Oracle Access Manager Integration
Oracle FLEXCUBE Universal Banking

Release 12.0.2.0.0

October 2013

Table of Contents

1. Preface

1.1 Introduction

This manual discusses the integration Oracle FLEXCUBE Universal Banking and the Oracle Access Manager system**.** The configurations required for the 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.
Back office Managers/Officers	Authorization functions.

1.3 Abbreviations

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

1.4 Documentation Accessibility

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

1.5 Organization

This manual is organized into the following chapters:

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

1.6 Glossary of Icons

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

Icons	Function
☒	Exit
⊞	Add row
⊟	Delete row
↗	Option List

1.6.1 Related Documents

You may refer the following manuals for more information

- Procedures User Manual
- 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 UBS is qualified with Oracle Identity Management 11.1.1 (Fusion Middleware 11gR1) – specifically using the Access Manager component of Oracle Identity Management. This feature is available in the releases FC UBS V.UM 7.3.0.0.0.0.0 and onwards of FLEXCUBE UBS.

This document is expected to provide an understanding as to how single sign-on can be enabled for a FLEXCUBE UBS deployment using Oracle Fusion Middleware 11g.

In addition to providing a background to the various components of the deployment, this document also talks about Configuration 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 Access Manager – OAM (11.1.1.5)

- Access Server – 11.1.1.5
- Webtier Utilities 11.1.1.6
- Web Gate 11.1.1.5
- Http Server

LDAP Directory Server

Please make sure that the LDAP which has been used for Flexcube Single Signon 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

Web Logic(10.3.5)

For the purpose of achieving single sign on for FCUBS in FMW 11gR1, 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 Identity Asserter

Identity Asserter uses Oracle Access Manager Authentication services and also validates already-authenticated Oracle Access Manager Users through the ObSSOCookie and creates a WebLogic-authenticated session. It also provides single sign-on between WebGates and portals. We can get more details on Identity asserter at
http://download.oracle.com/docs/cd/E12839_01/core.1111/e10043/osso.htm#CHDGCACF

Note: This document containts the configuration of Oracle Interner Directory as LDAP server and its configuration in weblogic. This document will not discuss the configuring and setting up of OAM and LDAP directory server of other LDAP servers. This will be provided by the corresponding Software provider.

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 provided below steps assume that Oracle Access Manager and the LDAP server have been installed already and the requisite setup already done with respect to connecting the two along 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

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:

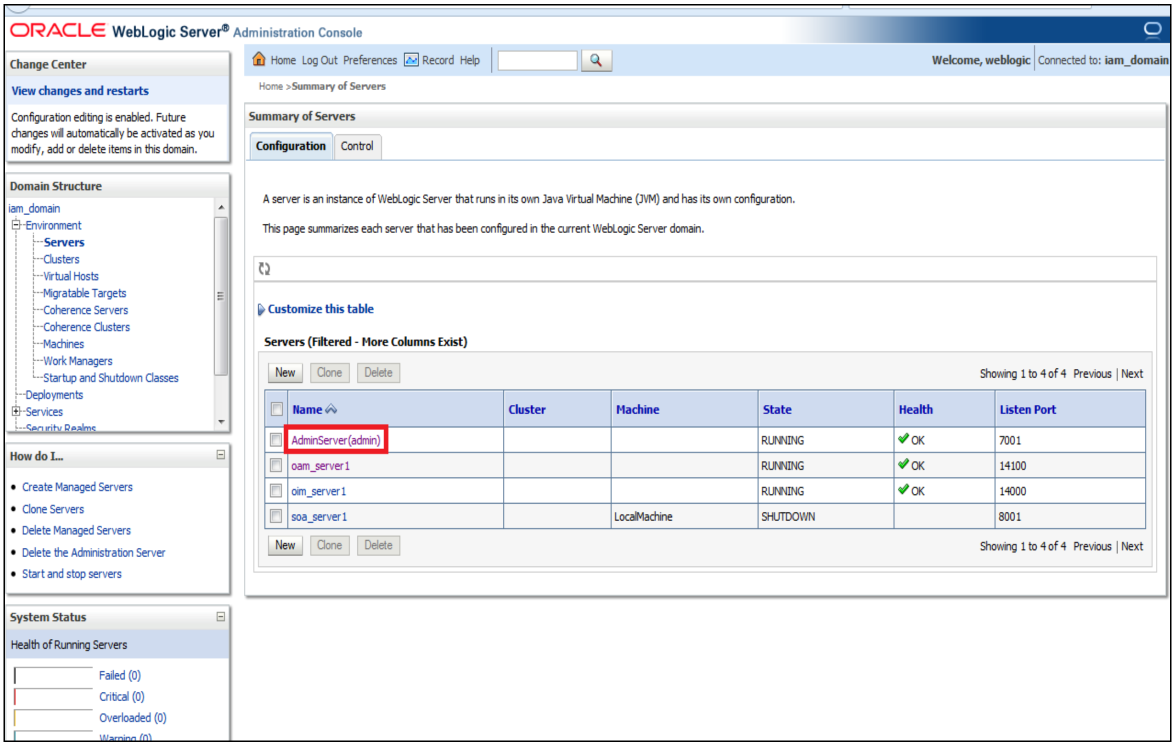
```
keytool -import -v -trustcacerts -alias rootcacert -file AdminFlexcubeCert.cer -keystore AdminFlexcubeKeyStore.jks -keypass Password@123 -storepass Password@123
```

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.

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

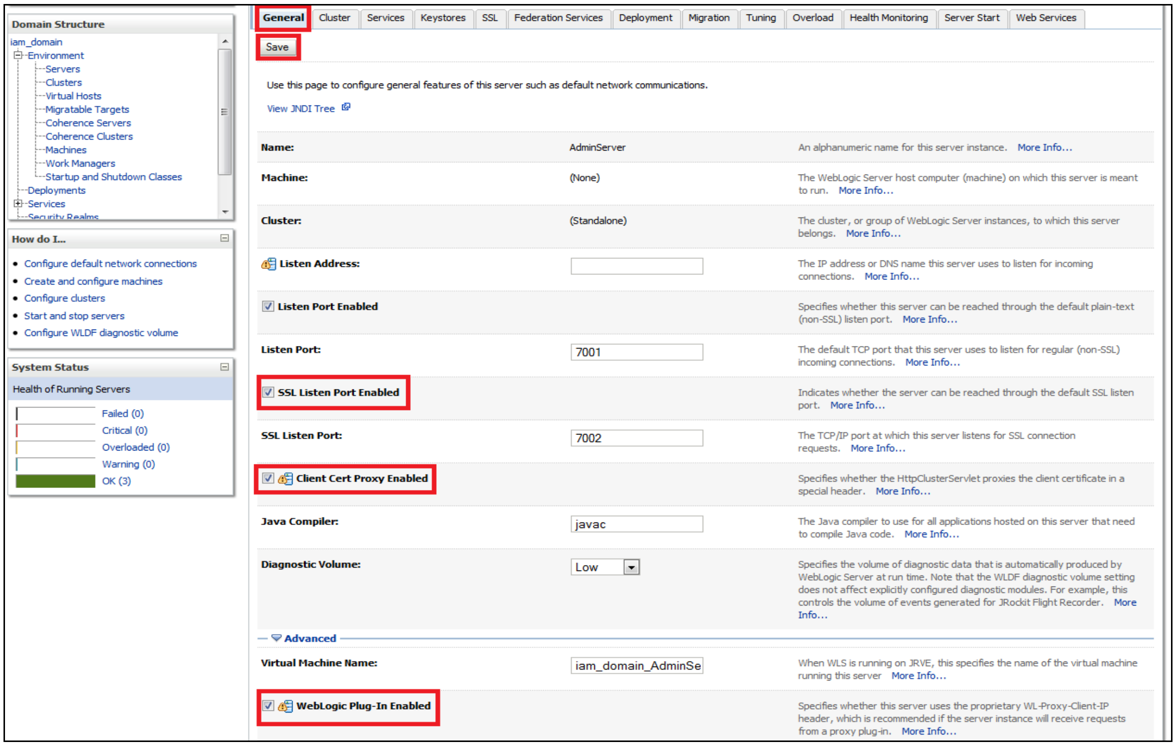
This page summarizes each server that has been configured in the current WebLogic Server domain.

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

2.5.2.2 Follow the steps in General Tab as shown below:

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



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 default network connections
- Create and configure machines
- Configure clusters
- Start and stop servers
- Configure WLDF diagnostic volume

System Status

Health of Running Servers

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

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

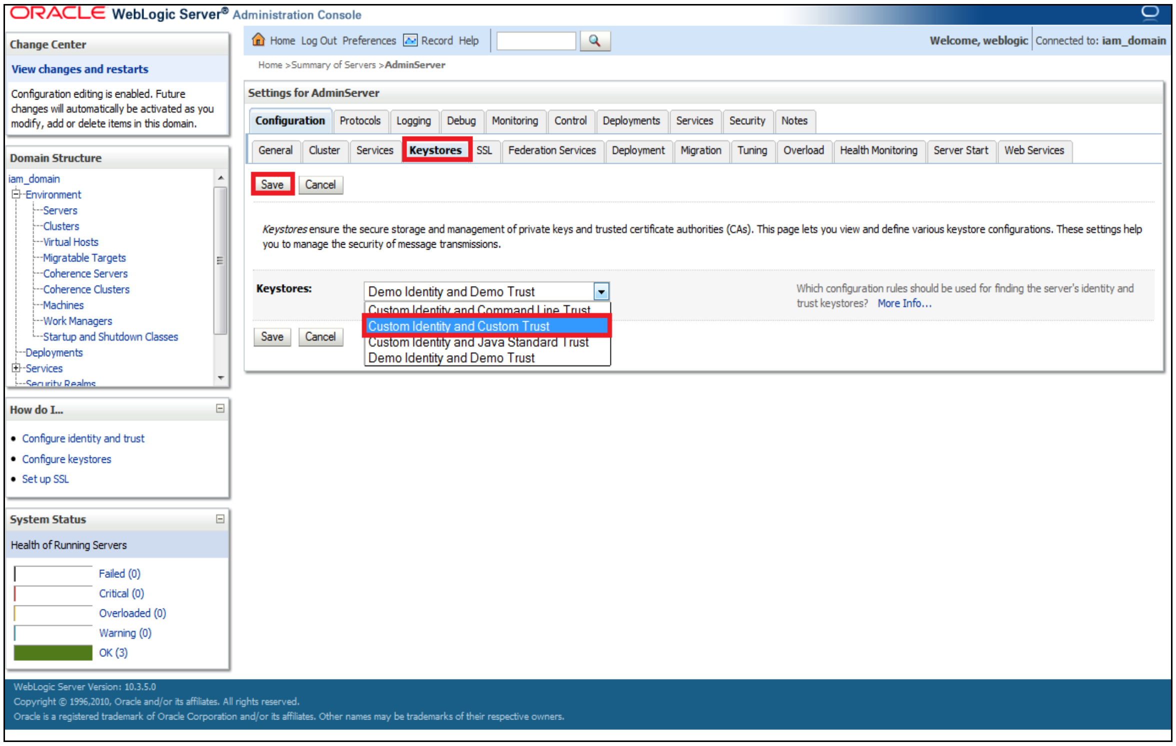
Name:	AdminServer	An alphanumeric name for this server instance. More Info...
Machine:	(None)	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Standalone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
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...

Advanced

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:

- Click Change and select Keystores as **Custom Identity and Custom Trust**
- Click on Save
- Note: 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

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
- Configure keystores
- Set up SSL

System Status

Health of Running Servers

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

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: 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

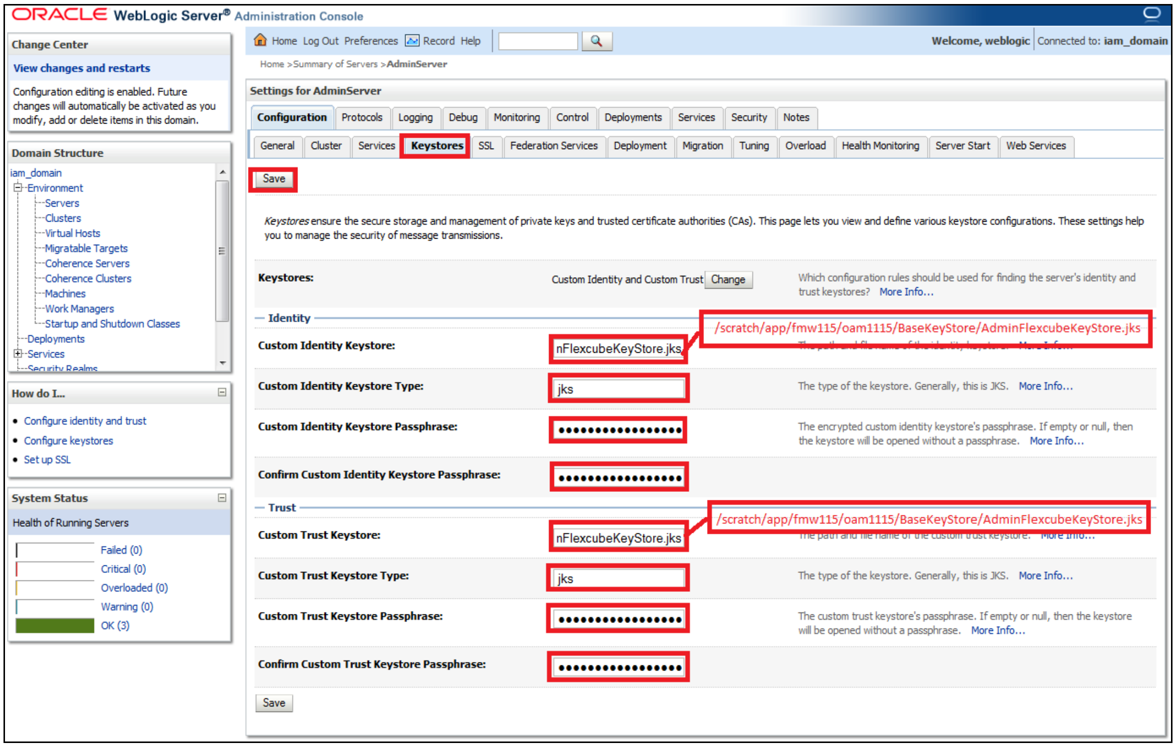
Which configuration rules should be used for finding the server's identity and trust keystores? More Info...

Save Cancel

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:

- Enter Custom Identity Keystore and Custom Trust Keystore as same as the Keystore Name created in step 3.2.1.1 with full path.
- Enter Custom Identity Keystore Type and Custom Trust Keystore Type as jks.
- Enter Custom Identity Keystore Passphrase, Confirm Custom Identity Keystore Passphrase, Custom Trust Keystore Passphrase and Confirm Custom Trust Keystore Passphrase as same as the Store Password entered in step 3.2.1.1.
- 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 — The path and file name of the custom trust keystore. More Info...

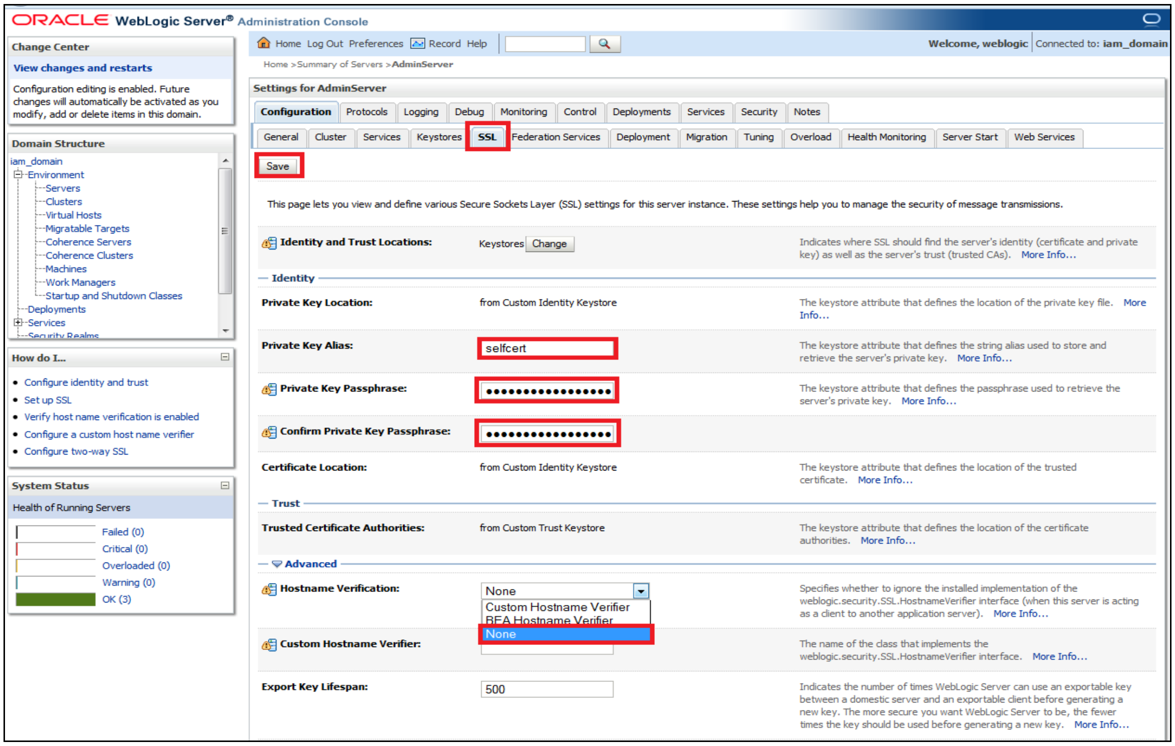
Custom Trust Keystore Type: jks — The type of the keystore. Generally, this is JKS. More Info...

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:

- Enter Private Key Alias as same as the alias name entered in step 3.2.1.1.
- Enter Private Key Passphrase and Confirm Private Key Passphrase as same as the Private Key Password entered in step 3.2.1.1.
- Change the Hostname Verification to None.
- Click on Save.



Home >Summary of Servers >AdminServer

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

How do I...

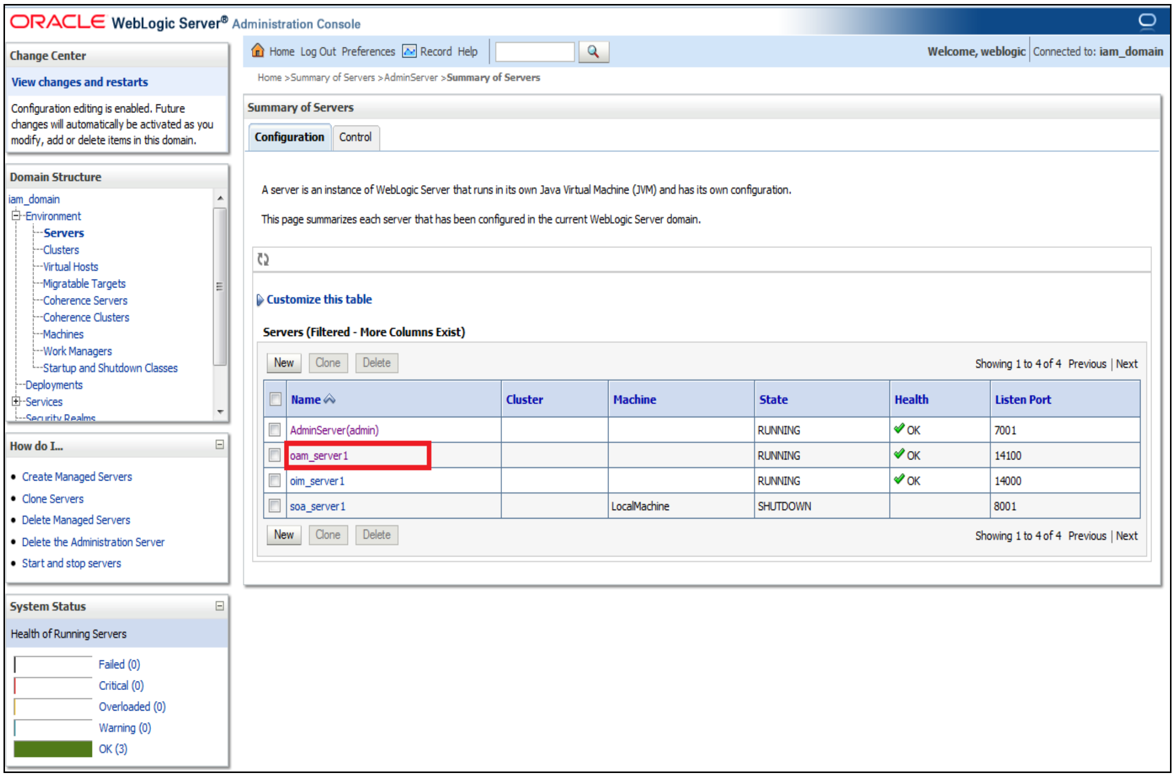
- Configure identity and trust
- Set up SSL
- Verify host name verification is enabled
- Configure a custom host name verifier
- Configure two-way SSL

Settings for AdminServer

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	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:	selfcert	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...

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



Home >Summary of Servers >AdminServer >Summary of Servers

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

How do I...

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

Summary of Servers

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

- Now the admin server and oam servers are SSL enabled. Restart both the servers.

2.6 Configuring SSO in OAM Console

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

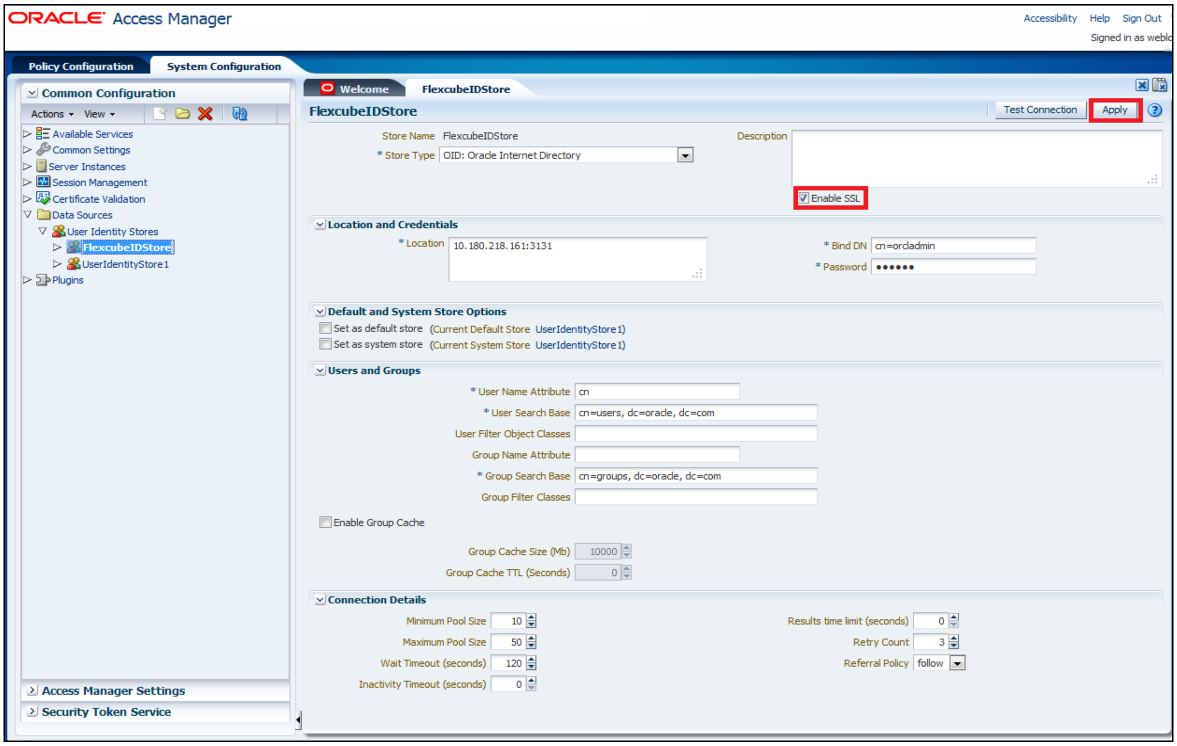
Follow the post installation scripts deployWebGate and EditHttpConf as provided in (http://docs.oracle.com/cd/E17904_01/install.1111/e12002/webgate004.htm

2.6.1 Identity Store Creation

2.6.1.1 To create new User Identity Store, Login to OAM Console and navigate to System Configuration>>Common configuration>>Data Sources>> User Identity Store

- Click New icon to create new Identity Store.
- Input below information in the new User Identity Store.
  - Choose Store Type as Oracle Internet Directory.
  - Location: LDAP server Host name and Port Number in <HOSTNAME>:PORT format
  - Select Enable SSL check box
  - Bind DN: User name to connect the LDAP Server
  - Password: Password to connect the LDAP Server
  - User Name Attribute: The attribute created in LDAP, which will be the User Name for the other application (here it will be treated as the FCUBS Username)
  - User Search Base: The container of the User Name in the LDAP server.
  - Group Search Base: The container of the Group Name in the LDAP server.
- Click on **Apply**.

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



FlexcubeIDStore

Store Name FlexcubeIDStore

* Store Type OID: Oracle Internet Directory

Description

☑ Enable SSL

Location and Credentials

* Location 10.180.218.161:3131

* Bind DN cn=orcladmin

* Password ••••••

Default and System Store Options

☐ Set as default store (Current Default Store UserIdentityStore1)

☐ Set as system store (Current System Store UserIdentityStore1)

Users and Groups

* User Name Attribute cn

* User Search Base cn=users, dc=oracle, dc=com

User Filter Object Classes

Group Name Attribute

* Group Search Base cn=groups, dc=oracle, dc=com

Group Filter Classes

☐ Enable Group Cache

Group Cache Size (Mb) 10000

Group Cache TTL (Seconds) 0

Connection Details

Minimum Pool Size 10

Maximum Pool Size 50

Wait Timeout (seconds) 120

Inactivity Timeout (seconds) 0

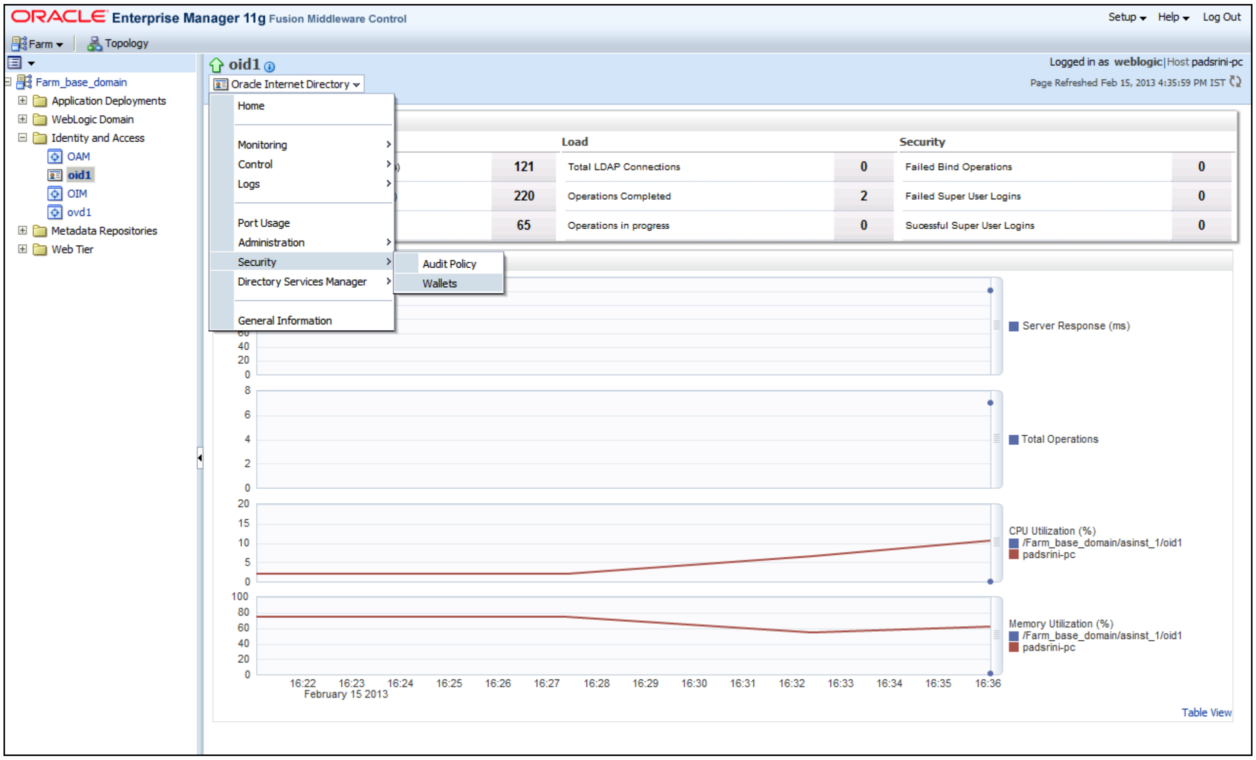
Results time limit (seconds) 0

Retry Count 3

Referral Policy follow

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

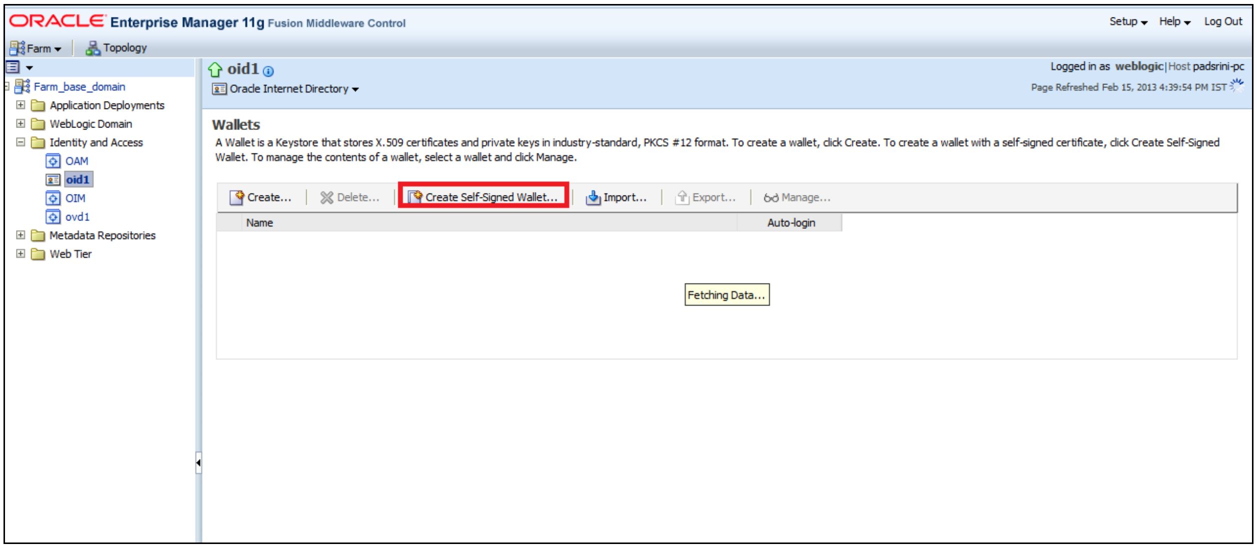


Logged in as weblogic|Host padsrini-pc

Page Refreshed Feb 15, 2013 4:35:59 PM IST

	Load		Security	
121	Total LDAP Connections	0	Failed Bind Operations	0
220	Operations Completed	2	Failed Super User Logins	0
65	Operations in progress	0	Sucessful Super User Logins	0

2. Click on **Create Self-Signed Wallet**



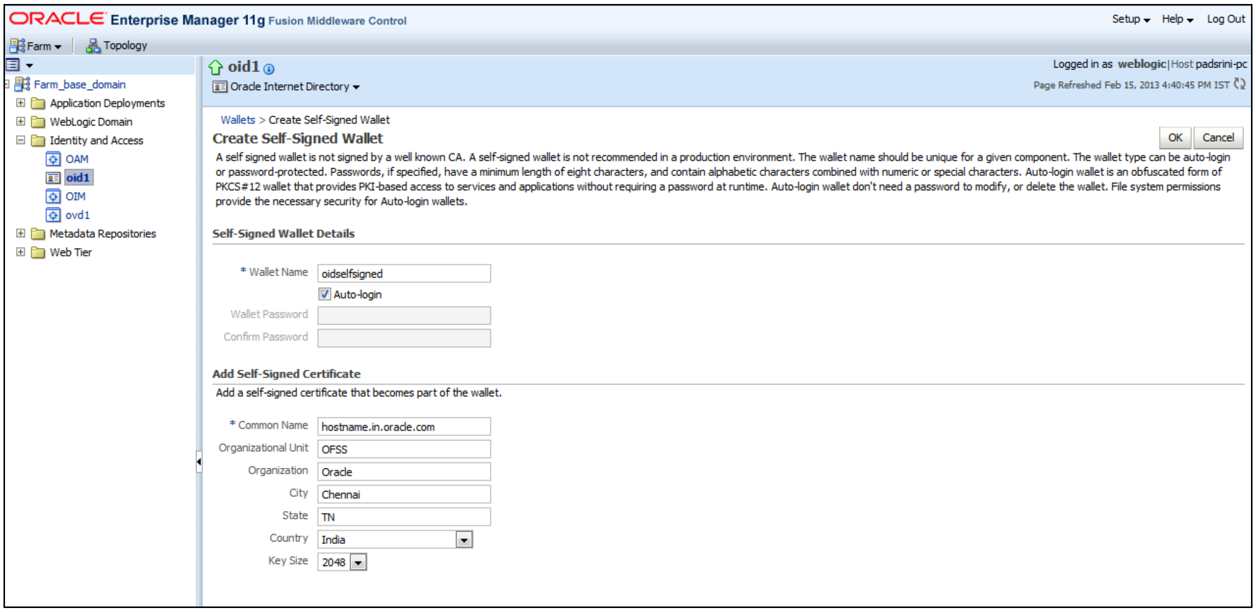
Logged in as **weblogic**|Host padsrini-pc

Page Refreshed Feb 15, 2013 4:39:54 PM IST

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 & Click on **OK**



Logged in as **weblogic**|Host padsrini-pc

Page Refreshed Feb 15, 2013 4:40:45 PM IST

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.

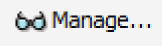
Self-Signed Wallet Details

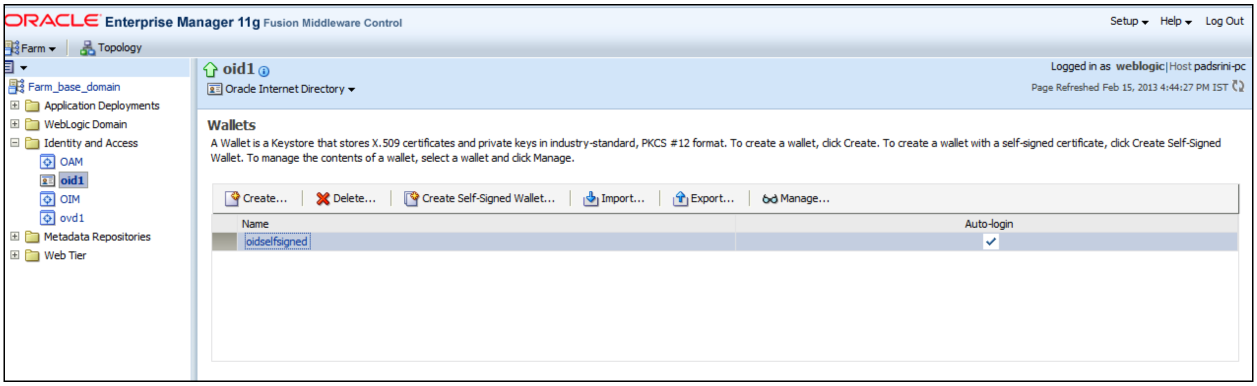
* Wallet Name	oidselfsigned
	☑ Auto-login
Wallet Password	
Confirm Password	

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 on 

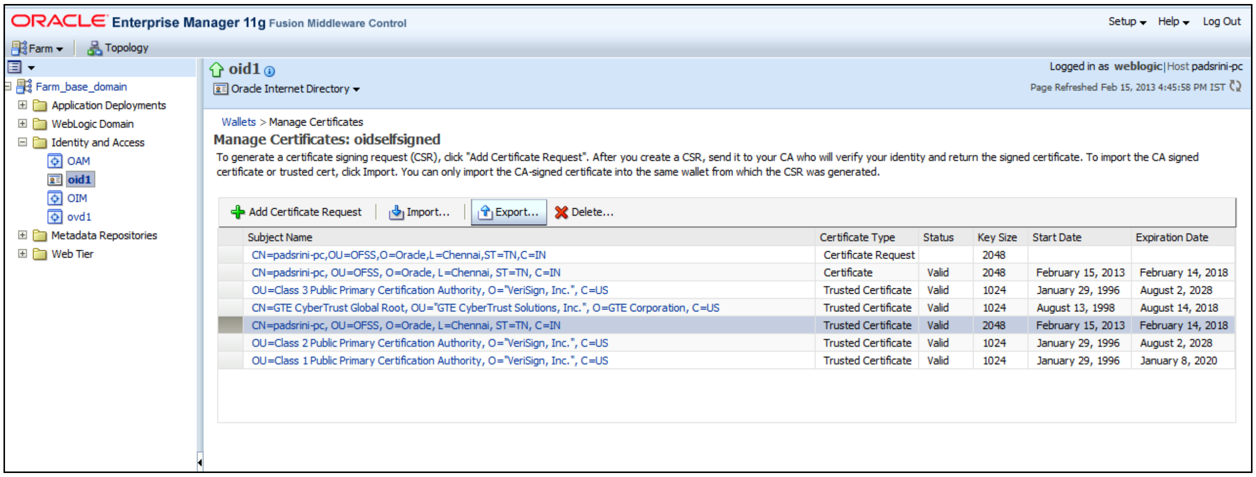

ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup Help Log Out
Farm Topology
Farm_base_domain
Application Deployments
WebLogic Domain
Identity and Access
OAM
oid1
OIM
ovd1
Metadata Repositories
Web Tier
oid1
Oracle Internet Directory
Logged in as weblogic | Host padsrini-pc
Page Refreshed 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 & Click on Export

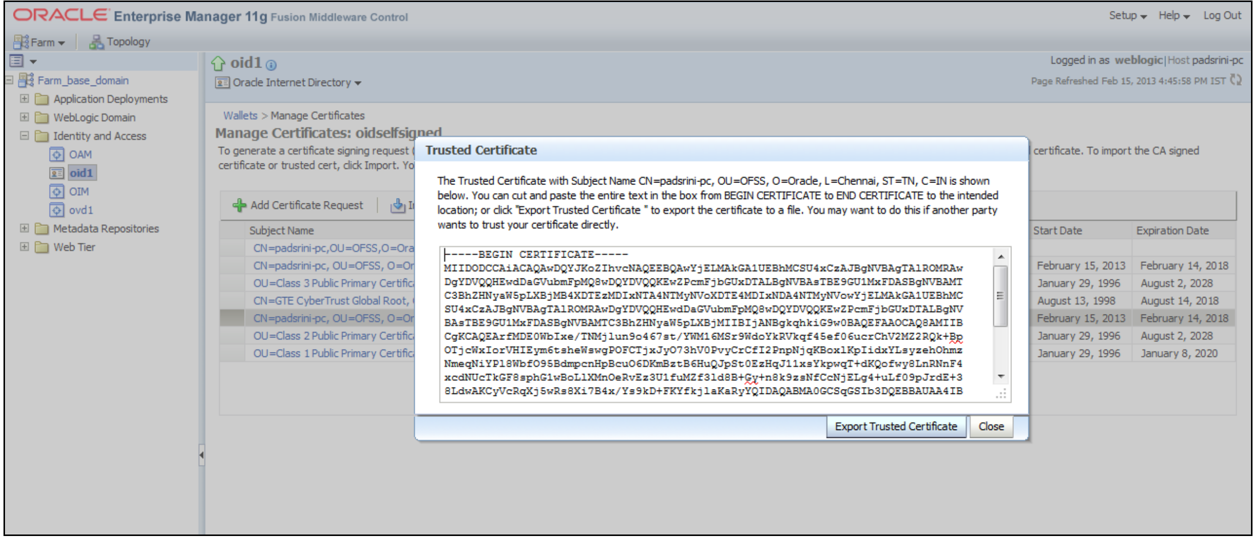

ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup Help Log Out
Farm Topology
Farm_base_domain
Application Deployments
WebLogic Domain
Identity and Access
OAM
oid1
OIM
ovd1
Metadata Repositories
Web Tier
oid1
Oracle Internet Directory
Logged in as weblogic | Host padsrini-pc
Page Refreshed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

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

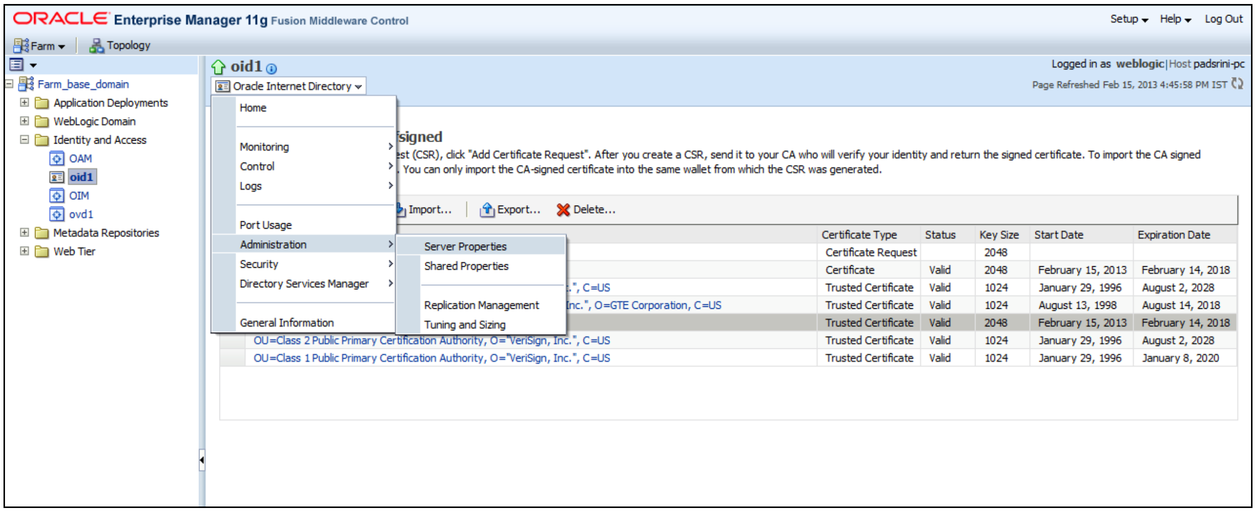
6. Click Export Trusted Certificate and save the certificate file.


ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup Help Log Out
Farm Topology
Trusted Certificate
Export Trusted Certificate
Close

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-----
MIIDODCCAiACAQAwDQYJKoZIhvcNAQEEBQAwYjELMAkGA1UEBhMCSU4xCzAJBgNVBAgTAlROMRAw
DgYDVQQHEwdDaGVubmFpMQ8wDQYDVQQKEwZPcmFjbGUxDTALBgNVBAsTBE9GU1MxFDASBgNVBAMT
C3BhZHNyaW5pLXBjMB4XDTEzMDIxNTA4NTMyNVoXDTE4MDIxNDA4NTMyNVowYjELMAkGA1UEBhMC
SU4xCzAJBgNVBAgTAlROMRAwDgYDVQQHEwdDaGVubmFpMQ8wDQYDVQQKEwZPcmFjbGUxDTALBgNV
BAsTBE9GU1MxFDASBgNVBAMTC3BhZHNyaW5pLXBjMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArfMDE0WbIxe/TNMjlun9o467st/YWM16MSr9WdoYkRVkqf45ef06ucrChV2MZ2RQk+Bp
OTjcWxIorVHIEym6tsheWswgPOFCTjxJyO73hV0PvyCrCfI2PnpNjqKBoxlKpIidxYLsyzehOhmz
NmeqNiYPl8WbfO95BdmpcnHpBcuO6DKmBztB6HuQJpSt0EzHqJ11xsYkpwqT+dKQofwy8LnRNnF4
xcdNUcTkGF8sphG1wBoLlXMnOeRvEz3U1fuMZf3ld8B+Gy+n8k9zsNfCcNjELg4+uLf09pJrdE+3
8LdwAKCyVcRqXj5wRs8Xi7B4x/Ys9kD+FKYfkjlaKaRyYQIDAQABMA0GCSqGSIb3DQEBBAUAA4IB
```

7. Click on Server Properties



Logged in as weblogic|Host padsrini-pc

Page Refreshed Feb 15, 2013 4:45:58 PM IST

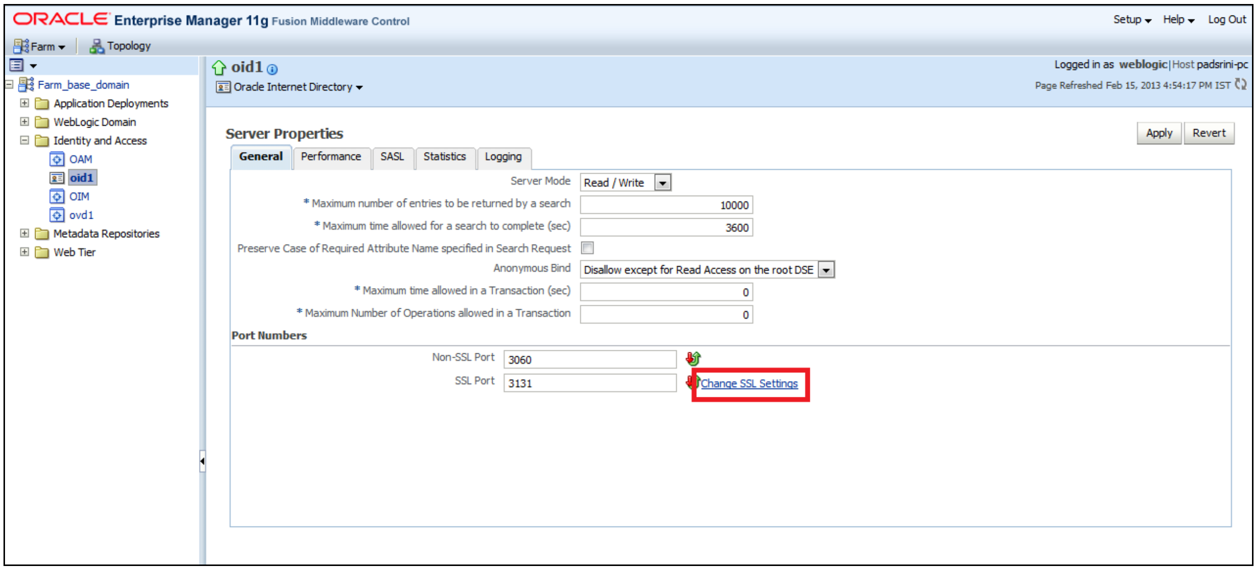
signed

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 on Change SSL Settings



Logged in as weblogic|Host padsrini-pc

Page Refreshed Feb 15, 2013 4:54:17 PM IST

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

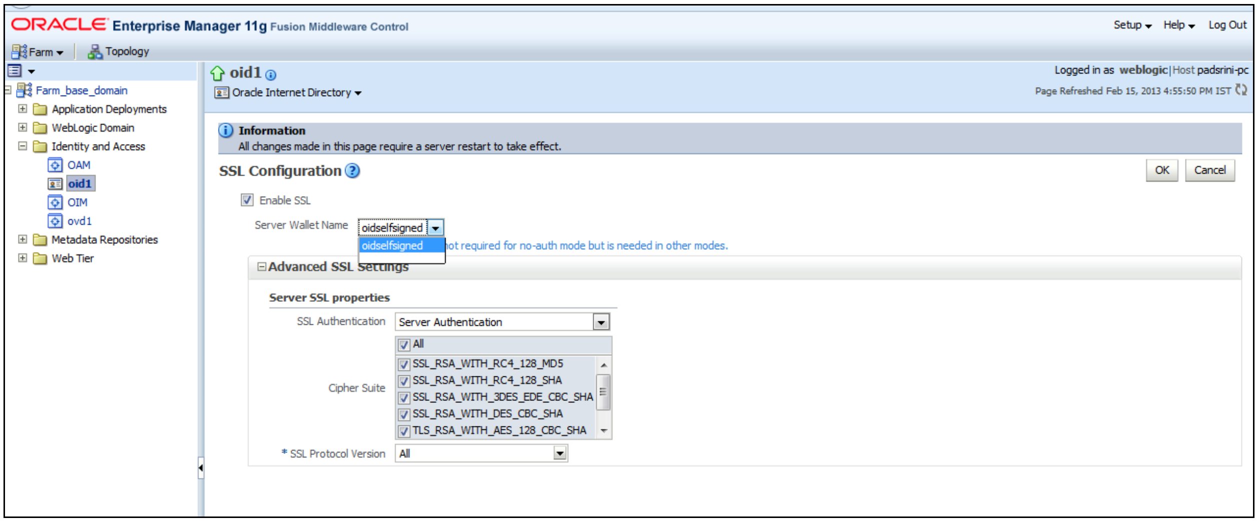
* Maximum Number of Operations allowed in a Transaction: 0

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 & Click on OK



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

SSL Configuration

☑ Enable SSL

Server Wallet Name: oidselfsigned

ot required for no-auth mode but is needed in other modes.

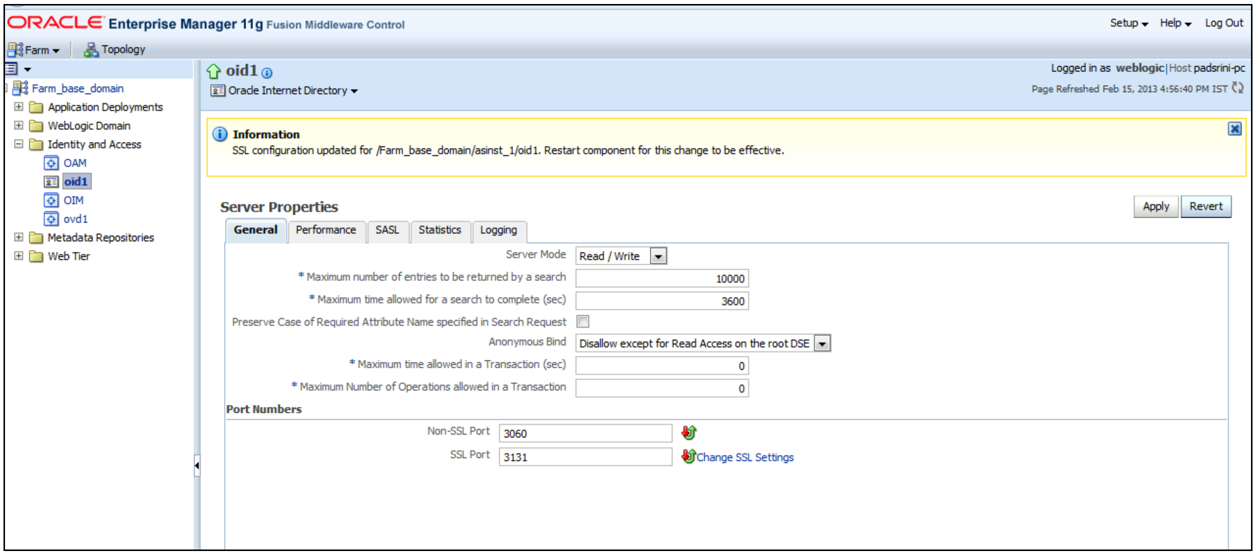
Server SSL properties

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 on Apply.



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

11. **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**"

    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.

12. **Import LDAP Server SSL Certificate into OIM Server**

    Import the Exported Certificate into **wlserver_10.3/server/lib/DemoTrust.jks** of OIM Server Domain using the below command [Store Password is **DemoTrustKeyStorePassPhrase**]

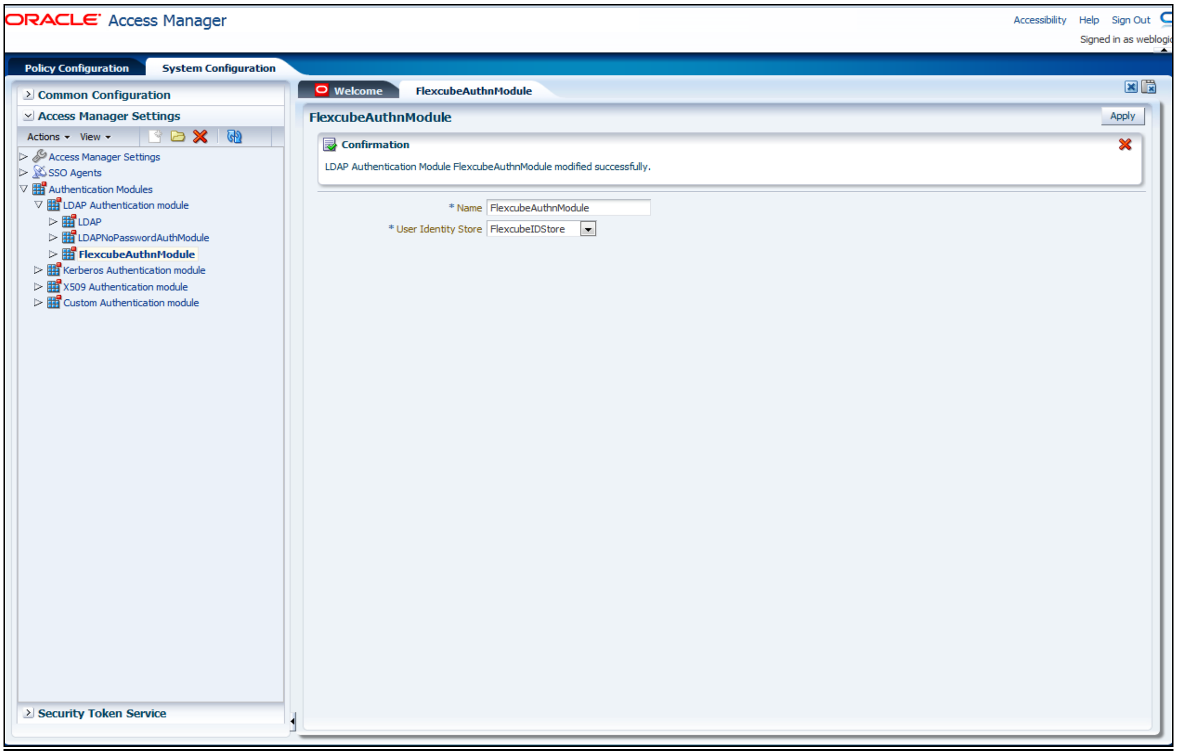
```
keytool -import -keystore MW_HOME/wlserver_10.3/server/lib/DemoTrust.jks -
file /home/testoc4j/OIM/globalv.crt -storepass DemoTrustKeyStorePassPhrase
```

Restart Both OID & OIM Server.

2.6.2 Creating Authentication Module

Navigate to **System Configuration >> Access Manager Settings >> Authentication Modules >> LDAP Authentication Module**

Click New Button to create new Authentication Module. Input the Name of the authentication module and choose the User Identity Store we created in step 1.



FlexcubeAuthnModule

Confirmation

LDAP Authentication Module FlexcubeAuthnModule modified successfully.

* Name: FlexcubeAuthnModule

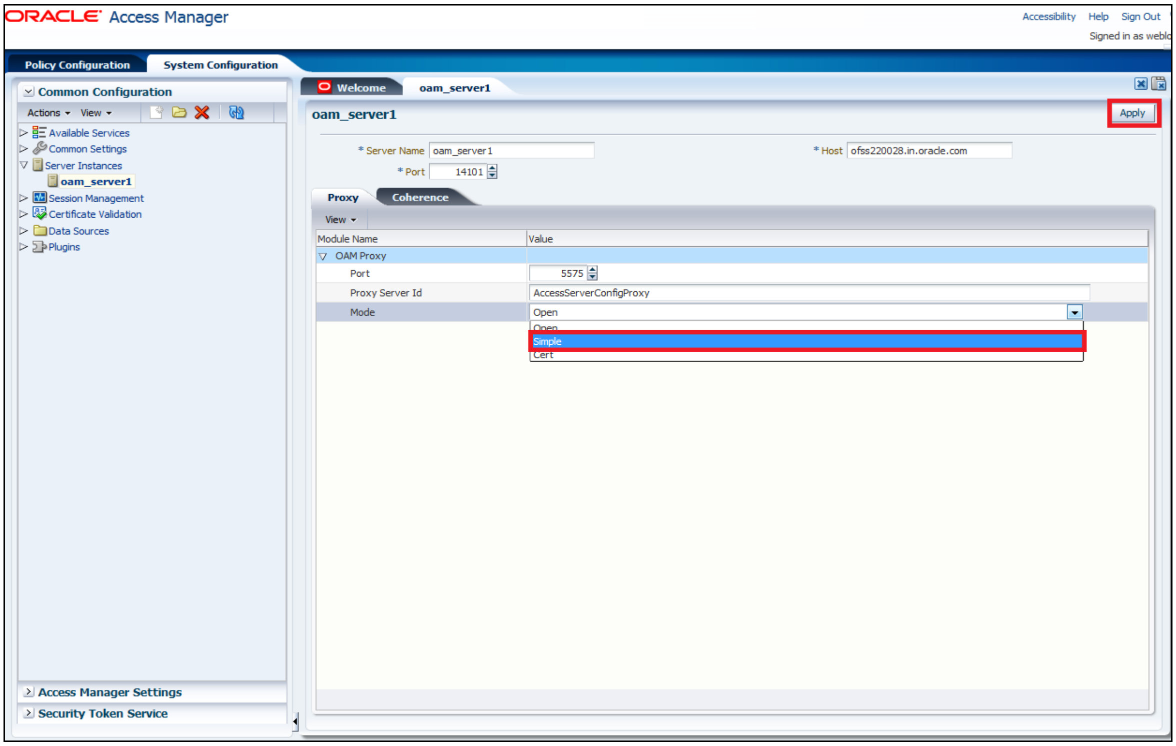
* User Identity Store: FlexcubeIDStore

2.6.3 Creating OAM 11g Webgate

Navigate to **System Configuration→Common Configuration→Server Instances→ oam_server1**

Change the Mode under Proxy Tab to Simple.

Click on Apply.



oam_server1

* Server Name oam_server1

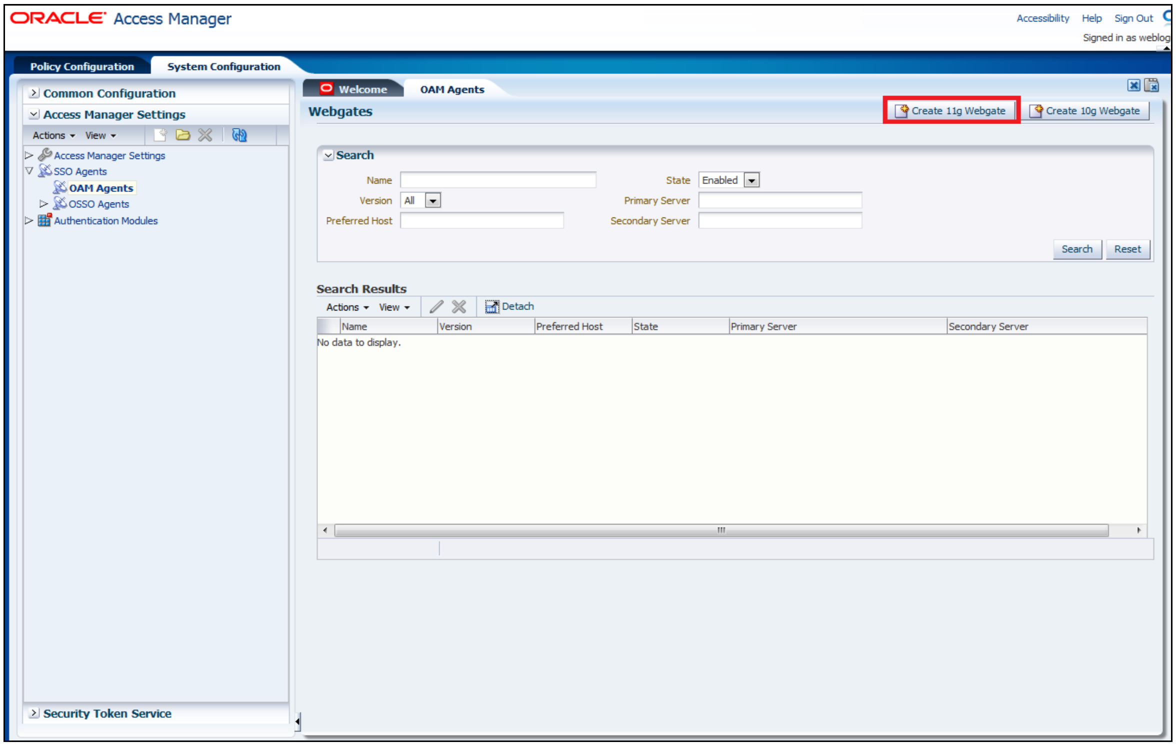
* Host ofss220028.in.oracle.com

* Port 14101

Module Name	Value
OAM Proxy	
Port	5575
Proxy Server Id	AccessServerConfigProxy
Mode	Open

Navigate to **System Configuration>>Access Manager Settings>>SSO Agents>>OAM Agents**.

Click on Create 11g Webgate.



Webgates

Search

Name

Version All

Preferred Host

State Enabled

Primary Server

Secondary Server

Search Results

Name	Version	Preferred Host	State	Primary Server	Secondary Server

No data to display.

Enter the Custom Webgate Name in **Name**

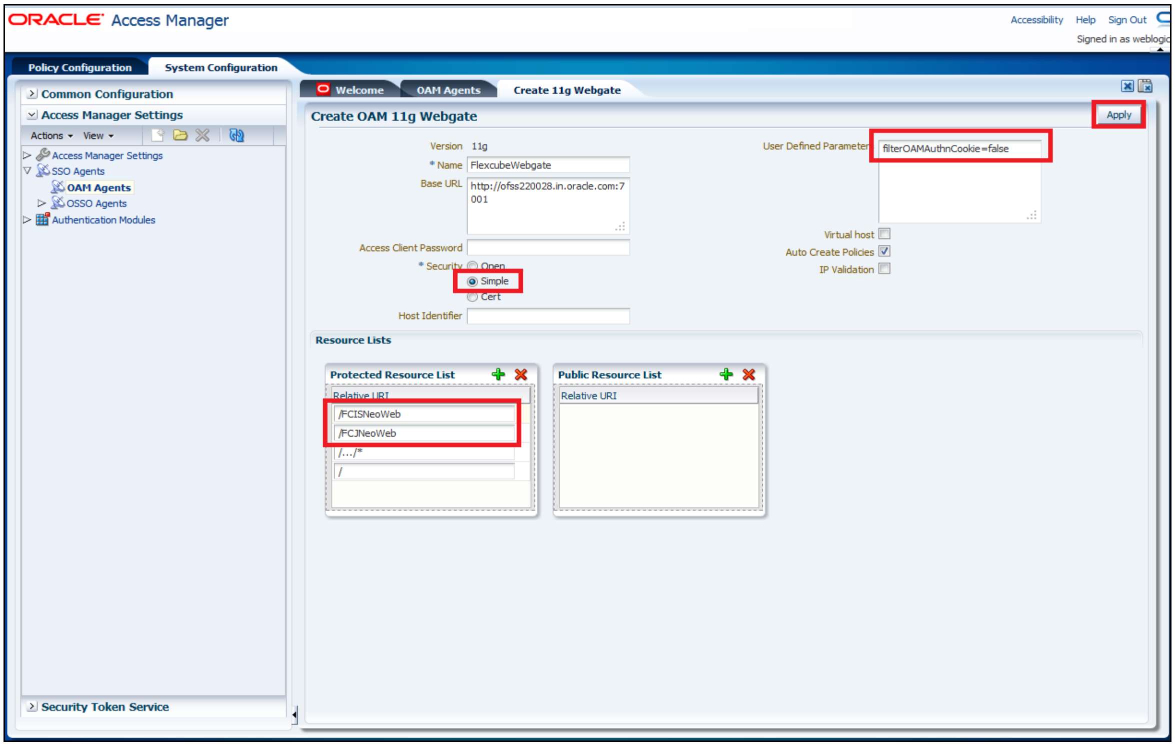
Enter the **Base URL** as in Weblogic Server's non-ssl URL

Select **Security** as **Simple**

Add the application context root under **Protected Resource List,** which we have to enable SSO

Add **filterOAMAuthnCookie=false** in **User Defined Parameters**

Click on **Apply**.



Create OAM 11g Webgate

Version 11g

* Name FlexcubeWebgate

Base URL http://ofss220028.in.oracle.com:7001

Access Client Password

* Security ○ Open ● Simple ○ Cert

Host Identifier

User Defined Parameter filterOAMAuthnCookie=false

Virtual host □

Auto Create Policies ☑

IP Validation □

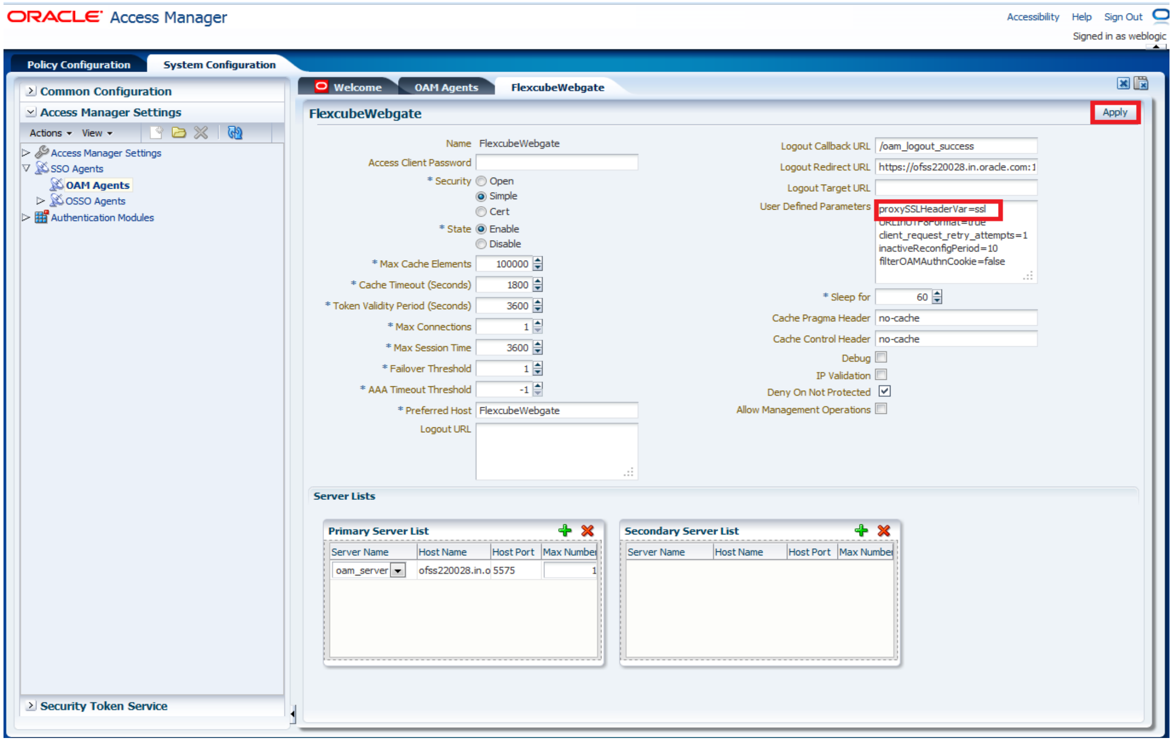
Resource Lists

Protected Resource List
Relative URI
/FCISNeoWeb
/FCJNeoWeb
/…/*
/

Public Resource List
Relative URI

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

Click on **Apply**.



FlexcubeWebgate

Name FlexcubeWebgate

Access Client Password

* Security ○ Open ● Simple ○ Cert

* State ● Enable ○ Disable

* Max Cache Elements 100000

* Cache Timeout (Seconds) 1800

* Token Validity Period (Seconds) 3600

* Max Connections 1

* Max Session Time 3600

* Failover Threshold 1

* AAA Timeout Threshold -1

* Preferred Host FlexcubeWebgate

Logout URL

Logout Callback URL /oam_logout_success

Logout Redirect URL https://ofss220028.in.oracle.com:1

Logout Target URL

User Defined Parameters

```
proxySSLHeaderVar=ssl
URLInUTF8Format=true
client_request_retry_attempts=1
inactiveReconfigPeriod=10
filterOAMAuthnCookie=false
```

* Sleep for 60

Cache Pragma Header no-cache

Cache Control Header no-cache

Debug □

IP Validation □

Deny On Not Protected ☑

Allow Management Operations □

Server Lists

Primary Server List

Server Name	Host Name	Host Port	Max Number
oam_server	ofss220028.in.o	5575	1

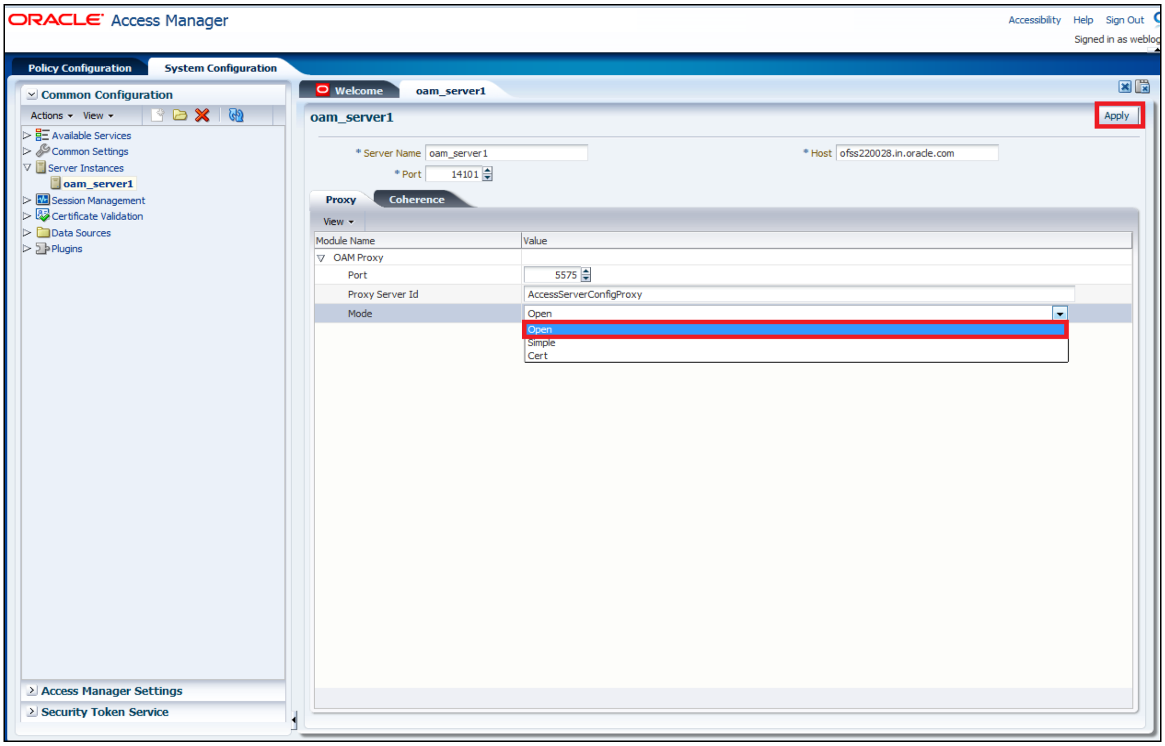
Secondary Server List

Server Name	Host Name	Host Port	Max Number

Navigate to **System Configuration→Common Configuration→Server Instances→ oam_server1**

Change the Mode under **Proxy Tab** to Open.

Click on **Apply.**



oam_server1

* Server Name oam_server1

* Host ofss220028.in.oracle.com

* Port 14101

Module Name	Value
OAM Proxy	
Port	5575
Proxy Server Id	AccessServerConfigProxy
Mode	Open

Open
Simple
Cert

2.6.4 Post OAM Webgate 11g Creation Steps

Perform the following steps to copy the artifacts to the Webgate installation directory:

2.6.4.1 On the Oracle Access Manager Console host, locate the OAM Agent folder

<DOMAIN_HOME>/output/$Agent_Name

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

ObAccessClient.xml

password.xml

cwallet.sso

And copy remaining below files to <ORACLE_MIDDLEWARE>/<ORACLE_WIBTIER_HOME> /instances/instance1/ config/OHS/ohs1/webgate/config/simple

aaa_key.pem

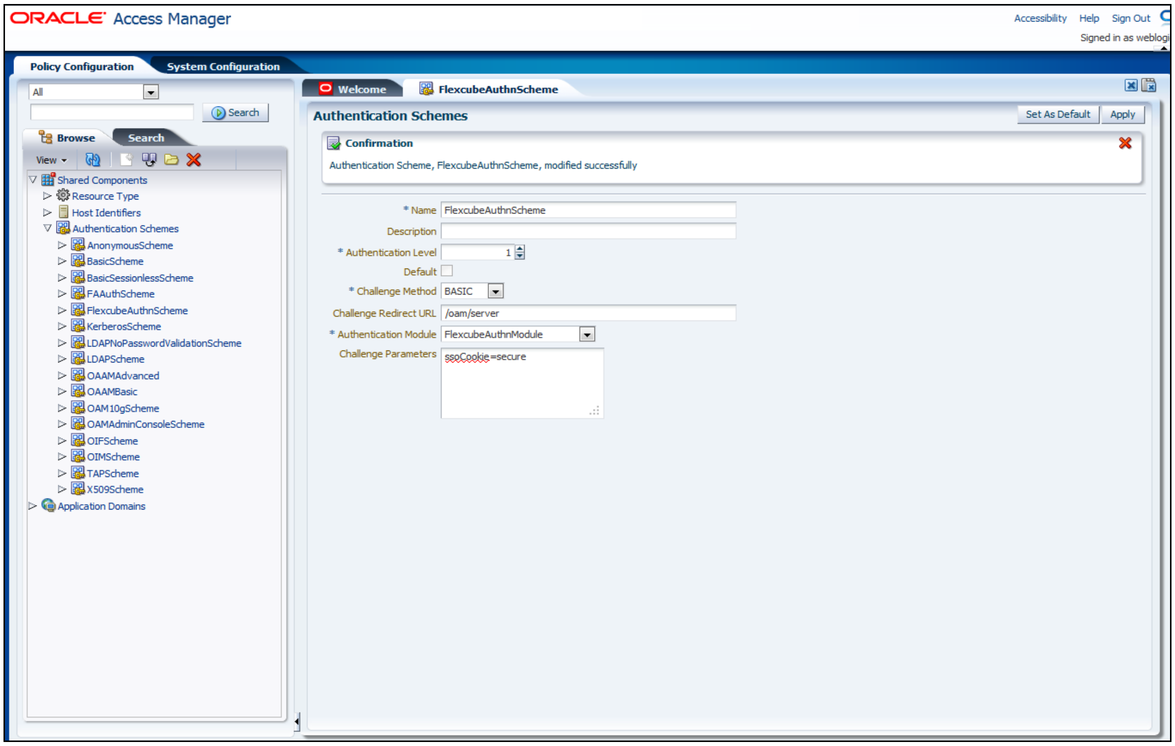
aaa_cert.pem

2.6.4.2 Creating Authentication Scheme

To create Authentication Scheme navigate to Policy Configuration >> Authentication Schemes

Click on Create button to create new Authentication Scheme.

Name	: Any name to identify Authentication Scheme
Authentication Level	: 1
Challenge Method	: BASIC
Challenge Redirect URL	: /oam/server
Authentication Module	: Choose the authentication module created in step 2.
Challenge Parameters	: ssoCookie=secure



Authentication Schemes

Confirmation

Authentication Scheme, FlexcubeAuthnScheme, modified successfully

* Name	FlexcubeAuthnScheme
Description	
* Authentication Level	1
Default	□
* Challenge Method	BASIC
Challenge Redirect URL	/oam/server
* Authentication Module	FlexcubeAuthnModule
Challenge Parameters	ssoCookie=secure

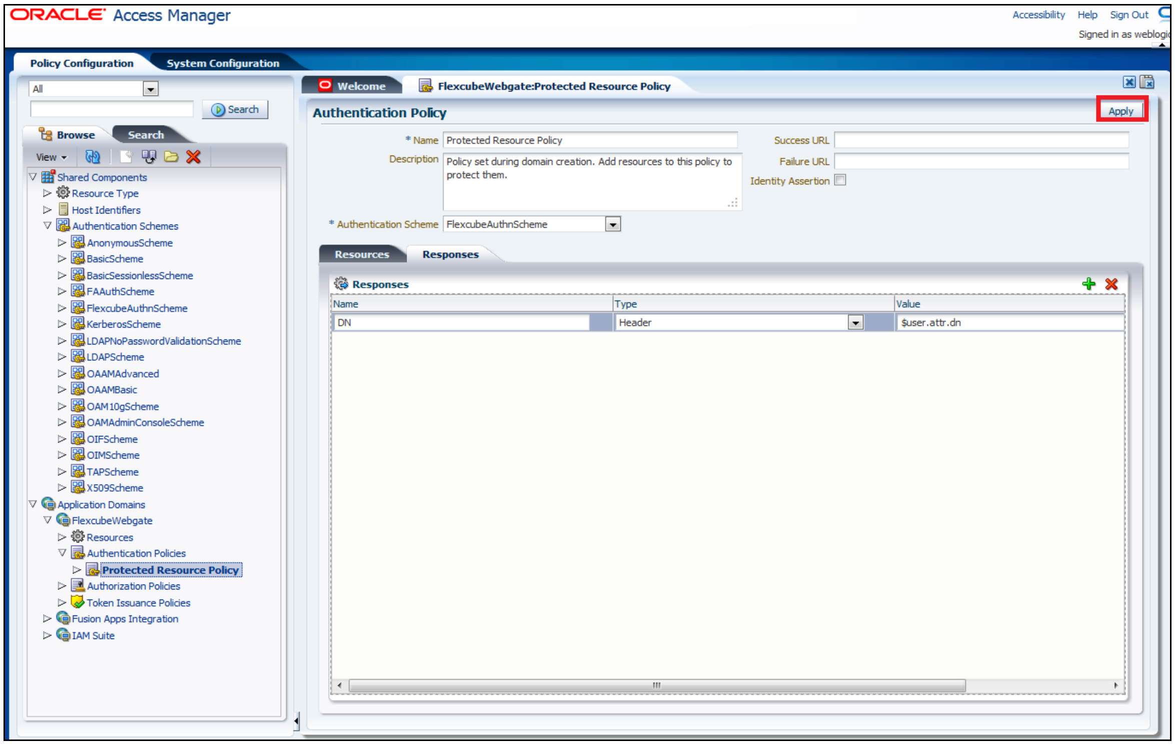
If it is a basic authentication scheme, we need to add the 'enforce-valid-basic-auth-credentials' tag to the config.xml file located under <weblogic deployment path>/user_projects/domains/<MyDomain>/config/. The tag must be inserted within the <security-configuration> tag as follows: [Just above </security-configuration> tag]

<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>

2.6.4.3 Application Domains Changes

Navigate to **Policy Configuration >> Application Domains >> [Webgate agent name] >> Authentication Policies>>Protected Resource Policy.**

- Click on Responses Tab
- Choose the Authentication Scheme created in step 5.
- Add a Response as: Name : DN Type : Header Value : $user.attr.dn
- Click on Apply.



Authentication Policy

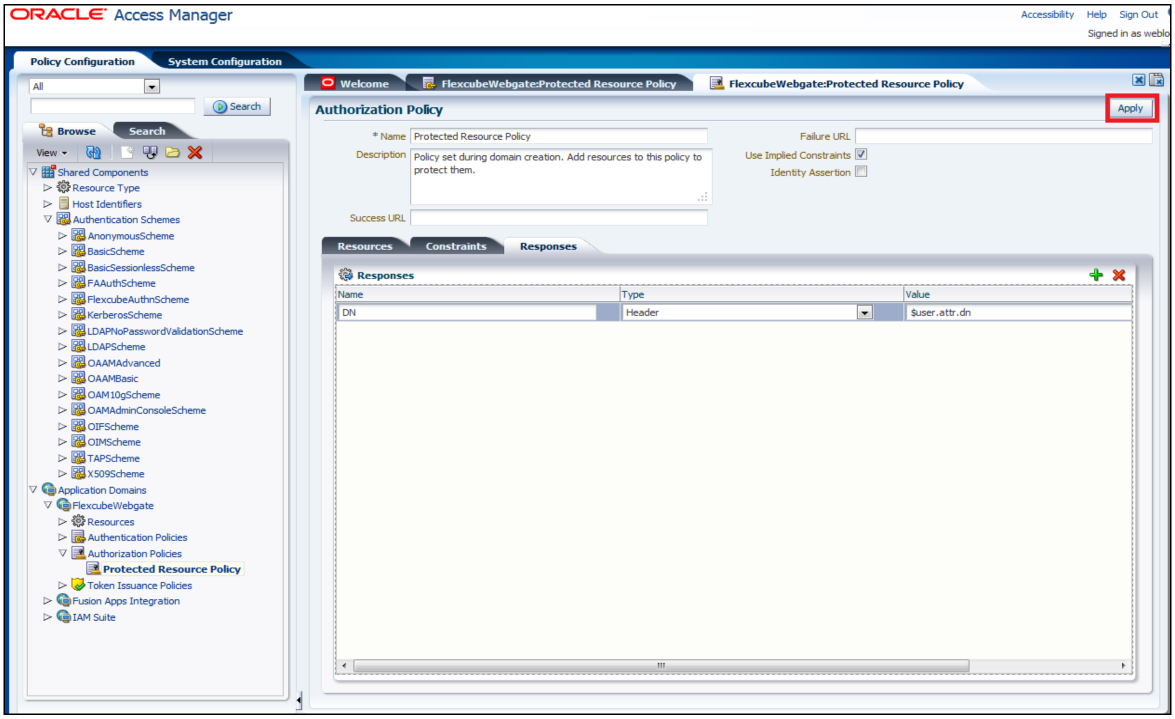
* Name	Protected Resource Policy	Success URL	
Description	Policy set during domain creation. Add resources to this policy to protect them.	Failure URL	
		Identity Assertion	☐
* Authentication Scheme	FlexcubeAuthnScheme		

Responses

Name	Type	Value
DN	Header	$user.attr.dn

Navigate to **Policy Configuration >> Application Domains >> [Webgate agent name] >> Authorization Policies>>Protected Resource Policy.**

- Click on Responses Tab
- Add a Response as: Name : DN Type : Header Value : $user.attr.dn
- Click on Apply.



Authorization Policy

* Name	Protected Resource Policy	Failure URL	
Description	Policy set during domain creation. Add resources to this policy to protect them.	Use Implied Constraints	☑
		Identity Assertion	☐
Success URL			

Responses

Name	Type	Value
DN	Header	$user.attr.dn

2.6.4.4 Add the Application Certificates to Oracle HTTP Server to work with 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

2.6.4.5 Configuring mod_wl_ohs for Oracle HTTP server Routing

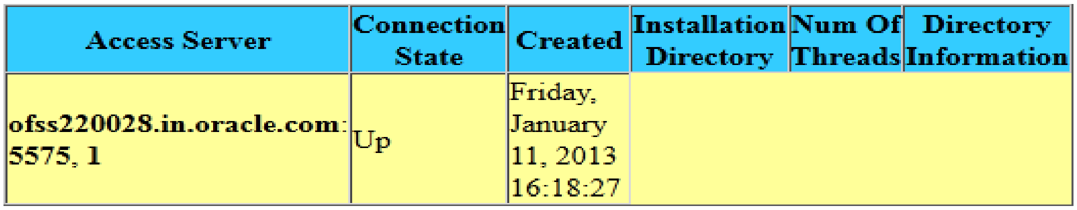
To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server, add the directive shown below to the mod_wl_ohs.conf file available in <ORACLE_MIDDLEWARE> /<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1.

```
<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/ohs
        1/keystores/default"
</Location>
```

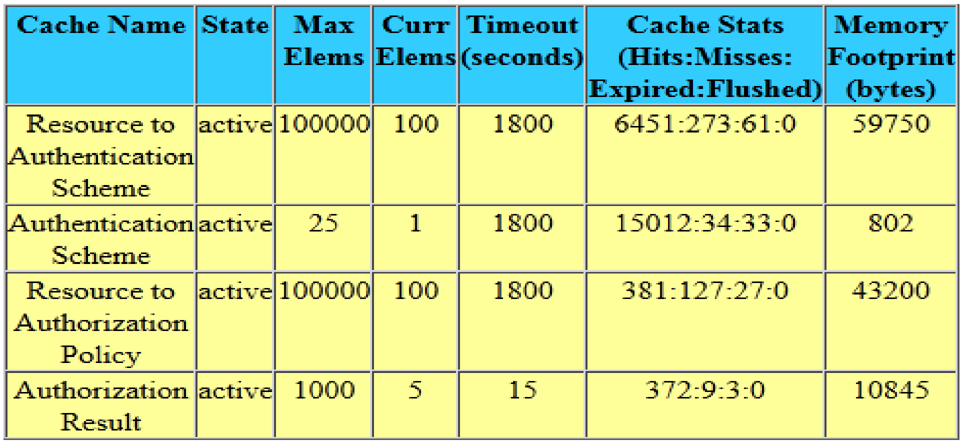
Note: in the above example, ofss00002.in.oracle.com is the server name where the Flexcube Application deployed, 7002 is the SSL port and FCJNeoWeb is the context root of the FLEXCUBE application

2.6.4.6 Checking the Webgate 11g Agent Creation

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



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			



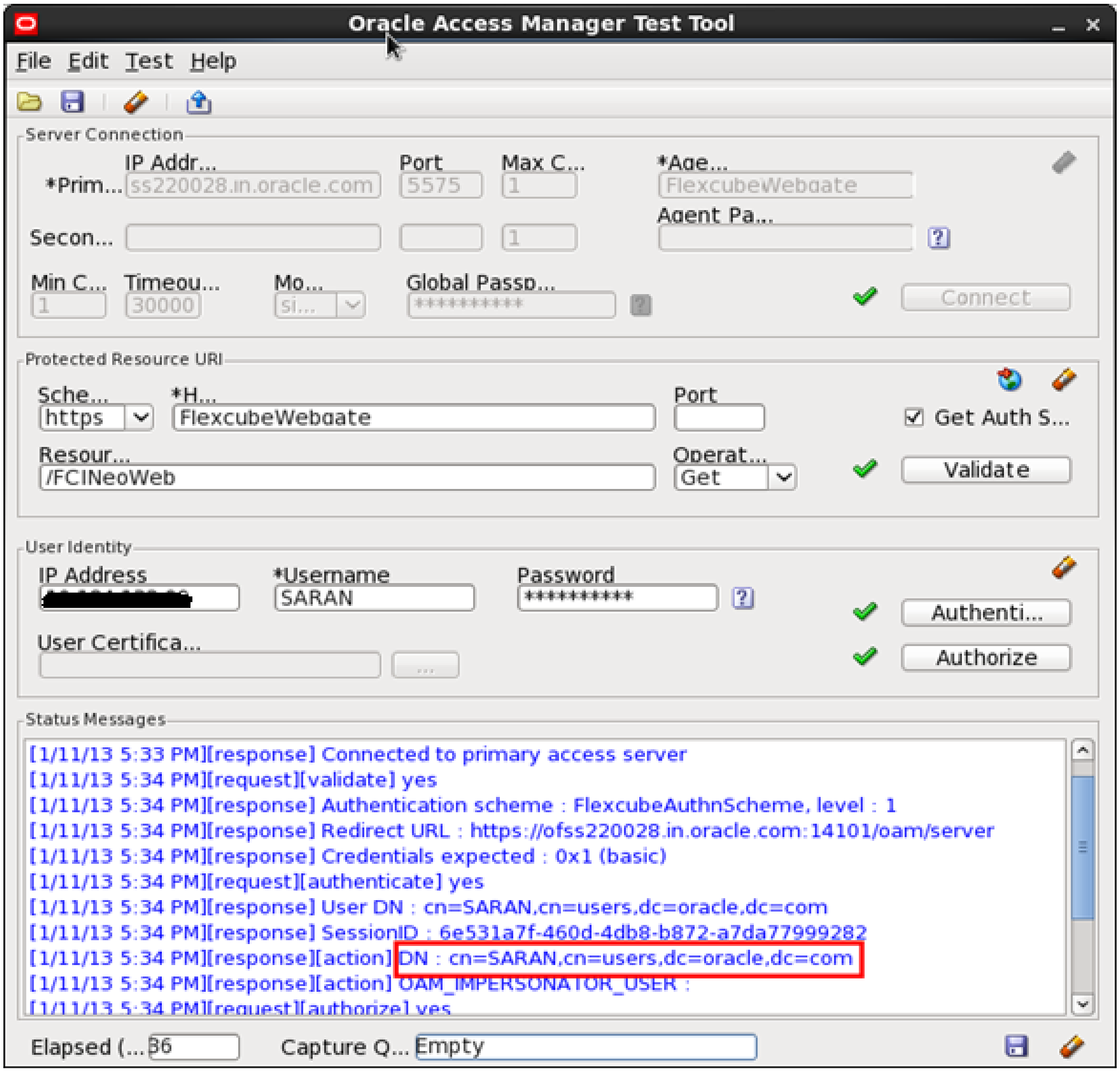
Cache Name	State	Max Elems	Curr Elems	Timeout (seconds)	Cache Stats (Hits:Misses: Expired:Flushed)	Memory Footprint (bytes)
Resource to Authentication Scheme	active	100000	100	1800	6451:273:61:0	59750
Authentication Scheme	active	25	1	1800	15012:34:33:0	802
Resource to Authorization Policy	active	100000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

2.6.4.7 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.



Server Connection

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

Secon... 1 Agent Pa...

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

Protected Resource URI

Sche... https *H... FlexcubeWebgate Port

☑ Get Auth S...

Resour... /FCINeoWeb Operat... Get

User Identity

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

User Certifica...

Status Messages

```
[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
```

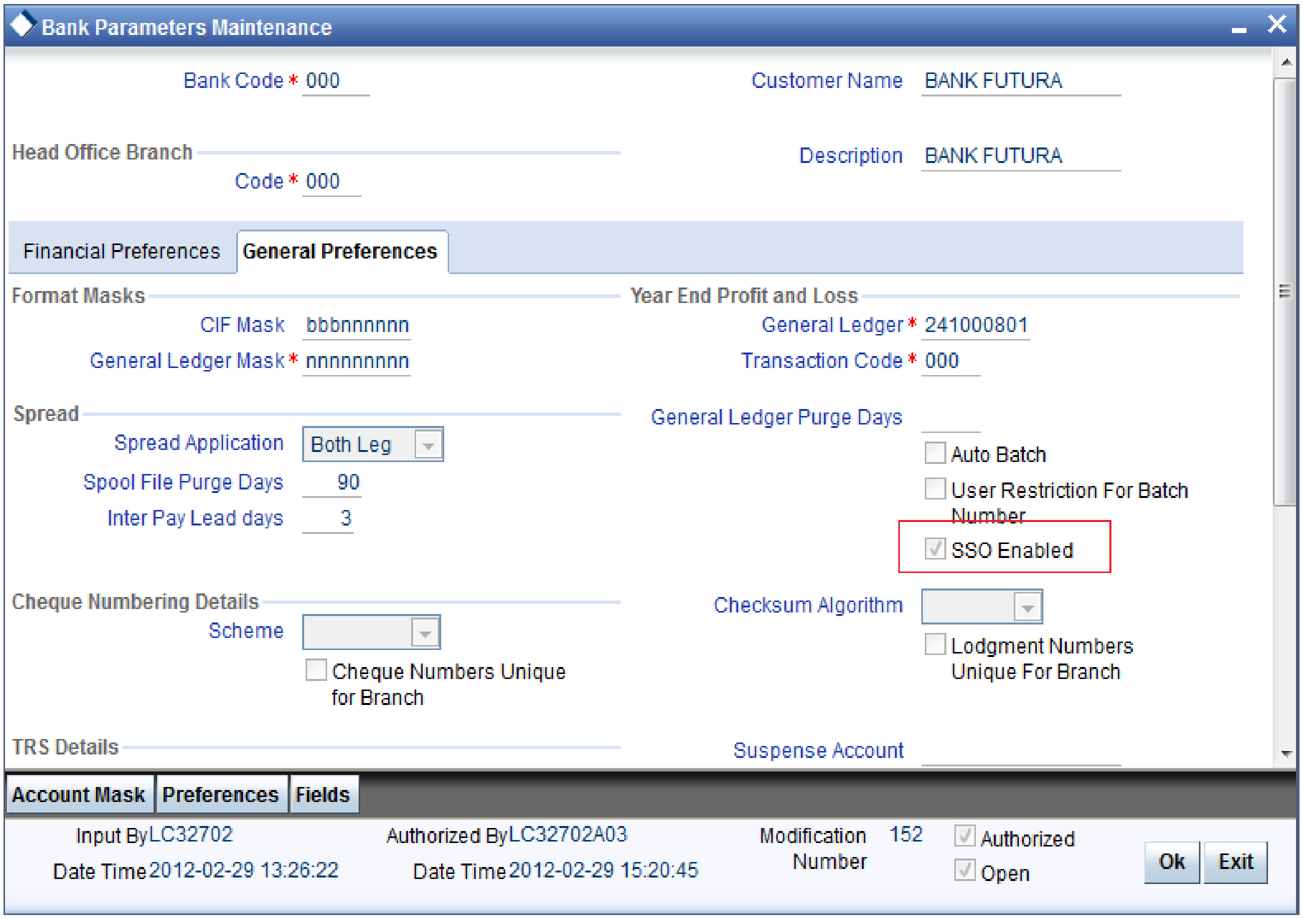
Elapsed (... 36 Capture Q... Empty

2.7 First launch of FLEXCUBE after installation

After installing FLEXCUBE and while launching it for first time, the normal FCUBS login screen with userid and password will appear, this is because when installing the ‘sso installed’ parameter will be set to ‘N’.

2.7.1 Bank Parameter maintenance

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



Bank Code * 000

Customer Name BANK FUTURA

Head Office Branch

Code * 000

Description BANK FUTURA

Format Masks

CIF Mask bbbnnnnnn

General Ledger Mask * nnnnnnnnn

Year End Profit and Loss

General Ledger * 241000801

Transaction Code * 000

Spread

Spread Application Both Leg

Spool File Purge Days 90

Inter Pay Lead days 3

General Ledger Purge Days

□ Auto Batch

□ User Restriction For Batch Number

☑ SSO Enabled

Cheque Numbering Details

Scheme

□ Cheque Numbers Unique for Branch

Checksum Algorithm

□ Lodgment Numbers Unique For Branch

TRS Details

Suspense Account

Input By LC32702

Date Time 2012-02-29 13:26:22

Authorized By LC32702A03

Date Time 2012-02-29 15:20:45

Modification Number 152

☑ Authorized

☑ Open

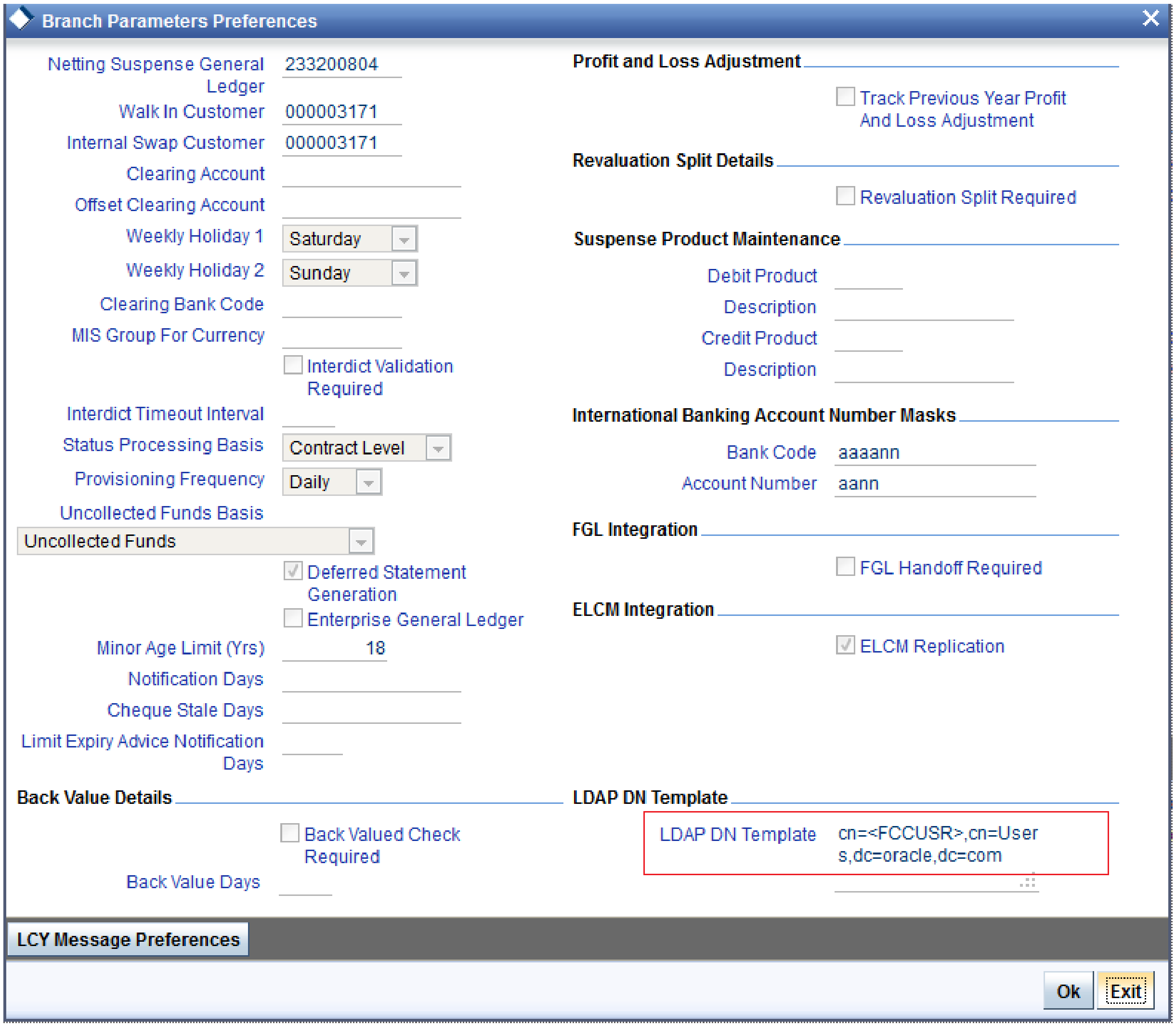
2.7.2 Maintaining Branch Level DN Template (Branch Maintenance)

Go to the “Branch Maintenance” of FLEXCUBE UBS.

For each branch LDAP DN template should be maintained, which is used in the FLEXCUBE user maintenance Form to populate corresponding LDAP userid automatically from this template. Go to branch level parameter screen and Click on Preferences Icon.

E.g.: LDAP DN Template: cn=<FCJUSR>,cn=Users,dc=i-flex,dc=com

Here in this above template cn=<FCJUSR> part preferably must be there and it should not be altered, but the rest of the DN name can change based on the configuration.



Branch Parameters Preferences

Netting Suspense General Ledger: 233200804

Walk In Customer: 000003171

Internal Swap Customer: 000003171

Clearing Account:

Offset Clearing Account:

Weekly Holiday 1: Saturday

Weekly Holiday 2: Sunday

Clearing Bank Code:

MIS Group For Currency:

□ Interdict Validation Required

Interdict Timeout Interval:

Status Processing Basis: Contract Level

Provisioning Frequency: Daily

Uncollected Funds Basis: Uncollected Funds

☑ Deferred Statement Generation

□ Enterprise General Ledger

Minor Age Limit (Yrs): 18

Notification Days:

Cheque Stale Days:

Limit Expiry Advice Notification Days:

Back Value Details

□ Back Valued Check Required

Back Value Days:

Profit and Loss Adjustment

□ Track Previous Year Profit And Loss Adjustment

Revaluation Split Details

□ Revaluation Split Required

Suspense Product Maintenance

Debit Product:

Description:

Credit Product:

Description:

International Banking Account Number Masks

Bank Code: aaaann

Account Number: aann

FGL Integration

□ FGL Handoff Required

ELCM Integration

☑ ELCM Replication

LDAP DN Template

LDAP DN Template: cn=<FCCUSR>,cn=Users,dc=oracle,dc=com

2.7.3 Maintaining LDAP DN for FCUBS users

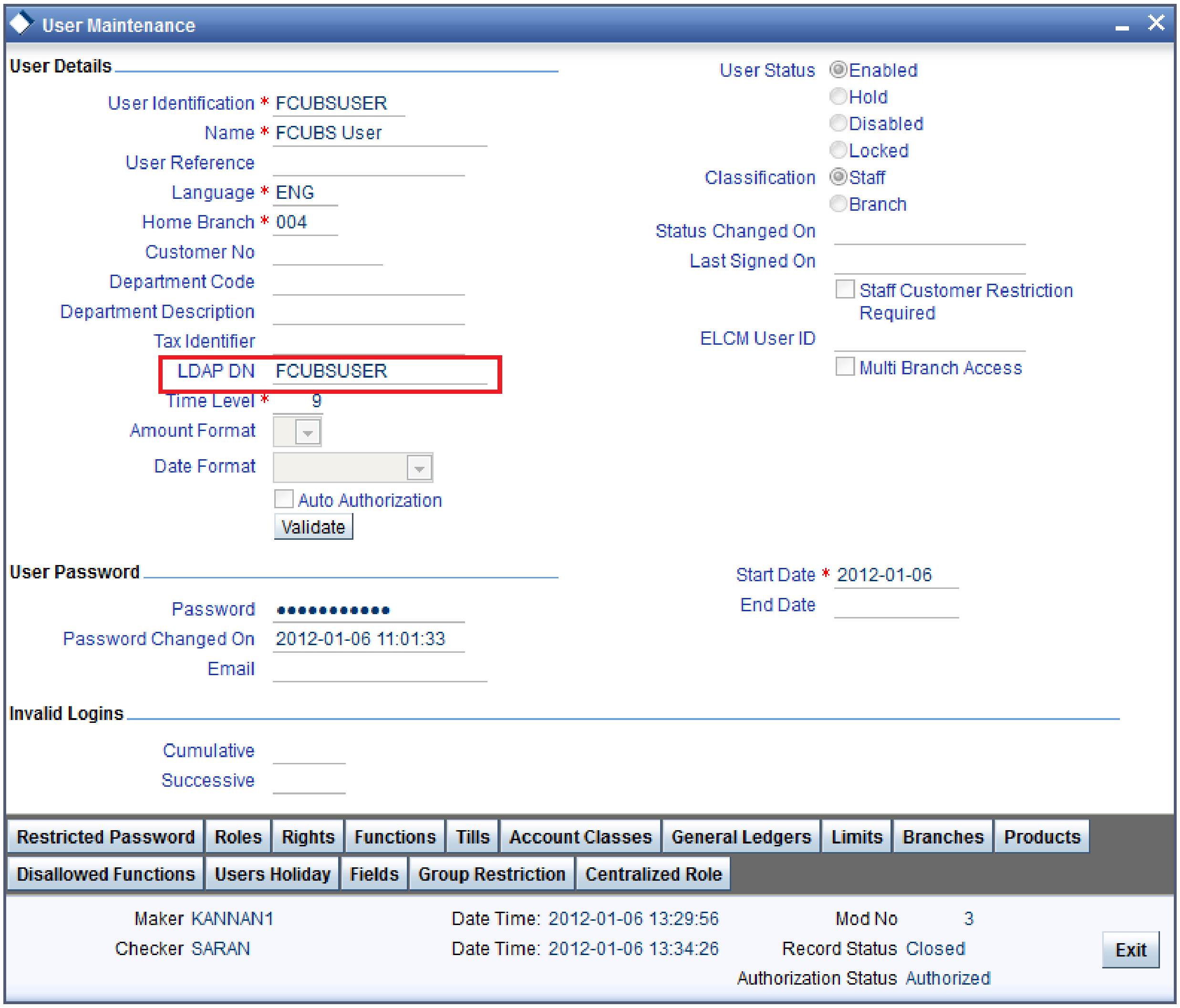
For each user id in FCUBS a user has to be created in the LDAP.

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



User Maintenance

User Details

User Identification * FCUBSUSER

Name * FCUBS User

User Reference

Language * ENG

Home Branch * 004

Customer No

Department Code

Department Description

Tax Identifier

LDAP DN FCUBSUSER

Time Level * 9

Amount Format

Date Format

□ Auto Authorization

User Status ● Enabled ○ Hold ○ Disabled ○ Locked

Classification ● Staff ○ Branch

Status Changed On

Last Signed On

□ Staff Customer Restriction Required

ELCM User ID

□ Multi Branch Access

User Password

Password ●●●●●●●●●●●●

Password Changed On 2012-01-06 11:01:33

Email

Start Date * 2012-01-06

End Date

Invalid Logins

Cumulative

Successive

Maker KANNAN1 Date Time: 2012-01-06 13:29:56 Mod No 3

Checker SARAN Date Time: 2012-01-06 13:34:26 Record Status Closed

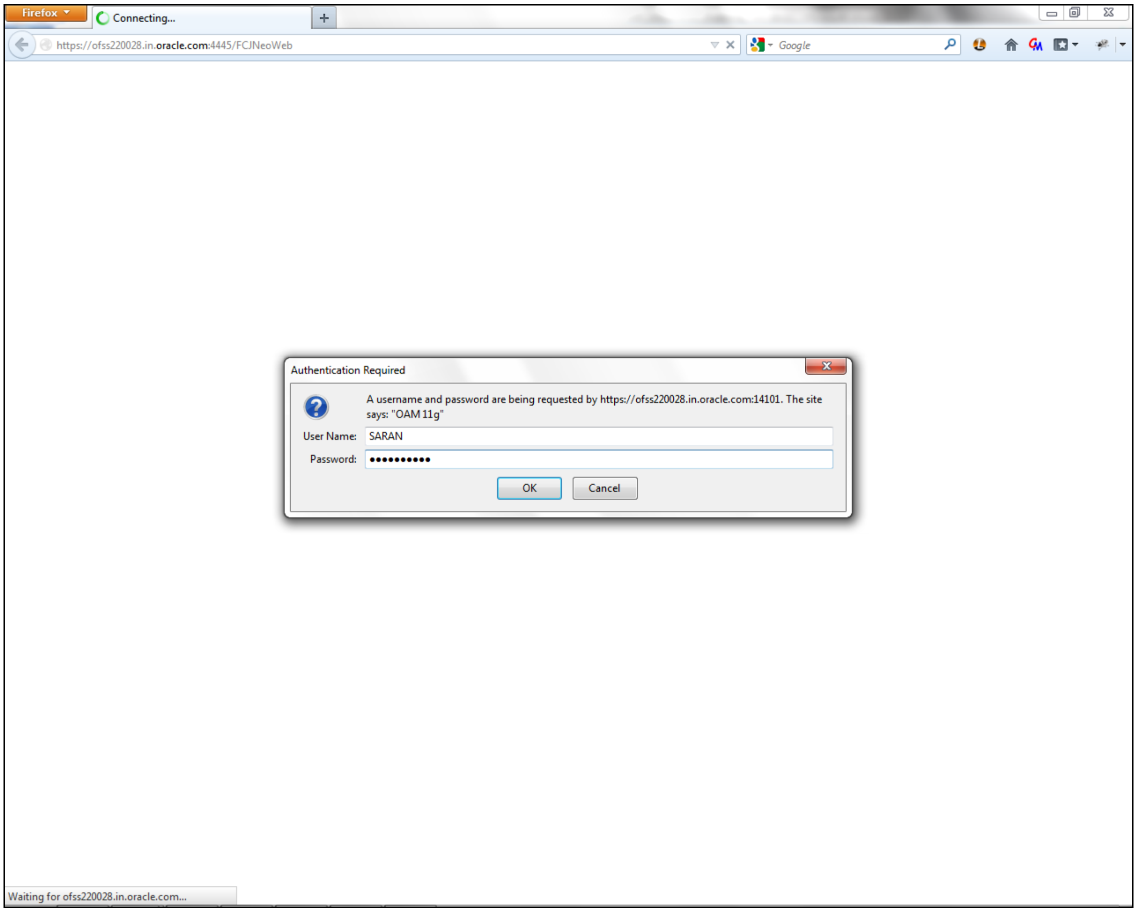
Authorization Status Authorized

2.7.4 Launching FLEXCUBE

After setting up FLEXCUBE to work on Single Sign on mode, navigate to the interim servlet 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.



Firefox
Connecting...
https://ofss220028.in.oracle.com:4445/FCJNeoWeb
Google

Authentication Required

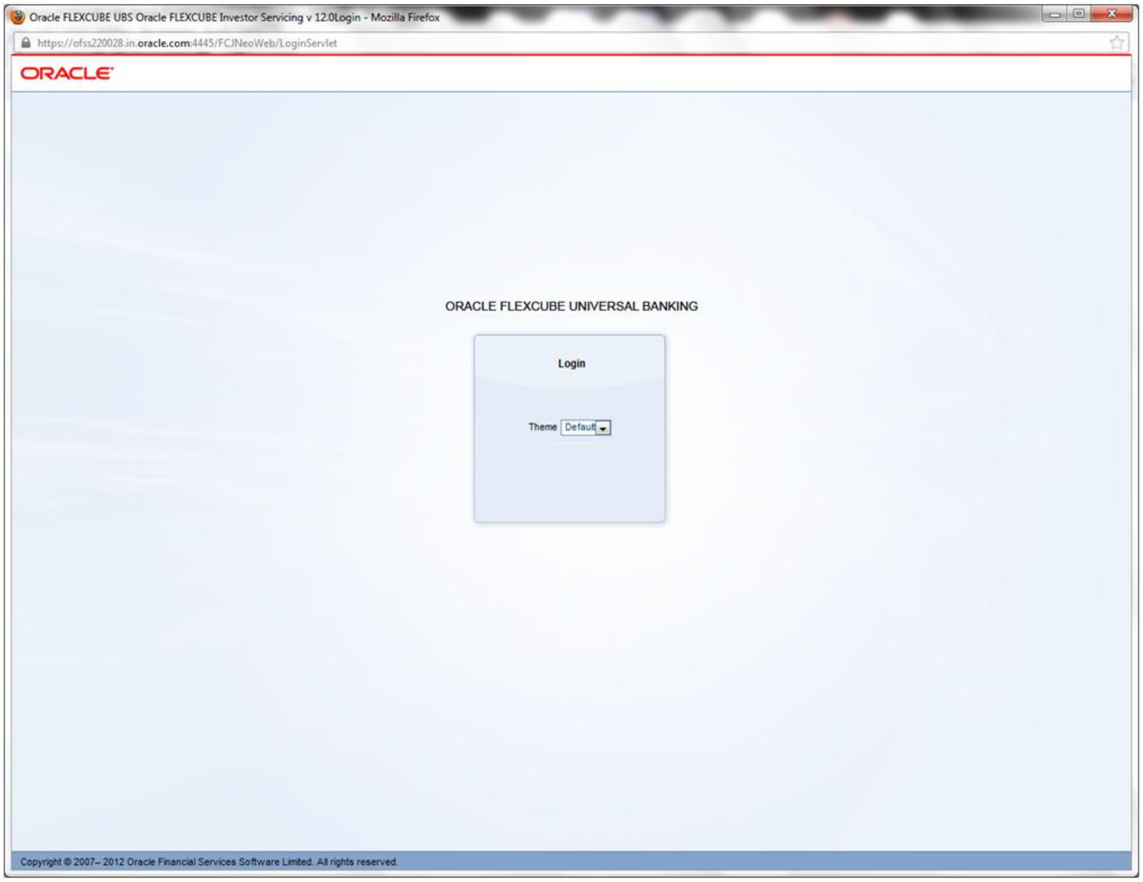
A username and password are being requested by https://ofss220028.in.oracle.com:14101. The site says: "OAM 11g"

User Name: SARAN

Password: ●●●●●●●●●●

OK
Cancel
Waiting for ofss220028.in.oracle.com...

Once the user is authenticated and authorized to access the resource, the servlet gets redirected to normal FLEXCUBE application server URL and now the new signon form will appear as below. The application will automatically redirect FLEXCUBE home page.


Oracle FLEXCUBE UBS Oracle FLEXCUBE Investor Servicing v 12.0Login - Mozilla Firefox
https://ofss220028.in.oracle.com:4445/FCJNeoWeb/LoginServlet
ORACLE
ORACLE FLEXCUBE UNIVERSAL BANKING
Login

Theme Default

Copyright © 2007– 2012 Oracle Financial Services Software Limited. All rights reserved.

2.7.5 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
[October] [2013]
Version 12.0.2.0.0

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/

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.