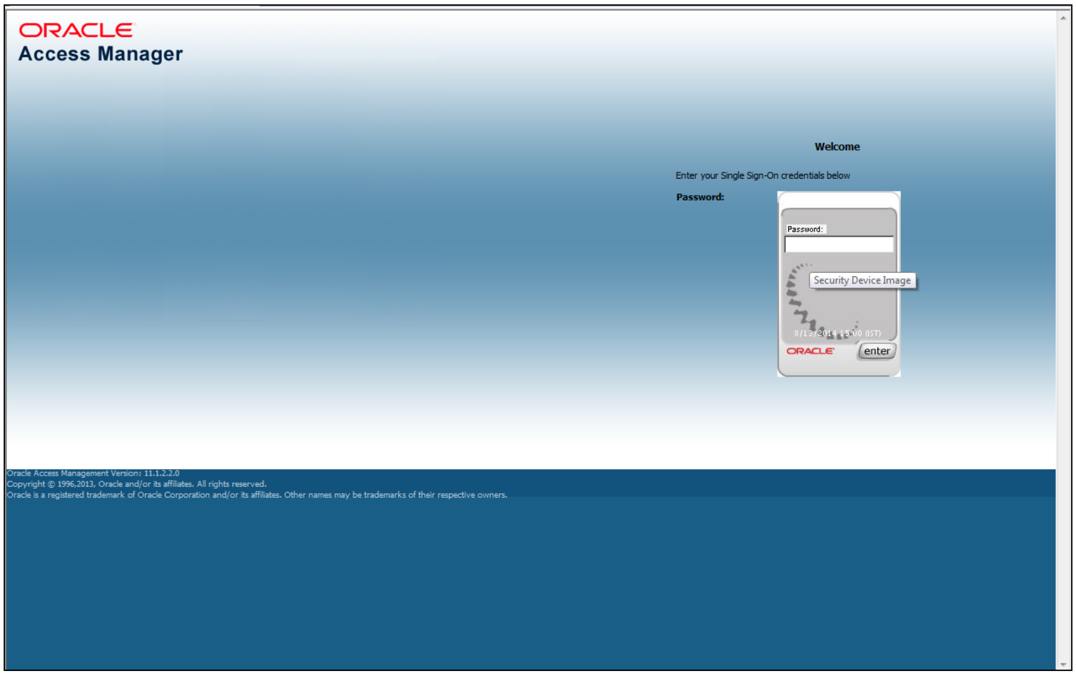
Welcome

Enter your Single Sign-On credentials below

Username: nvemban

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.

First Time Login

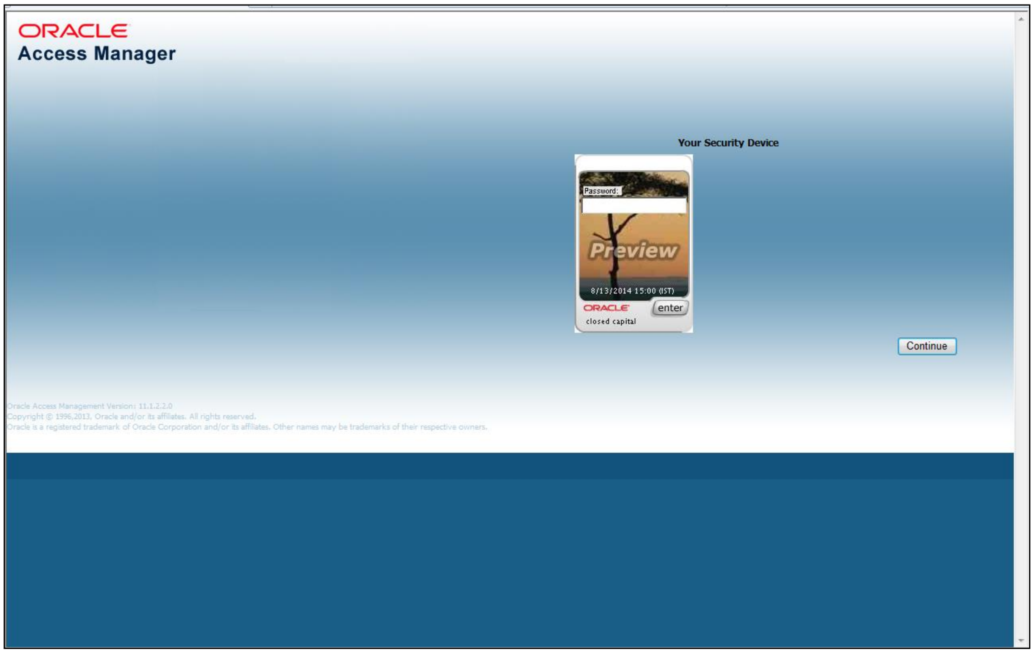


Access Manager

Welcome

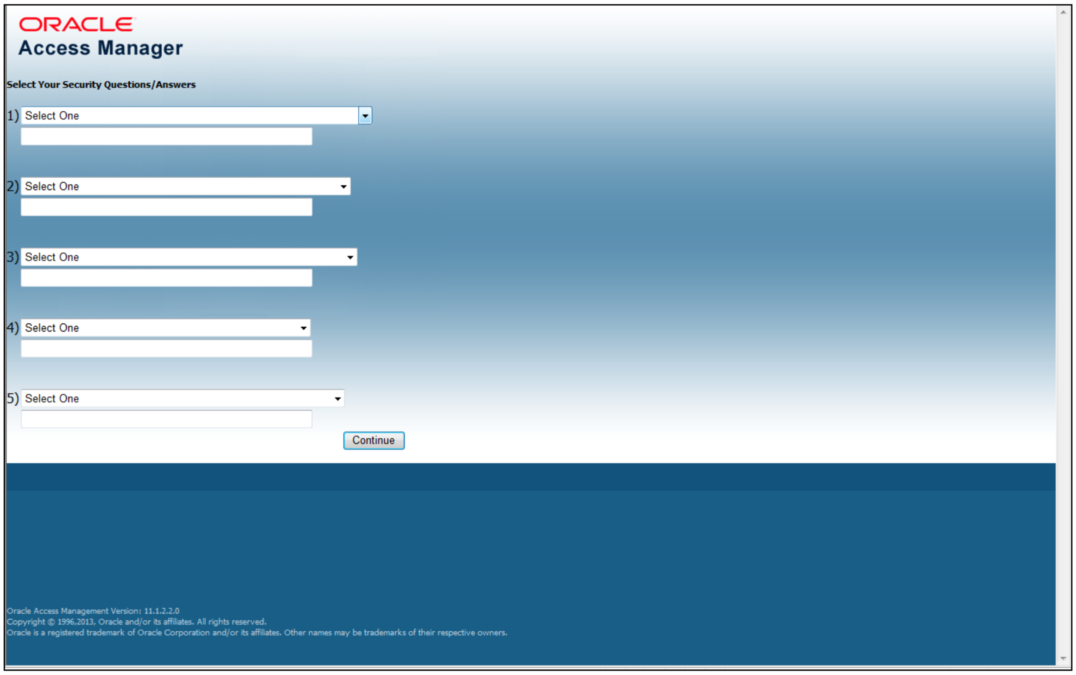
Enter your Single Sign-On credentials below

Password:



Access Manager

Your Security Device



ORACLE
Access Manager

Select Your Security Questions/Answers

1) Select One

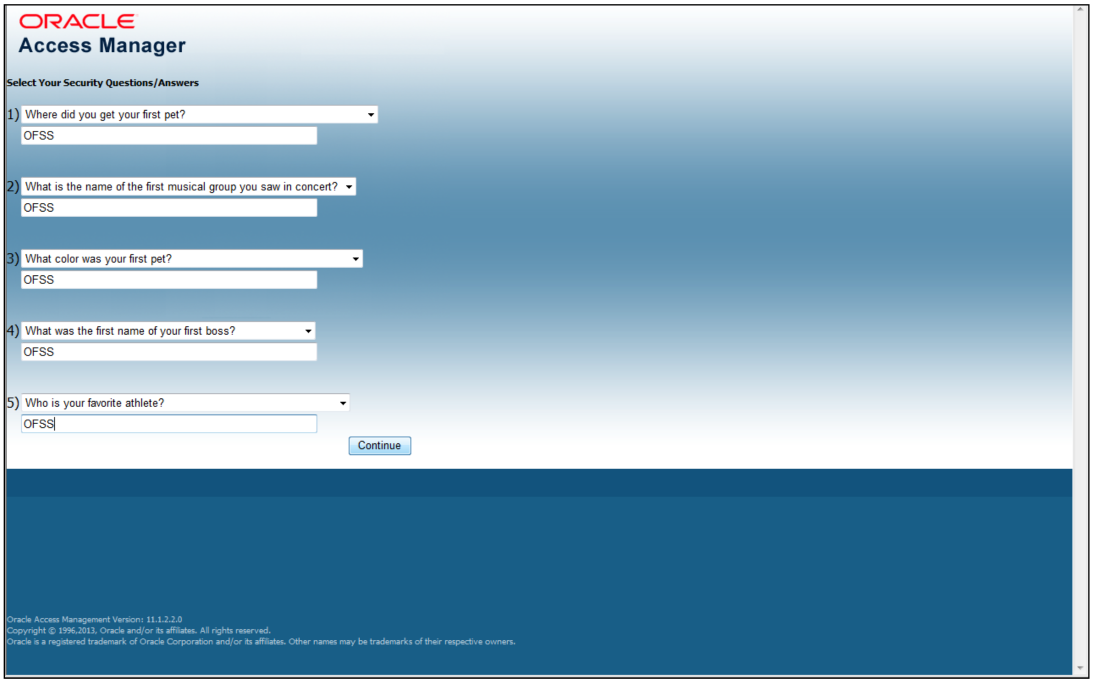
2) Select One

3) Select One

4) Select One

5) Select One

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.



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

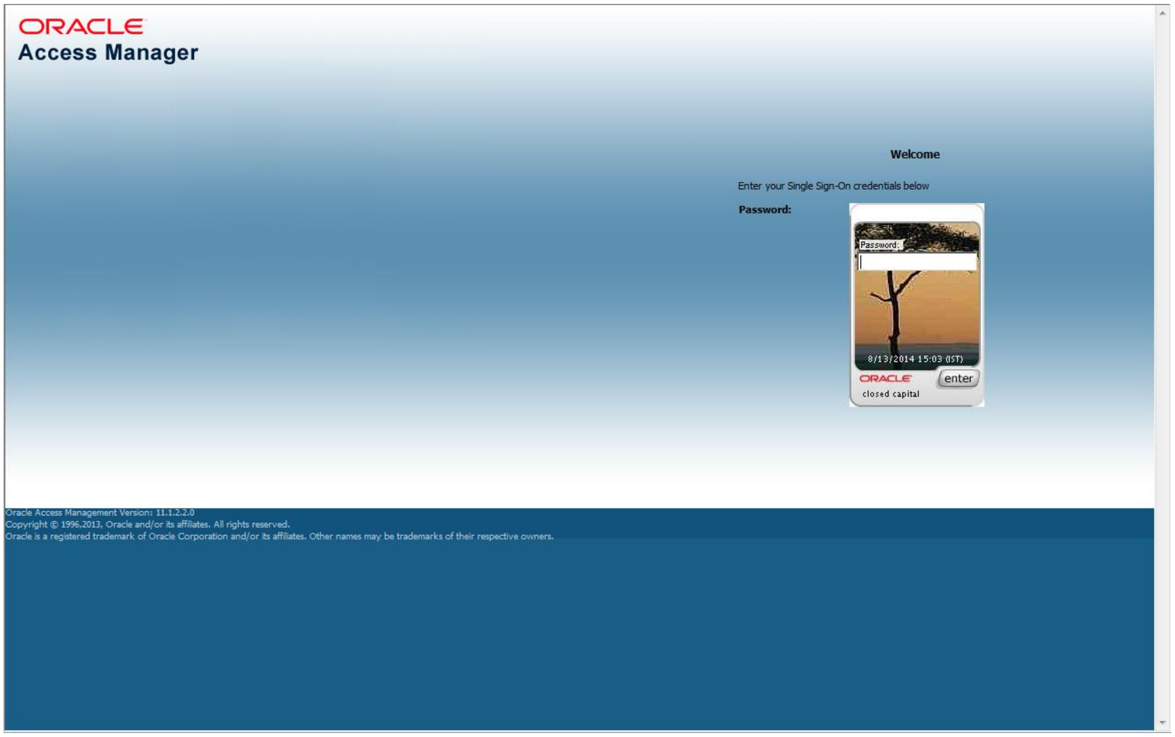
3) What color was your first pet?
OFSS

4) What was the first name of your first boss?
OFSS

5) Who is your favorite athlete?
OFSS

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.

Post First Login



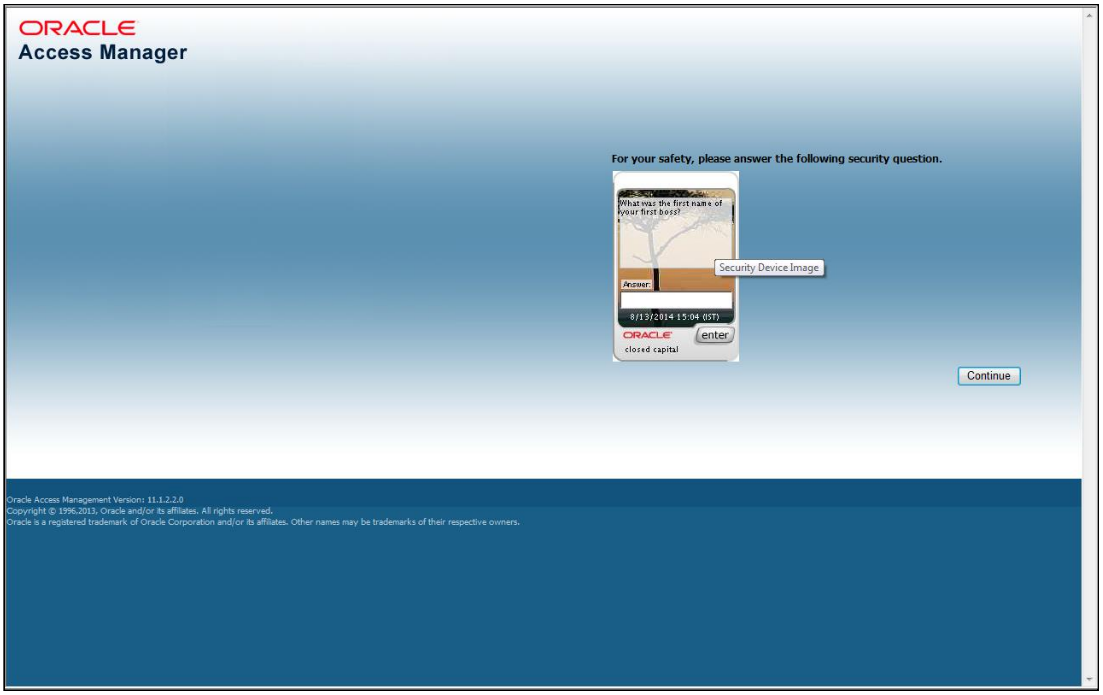
ORACLE
Access Manager

Welcome

Enter your Single Sign-On credentials below

Password:

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.



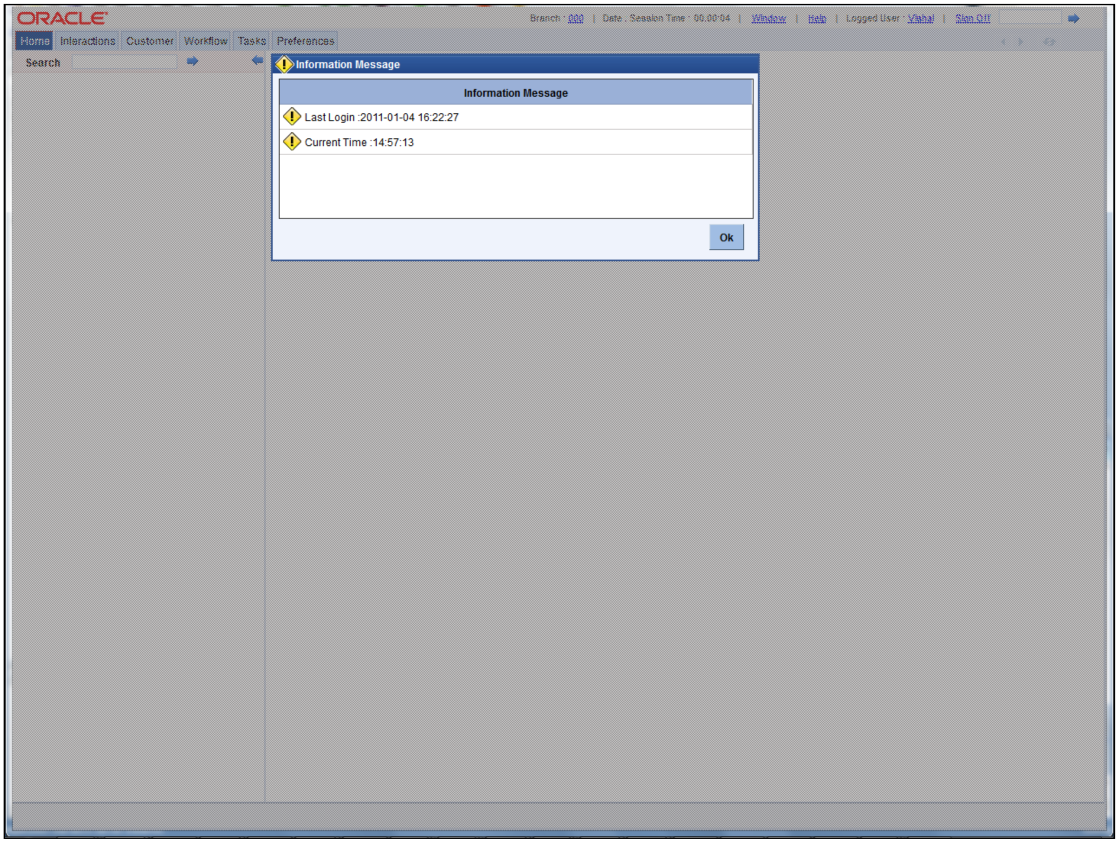
ORACLE
Access Manager

For your safety, please answer the following security question.

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.

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


ORACLE
Branch : 000 | Date . Session Time : 00:00:04 | Window | Help | Logged User : Vishal | Sign Off
Home
Interactions
Customer
Workflow
Tasks
Preferences
Search
Information Message

Information Message

Last Login :2011-01-04 16:22:27

Current Time :14:57:13

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.