Oracle Access Manager Integration Oracle FLEXCUBE Universal Banking Release 12.2.0.0.0 May 2016 Part No. E74659-01





# Table of Contents

1. PREFA	ACE	
1.1 IN	TRODUCTION	
1.2 A	JDIENCE	
1.3 A	3BREVIATIONS	
1.4 D	DCUMENTATION ACCESSIBILITY	
1.5 O	RGANIZATION	
1.6 G	LOSSARY OF ICONS	
1.6.1	Related Documents	
2. ENAB	LING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER	
2.1 IN	TRODUCTION	
2.2 B	ACKGROUND AND PREREQUISITES	
2.2.1	Software Requirements	
2.3 B.	ACKGROUND OF SSO RELATED COMPONENTS	
2.3.1	Oracle Access Manager (OAM)	
2.3.2	LDAP Directory Server	
2.3.3	WebGate/AccessGate	
2.3.4	Oracle Adaptive Access Manager	
2.4 Co	DNFIGURATION	
2.4.1	Pre-requisites	
2.5 Er	VABLING SSL FOR WEBLOGIC AND OAM CONSOLE	
2.5.1	Self-signed Certificate Creation:	
2.5.2	Configuring Weblogic Console	
2.5.3	Configuring SSL Mode in Oracle Internet Directory	
2.6 Co	DNFIGURING SSO IN OAM CONSOLE	
2.6.1	Identity Store Creation	
2.6.2	Creating Authentication Module	
2.6.3	Creating Authentication Scheme	
2.6.4	Creating OAM 11g Webgate	
2.6.5	Post OAM Webgate 11g Creation	
	RST LAUNCH OF FLEXCUBE AFTER INSTALLATION	
2.7.1	Parameter Maintenance	
2.7.2	Maintaining LDAP DN for FLEXCUBE users	
2.7.3	Launching FLEXCUBE	
2.7.4	Signoff in a SSO Situation	



# 1. Preface

# 1.1 Introduction

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

# 1.2 <u>Audience</u>

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 <u>Abbreviations</u>

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 <a href="http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc">http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc</a>.

# 1.5 Organization

This manual is organized into the following chapters:

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

# 1.6 **Glossary of Icons**

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



Icons	Function
×	Exit
+	Add row
I	Delete row
2	Option List

## 1.6.1 Related Documents

You may refer the following manual for more information

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



# 2. Enabling Single Sign-on with Oracle Access Manager

# 2.1 Introduction

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

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

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

# 2.2 **Background and Prerequisites**

### 2.2.1 Software Requirements

Oracle Identity and Access Management 11g R2 - 11.1.2.3.0

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

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

#### LDAP Directory Server

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

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

- Oracle Internet Directory
- Active Directory
- ADAM
- ADSI
- Data Anywhere (Oracle Virtual Directory)
- IBM Directory Server
- NDS
- Sun Directory Server



#### Oracle Weblogic (10.3.6)

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

# 2.3 Background of SSO related components

### 2.3.1 Oracle Access Manager (OAM)

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

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

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

#### 2.3.2 LDAP Directory Server

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

#### 2.3.3 WebGate/AccessGate

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

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

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

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



## 2.3.4 Oracle Adaptive Access Manager

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

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

# 2.4 Configuration

## 2.4.1 Pre-requisites

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

# 2.5 Enabling SSL for Weblogic and OAM Console

## 2.5.1 Self-signed Certificate Creation:

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

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

#### 2.5.1.1 Keystore Creation

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

For example:

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



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

#### 2.5.1.2 Export private key as certificate

keytool -export -v -alias <alias\_name> -file <export\_certificate\_file\_name\_with\_location.cer> -keystore <keystore\_name.jks> > -keypass <Private key Password> -storepass <Store Password>

For example:

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

If successful the following message will be displayed :

Certificate stored in file < AdminFlexcubeCert.cer>

#### 2.5.1.3 Import as trusted certificate

keytool -import -v -trustcacerts -alias rootcacert -file <export\_certificate\_file\_name\_with\_location.cer> - keystore <keystore\_name.jks> > -keypass <Private key Password> -storepass <Store Password>

For example:

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

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



# 2.5.2 Configuring Weblogic Console

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

### 2.5.2.1 Select Admin Server to enable SSL options

	Administration Console						õ					
Change Center	🔒 Home Log Out Preferences 🛃 Record	Help	2		Welcor	me, weblogic Connected to: ia	am_domaii					
View changes and restarts	Home >Summary of Servers											
Configuration editing is enabled. Future Summary of Servers changes will automatically be activated as you												
changes will automatically be activated as you modify, add or delete items in this domain.	Configuration Control											
Domain Structure iam_domain □ Environment □ Servers □ Outers □ Wrtuel Hosts □ Coherence Servers □ Coherence Clusters □ Mork Managers □ Startu and Shutdown Classes	A server is an instance of WebLogic Server This page summarizes each server that has C2 C3 C4 C4 C4 C4 C4 C4 C4 C4 C4 C4 C4 C4 C4	been configured in the current 1		wm configuration.		Showing 1 to 4 of 4 Previous	s   Next					
Deployments	🔲 Name 🌣	Cluster	Machine	State	Health	Listen Port						
Security Realms	AdminServer(admin)			RUNNING	✓ OK	7001						
How do I	oam_server1			RUNNING	✓ OK	14100						
Create Managed Servers	oim_server1			RUNNING	✓ OK	14000						
Clone Servers	soa_server1		LocalMachine	SHUTDOWN		8001						
Delete Managed Servers     Delete the Administration Server     Start and stop servers	New Clone Delete					Showing 1 to 4 of 4 Previous	s   Next					
System Status 🖃	j											
Health of Running Servers												
Failed (0) Critical (0) Overloaded (0) Warning (0)												

#### 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.



Domain Structure	General Cluster Services Keyston	res SSL Federation Services Deplo	yment Migration Tuning	Overload Health Monitoring	Server Start Web Services			
Iam_domain ← C-Environment Custers Custers Vironal Hosts Vironal Hosts Coherence Servers	Save Use this page to configure general feature View INDI Tree @	es of this server such as default network co	mmunications.					
Coherence Clusters     Machines     Work Managers	Name:	AdminServer	An alphanumeric name for this server instance. More Info					
Startup and Shutdown Classes	Machine:	(None)		The WebLogic Server host com to run. More Info	The WebLogic Server host computer (machine) on which this server is meant to run. More Info			
How do I	Cluster:	(Standalone)		The duster, or group of WebLogic Server instances, to which this server belongs. More Info				
Configure default network connections     Create and configure machines	🦺 Listen Address:			The IP address or DNS name this server uses to listen for incoming connections. More Info				
Configure clusters     Start and stop servers     Configure WLDF diagnostic volume	☑ Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More $Info\ldots$					
System Status	Listen Port: 7001			The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info				
Health of Running Servers Failed (0)	SSL Listen Port Enabled			Indicates whether the server of port. More Info	can be reached through the default SSL listen			
Critical (0) Overloaded (0) Warning (0)	SSL Listen Port:	7002		The TCP/IP port at which this s requests. More Info	server listens for SSL connection			
OK (3)	Client Cert Proxy Enabled			Specifies whether the HttpClus special header. More Info	sterServlet proxies the client certificate in a			
	Java Compiler:	javac		The Java compiler to use for a to compile Java code. More I	II applications hosted on this server that need info			
	Diagnostic Volume:	Low		WebLogic Server at run time. I does not affect explicitly confi	stic data that is automatically produced by Note that the WLDF diagnostic volume setting gured diagnostic modules. For example, this generated for JRockit Flight Recorder. More			
	- 🖓 Advanced							
	Virtual Machine Name:	iam_domain	AdminSe	When WLS is running on JRVE, running this server More Info	, this specifies the name of the virtual machine			
	🖉 🛃 WebLogic Plug-In Enabled				uses the proprietary WL-Proxy-Client-IP d if the server instance will receive requests nfo			

## 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.

	dministrati	on Cons	ole												Õ
Change Center	쉺 Home	Log Out F	reference	s 🔤 Record H	elp		٩						Welcome, w	eblogic Conner	cted to: iam_domain
View changes and restarts	Home >Su	ummary of	Servers >A	dminServer											
Configuration editing is enabled. Future	Settings for AdminServer														
changes will automatically be activated as you modify, add or delete items in this domain.	Configura	ation P	rotocols	Logging Deb	ug I	Monitoring C	Control	Deployments	Services	Security	Notes				
Domain Structure	General	Cluster	Services	Keystores	SSL	Federation S	Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services	
iam_domain	Keystore	anage the	Dem Cust	storage and man f message transm or Identity and orn Identity ar on Identity ar on Identity ar o Identity and	I Den I Den I d Cu I d Cu	s. no Trust mmand Line stom Trust va Standard	• Trust	vusted certificat	e authorities	s (CAs). Thi	Which	ou view and define va configuration rules shr cystores? More Info.	ould be used for	-	
System Status															
Health of Running Servers           Failed (0)           Critical (0)           Overloaded (0)           Warning (0)           OK (3)			names may	be trademarks of	their re	espective owners	5.								



#### 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.

	dministration Console					Õ				
Change Center	🔒 Home Log Out Preferences 🖂 Record Help	Q			Welcome, weblogi	c Connected to: iam_domain				
View changes and restarts	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.	Settings for AdminServer Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes									
Domain Structure	General Cluster Services Keystores SSL Fed	leration Services Deployment	Migration Tuning	Overload Health Monito	ing Server Start Web	Services				
Iam_domain ▲ Environment ↓ Servers ↓ Ousters ↓ -Virual Hosts ↓ -Virual Hosts ↓ -Onerence Servers ↓ - Coherence Clusters	Save Acystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page kets you view and define various keystore configurations. These settings help you to manage the security of message transmissions. Keystores: Custom Identity and Custom Trust Change. Which configuration rules should be used for finding the server's identity and									
Wachines 	— Identity Custom Identity Keystore:	info aseKeyStore/AdminF file the tip, lag, in the tip	 KeyStore/AdminFlexcubeKeyStore.jks- North, heydrone March form							
How do I	Custom Identity Keystore Type:	jks		The type of the keyston	. Generally, this is JKS. N	fore Info				
Configure identity and trust     Configure keystores	Custom Identity Keystore Passphrase:	•••••	••		entity keystore's passphra: ed without a passphrase.					
Set up SSL  System Status	Confirm Custom Identity Keystore Passphrase:	•••••	••							
Health of Running Servers	- Trust		/scratch/a	pp/fmw115/oam1115/E	aseKevStore/AdminE	lexcubeKeyStore iks				
Failed (0)	Custom Trust Keystore:	nFlexcubeKeyStore.j			T the custom trust keystore					
Critical (0) Overloaded (0)	Custom Trust Keystore Type:	jks		The type of the keystor	. Generally, this is JKS.	tore Info				
Warning (0) OK (3)	Custom Trust Keystore Passphrase:	•••••	•••••		e's passphrase. If empty o passphrase. More Info	s passphrase. If empty or null, then the keystore issphrase. More Info				
	Confirm Custom Trust Keystore Passphrase:	•••••	••							
	Save									

#### 2.5.2.5 Follow the steps in SSL Tab as shown below:

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



Change Center	🏠 Home Log Out Preferences 🖂 Recor	d Help		Welcome, weblogic Connected to: iam_domain
View changes and restarts	Home >Summary of Servers >AdminServer			
Configuration editing is enabled. Future changes will automatically be activated as you	Settings for AdminServer			
modify, add or delete items in this domain.	Configuration Protocols Logging	Debug Monitoring Control Deployments S	Services Security	Notes
Domain Structure	General Cluster Services Keystore	s SSL Federation Services Deployment M	igration Tuning	Overload Health Monitoring Server Start Web Services
iam_domain	Save			
Virtual Hosts Migratable Targets			instance. These sett	ings help you to manage the security of message transmissions.
Coherence Servers Coherence Clusters Machines	(f) 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
	Private Key Location:	from Custom Identity Keystore		The keystore attribute that defines the location of the private key file. More Info
How do I	Private Key Alias:	FlexcubeCert		The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info
Configure identity and trust	🚝 Private Key Passphrase:			The keystore attribute that defines the passphrase used to retrieve the server's private key. More Info
Set up SSL     Verify host name verification is enabled	街 Confirm Private Key Passphrase:			
Configure a custom host name verifier     Configure two-way SSL	Certificate Location:	from Custom Identity Keystore		The keystore attribute that defines the location of the trusted certificate. More Info
System Status	- Trust			
Health of Running Servers Failed (0)	Trusted Certificate Authorities:	from Custom Trust Keystore		The keystore attribute that defines the location of the certificate authorities. More Info
Critical (0)	- V Advanced			
Overloaded (0) Warning (0) OK (2)	倭 Hostname Verification:	None   Custom Hostname Verifier BEA Hostname Verifier		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:	None		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
Warning (0) OK (2)				client to another application server). More Info
UK (2)	👸 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
	街 Cert Authenticator:			The name of the Java class that implements the weblogic.security.acl.Cart/uthenticator 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	V	Indicates the client certificate validation rules for inbound SSL. More Info
	Outbound Certificate Validation:	Builtin SSL Validation Only	V	Indicates the server certificate validation rules for outbound SSL. More Info
	✔ 🖑 Use JSSE SSL			Select the JSSE SSL implementation to be used in Weblogic. More Info
	Save			

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



ORACLE WebLogic Server®						0					
URACLE weblogic Server			0								
Change Center	🔒 Home Log Out Preferences 🔤 Record H		Q		Welcor	ne, weblogic Connected to: iam_domain					
View changes and restarts	Home >Summary of Servers >AdminServer >Sur	mmary of Servers									
Configuration editing is enabled. Future	Summary of Servers										
changes will automatically be activated as you modify, add or delete items in this domain.	Configuration Control	Configuration Control									
	1										
Domain Structure	A server is an instance of WebLogic Server th	nat runs in its own Java Virtu	al Machine (JVM) and has its o	own configuration.							
iam_domain ^ İ⇒-Environment	This page summarizes each server that has b			-							
Servers	This page summarizes each server that has be	een configured in the curren	WebLogic Server domain.								
Clusters	0										
Virtual Hosts Migratable Targets ==											
Coherence Servers	Customize this table										
Coherence Clusters	Servers (Filtered - More Columns Exist	)									
Work Managers		,									
Startup and Shutdown Classes	New Clone Delete					Showing 1 to 4 of 4 Previous   Next					
Deployments	🔲 Name 🗇	Cluster	Machine	State	Health	Listen Port					
Security Realms	AdminServer(admin)			RUNNING	✓ ок	7001					
How do I 😑				RUNNING	v ok ≪ok	14100					
Create Managed Servers	oim_server1			RUNNING	<pre>✓ ok</pre>	14000					
Clone Servers	soa server1		LocalMachine	SHUTDOWN	- OK	8001					
Delete Managed Servers			Localitaci il le	anorbowie							
Delete the Administration Server	New Clone Delete					Showing 1 to 4 of 4 Previous   Next					
<ul> <li>Start and stop servers</li> </ul>											
System Status	)										
Health of Running Servers											
Failed (0)											
Critical (0)											
Overloaded (0)											
Warning (0)											
OK (3)											

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

## 2.5.3 Configuring SSL Mode in Oracle Internet Directory

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

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



	Manager 11g Fusion Middleware Contr	rol			Setup	p ← Help ← Log Out
👫 Farm 👻 🔒 Topology						
∃ -	🕜 oid1 🕡				Logged in as well	blogic Host padsrini-pc
🗉 📑 Farm_base_domain	📰 Oracle Internet Directory 🛩				Page Refreshed Feb 15,	, 2013 4:35:59 PM IST 🤇
Application Deployments	Home					
I 🔁 🛅 WebLogic Domain						
🖃 🚞 Identity and Access	Monitoring >		Load		Security	
OAM	Control >	) 121	Total LDAP Connections	0	Failed Bind Operations	0
0id1	Logs >					
OIM Ovd1		220	Operations Completed	2	Failed Super User Logins	0
📧 🚞 Metadata Repositories	Port Usage Administration >	65	Operations in progress	0	Sucessful Super User Logins	0
🗉 🚞 Web Tier	Security >					
	Directory Services Manager >	Audit Policy Wallets				
	Directory der vices Manager	wallets			+	
	General Information					
	40	1			Server Response (ms)	
	20					
	0					
	8				•	
	6					
	4				Total Operations	
	2					
	0					
	20					
	15					
	10				CPU Utilization (%) /Farm_base_domain/asi	inst 1/oid1
	5				padsrini-pc	-
	0					
	100					
	80 60				Memory Utilization (%)	
	40				/Farm_base_domain/asi padsrini-pc	inst_1/oid1
	20				padamepe	
	0 16:22 16:23 16 February 15 2013	6:24 16:25 16:26 16	:27 16:28 16:29 16:30	16:31 16:32 16:33 16:	34 16:35 16:36	
						Table View

2. Click 'Create Self-Signed Wallet'.

	nager 11g Fusion Middleware Control	Setup → Help → Log Out
📑 Farm 👻 🔒 Topology		
Farm_base_domain     Application Deployments	Orade Internet Directory	Logged in as weblogic  Host padsminp; Page Refreshed Feb 15, 2013 4:39:54 PM IST 3 <sup>46</sup>
WebLogic Domain     Jentity and Access     OAM     Solution	Wallets A Vallet is a Keystore that stores X.509 certificates and private keys in industry-standard, PKCS #12 format. To cred Wallet. To manage the contents of a vallet, select a wallet and click Manage.	ate a wallet, dick Create. To create a wallet with a self-signed certificate, dick Create Self-Signed
OIM Ovd1		
	rame	Auto-logn
	Logged in as weblagic Host pa de Internet Directory → Page Refreshed Peb 15, 2013 4:39:54 PM ts ts a Keystore that stores X.599 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-Sign To manage the contents of a wallet, select a wallet and click Manage. Create   % Delete   @ Create Self-Signed Wallet   @ Import   @ Export   6d Manage	
	Create      Create Self-Signed Walet     Availet is a Keystore that store X.509 certificates and private keys in industry-standard, PKCS #12 format. To create a walet, dick Create. To create a walet with a self-signed certificate, dick Create Self-Signed Walet     Mane     Auto-login	

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



	anager 11g Fusion M	iddleware Control		Setup → Help → Log Out
Farm - A Topology				
Farm_base_domain     Application Deployments	<pre>     oid1 ₀</pre>	rectory 🕶		Logged in as weblogic Host padsrini-pc Page Refreshed Feb 15, 2013 4-40-45 PM IST ()
Population Composition of the second se	or password-protecte PKCS#12 wallet that	ned Wallet not signed by a well known CA. A se cd. Passwords, if specified, have a m provides PKI-based access to service y security for Auto-login wallets.	minimum length of eight characters, and contain alphabe	OK Cancel wronment. The wallet name should be unique for a given component. The wallet type can be auto-login thic characters combined with numeric or special characters. Auto-login wallet s an oblicated form of time. Auto-login wallet don't need a password to modify, or delete the wallet. File system permissions
	* Wallet Name Wallet Password Confirm Password Add Self-Signed Ce	oidselfsigned		
	* Common Name Organizational Unit Organization City State Country	Chennai TN	det.	

4. Click 6d Manage...

	nager 11g Fusion Middleware Control	Setup → Help → Log Out
🕂 Farm 👻 🔒 Topology		
Farm_base_domain Application Deployments	<pre></pre>	Logged in as weblogic (Host padsrini-pc Page Refreshed Feb 15, 2013 4:44:127 PM IST 🖏
WebLogic Domain  Identity and Access O OAM C Odf O OAM O OAM O OIM	Wallets         A Vallet is a Keystore that stores X.509 certificates and private keys in industry-standard, PKCS #12 format. To Wallet. To manage the contents of a wallet, select a wallet and cick Manage.         Yereate       Yereate         Yereate       Yereate	
📀 ovd1	Name	Auto-login
Metadata Repositories	oidselfsigned	✓
(B) 🎦 Web Tier		

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

Farm 👻 💑 Topology					1	
•	☆ oid1 0					blogic   Host padsrin
🖁 Farm_base_domain	😰 Oracle Internet Directory 🗸				Page Refreshed Feb 15	, 2013 4:45:58 PM IST
Application Deployments						
🚞 WebLogic Domain	Wallets > Manage Certificates					
Identity and Access	Manage Certificates: oidselfsigned					
OAM	To generate a certificate signing request (CSR), click "Add Certificate Request". After you create a CSR, send it to yo		ty and retu	irn the signe	d certificate. To import	the CA signed
2 oid1	certificate or trusted cert, click Import. You can only import the CA-signed certificate into the same wallet from which t	the CSR was generated.				
ovd1	🛉 🕂 Add Certificate Request 🛛 💩 Import 🕆 Export 💥 Delete					
Metadata Repositories	Subject Name	Certificate Type	Status	Key Size	Start Date	Expiration Date
📄 Web Tier	CN=padsrini-pc.OU=OFSS.O=Orade.L=Chennai.ST=TN.C=IN	Certificate Request		2048		
Web her	CN=padsrini-pc, OU=OFSS, O=Orade, L=Chennal, ST=TN, C=IN	Certificate	Valid	2048	February 15, 2013	February 14, 20
web ner			Valid Valid	2048 1024	February 15, 2013 January 29, 1996	February 14, 20 August 2, 2028
	ON=padsrini-pc, OU=OFSS, O=Orade, L=Chennai, ST=TN, C=IN	Certificate				
	ON=padsrini-pc, OU=OFSS, O=Orade, L=Chennal, ST=TN, C=IN OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Certificate Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028 August 14, 2018
	CN-padorini-prc, OU-OFSS, O-Orade, L=Chernal, ST=TN, C=IN OU-Glass Value Primary Certification Authority, O="VerSign, Inc.", C=US CN=GTE CyberTrust Global Root, OU-GTE CyberTrust Solutions, Inc.", O=GTE Corporation, C=US	Certificate Trusted Certificate Trusted Certificate	Valid Valid	1024 1024	January 29, 1996 August 13, 1998	August 2, 2028 August 14, 2018

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



	Anager 11g Fusion Middleware Control		Setu	up 👻 Help 👻 Log Out
🕂 Farm 👻 💦 Topology				
<b>□</b> •	☆ oid1 @		Logged in as we	blogic Host padsrini-pc
Farm_base_domain     Application Deployments	Image: Oracle Internet Directory ▼		Page Refreshed Feb 15	5, 2013 4:45:58 PM IST 🔇
WebLogic Domain     Jentity and Access     OAM     OAM     OI     OI	Walets > Manage Certificates Manage Certificates: oldselfsign To generate a certificate signing request ( certificate or trusted cert, dick import. Yo Add Certificate Request	Trusted Certificate The Trusted Certificate with Subject Name ON=padorni-pc, OU=OFSS, O=Orade, L=Chennal, ST=TN, C=IN is shown below. You can out and paste the entre text in the box from BEGIN CERTIFICATE to DIO CERTIFICATE to the intended	certificate. To impor	t the CA signed
💿 ovd1	Add Certificate Request	location; or click "Export Trusted Certificate " to export the certificate to a file. You may want to do this if another party		
<ul> <li>Metadata Repositories</li> <li>Web Tier</li> </ul>	Subject Name CN=padsrini-pc,OU=OFSS,O=Ora	wants to trust your certificate directly.	Start Date	Expiration Date
	CN=padsrini-pc, OU=OFSS, O=Or	MIIDODCCAIACAOAwDOYJKoZIhvcNAOEEBOAwY†ELMAkGA1UEBhMCSU4xCzAJBgNVBAgTA1ROMRAw	February 15, 2013	February 14, 2018
	OU=Class 3 Public Primary Certific	DgYDVQQHEwdDaGVubmFpMQ8wDQYDVQQKEwZPcmFjbGUxDTALBgNVBAsTBE9GU1MxFDASBgNVBAMT	January 29, 1996	August 2, 2028
	CN=GTE CyberTrust Global Root,	C3Bh2HNyaW5pLXBjMB4XDTEzMDIxNTA4NTMyNVoXDTE4MDIxNDA4NTMyNVowYjELMAkGA1UEBhMC	August 13, 1998	August 14, 2018
	CN=padsrini-pc, OU=OFSS, O=Or	SU4xCzAJBgNVBAgTA1ROMRAwDgYDVQQHEwdDaGVubmFpMQ8wDgYDVQQKEw2PcmFjbGUxDTALBgNV BAsTBE9GU1MxFDASBgNVBAMTC3BhZHNyaW5pLXBjMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB	February 15, 2013	February 14, 2018
	OU=Class 2 Public Primary Certific	CgKCAQEArfMDE0WbIxe/TNMjlun9o467st/YWM16MSr9WdoYkRVkgf45ef06ucrChV2MZ2RQk+Bp	January 29, 1996	August 2, 2028
	OU=Class 1 Public Primary Certific	OTjcWxIorVHIEym6tsheWswgPOFCTjxJyO73hV0PvyCrCfI2PnpNjqKBox1KpIidxYLsyzehOhmz NmeqNiYP18Wbf095BdmpcnHpBcu06DKmBztB6HuQJpSt0EzHqJ11xsYkpwqT+dKQofwy8LnRNnF4	January 29, 1996	January 8, 2020
		xcdNUcTkGF8sphG1wBoLlXMnOeRvEz3U1fuMZf3ld8B+Gy+n8k9zshfCcNjElg4+uLf09pJrdE+3 8LdwAKCyVcRqXj5wRs8X17B4x/Ys9kD+FKYfkj1sKsRyYQIDAQABMA0GCSqGSIb3DQEBBAUAA4IB		
		Export Trusted Certificate Close	-	
	1		_	

7. Click 'Server Properties'.

🖁 Farm 👻 🔒 Topology									
] +		oid1 🕡						Logged in as we	blogic Host padsrini-
Farm_base_domain	2:	Oracle Internet Directory 🛩						Page Refreshed Feb 15	, 2013 4:45:58 PM IST
Application Deployments     Deployment     WebLogic Domain		Home	isigned						
Identity and Access     OAM     OAM     OIM     OIM		Monitoring Control Con	est (CSR), click "Add Certificate Re	equest". After you create a CSR, send it to yo ed certificate into the same wallet from which t		ty and retu	rn the signe	d certificate. To import	the CA signed
ovd1     Metadata Repositories		Port Usage	Import 😭 Export	X Delete	Certificate Type	Status	Key Size	Start Date	Expiration Date
E Dier		Administration 3	Server Properties		Certificate Request	510105	2048	Start Bate	Expression
<b>_</b>		Security	Shared Properties		Certificate	Valid	2048	February 15, 2013	February 14, 201
		Directory Services Manager	>	, , C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
			Replication Management	Inc.", O=GTE Corporation, C=US	Trusted Certificate	Valid	1024	August 13, 1998	August 14, 2018
		General Information	Tuning and Sizing		Trusted Certificate	Valid	2048	February 15, 2013	February 14, 201
		OU=Class 2 Public Primary Ce	ertification Authority, O="VeriSign,	Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
		OU=Class 1 Public Primary Ce	ertification Authority, O="VeriSign,	Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	January 8, 2020

8. Click 'Change SSL Settings'.

	Inager 11g Fusion Middleware Control	Setup → Help → Log Out
🕂 Farm 👻 👗 Topology		
<b>□</b> -	☆ oid1 ₀	Logged in as weblogic Host padsrini-pc
🗉 🚟 Farm_base_domain	E Orade Internet Directory -	Page Refreshed Feb 15, 2013 4:54:17 PM IST 🗘
E Application Deployments		
🗉 🚞 WebLogic Domain	Server Properties	Apply Revert
Identity and Access		Apply Revert
OAM		
Did1	Server Mode Read / Write	
OIM 호 ovd1	* Maximum number of entries to be returned by a search 10000	
Metadata Repositories	* Maximum time allowed for a search to complete (sec) 3600	
Web Tier	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	
	SISI Contraction of the second sister of the second	

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



<u> </u>		
	nager 11g Fusion Middleware Control	Setup 🗸 Help 🗸 Log Out
📲 Farm 👻 🔒 Topology		
	☆ oid1 ₀	Logged in as weblogic   Host padsrini-pc
E 📲 Farm_base_domain	E Orade Internet Directory -	Page Refreshed Feb 15, 2013 4:55:50 PM IST ₹2
Application Deployments     Deployment     WebLogic Domain		
Identity and Access	<ol> <li>Information         All changes made in this page require a server restart to take effect.     </li> </ol>	
O OAM	SSL Configuration @	OK Cancel
OIM     OVd1		
Metadata Repositories	Server Wallet Name odselfsigned	
E 📄 Web Tier	oldselfsigned not required for no-auth mode but is needed in other modes.	
_	Advanced SSL Security	
	Server SSL properties	
	SSL Authentication Server Authentication	
	SSL_RSA_WITH_RC4_128_MD5	
	Cipher Suite	
	VISSL_RSA_WITH_DES_EDE_CBC_SHA	
	VILS_RSA_WITH_AES_128_CBC_SHA +	
	* SSL Protocol Version All	

#### 10. Click 'Apply'.

	lanager 11g Fusion Middleware Control	Setup ≠ Help ≠ Log Out
📑 Farm 👻 🔒 Topology		
∃ -	û oid1 ₀	Logged in as weblogic   Host padsrini-pc
🛙 🚟 Farm_base_domain	😰 Oracle Internet Directory 🗸	Page Refreshed Feb 15, 2013 4:56:40 PM IST 🗘
Application Deployments		
WebLogic Domain     Identity and Access	Information SSL configuration updated for /Farm_base_domain/asinst_1/oid1. Restart component for this change to be effective.	×
OAM		
oid1	Server Properties	Apply Revert
🐼 ovd1	General Performance SASL Statistics Logging	
🗄 🫅 Metadata Repositories		
🗷 🚞 Web Tier		
	* 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	Page Refreshed Feb 15, 2013 4:56:40 PM 15T (2) e effective.
	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)

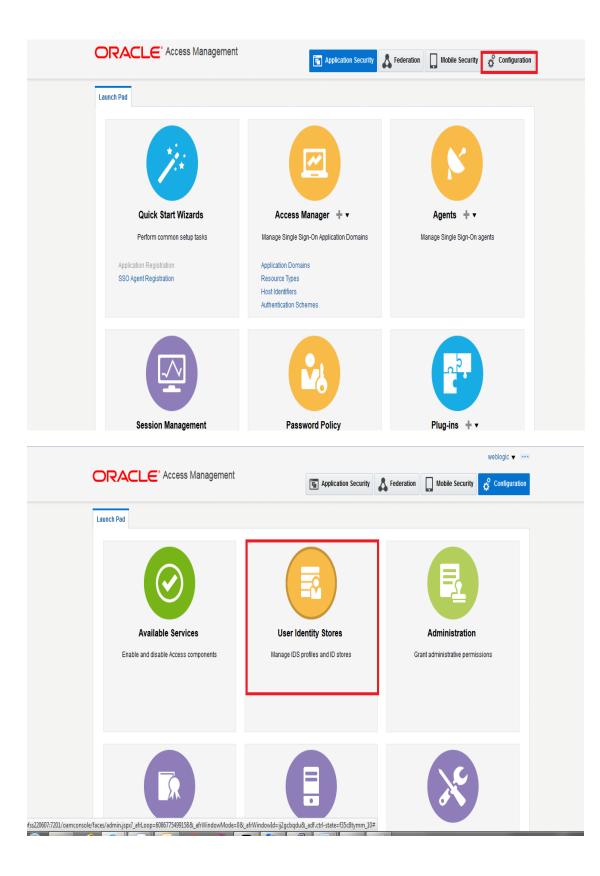


# 2.6.1 Identity Store Creation

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

	Management	About Oracle
	<b>Sign In</b> Sign in to administer Oracle Access Management	t de la constante de
	Username	
	Password Sign In	
Copyright ⊜ 2000, 2015, Oracle and/or its aff	tes. All rights reserved.	





2. Click 'Create' under OAM ID Stores.



Configuration >				
User Identity Sto	ores			
Default and System	Store			App
* De	fault Store UserIdentityStore1	•		
* Sy:	stem Store UserIdentityStore1	•		
4 OAM ID Stores				Sync IDS Profil
A OAM ID Stores Manage local User Identit	y Stores. This includes IDS Profile:	s that are synchronized by using Sync ID	S Profiles button.	Sync IDS Profil
	•	s that are synchronized by using Sync ID Delete	S Profiles button.	Sync IDS Profil
Manage local User Identit	•		S Profiles button.	Sync IDS Profil Synched IDS Profiles
Manage local User Identit	🍽 Duplicate 🇳 Edit 🗙	Delete		

- 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.



Configuration >							
reate: User Ident	ity Store User Identity	Store Service				Test Connection	Appl
* Store Name	FLEXCUBEStore				Enable SSL		
* Store Type	OID: Oracle Internet Direct	Dry	•		Use Native ID Store S	ettings	
Description				Prefetched Attributes			
Location and Crede	entials						
* Location	ofss220607.in.oracle.com	3131 .d		* 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				
l. l.	Jser 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.

	Stores × Create: User Ide	entity Sto ×					
Configuration >	ity Store					Test Connection	Apply
Create: User Ident		Store Service			Connection Status	×	Abbil
* Store Name	FLEXCUBEStore						
* Store Type	OID: Oracle Internet Direct	ory	•		Connection to the User Ide		
			Devé	4 - 1 - 1 - 1 - 1 - 1 - 1		OK Cancel	
Description			Prete	etched Attribut	es		
Location and Crede							
Location and crede	entials						
* Location	ofss220607.in.oracle.com	3131		* Passwo	rd ••••••		
* 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				
		0.0000,000,000,000,000	01000,00 0				
	Jser Filter Object Classes						
	Group Name Attribute						
	* Group Search Base	cn=Groups,dc=ofss,dc=in,d	c=oracle,dc=				

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



LEXCODESION	User Identity Store Service					Duplicate	Test Connection	Ар
Ocnfirmation								>
User Identity Store FLEX	CUBEStore created success	fully.						
Store Name	FLEXCUBEStore				Enable SSL			
* Store Type	OID: Oracle Internet Direct	огу	•		Use Native I	D Store Setti	ngs	
Description				Prefetched Attributes				
boonpaon								
Location and Crede	entials							
* Location	ofss220607.in.oracle.com	:3131		* Password	•••••			
* Bind DN	cn=orcladmin							
Users and Groups								
	* Login ID Attribute	cn						

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

# 2.6.2 Creating Authentication Module

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



ORACLE' Access Management	Application Security	Federation          Mobile Security
Launch Pad		
Quick Start Wizards	Access Manager + 🔻	Agents + -
Perform common setup tasks Application Registration SSO Agent Registration	Manage Single Sign-On Application Domains Application Domains Resource Types Host Identifiers Authentication Schemes	Manage Single Sign-On agents
Session Management	Password Policy	Plug-ins 🛉 🔻
Manage Single Sign-On sessions	Manage Common Password Policy for Single Sign-On	Manage Authentic Authentication Module Authentication Module Authentication Plug-ins Create Kaberos Authentication Module Create X509 Authentication Module Create Custom Authentication Module

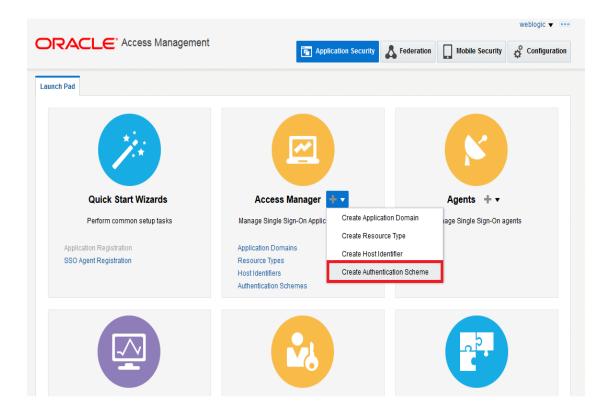
Enter the Name for the Authentication Module and choose the proper User Identification Store, ie created in <u>2.6.1</u>. Click on 'Apply' to create Authentication Module.

	The Application Securit	ty 👗 Federation	ty 🖧 Configuration
Launch Pad FlexcubeAuthModule ×			
Access Manager >			
FlexcubeAuthModule LDAP Authentication Module			Duplicate Apply
Use the LDAP Authentication module for Basic and Form challe definition stored in an LDAP directory server.	ge methods. It matches the credentials (username	and password) of the user who requests a r	esource to a user
S Confirmation			×
LDAP Authentication Module FlexcubeAuthModule created si	ccessfully.		
* Name FlexcubeAuthModule			
* User Identity Store FLEXCUBEStore			
opyright © 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 and refer to OAM documentation for more details on the same.

## 2.6.3.1.1 https://docs.oracle.com/cd/E52734\_01/oam/AIAAG/shared.htm#AIAAG488



## **Basic Style Authentication Scheme**

Enter the below details and click 'Apply':

Name	: Name of the Authentication Scheme
Authentication Level	:1
Challenge Method	: BASIC
Challenge Redirect URL	: /oam/server
Authentication Module	: Authentication Module
Refer the section 'Creating Auth	entication Module 2.6.2' of this document.
Challenge Parameters	: ssoCookie=Secure
	contextType=default
	contextValue=/oam
	challenge_url=/CredCollectServlet/BASIC

Launch Pad FlexcubeBa	sicOAMScheme ×	
Access Manager >		
	ation Scheme Authentication Scheme Set As Default Duplica	
An Autrentication Scheme	defines the challenge mechanism required to authenticate a user. Each Authentication Scheme must also include a defined Authentication Mod	Jie.
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	sscCookig=Secure context/Tipg=default challenge_ytl=/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 Aut	hentication Module 2.6.2' of this document.
Challenge URL	: /pages/login.jsp
Context Type	: default
Context Value	: /oam
Challenge Parameters	: ssoCookie=Secure

Launch Pad FlexcubeFo	rmOAMScheme ×				
Access Manager >					
	ation Scheme Authentication Scheme		Set As Default	Duplicate	Apply
An Authentication Scheme	defines the challenge mechanism required to authention	cate a user. Each Authentication Scheme must also include a	defined Authentica	ation 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				
	ssoCookie=Secure				
Challenge Parameters					



#### 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 Auth	nentication 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

Set As Default Duplicate Apply 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, FlexcubeKBAOAAMScheme, created successfully \* Name FlexcubeKBAOAAMScheme 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

# 2.6.4 Creating OAM 11g Webgate

Follow the below steps to create a Webgate:

1. Click on 'Server Instances' under Configuration.



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



#### 2. Click on 'Search'.

										weblogic 🔻 🚥
JRA	CLE	Access	Managemer	nt		The Applie	ation Security	Sederation	Mobile Security	of Configuration
aunch Pad	Server Ins	stances ×								
Configura	ation >									
Search O	OAM Sei	vers							+ c	reate OAM Server
Searce										
Name									_	
										Search Reset
Search Re	esults									
Actions 🔻	View 🔻	+ Create	O Duplicate	/ Edit	🗙 Delete	Monitor	Detach			
Row	Name									
No data to dis	splay.									

3. Edit oam\_server1.

		- ** **-	• Fadauation			-
		ation Security	Sederation	Mobile S	ecurity 🔅	Configuratio
aunch Pad Server Instances x						
Configuration >						
Search OAM Servers					+ Create OA	M Server
Search						
Name						
					Search	Reset
Search Results						
Actions 🔻 View 👻 🕂 Create 🔿 Duplicate 🧪 Edit 💥 Delete	Monitor	Detach				
Row Name						
1 oam_server1						

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

				weblog	ic 🔻
	Application Security	Sederation	Mobile Security	Conf	iguration
Launch Pad Server Instances x oam_server1 x					
Configuration > Oam_server1 OAM Server Instance				Duplicate	Apply
* Server Name oam_server1	* Host	ofss220607.in.orac	cley		
* Port 14101 ^ ~					
A OAM Proxy					
* Proxy Server Id AccessServerConfigP					
* Port 5575 🔨 🗸					
* Mode Simple 👻					
Coherence Simple on					
* Log Level 3 ^ ~					
* Local Port 9095 A V					
* Log Limit 4096 🔨 🗸					
Copyright $\circledast$ 2000, 2015, Oracle and/or its affiliates. All rights reserved.					



	Application Security	weblogic 👻 📼
aunch Pad Server Instances x oam_server1 x		
Dam_server1 OAM Server Instance		Duplicate Apply
* Server Name oam_server1	* Host ofss220607.in.ora	cle.
* Port 14101 ^ v	n Edit ×	
	ver instance oam_server1 might be in use. sure you want to edit it?	
Proxy Server Id AccessServerConfigP	Yes No	
* Mode Simple 👻		
Coherence Configuration		
Log Level 3 🔨 🗸		
Local Port 9095 🔨 🗸		
* Log Limit 4096 🔨 🗸		

am_server1 OAM Server Instance	Duplicate Apply
© Confirmation	×
OAM Server Instance oam_server1 modified successfully.	
* Server Name oam_server1 * Host ofss220607.ir	n.oracle.
* Port 14101 ^ ~	
OAM Proxy	
Proxy Server Id essServerConfigProxy	
* Port 5575 A V	
* Mode Simple 💌	
Coherence Configuration	
Log Level 3 A V	
Local Port 9095 🔨 🗸	
* Log Limit 4096 🔨 🗸	



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

	Application Security	Federation Mobile Security	weblogic
Launch Pad	Access Manage + • Manage Sign-On Application Domains Resource Types Host Identifiers Authentication Schemes	Cre	eate Webgate sate OSSO Agent sate OpenSSO Agent
		F	

6. Enter the below and Click 'Apply':

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



unch Pad Create Webga	te x				
Access Manager >					
reate Webgate	gister an OAM Agent. Before yo	ou register, ensure that at least one OAM	1 Server is running in th	e same mode as the Ag	Apply ent to be registered.
* Version	n 11g 💌		* Security		
* Name	FlexcubeWebgate		•	Simple Cert	
Description	Flexcube 11g Webgate	Enter the Base URLs for Agent	Virtual host		
Base URI	https://ofss220607.in.oracle. com	Au	to Create Policies 📝		
Access Client Password	1				
Host Identifie	r FlexcubeWebgate				
	filterOAMAuthnCookie=false				
User Defined Parameters	i -				
source Lists Protected Resou	rce List	Add Delete Public	Resource List	A	dd Delete
Relative URI		Relati	ve URI		
/FCJNeoWeb					
excubeWebgate we	ogate			Apply Dov	mload
Confirmation	gate created successfully.				×
Version 1	1g	Logout Tar	get URL		
Name F	FlexcubeWebgate	Deny On Not Pr	otected 🔽		
	Flexcube 11g Webgate		proxySSLHeade SSL URLInUTF8Forn		
Access Client Password * Security	) Open	User Defined Para	dient_request_r mpts=1	etry_atte	
	) Simple ) Cert	* Sleep for (Se	conds) 60 ^		
	) Enable		Header no-cache		
-					
0	Disable	Cache Control	Header no-cache		
-	Disable		Header no-cache Debug		

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



	weblogic 👻 🚥
	🔄 Application Security
Launch Pad SSO Agents x FlexcubeWebgate x	
Access Manager > FlexcubeWebgate Webgate	Apply Download
Version 11g	Logout Target URL
Name FlexcubeWebgate	Deny On Not Protected
Description Flexcube 11g Webgate	proxySSLHeaderVar=
Access Client Password	User Defined Parameters ue client_request_retry
* Security Open Simple Cert	* Sleep for (Seconds)
* State      Enable     Disable	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'.

Refer '<u>Creating OAM 11g Webgate 2.6.3'</u> section of this document.

RACLE <sup>®</sup> Access Management	🖀 Application Security 👗 Federation 🔲 Mobile Security 🧳 Configuration
unch Pad Server Instances x oam_server1 x	
Configuration >	
am_server1 OAM Server Instance	Duplicate Apply
<ul> <li>Confirmation</li> <li>OAM Server instance cam_server1 modified successfully.</li> </ul>	×
* Server Name oam_server1 * Port 14101 * *	* Host ofss220607.in.oracle.con
Proxy Server Id AccessServerConfigProxy Port 5575	
Mode Open	
Log Level 3 ^ Y	
Local Port 9095 A V	
* Log Limit 4096 🔨 🗸	

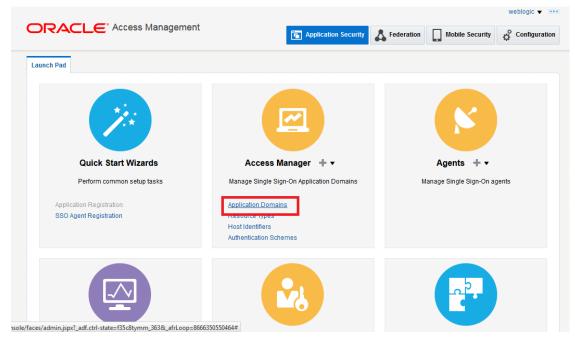


## 2.6.5 Post OAM Webgate 11g Creation

Follow the below steps to configure the webgate created .

#### 2.6.5.1 Application Domains Changes

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



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

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

aunch Pad	Applicatio	on Domain 🗙				
Search		tion Domains	k the Create Application D	omain hutton to create a neu	v 000	- Create Application Domain
⊿ Sea	rch	an existing Application Domain of circle	k the ofeate Application D	offiair buttor to create a res	vone.	
Nam	e					Search Reset
earch R	Results					
Actions -		🕂 Create 💉 Edit 🔀 Delete	Detach			
Row	View ▼ Name	+ Create 🖍 Edit 🗙 Delete	Detach	Description		
Actions -	View ▼ Name	🕂 Create 🧪 Edit 🗶 Delete	Detach	Description		



	CLE <sup>®</sup> Acc	ess Managen	nent		Application Security	Federation	Mobile Se	ecurity 🔅	Configurati
aunch Pad	Application Domai	×							C
Access M	anager >								
Search A	pplication D	mains					+ Cr	reate Applicati	on Domain
	••		main or click	the Create Applic	ation Domain button to create a nev	vone.			
	in tool to find an exis								
⊿ Searc				and distance applied					
✓ Searce									
✓ Searce Name	ch							Search	Reset
✓ Searce	ch							Search	Reset
✓ Searce Name	sults			Detach				Search	Reset
A Search Re	sults				Description			Search	Reset
A Search Name Search Re Actions V	ch sults View ▼ + Cre				Description Application Domain create	d through Remote R	Registration	Search	Reset
A Search Name Search Re Actions V Row	sults View ▼ Cre Name	ate 🖋 Edit 💈			· ·	-	-		Reset

3. Click on 'Authentication Polices'.

					weblogic 🔻 🚥
	Management	Application Security	Federation	Mobile Security	Configuration
aunch Pad Application Domain 🗙	FlexcubeWebgate ×				
Access Manager >					
lexcubeWebgate Applicat	ion Domain				
pplication Domain provides a logical	container for resources or sets of resources, and th	e associated policies that dicta	te who can access	s specific protected resou	Irces.
Summary Resources Authentic	cation Policies Authorization Policies Token Is:	suance Policies Administratio	n		
					Apply
					Арріу
* Name	FlexcubeWebgate				
	Application Domain created through Remote				
	Registration				
Description					
* Session Idle Timeout (minutes)	0 🔨 🗸				
Allow OAuth Token					
Allow Session Impersonation					
Enable Policy Ordering					

4. Click on 'Protected Resource Policy'.



aunch Pad	Application	Domain x FlexcubeWebgate	×				C
Access	Manager >						
lexcub	eWebgate	Application Domain					
pplication E	Domain provide	es a logical container for resource	s or sets of resources,	and the associated policies th	at dictate who can acces	s specific protected reso	ources.
Summary	Resources	Authentication Policies Auth	orization Policies To	oken Issuance Policies Admi	nistration		
	wicting Authon	tication Policy from the list or click	the Create Authenticati	ion Policy button to croate a nov			
Select an e	existing Authen	tication Policy from the list or click	the Create Authenticati	ion Policy button to create a new	vone.		
	existing Authen ▼ View ▼	tication Policy from the list or click		ion Policy button to create a net	v one.		
	-	·			v one.		
Actions	▼ View ▼ Name	·		Detach Description		rces to this policy to allow	w anyone access.

5. Choose the Authentication Scheme created earlier in 'Creating Authentication Scheme'.

Refer the section 'Creating Authentication Scheme 2.6.3' of this document.

aunch Pad Appl	ication Domain $\times$ FlexcubeWebgate $\times$	Flexcub	eWebgate : Protect 🗙				
Access Manag	er >						
Protected Re	Source Policy Authentication Po	licy				Duplicate	Appl
	y defines the type of verification that must le defined to protect one or more resources		ed to provide a sufficient level of trust for Acc ication Domain.	ess Manager to g	grant access to the user m	naking the reque	est. A
* Name	Protected Resource Policy		Success URL				
Description	Policy set during domain creation. Add re to this policy to protect them.	sources	Failure URL				
	to this policy to protect them.		t the challenge mechanism required to nticate the user.				
* Authentication Scheme	LDAPScheme						
Resources Re	AdaptiveAuthenticationScheme AnonymousScheme BasicFAScheme BasicScheme BasicSessionlessScheme ESSOProvAuthnScheme						
Resources	FAAdminLocalScheme FAAuthScheme						
Resource T	reacrationochemic	-	Query String				
This Policy o	FlexcubeBasicOAMScheme FlexcubeFormOAMScheme FlexcubeKBAOAAMScheme						
_	LDAPNoPasswordValidationScheme LDAPScheme OAAMAdvanced OAAMBasic						
oyright © 2000, 2015,	041440-0-6						

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



Access Manag	97. D			
-			Du	plicate App
Authentication Polic	esource Policy Authentication Policy by defines the type of verification that must be p e defined to protect one or more resources in the	performed to provide a sufficient level of trust for Acces		
* Name	Protected Resource Policy	Success URL		
Description	Policy set during domain creation. Add resort to this policy to protect them.			
* Authentication Scheme	FlexcubeBasicOAMScheme			
Resources	Advanced Rules			
— Identity Ass This will cause		ionally containing any Asserted Attribute set below.		
Responses	🕂 Add 🧪 Edit 🗙 Delete			
		уре	Value	

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

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

Туре	: Header
Name	: DN
Value	: \$user.attr.dn

Click on Add button

Access Manag	er >			
Authentication Polic		performed to provide a sufficient level of trust for	Access Manager to grant access to the user m	Duplicate Apple
	e defined to protect one or more resources in Protected Resource Policy	Add Response	×	
Description	Policy set during domain creation. Add res to this policy to protect them.	* Type Header   Name DN Value		
* Authentication Scheme	FlexcubeBasicOAMScheme	* Value	·	
— Identity As: This will cause	· sertion an assertion to be generated for the user, o	Identity Assertion has not been enab this policy. Enable Identity Assertion i		
Responses	es not have any Responses	Гуре	Value	

8. Click on Apply to Save the Changes

	e defined to protect one or more resources in		s Manager to grant access to the user making the request.
Confirmat	ion		
uthentication F	Policy, Protected Resource Policy, modified su	ccessfully	
* Name	Protected Resource Policy	Success URL	
Description	Policy set during domain creation. Add reso to this policy to protect them.	Failure URL	
uthentication Scheme	FlexcubeBasicOAMScheme		
sources Re	sponses Advanced Rules		
Identity Ass	sertion		
	an assertion to be generated for the user on	ionally containing any Asserted Attribute set below.	

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

and Ded	Application Descripton	
aunch Pad	Application Domain x FlexcubeWebgate x	
Access	Manager >	
lexcub	DeWebgate Application Domain	
pplication E	Domain provides a logical container for resources or sets	of resources, and the associated policies that dictate who can access specific protected resources.
Summary	Resources Authentication Policies Authorization	Policies Token Issuance Policies Administration
		Policies Token Issuance Policies Administration
	1	
	existing Authorization Policy from the list or click the Create	
Select an e	existing Authorization Policy from the list or click the Create	e Authorization Policy button to create a new one.
Select an e	1	e Authorization Policy button to create a new one.  Comparison Detect
Select an e	existing Authorization Policy from the list or click the Create	e Authorization Policy button to create a new one.
Select an e	vising Authorization Policy from the list or click the Create     View      + Create      Duplicate      Edit     Name     Public Resource Policy	Authorization Policy button to create a new one.     Delete     Description     Policy set during domain creation. Add resources to this policy to allow anyone access.
Select an e	existing Authorization Policy from the list or click the Create View View + Create Duplicate / Edit Name	Authorization Policy button to create a new one.      Delete     Description
Select an e	vising Authorization Policy from the list or click the Create     View      + Create      Duplicate      Edit     Name     Public Resource Policy	Authorization Policy button to create a new one.     Delete     Description     Policy set during domain creation. Add resources to this policy to allow anyone access.
Select an e	vising Authorization Policy from the list or click the Create     View      + Create      Duplicate      Edit     Name     Public Resource Policy	Authorization Policy button to create a new one.     Delete     Description     Policy set during domain creation. Add resources to this policy to allow anyone access.

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



aunch Pad Application Domair	n x FlexcubeWebgate x	FlexcubeWebgate : Protect	×			[
Access Manager >						
rotected Resource P	olicy Authorization Polic	y			Duplicate	Appl
Identity Assertion						
This will cause an assertion t		optionally containing any Asserte	d Attribute set below.			
	o be generated for the user, o	pptionally containing any Asserte	d Attribute set below.			

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

Туре	: Header
Name	: DN
Value	: \$user.attr.dn

Click on Add button

ch Pad Application Domain x FlexcubeWebgate	FlexcubeWebgate : Protect x	C.
Access Manager > tected Resource Policy Authorization Pr		Duplicate Apply
rization policy contains a set of conditions that define v tions apply to all resources within a specific Authorizat mmary Resources Conditions Rules Respo	*Type Header	ization rules and
Identity Assertion	Name DN	
This will cause an assertion to be generated for the us	Suser.attr.gn	
Responses + Add / Edit X Delete	Identity Assertion has not been enabled for	
This Policy does not have any Responses	this policy Enable Identity Assertion in order	
nt © 2000, 2015, Oracle and/or its affiliates. All rights reserve		

12. Click on 'Apply' to Save the changes.



	ess Management	Ta Appli	cation Security	Mobile Security	🛱 Configura
nch Pad Application Domain	× FlexcubeWebgate ×	FlexcubeWebgate : Protect ×			
Access Manager > rotected Resource Po horization policy contains a set o iditions apply to all resources with	of conditions that define wheth	ner a user should be permitted or den olicy.	ied access to the resources protec		Duplicate App
					×
Confirmation Authorization Policy, Protected R	Resource Policy, modified suc	cessfully			
Authorization Policy, Protected R		-			
Authorization Policy, Protected R ummary Resources Condi	tions Rules Responses	-	ute set below.		
Authorization Policy, Protected R ummary Resources Condi Identity Assertion This will cause an assertion to	tions Rules Responses	3	ute set below.		
Authorization Policy, Protected R ummary Resources Condi Identity Assertion This will cause an assertion to	tions Rules Responses	3	ute set below. Value		

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

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

- Navigate to <DOMAIN\_HOME>/output/\$WebgateAgentName
- Select the following files

ObAccessClient.xml

password.xml

cwallet.sso

cwallet.sso.lck

Copy the files to <ORACLE\_MIDDLEWARE>/<ORACLE\_WIBTIER\_HOME> /instances/instance1/ config/OHS/ohs1/webgate/config/

• Select the remaining 2 files

aaa\_key.pem

aaa\_cert.pem

• Copy the files to <ORACLE\_MIDDLEWARE>/<ORACLE\_WIBTIER\_HOME> /instances/instance1/ config/OHS/ohs1/webgate/config/simple

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

Use the ORAPKI tool to import the Flexcube and OAM Server certificates to Oracle HTTP Server. Add <Oracle\_MIDDLEWARE>/oracle\_common/bin to PATH environment variable and also set JAVA\_HOME environment variable. Execute the below command in the command line.



orapki wallet add -wallet

<Oracle\_MIDDLEWARE>/<ORACLE\_WEBTIER\_HOME>/instances/instance1/config/OHS/ohs1/keystore
s/default -trusted\_cert -cert <export\_certificate\_file\_name\_with\_location.cer> -auto\_login\_only

Note: Certificate has to be imported into OHS Wallet.

#### 2.6.5.4 Configuring mod\_wl\_ohs for Oracle HTTP server Routing

To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server, add the directive shown below to the mod\_wl\_ohs.conf file available in <ORACLE\_MIDDLEWARE> /<ORACLE\_WEBTIER\_HOME>/instances/instance1/config/OHS/ohs1.

<Location /FCJNeoWeb>

SetHandler weblogic-handler

WebLogicHost ofss00002.in.oracle.com

WeblogicPort 7002

WLProxySSL ON

SecureProxy ON

WLSSLWallet

"<ORACLE\_MIDDLEWARE>/<ORACLE\_WEBTIER\_HOME>/instances/instance1/config/OHS/ohs1/keystores/default"

</Location>

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

#### 2.6.5.5 Verify the Webgate 11g Agent Created

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

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



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

Cache Name	State			(seconds)		Memory Footprint (bvtes)
Resource to Authentication Scheme		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.



Oracle Access Manager Test Too	_ ×
File Edit Test Help	
Server Connection	
IP Addr Port Max C *Age	
	beWebgate
Secon	Pa ?
Min C Timeou Mo Global Passp	
Min C         Timeou         Mo         Global Passo           1         30000         si         >         ***********         III	<ul> <li>Connect</li> </ul>
Protected Resource URI	3
Sche *H Port	Get Auth S
Resour Oper	
/FCINeoWeb Get	Validate
User Identity	
IP Address *Username Password	
	Authenti
User Certifica	✓ Authorize
_ Status Messages	
[1/11/13 5:33 PM][response] Connected to primary access server	
[1/11/13 5:34 PM][request][validate] yes	channe lavel - 1
[1/11/13 5:34 PM][response] Authentication scheme : FlexcubeAuthn [1/11/13 5:34 PM][response] Redirect URL : https://ofss220028.in.orad	
[1/11/13 5:34 PM][response] Credentials expected : 0x1 (basic)	E
[1/11/13 5:34 PM][request][authenticate] yes	
[1/11/13 5:34 PM][response] User DN : cn=SARAN,cn=users,dc=oracl	
[1/11/13 5:34 PM][response] SessionID : 6e531a7f-460d-4db8-b872-a	
[1/11/13 5:34 PM][response][action] DN : cn=SARAN,cn=users,dc=ord	icle,dc=com
[1/11/13 5:34 PM][response][action] OAM_IMPERSONATOR_USER :	
[1/11/13 5:34 PMI(request)[authorize] ves	
Elapsed (β6 Capture Q Empty	🗌 🖬 🗟 🥔

# 2.7 First launch of FLEXCUBE after installation

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

# 2.7.1 Parameter Maintenance

#### 2.7.1.1 Bank Parameter maintenance - UBS

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



Image: Sank Parameters Maintenance		_ ×
🗄 Save		
Bank Code * 000	Bank Name Bank Futura	
Head Office Branch		- 1
Branch Code * 000	Branch Description Bank Futura	
Financial Preferences General Preferences	FATCA	
Format Mask	Year End Profit and Loss	- 1
Cif Mask bbbnnnn	General Ledger * 221000002	
General Ledger Mask * nnnnnnnr	Transaction Code * YET	
Spread	General Ledger Purge Days	
Spread Application Both Legs	Auto Batch	
Spoof Files Purge Days	90	
Inter Pay Lead Days	3	
Cheque Numbering Details	Checksum Algorithm 🔹	
Scheme Automatic	Checksum Algorithm	
Cheque Number Mask NNNNNN	Tor C.	
	Lodgement Numbers Unique For Branch	
TRS Details	Suspense Account	-
Preferences   Account Mask   Field Pr	operties	
Maker	Date Time:	
Checker	Date Time:	
Mod No 229	Record Status Open	ancel
	Authorization Status	

## 2.7.1.2 Parameters Maintenance – IS

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

## 2.7.2 Maintaining LDAP DN for FLEXCUBE users

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

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

LDAP DN value should be entered as complete DN value.

eg.

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



## For FLEXCUBE – UBS

🔶 User Maintenance			-	
🛃 Save				
User Details		User Status	Enabled	
User Identification * Name * User Reference	FCUBSUSER		Hold     Disabled     Locked	
Language * Home Branch *		Classification	<ul><li>Staff</li><li>●Branch</li></ul>	
Customer No Department Code		Status Changed On Last Signed On	2011-01-04	
Department Description Tax Identifier		ELCM User ID	Staff Customer Restriction Required	
LDAP DN Time Level ?	cn=FCUBSUSER,cn=Us	ELCMOSEND	Multi Branch Access	
Amount Format Date Format	T T		Restricted Show Dashboards	
	Auto Authorization		Alerts on Home MFI User F10 Access Required	
Supervisor Identification Supervisor Name	Ξ		<ul> <li>✓ F11 Access Required</li> <li>✓ F12 Access Required</li> </ul>	
User Password		Start Date * 2011-01-04		
Password Password Changed On Email Reference No	2012-01-04	End Date		
Invalid Logins		Screen Saver Details		
No of Cumulative Logins No of Successive Logins	17 0	Screensaver Interval (in seconds)	3600	
Restricted Password   Role	s   Rights   Functions   Tills	Account Classes   Genera	al Ledgers   Limits   Branches	

# For FLEXCUBE - IS

🔶 User Admin					_ >
🗄 Save					
User Details					
Externel Identifier LDAP DN	FCISUSER FCIS User cn=FCUSR,cn=Users,d(	Language * Home Branch * Home Module *	• 000	Classification	<ul> <li>Staff</li> <li>Auto End Of Day</li> <li>Customer</li> </ul>
Modules	Investments Corporate	Status Description User Status	<ul> <li>Enabled</li> <li>Hold</li> <li>Disabled</li> <li>Locked</li> </ul>	Time Level Status Changed On Last Signed On	
Invalid Logins		User Passwords			
Cumulative Successive	0	Password Password Changed On Email		Start Date End Date	* 07/26/2014
Amount Limits					
Override Amount * Transaction Amount * Auth Amount * Date Format	×	Auto Auth Amount Format	No 💌 Dot Comma 💌		
Restricted Passwords	Roles   Functions   Bran	ches   Module   Disallo	wed Functions		
Input by Authorized by		ateTime ateTime	Mod No Open Authorized		Ok Cancel



# 2.7.3 Launching FLEXCUBE

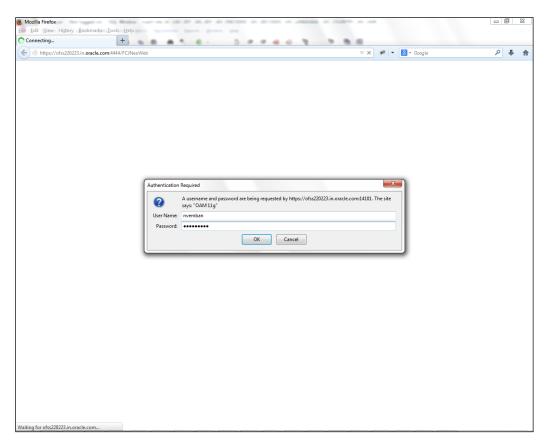
After setting up FLEXCUBE to work on Single Sign on mode, navigate to the URL <u>https://<hostname>:<OHS</u> SSL Port>/<Context Root> from your browser

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

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

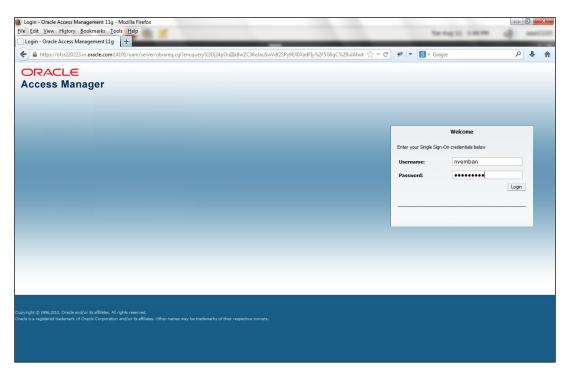


# 2.7.3.1 Basic Style Challenge by Webgate

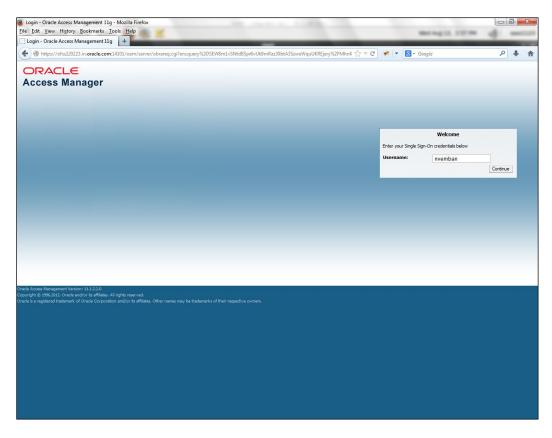




## 2.7.3.2 Form Style Challenge by Webgate



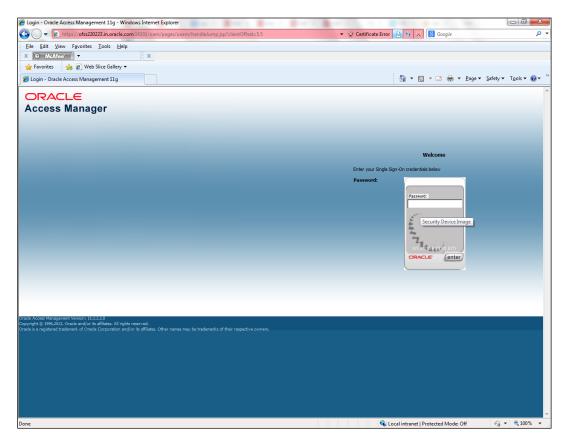
# 2.7.3.3 KBA Based Strong Authentication Challenge by Webgate( Only when OAAM is used)



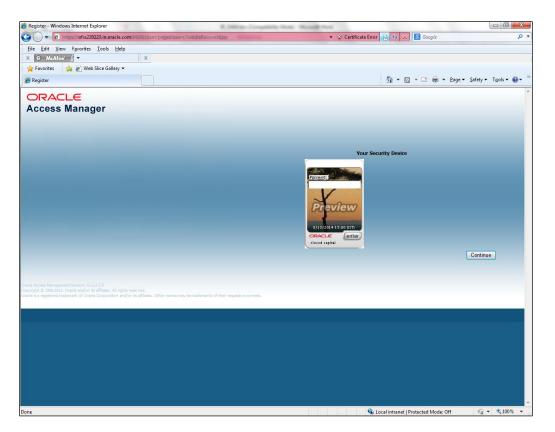


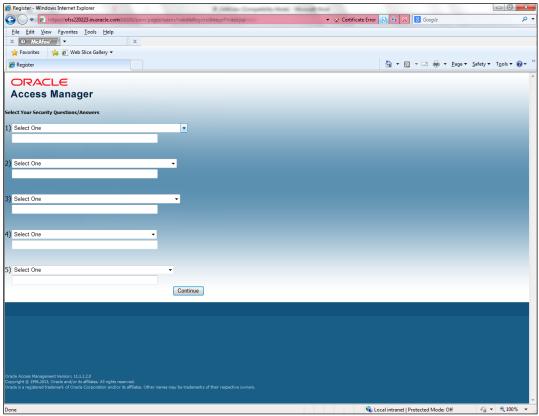


## First Time Login







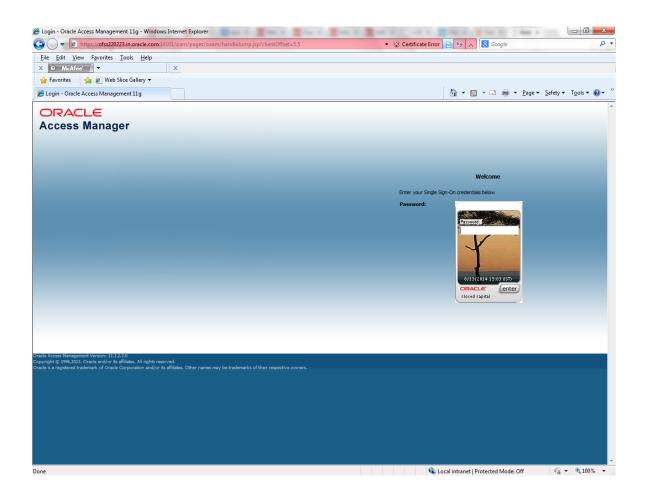




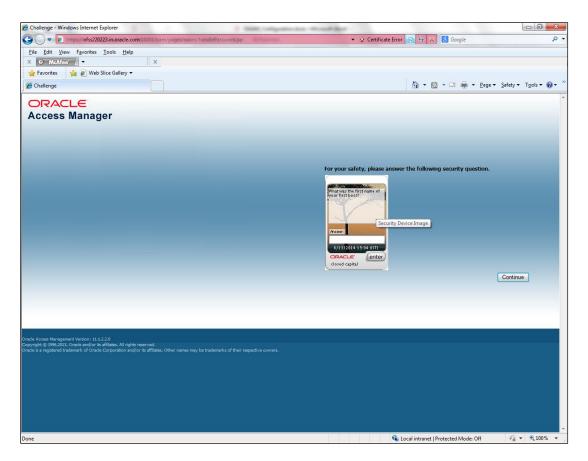
🏀 Register - Windows Internet Explorer	And the second sec	
C v Attps://ofss220223.in.oracle.com:14101/oam/pages/oaam/handleRegisterImagePhrase.jsp	👻 🎗 Certificate Error 💀 🍫 🗙 🖪 Google	+ م
<u>File Edit View Favorites Tools H</u> elp		
X 🛛 McAfee 🕺 🕶 X		
👷 Favorites 🛛 🙀 🙋 Web Slice Gallery 🕶		
<i>€</i> Register	🖄 🕶 🗟 👻 🚍 🖶 Page 🖛 S	afety 🕶 T <u>o</u> ols 🕶 🔞 🕶 🦈
ORACLE		~
Access Manager		
Select Your Security Questions/Answers		
1) Where did you get your first pet?		
OFSS		
2) What is the name of the first musical group you saw in concert? -		
OFSS		
3) What color was your first pet?		
OFSS		
4) What was the first name of your first boss?		
OFSS		
5) Who is your favorite athlete?		
OFSS		
Continue		
Oracle Access Management Version: 11.1.2.2.0 Copyright © 1996,2013, Oracle and/or its affiliates. All rights reserved.		
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.		
		-
/oam/pages/oaam/handleRegisterQuestions.jsp	👊 Local intranet   Protected Mode: Off	🖓 🔻 🔍 100% 🔻 🖉

Post First Login



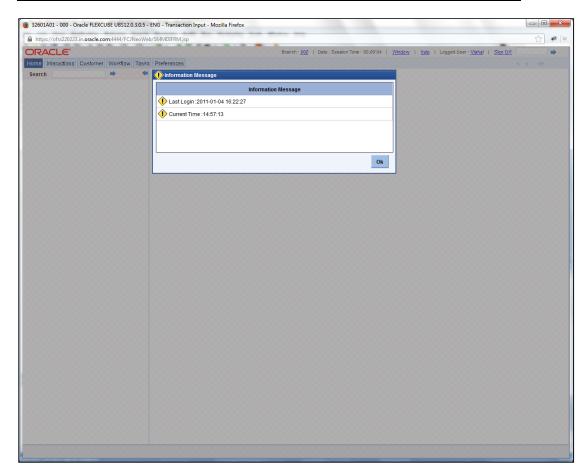






Once the user is authenticated and authorized to access the resource, the request gets redirected to normal FLEXCUBE application and it will take the user to Home Branch.





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

## 2.7.4 Signoff in a SSO Situation

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

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





Oracle Access Manager Integration [May] [2016] Version 12.2.0.0.0

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/

Copyright © [2007], [2016], Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

