Oracle Access Manager Integration Oracle FLEXCUBE Universal Banking

Release 12.87.\$' .0.0

Part No. 9, , \$&1 \$%

FINANCIAL SERVICES



Table of Contents

1. PI	REFACE	
1.1	INTRODUCTION	1-3
1.2	Audience	
1.3	Abbreviations	
1.4	DOCUMENTATION ACCESSIBILITY	
1.5	ORGANIZATION	
1.6	GLOSSARY OF ICONS	
1.0	6.1 Related Documents	
2. EI	NABLING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER	
2.1	INTRODUCTION	
2.2	BACKGROUND AND PREREQUISITES	
2.2	2.1 Software Requirements	
2.3	BACKGROUND 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	1 0	
2.4	4.1 Pre-requisites	
2.5	ENABLING SSL FOR WEBLOGIC AND OAM CONSOLE	
2.3	5.1 Self-signed Certificate Creation:	
2.3	5.2 Configuring Weblogic Console	
2.3	5.3 Configuring SSL Mode in Oracle Internet Directory	
2.6		
2.0	6.1 Identity Store Creation	
2.0	6.2 Creating Authentication Module	
2.0	6.3 Creating Authentication Scheme	
2.0	6.4 Creating OAM 11g Webgate	
2.0	6.5 Post OAM Webgate 11g Creation	
2.7	FIRST LAUNCH OF FLEXCUBE AFTER INSTALLATION	
2.2	7.1 Parameter Maintenance	
2.2	7.2 Maintaining LDAP DN for FLEXCUBE users	
2.2	7.3 Launching FLEXCUBE	
2.2	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 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

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
	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 - 11.1.2.2.0

- Oracle Access Manager 11.1.2.2.0
- Oracle Fusion Middleware Web Tier Utilities 11g Patch Set 6 11.1.1.7.0
 - > Oracle HTTP Server
- Oracle Access Manager OHS 11gR2 WebGates 11.1.2.2.0
- Oracle Access Manager patch set 18333689, 19269297, 18662903
- Optional: Oracle Adaptive Access Manager 11.1.2.2.0 (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						Q
Change Center	🔒 Home Log Out Preferences 🔤 Record H	sip di	٩		Welcor	ne, weblogic Connected to: ia	am_domai
View changes and restarts	Home >Summary 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						
Domain Structure Iam Jonain Charling Constant Servers Custers Virtual Hosts Migratable Targets Coherence Servers Coherence Servers Coherence Servers Sartup and Shutdown Classes Servers Coelevents	A server is an instance of WebLogic Server tha This page summarizes each server that has be () Customize this table Servers (Filtered - More Columns Exist) New Cone Delete			own configuration.		Showing 1 to 4 of 4 Previous	s Next
Services	🔲 Name 🏟	Cluster	Machine	State	Health	Listen Port	
How do I	AdminServer(admin)			RUNNING	🖋 ОК	7001	
	oam_server1			RUNNING	✓ OK	14100	
Create Managed Servers Clone Servers	oim_server1			RUNNING	🖋 ОК	14000	
Cone Servers Delete Managed Servers	soa_server1		LocalMachine	SHUTDOWN		8001	
Delete the Administration Server Start and stop servers	New Clone Delete					Showing 1 to 4 of 4 Previous	3 Next
System Status							
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.



	General	Cluster	Services	Keystores	SSL	Federation Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services		
Domain Structure															
iam_domain	Save														
ServersClustersVirtual HostsMigratable TargetsCoherence Servers	Use this pa View JNDI	-	igure gener	ral features o	f this se	erver such as default ne	twork communic	ations.							
Coherence Clusters Machines Work Managers	Name:					AdminSe	rver			An alphanumeric name for this server instance. More Info					
Startup and Shutdown Classes Deployments Deployments	Machine:					(None)					The WebLogic Server host computer (machine) on which this server is meant to run. More \ensuremath{Info}				
How do I	Cluster:					(Standal	one)			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:									dress or DNS name t ns. More Info	his server uses t	o listen for incom	ing	
Configure clusters Start and stop servers Configure WLDF diagnostic volume	💟 Listen I	Port Enab	led							Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info					
System Status	Listen Por	t				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 Lis	ten Port E	inabled							Indicates port. Mo	whether the server one Info	can be reached t	through the defau	ult SSL listen	
Critical (0) Overloaded (0) Warning (0)	SSL Listen	Port:				7002				The TCP/IP port at which this server listens for SSL connection requests. More Info					
OK (3)	🗹 👌 Clie	ent Cert Pi	roxy Enab	oled						Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info					
	Java Com	piler:				javac				The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info					
	Diagnostic	: Volume:				Low	T			Specifies the volume of diagnostic data that is automatically produced by WebLogic Server at run time. Note that the WDP diagnostic volume setting does not affect exploitly configured diagnostic modules. For example, this controls the volume of events generated for 'Rodit Flight Recorder. More Info					
	— 🛡 Advar	nced —													
	Virtual Ma	Virtual Machine Name:					lomain_Adm	inSe		When WLS is running on JRVE, this specifies the name of the virtual machine running this server $\mbox{More Info}$					
	🗹 👌 We	☑ d 문 WebLogic Plug-In Enabled							Specifies whether this server uses the proprietary WL-Proxy-Client-IP header, which is recommended if the server instance will receive requests from a proxy plug-in. More Info						

2.5.2.3 Follow the steps in Keystores Tab as shown below:

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

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

	Administration Conso	ole									õ
Change Center	🔒 Home Log Out P	references 🔤 Record He	lp	Q					Welcome, we	eblogic Connec	ted to: iam_domain
View changes and restarts	Home >Summary of S	ervers >AdminServer									
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Settings for Admins Configuration Pr	otocols Logging Debu	g Monitoring Contro	Deployments	Services	Security	Notes				
Domain Structure	General Cluster	Services Keystores	SSL Federation Servi	es Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services	
am_domain		ne secure storage and mana security of message transmi		id trusted certifica	te authorities	: (CAs). This	s page lets yo	ou view and define va	rious keystore o	onfigurations. Th	ese settings help
Coherence Clusters Machines Work Managers Startup and Shutdown Classes Deployments Generative Beating	Keystores: Save Cancel	Custom Identity and	LCommand Line Tru Custom Trust Java Standard Trus					configuration rules shi :ystores? More Info		finding the serve	r's identity and
How do I											
Configure identity and trust Configure keystores Set up SSL											
System Status											
Health of Running Servers Faled (0) Critical (0) Critical (0) Verloaded (0) Warning (0) Ok (3) WebLogic Server Version: 10.3.5.0 Copyright © 1966.0010, Cracle and/or to affiliates. Al 1	i rights reserved.										
Oracle is a registered trademark of Oracle Corporation	n and/or its affiliates. Other r	names may be trademarks of t	heir respective owners.								



2.5.2.4 Follow the steps in Keystores Tab as shown below:

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

ORACLE WebLogic Server® A	Administration Console		Q										
Change Center	🏦 Home Log Out Preferences 🐼 Record Help	Q	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	g Control Deployments Services Security	Notes										
Domain Structure	General Cluster Services Keystores SSL Feder	ation Services Deployment Migration Tuning	Overload Health Monitoring Server Start Web Services										
iam_domain	Save												
Servers													
Clusters Virtual Hosts Migratable Targets ==	Keystores ensure the secure storage and management of priv you to manage the security of message transmissions.	ate keys and trusted certificate authorities (CAs). This p	age lets you view and define various keystore configurations. These settings help										
Coherence Servers													
Coherence Clusters Machines	Keystores:	Custom Identity and Custom Trust Change	Which configuration rules should be used for finding the server's identity and trust keystores? More Info										
Work Managers Startup and Shutdown Classes	- Identity /scratch/app/fmw115/0am1115/BaseKeyStore/AdminFlexcubeKeyStor												
Deployments HServices	Custom Identity Keystore:	nFlexcubeKeyStore.jks	The stand of the s										
-Security Realms													
How do I 😑	Custom Identity Keystore Type:	jks	The type of the keystore. Generally, this is JKS. More Info										
Configure identity and trust Configure keystores	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										
Set up SSL	Confirm Custom Identity Keystore Passphrase:	•••••											
System Status	Trust												
Health of Running Servers Failed (0)	Custom Trust Keystore:	nFlexcubeKeyStore.jks	o/fmw115/oam1115/BaseKeyStore/AdminFlexcubeKeyStore.jks										
Critical (0) Overloaded (0)	Custom Trust Keystore Type:	jks	The type of the keystore. Generally, this is JKS. More Info										
Warning (0) OK (3)	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:	•••••											
	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. Click on Save.



Change Center	館 Home Log Out Preferences 🔤 Rec	ord Help	Q	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 I	Deployments Services Securit	Notes							
Domain Structure	General Cluster Services Keysto	res SSL Federation Services [Deployment Migration Tuning	Overload Health Monitoring Server Start Web Services							
ian_domain ▲ Environment -Servers -Clusters -Virtual Hosts -Virtual Hosts -Virtual Hosts -Virtual Hosts -Virtual Hosts -Virtual Hosts -Virtual Hosts -Virtual Hosts -Coherence Servers -Coherence Servers -Coherence Servers -Machines -Machin	Save										
	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								
Work ManagersStartup and Shutdown Classes	Private Key Location:	from Custom Identity Keystore		The keystore attribute that defines the location of the private key file. More Info							
-Security Realms	Private Key Alias:	FlexcubeCert		The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info							
How do I											
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 Configure a custom host name verifier 	街 Confirm Private Key Passphrase:										
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)	- 🗢 Advanced										
Overloaded (0) Warning (0) OK (2)	億日 Hostname Verification:	None Custom Hostname Verifie BEA Hostname Verifier	Specifies whether to ignore the installed implementation of the weblogic.security.SSLHostnameVerifier interface (when this server is acting as a client to another application server). More Info								
	街 Custom Hostname Verifier:	None	The name of the class that implements the weblogic.security.SSLHostnameVerifier 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							

5. 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®	Administration Console					õ								
Change Center	🔒 Home Log Out Preferences 🔤 Record Help	Q			Welcome, v	veblogic Connected to: iam_domain								
View changes and restarts	Home >Summary of Servers >AdminServer >Summa	ary of Servers												
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Summary of Servers Configuration Control													
Domain Structure iam_domain	A server is an instance of WebLogic Server that n This page summarizes each server that has been () () (ustomize this table Servers (riltered - More Columns Exist) New (Cone) Delete			fguration.	S	rowing 1 to 4 of 4 Previous Next								
Deployments Services	🔲 Name 🏟	Cluster	Machine	State	Health	Listen Port								
Security Realms	AdminServer(admin)			RUNNING	✓ ОК	7001								
How do I	oam_server1			RUNNING	🖋 ОК	14100								
Create Managed Servers	oim_server1			RUNNING	🖋 ОК	14000								
Clone Servers	soa_server1		LocalMachine	SHUTDOWN		8001								
Delete Managed Servers Delete the Administration Server Start and stop servers	New Clone Delete				Sł	owing 1 to 4 of 4 Previous Next								
System Status														
Critical (0) Overloaded (0) Warning (0) OK (3)														

6. 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.

ORACLE Enterprise Ma	inag	er 11g Fusion Middleware	Contro	l.											Setup 🗸 H	elp 👻 Log Out
📲 Farm 👻 🔒 Topology																
•		oid1 🕡													Logged in as weblogic	Host padsrini-pr
🗄 📲 Farm_base_domain															Page Refreshed Feb 15, 2013 4	35:59 PM IST 🕻
Application Deployments		Home														
			-													
		Monitoring	>			Load						5	ecurity			
Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system			>))		121	Total LDA	P Connectio	ns			0		Failed Bind C	Operation	ns	0
		Logs			220	Operation	s Completed	1			2		Failed Super	User Log	gins	0
		Dest lisses	-													0
		Administration	,		60	Operation	s in progress				U		Sucessful Sup	per User	Logins	U
Farm ~ Image: Comparing the second and the second a		Security	>	Audit Policy												
Form base_domain Application Deployments Application Deployments																
			—T													
															Server Response (ms)	
		8														
		6														
		4													Total Operations	
		2														
		0														
		20														
															CPU Utilization (%)	
														-	/Farm_base_domain/asinst_1/	pid1
		-														
														-		
															Memory Utilization (%)	
														=	<pre>/Farm_base_domain/asinst_1// padsrini-pc</pre>	pid1
		20													padshin-pc	
		0 16:22 16:23 February 15	16:	24 16:25 16:	26 16:2	27 16:28	16:29	16:30	16:31	16:32	16:33	16:34	16:35	16:36		
		February 15	2013													Table View
																FORCE HEH

2. Click 'Create Self-Signed Wallet'.

	nager 11g Fusion Middleware Control Setup - Help - Log Out
📑 Farm 👻 🔒 Topology	
	û oid1 ₀ î Orade Internet Directory ▼ Page Refreshed Feb 15, 2013 43954 PM IST (***)
	Wallets A Vallet 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.
OIM OVd1	Create % Delete Create Self-Signed Walet 🔄 Export 6d Manage
Metadata Repositories	Name Auto-login
🗄 🚞 Web Tier	
	Fetring Data
ł	

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



	anager 11g Fusion M	liddleware Control	Setup → Help → Log Out			
Farm - A Topology						
□ •	🔂 oid1 🗿		Logged in as weblogic Host padsrini-pc			
Farm_base_domain Application Deployments	Oracle Internet Di	irectory 🕶	Page Refreshed Feb 15, 2013 4:40:45 PM IST €2			
WebLogic Domain	Wallets > Create Se					
Identity and Access	Create Self-Sig		OK Cancel			
OAM E oid1 OIM ovd1	or password-protecte PKCS#12 wallet that	ed. Passwords, if specified, have a mi	If signed wallet is not recommended in a production environment. The wallet name should be unique for a given component. The wallet pipe can be auto-login timum length of eight characters, and contain alphabetic characters combined with numeir or special divarcters. Auto-login wallet is an obfiscated from of es 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			
🗄 🚞 Metadata Repositories	Self-Signed Wallet	Details				
🗉 🚞 Web Tier						
	* Wallet Name	-				
	Wallet Password	V Auto-login				
	Confirm Password					
	Add Self-Signed Certificate					
	Add a self-signed cer	tificate that becomes part of the wall	let.			
	* Common Name	hostname.in.orade.com				
	Organizational Unit	OFSS				
	 Organization 	Orade				
	City	Chennai				
	State	TN				
	Country	India 💌				
	Key Size	2048 💌				

4. Click 6d Manage...

ORACLE Enterprise Ma	nager 11g Fusion Middleware Control	Setup → Help → Log Out
🛱 Farm 👻 🔒 Topology		
▼ Farm_base_domain		Logged in as weblogic (Host padsrini-pc Page Refreshed Feb 15, 2013 4144127 PM IST 🖏
	Wallets A Wallet 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 dick Manage.	create a wallet, click Create. To create a wallet with a self-signed certificate, click Create Self-Signed
OIM Ovd1	Create 🗙 Delete 😭 Create Self-Signed Wallet 💁 Import 🏠 Export	6d Manage
Metadata Repositories	Name ioidselfsigned	Auto-login
ା 플 Metadata Repositories 중 📄 Web Tier	modular of plants	

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

🗟 Farm 👻 🛛 💑 Topology						
-	<pre>介 oid1 ₀</pre>				Logged in as we	blogic Host padsri
Farm_base_domain	■ Oracle Internet Directory				Page Refreshed Feb 15	, 2013 4:45:58 PM IS
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 the	the CSR was generated.				
A OTM						
OIM O ovd1	👍 Add Certificate Request 🛛 👌 Import 🕅 😭 Export 💥 Delete					
🐼 ovd1	Add Certificate Request Market Market Market	Certificate Type	Status	Key Size	Start Date	Expiration Date
🐼 ovd1 🛅 Metadata Repositories		Certificate Type Certificate Request		Key Size 2048	Start Date	Expiration Date
🐼 ovd1 🛅 Metadata Repositories	Subject Name				Start Date February 15, 2013	
🐼 ovd1 🛅 Metadata Repositories	Subject Name CN=paderini-pc,OU=OFSS,O=Orade,L=Chennal,ST=TN,C=IN	Certificate Request		2048		
🐼 ovd1 🛅 Metadata Repositories	Subject Name ON=padsrini-pc,OU=OFSS,O=Orade,L=Chernal,ST=TN,C=IN ON=padsrini-pc,OU=OFSS,O=Orade,L=Chernal,ST=TN,C=IN	Certificate Request Certificate	Valid	2048 2048	February 15, 2013	February 14, 20 August 2, 2028
🐼 ovd1 🫅 Metadata Repositories	Subject Name CN=paddrni+p_cOU=OPSS,0=Orade_L=Chernal,ST=TN,C=IN CN=paddrni+p_c,OU=OPSS,0=Orade_L=Chernal,ST=TN,C=IN COU=Opaddrni+p_cOU=OPSS,0=Orade_L=Chernal,ST=TN,C=IN CU=Gasd 3-Public Primary Certification Authority, 0="Verifight, nic.", C=US Cuertification Authority, 0="Verification Authority, 0="Verification"	Certificate Request Certificate Trusted Certificate	Valid Valid	2048 2048 1024	February 15, 2013 January 29, 1996	February 14, 20: August 2, 2028 August 14, 2018
	Subject Name ON=podsrini-pc_OU=OFSS,O=Orade,L=Chemnal,ST=TN,C=IN ON=podsrini-pc_OU=OFSS,O=Orade,L=Chemnal,ST=TN,C=IN OU=Otass Public Primary Certification Autority, o=VerSign, Inc.*, C=US OU=Otass Public Primary Certification Autority, o=VerSign, Inc.*, C=US OU=Otass Public Primary Certification Autority, o=VerSign, Inc.*, C=US	Certificate Request Certificate Trusted Certificate Trusted Certificate	Valid Valid Valid	2048 2048 1024 1024	February 15, 2013 January 29, 1996 August 13, 1998	February 14, 201 August 2, 2028 August 14, 2018

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



	anager 11g Fusion Middleware Control		Setu	p 👻 Help 👻 Log Out
Farm - 🔒 Topology				
	☆ oid1 ^③			blogic Host padsrini-pc
Farm_base_domain Application Deployments	🖭 Orade Internet Directory 🔻		Page Refreshed Feb 15	, 2013 4:45:58 PM IST 🗘
Application Departments Application Comparison Identity and Access OAM Odd Odd Odd Odd Odd Odd Odd Odd	Walets > Manage Certificates Manage Certificates: oidselfsig To generate a certificate signing request (certificate or trusted cert, citck Import. Yo Add Certificate Request 1 2 1	Trusted Certificate The Trusted Certificate with Subject Name CN=paddrini-pc, OU=OFSS, O=Orade, L=Chennal, ST=TN, C=IN is shown below. You can cut and paste the entire text in the box from BEGIN CERTIFICATE to BIO CERTIFICATE to the interded to catalon; or dut "Export Trusted Certificate" to export the certificate to a Site. You may want to do this if another party	certificate. To import	the CA signed
Metadata Repositories Web Tier	Subject Name CH-padatri-pc, CU-OPS, O-Ora CH-padatri-pc, CU-OPS, O-Or CU-Class 3 Public Primary Cettific CH-OTEC-UperTrust Clabal Root, I CH-padatri-pc, CU-OPES, O-OU CU-Class 2 Public Primary Cettific OU-Class 1 Public Primary Cettific	wants to tust your certificate directlyBSCIII CERTIFICATE HIIDDOCCALAQAMPOYINGETHORINGETHERGAWY)ELMAKGAUTEBBMOSUFACCAJB9HVBAgTALBOHRAW DGYTUYQDBWAGAGWUAHAPWGAUQTUYQDBWAGAGWUAHATBBWOSUFACCAJB9HVBAGTALBOHRAWT CSUBLDWYANGULASWAGWUAHATANHTWANTUKATANTTANTUKAYUNYUNYILANAKAITUBBAH CGUNAGAUNAHATANTUKATANHTWANTUKATANTUKAYUNYUNYILANAKAITUBBAHO CGUNAGAUNAHATANTUKATANHTWANTUKATANTUKAYUNYUNYILANAKAITUBBAHO CGUNAGAUNAHATANTUKATANTUKATANTUKATANTUKAYUNYUNYILANAKAITUBBAHO CGUNAGAUNAHATANTUKATANTUKATANTUKAYUNYILANATANTUKATUKATUKATUKATUKATUKATUKATUKATUKATUKA	Start Date February 15, 2013 January 29, 1996 August 13, 1998 February 15, 2013 January 29, 1996 January 29, 1996	Expiration Date February 14, 2018 August 2, 2028 August 14, 2018 February 14, 2018 August 2, 2028 January 8, 2020

7. Click 'Server Properties'.

Logged in as weblogic Host par						
Page Refreshed Feb 15, 2013 4:45:58 PM						
Page Kerreshed Heb 15, 2013 4145158 PM						
signed st (CSR), dx. "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.						
Start Date Expiration Date						
February 15, 2013 February 14,						
January 29, 1996 August 2, 202						
August 13, 1998 August 14, 20						
February 15, 2013 February 14,						
January 29, 1996 August 2, 202						
January 29, 1996 January 8, 20						
January 29, 1996 Augu August 13, 1998 Augu February 15, 2013 Febru January 29, 1996 Augu						

8. Click 'Change SSL Settings'.

	lanager 11g Fusion Middleware Control	Setup → Help → Log Out
📑 Farm 👻 👗 Topology		
≡ -	☆ oid1 ₀	Logged in as weblogic Host padsrini-pc
🗉 丹 Farm_base_domain	Oracle Internet Directory	Page Refreshed Feb 15, 2013 4:54:17 PM IST €2
Application Deployments		
🗄 🛅 WebLogic Domain	Server Properties	Apply Revert
Identity and Access		Apply Revert
OAM	General Performance SASL Statistics Logging	
2 oid1	Server Mode Read / Write 💌	
OIM	* Maximum number of entries to be returned by a search 10000	
 ovd1 Metadata Repositories 	* Maximum time allowed for a search to complete (sec) 3600	
Metadata Repositories 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)	
	* Maximum Number of Operations allowed in a Transaction 0	
	Port Numbers	
	SSL Port 3131 Change SSL Settings	
	•	

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 🖏
E Application Deployments		
🗉 🛅 WebLogic Domain	1 Information	
Identity and Access	All changes made in this page require a server restart to take effect.	
OAM	SSL Configuration ③	OK Cancel
	Enable SSL	
🐼 ovd1	Server Wallet Name oidselfsigned 🔻	
🗄 🛅 Metadata Repositories	oldselfslaned to required for no-auth mode but is needed in other modes.	
🖭 🛅 Web Tier	□Advanced SSL settings	
	Server SSL properties	
	SSL Authentication Server Authentication	
	VSL_RSA_WITH_RC4_128_MD5	
	Ciober Suite SSL_RSA_WITH_RC4_128_SHA	
	V SSL_RSA_WITH_3DES_EDE_CBC_SHA	
	VITLS_RSA_WITH_DES_CBC_SHA	
	* SSL Protocol Version All	
1		

10. Click 'Apply'.

ORACLE Enterprise Ma	anager 11g Fusion Middleware Control	Setup ▾ Help ▾ Log Out
📑 Farm 👻 🔒 Topology		
□ •	☆ oid1 ₀	Logged in as weblogic Host padsrini-pc
1 📑 Farm_base_domain	E Orade Internet Directory -	Page Refreshed Feb 15, 2013 4:56:40 PM IST 🗘
Application Deployments		
🗄 🚞 WebLogic Domain	1 Information	×
Identity and Access OAM	SSL configuration updated for /Farm_base_domain/asinst_1/oid1. Restart component for this change to be effective.	
DI OAM		
Ø ovd1	Server Properties	Apply Revert
🗄 🚞 Metadata Repositories	General Performance SASL Statistics Logging	
🗉 🚞 Web Tier	Server Mode Read / Write 💌	
	* Maximum number of entries to be returned by a search 10000	
	* Maximum time allowed for a search to complete (sec) 3600	
	Preserve Case of Required Attribute Name specified in Search Request	
	Anonymous Bind Disallow except for Read Access on the root DSE	
	* Maximum time allowed in a Transaction (sec) 0	
	* Maximum Number of Operations allowed in a Transaction 0	
	Port Numbers	
	Non-SSL Port 3060	
	SSL Port 3131	

2.5.3.1 Import LDAP Server SSL Certificate into OAM Server

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

For eg:

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

Restart Both OID & OAM Server.

2.6 Configuring SSO in OAM Console

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

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



Refer the Oracle Support Document ID: 1678062.1 , before configuring Webgate against Oracle HTTP Server.

2.6.1 Identity Store Creation

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

ORACLE' Access Management			Accessibility Help Sign Ou	it weblogic
C Launch Pad				
Welcome to Oracle Access Management				
		Host Identifiers	 Esssion Management Password Policy 	
B Identity Federation Ø	+ -	🚆 Security Token Service 🖉		+ -
3 Identity Provider Administration Service Provider Administration		් Partners හිනි Partner Profiles ලී Endpoints	🛃 Token Valdation Templates 🗃 Token Issuance Templates 🎬 Custom Tokens	
Mobile and Social 🖉		Access Portal Service 🖉		+ -
Mobile Services 💦 OAuth Service		∰ Credential Sharing Groups ► Password Generation Policies	🕵 Global Agent Settings	
& Configuration				
Available Services Service Settings Service Settings Service Settings Settings Settings Service Settings				

2. Click 'Create' under OAM ID Stores.



	nagement			A	ccessibility Help	Sign Out weblogic 📿
🖸 Launch Pad 🛛 🌋 User Identity	/ Stores ×					
User Identity Stores						
Default and System Store						Apply
1.1	Default Store UserIdentityStore1					
	* System Store UserIdentityStore 1 💌					
	System Store Use IdentityStore I					
OAM ID Stores						Sync IDS Profiles
Manage local User Identity Stores. Th	nis includes IDS Profiles that are synchronize	ed by using Sync IDS Profiles button.				
View 🔻 🎴 Create 🖉 Edit	💥 Delete					
Name	Directory Type	Host Information		Description		Synched IDS Profiles
UserIdentityStore 1	EMBEDDED LDAP	ldap-host:7001				No
Manage common Identity Directory		will appear in OAM ID Stores table. You h	ave to synchronize IDS Profiles created o	utside Oracle Access Management Console using Sy	nc IDS Profile button	
Wew - Coreste / Lore						
Name	Description		Repository Name	Created By		
Name userrole	Description User/Role entities in Def	fault Identity Directory	Repository Name	Created By OPSS		
	User/Role entities in Def	fault Identity Directory is in Default Identity Directory	Repository Name			
userrole idxuserrole IDS Repositories Manage Identity Directory Service R	User/Role entities in Del Fusion User/Role entitie Repositories that are common across Orade	is in Default Identity Directory	Repository Name	OPSS		
userrole idxuserrole IDS Repositories Manage Identity Directory Service R View Create Create	User/Role entities in Del Fusion User/Role entitie Repositories that are common across Orade	is in Default Identity Directory		OPSS OPSS		
userrole idxuserrole IDS Repositories Manage Identity Directory Service R	User/Role entities in Del Fusion User/Role entitie Repositories that are common across Orade	is in Default Identity Directory	Repository Name	OPSS OPSS		

- 3. Enter the below details in the Create User Identity Store Form
 - 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.
 - User Search Base: Full DN for the node at which enterprise users are stored in the directory; for example, cn=Users,realm_DN.
 - Group Search Base: Currently only static groups are supported, with the uniquemember attribute. The node in the directory information tree (DIT) under which group data is stored, and the highest possible base for all group data searches.



Launch Pad Store User Identity Store	res × Create: User Identity Sto.				Test Connection	(Apply
•	-			Enable SSL	Test connection	obbit 1
* Store Name			Prefetched Attributes	V LIADIE 33L		
* Store Type Description	OID: Orade Internet Directory					
Description						
Location and Credentials						
* Location	ofss220223.in.oracle.com:3131			cn=ordadmin		
			* Password	•••••		
Users and Groups						
osers and Groups	* Login ID Attribute	-				
	User Password Attribute					
		cn=Users,dc=in,dc=oracle,dc=com				
	User Filter Object Classes					
	Group Name Attribute					
		cn=Groups,dc=in,dc=orade,dc=com				
	Group Filter Classes					
Enable Group Membership Cache						
	Group Membership Cache Maximum Size	10000				
	bership Cache Time to Live (in seconds)	0 🛊				
Connection Details						
Minir	num Pool Size 10 🗘		Results time limi	t (in seconds) 0 🛢		
Maxim	num Pool Size 50 🖨			Retry Count 3 🗘		
Wait Timeout	t (in seconds) 120 🖨		R	eferral Policy follow		
Inactivity Timeou	t (in seconds)					

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

aunch Pad 🛛 🌋 User Identity Stores × Create: User Identity Sto ×			
ate: User Identity Store			Test Connection Apply
* Store Name FlexcubeStore		Tenable SSL	Connection Status ×
* Store Type OID: Orade Internet Directory	Prefetched Attributes		Connection to the User Identity Store
Description			successful!
			OK Cancel
ocation and Credentials			
*Location ofss220223.in.orade.com:3131	* Bind D/	cn=orcladmin	
	* Password	i •••••	
* Login ID Attribute on			
User Password Attribute userPassword			
* User Search Base on=Users.dc=in.dc=orade.dc=com			
User Filter Object Classes			
Group Name Attribute			
* Group Search Base cn=Groups,dc=in,dc=orade,dc=com			
Group Filter Classes			
Enable Group Membership Cache			
Group Membership Cache Maximum Size 10000 🗘			
Group Membership Cache Time to Live (in seconds)			
onnection Details			
Minimum Pool Size 10 🗘	Results time lim	it (in seconds) 0	
Maximum Pool Size 50 💲		Retry Count 3 🗘	
Wait Timeout (in seconds) 120 🗘	F	Referral Policy follow	
Inactivity Timeout (in seconds)			

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

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



ORACLE' Access M	anagement				Accessibility Help Sign Out weblogic	9
🖸 Launch Pad 🛛 🌋 User Identity	Stores × FlexcubeStore ×				l	ž
FlexcubeStore					Test Connection Apply	
Confirmation					×	٦
User Identity Store FlexcubeSto	re created successfully.					
Shore Marr	e FlexcubeStore			Enable SSL		-
	e OID: Orade Internet Directory	•	Prefetched Attributes	Lindoic Sac		
Descriptio						
▲ Location and Credentials						
_	tion ofss220223.in.orade.com:3131		* Bind DN	cn=orcladmin		
			* Password	•••••		
✓ Users and Groups						
	* Login ID Attribute	a				
	User Password Attribute	userPassword				
	* User Search Base	cn=Users,dc=in,dc=orade,dc=com				
	User Filter Object Classes					
	Group Name Attribute					
	* Group Search Base	cn=Groups,dc=in,dc=oracle,dc=com				
	Group Filter Classes					
Enable Group Membership Cach	e					
	Group Membership Cache Maximum Size	10000 0				
Group M	embership Cache Time to Live (in seconds)	0 🗘				
Connection Details						
_	inimum Pool Size 10 🗘		Results time limit	t (in seconds) 0 🛊		
	aximum Pool Size 50 🗘			Retry Count 3 \$		
	out (in seconds) 120 🗘			eferral Policy follow		
	out (in seconds) 0					

2.6.2 Creating Authentication Module

1. Click on in Access Manager to Create LDAP Authentication Modules .

		Accessibility Help Sign Out web
Launch Pad /elcome to Oracle Access Management		
Quick Start Wizards Application Registration SSO Agent Registration	Access Hanager Application Domains Applications Resource Type Host Identifiers Proj.vis	Auther Create Application Domain Auther Create Application Son Create Application Son Create Host Identifier Sessio Create Resource Type Person Create IDAP Authentication Module
il Identity Federation i Identity Frovider Administration i Service Provider Administration	Image: Security Token Service Image: Partners Image: Partner Profiles Image: Partner Partner Partner Profiles Image: Partner	Create Karberos Autrentication Module Create X509 Authentication Module Create Custom Authentication Module Create Authentication Scheme Create 11g Webgate Create 11g Webgate Create 10g Webgate Create 10g Webgate
Mobile and Social	Access Portal Service	🕂 🕁
Configuration I≣ Available Services		

- 2. Click 'Apply' to create Authentication Module.
- 3. Choose the User Identity Created.



Refer the section 'Identity Store Location' of this document.

ORACLE [®] Access Management	Accessibility Help Sign Out weblogic 드			
O Launch Pad 🔡 Authentication Modules × 📑 FlexcubeAuthnHodule ×				
FlexcubeAuthnModule				
Confirmation	×			
LDAP Authentication Module FlexcubeAuthmModule modified successfully.				

2.6.3 Creating Authentication Scheme

1. Click 'Create Authentication Scheme' under Access Manager

ORACLE' Access Management				Accessibility Help Sign Out weblogic	
Launch Pad					
Welcome to Oracle Access Management					
Quick Start Wizards Application Registration Stop Application Stop Application			Access Hanager	Author Create Application Domain Author Create Application () SSO A Create Notifient Session Create Resource Type	
Identity Federation		+ -	Plug-Ins ■ Plug-Ins ■ Security Token Service ② ③ Partners	Pasw Create LDAP Authentication Module Create Konteron Authentication Module Create Konteron Authentication Module Create Custom Authentication Module Create Custom Authentication Module Create Custom Authentication Science Create 11g Webgate	
Letring Provider Administration Service Provider Administration			및 Particles 않 Particles 출 Endpoints	isag Tuken Saj Tuken Create 10g Webgate ∰ Custorii Tokens	
Hobile and Social O	🍓 OAuth Service		Access Portal Service	+ 👻	
& Configuration					
E Available Services	Scormon Settings Access Manager Settings				

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.

http://docs.oracle.com/cd/E27559_01/admin.1112/e27239/shared.htm#BABFCIHA



2.6.3.1.1 Basic Style Authentication Scheme

Enter the below details and click 'Apply':

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

challenge_url=/CredCollectServlet/BASIC

O	DRACLE Access Management Accessability Help Sign Out weblogic Q					
	🖸 Launch Pad 🛛 🍘 FlexcubeBasicOAMScheme ×					
A	Authentication Sche	mes	Set As Default D	uplicate Apply		
	Confirmation			×		
	Authentication Scheme,	FlexcubeBasicOAMScheme, modified successfully				
	• Name	FlexcubeBasicOAMScheme				
	Description	Basic Style SSO Login for FLEXCUBE				
	* Authentication Level	1 0				
	Default					
	* Challenge Method	BASIC				
	Challenge Redirect URL	/oam/server				
	* Authentication Module	FlexcubeAuthnModule				
		SSCCOBBE-Secure SCOREXIVage-default SCOREXIVage-default Challenge_upt= //credicales/Seculet/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 Auth	nentication Module' of this document.
Challenge URL	: /pages/login.jsp
Context Type	: default
Context Value	: /oam
Challenge Parameters	: ssoCookie=Secure

ORACLE' Acces	ss Management	Accessbilty Help	Sign Out weblogic 🧲
🖸 Launch Pad 🛛 🔀 Flexo	ubeForm0AMScheme ×		
Authentication Sche	mes	Set As Defaul	t Duplicate Apply
Gamma Confirmation			×
Authentication Scheme,	FlexcubeFormOAMScheme, created successfully		
* Name	FlexcubeFormOAMScheme		
Description	Form Based SSO Login for FLEXCUBE		
* Authentication Level	2 🗘		
Default			
* Challenge Method	FORM •		
Challenge Redirect URL	/oam/server		
* Authentication Module	FlexcubeAuthnModule		
* Challenge URL	/pages/login.jsp		
* Context Type	default 💌		
Context Value	/oam		
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' of this document.		
Challenge URL	: /pages/oaam/login.jsp		
Context Type	: default		
Context Value	: /oam		
Challenge Parameters	: ssoCookie=Secure		
	oaamPostAuth=true		
	oaamPreAuth=true		

Access Management sibility Help Sign Out Launch Pad BlexcubeKBAOAAMScheme × Authentication Schemes Set As Default Duplicate Apply Confirmation × Authentication Scheme, FlexcubeKBAOAAMScheme, created successfully * Name FlexcubeKBAOAAMScheme Description OAAM - KBA Based Strong SSO Login for FLEXCUBE Authentication Level 2 🗘 Default * Challenge Method FORM Challenge Redirect URL /oam/server * Authentication Module FlexcubeAuthnModule * Challenge URL /pages/oaam/login.jsp * Context Type default 💌 * Context Value /oam

ORACLE

	subeKBAOAAMScheme ×	
thentication Sche	mes	Set As Default Dup
Confirmation		
Authentication Scheme,	FlexcubeKBAOAAMScheme, modified successfully	
* Name	FlexcubeKBAOAAMScheme	
Description	OAAM - KBA Based Strong SSO Login for FLEXCUBE	
* Authentication Level	2 🖨	
Default		
* Challenge Method	FORM	
Challenge Redirect URL	/oam/server	
Authentication Module	FlexcubeAuthnModule	
* Challenge URL	/pages/oaam/login.jsp	
* Context Type	default 💌	
* Context Value	/oam	
Challenge Parameters	9aanRostAuth=true 9aanRosAuth=true ssoCaplig=Secure	

2.6.4 Creating OAM 11g Webgate

Follow the below steps to create a Webgate:

1. Click 'Server Instances' under Configuration.

ORACLE' Access Management			Accessibility Help	Sign Out weblogic
Launch Pad Welcome to Oracle Access Management				
		Host Identifiers S≱ Plug-ins	 Session Management Password Policy 	
B Identity Federation Ø	+ -	Security Token Service 🖉		+ -
3 Identity Provider Administration		් Partners දිඩු Partner Profiles ලී Endpoints	₩ Token Valdation Templates	
🔋 Mobile and Social 🥝		Access Portal Service 🖉		+ -
🖥 Mobile Services 🛛 🐚 OAuth	Service	않 Oredential Sharing Groups @> Password Generation Policies	🐒 Global Agent Settings	
& Configuration				
Liser Lidentity Stores Liser Lidentity Stores Liser Lidentity Stores Liser Lidentity Liser Linstances	n Settings Manager Settings and Social Settings tion Settings Y Token Service Settings Portal Service Settings			



2. Click 'Search'.

	ment Accessibility H	elp Sign Out w	eblogic 🧲
Launch Pad Server Instances ×			
Search OAM Servers		Create OAM	Server
⊿ Search			
Name			
		Search	Reset
Search Results			
Actions 🕶 View 🖛 🎴 🧪 💥 🔛	Detach		
Row Name			
No data to display.			

3. Edit oam_server1.

ORACLE Access Management	cessibility Help Sign Out we	eblogic Q
🖸 Laundh Pad 📲 Server Instances ×		
Search OAM Servers	Create OAM S	Server
⊿ Search		
Name		
	Search	Reset
Search Results		
Actions 🗸 View 👻 🔮 🥒 💥 🔣 🔂 Detach		
Row Name 1 gam server1		

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

ORACLE Access Management	Accessibility	Help Sig	gn Out we	blogic O
C Launch Pad 🔋 Server Instances × 📳 oam_server1 ×				
oam_server1				Apply
* Server Name Goam_server 1 * Host ofss220223.in.orade.com				
* Port 14101 \$				
A OAM Proxy				
* Proxy Server Id AccessServerConfigProxy				
* Port 5575 🗘				
* Mode Copen				
Coherence C n. Smple				
*Log Level 3 3				
* Local Port 9095 \$				
* Log Limit 4096 🗘				



	Acco	essibility Help Sign Out weblogic Ϙ
🖸 Launch Pad 📲 Server Instances X 📳 oam_server1 X		
oam_server1		Apply
* Server Name oam_server1 * Port 14101 ©	* Host ofss220223.in.oracle.com	
A OAM Proxy		
* Proxy Server Id AccessServerConfigProxy * Port 5575 () * Mode Simple		
*Log Level 3 C		
* Log Linit 4096 C	Confirm Edit × OAM Server instance eam server 1 might be in use. Are you sure you want to edit it?	

ORACLE [®] Access Management	Accessibility Help	Sign Out weblogic Q
🖸 Launch Pad 📗 Server Instances 🗙 📳 oam_server1 ×		
oam_server1		Apply
Confirmation		×
OAM Server instance oam_server1 modified successfully.		
* Server Name oam_server 1 * Host ofss220223.in.orade.com		
*Port 14101 🗘		
A DAM Proxy		
* Proxy Server Id AccessServerConfigProxy		
* Port 5575 ©		
* Mode Smple 💌		
✓ Coherence Configuration		
*Log Level 3 🗘		
* Local Port 9095 0		
* Log Limit 4096 🖗		



5. Click on Create 11g Webgate under Access Manager



Launch Pad				
elcome to Oracle Access Management				
Quick Start Wizards Application Registration Store Application Registration			Cess Hanager Cess	Auther Create Application Domain Auther Create Application Authernication Module Create Korbores Authernication Module Create Korbores Authernication Module Create Korbores Authernication Module Create Korbores Authernication Module Create Create
 Identity Federation Ø Identity Provider Administration Service Provider Administration 		+ •	Security Token Service 🖉	Create Custom Authentication Nodule Create Authentication Scheme Create II gu Webgate
Mobile and Social O Mobile Services	👸 OAuth Service		Access Portal Service	🕂
& Configuration			L	
E Available Services	Common Settings Access Manager Settings			

6. Enter the below and Click 'Apply':

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



e OAM 11g Webgate			
			Арр
Version 11g		User Defined Parameters filter OAMAutho Cookie=false	
* Name Flexe	subeWebgate		
Description			
Base URL https	://ofss220223.in.oracle.com		
		Virtual host	
		Auto Create Policies 🗹	
Access Client Password		IP Validation	
* Security 🔘 Op			
 Sin Ce 			
Host Identifier Flexe			
	ubewebgate		
irce Lists			
otected Resource List 🛛 💠 💥	Public Resource List 🛛 💠 🗙		
lative URI	Relative URI		
CJNeoWeb			
CISNeoWeb			
	2		

xcubeWebgate					Appl
Confirmation					×
OAM 11g Webgate FlexcubeWebgate creat	ed successfully.				
Artifacts are generated in following location	: /scratch/app/sso1123/wl1036/Mi	ldleware/user_projects/domains/domain_two/output/Fle	excubeWebgate		
Name I	FlexcubeWebgate		Lopput Redirect URL	https://ofss220223.in.oracle.com:1	
Description			Logout Target URL		
Access Client Password				proxySSLHeaderVar=IS_SSL	
* Security @				URLINUTF8Format=true dient_request_retry_attempts	
) Simple) Cert			=1	
* State				inactiveReconfigPeriod=10 maxSessionTimeUnits=minutes	
() Disable		* Sleep for (Seconds)	60	
* Max Cache Elements	100000 🗘		Cache Pragma Header		
* Cache Timeout (Seconds)	1800 🗘		Cache Control Header		
* Token Validity Period (Seconds)	3600 \$		Debug		
* Max Connections	1 🚔		IP Validation		
* Max Session Time	60 🗘		Deny On Not Protected		
* Failover Threshold	1 🗘		Allow Management Operations		
* AAA Timeout Threshold	-1 🚆		Allow Token Scope Operations Allow Master Token Retrieval		
* Preferred Host	=lexcubeWebgate	Allor	v Credential Collector Operations		
Logout URL					
L					
Logout Callback URL	/oam_logout_success				
rver Lists					
		Server List 🕂 👫 💥			
Primary Server List	🕂 💥 🛛 Secondary				

- 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 'Apply'.



aunch Pad 🛛 🔊 SSO Agents × 🛛 Flexo xcubeWebgate							Арр
Confirmation OAM 11g Webgate FlexcubeWebgate mo	dified successfully.						Х
Name	FlexcubeWebgate				Logout Redirect URL	https://ofss220223.in.orade.com:1	
Description					Logout Target URL		
* State	 Simple Cert Enable 				User Defined Parameters	proxySSLHeaderVar=ssl URLInUTF8Format=true dient_request_retry_attempts=1 inactiveReconfigPeriod=10 maxSessionTmeUnits=minutes filterOAMAuthnCookie=false	
	Disable				* Sleep for (Seconds)	60 🗘	
* Max Cache Elements	100000 ‡				Cache Pragma Header	no-cache	
 Cache Timeout (Seconds) 	1800 🌻				Cache Control Header		
 Token Validity Period (Seconds) 	3600 🖨				Debug		
* Max Connections	1 🛫				IP Validation		
* Max Session Time	60 🗘				Deny On Not Protected	*	
* Failover Threshold	1 🗘				Allow Management Operations		
* AAA Timeout Threshold	-1 🔹				Allow Token Scope Operations		
* Preferred Host	FlexcubeWebgate				Allow Master Token Retrieval		
Logout URL					Allow Credential Collector Operations		
Logout Caliback URL	/oam_logout_success						
rimary Server List	+ x	Secondary Ser	ver List	4	×		
Access Server Host Name Host	Port Max Number	Access Server	Host Name	Host Port Max N	umber		
oam_server ofss220223.in.o 5575	1						

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

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

ORACLE Access Management	Accessibility	Help Sigr	Out weblogic 🧲
🖸 Launch Pad 📳 Server Instances X 📳 oam_server1 X			
oam_server1			Apply
Confirmation			×
OAM Server instance oam_server 1 modified successfully.			
* Server Name oam_server 1 * Host ofss220223.in.orade.com			
* Port 14101 🗘			
AM Proxy			
* Proxy Server Id AccessServerConfigProxy			
* Port 5575 \$			
* Mode Deen w			
Coherence Cont Control			
* Log Level 3 D			
*Local Port 9095 \$			
* Log Limit 4096 C			



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 'Application Domains' under Access Manager

ORACLE: Access Managemen	t			Accessibility Help	Sign Out weblogic
Launch Pad					
Quick Start Wizards Application Registration Strong Stop Agent Registration			Constant Co	Withentication Modules Authentication Schemes Sol Agents Session Management ► Password Policy	+ •
 Identity Federation ? Identity Provider Administration Service Provider Administration 		+•	III Security Taken Service ⊘	िख्ले Token Valdation Templates ब्लि Token Issuance Templates ﷺ Custom Tokens	+ •
Hobile and Social 🖉	ing OAuth Service		Access Portal Service C C Cedential Sharing Groups Password Generation Policies	🎉 Global Agent Settings	+ •
Configuration Available Services Les Identity Stores	Difference Settings				

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

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

DRACLE Access Management	Accessibility Help Sign Out weblogic 드
🖸 Launch Pad 🛛 🍓 Application Domain ×	
Search Application Domains	Create Application Domain
∡ Search	
Name	
	Search Reset
Search Results	
Actions - View - 🔮 🧷 💥 🛃 Detach	
	Description
No data to display.	



ORACLE' Access Management	Accessibility Help Sign Out weblogic 🚍
Launch Pad 🌀 Application Domain ×	E.
Search Application Domains	Create Application Domain
⊿ Search	
Name	
	Search Reset
Search Results Actions • View •	
Row Name	Description
1 ElexcubeWebgate 2 Husion Apps Integration	Application Domain created through Remote Registration Policy objects enabling integration with crace Fusion Applications
3 IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications

3. Click 'Authentication Polices'.

ACLE' Access Ma		Accessibility	Help Sign Out	weblogic
	nan X 🛯 🍓 FlexcubeWebgate X			
lication Domains				
mmary 🔅 Resources 🚦	👼 Authentication Policies 🛛 🛃 Authorization Policies 🛛 🤯 Token Issuance Policies 🛛 Administration			
				Apply
* Name	FlexcubeWebgate			
	Application Domain created through Remote			
	Registration			
Session Idle Timeout (minutes)				
Allow OAuth Token				
Allow Session Impersonation				
licy Ordering				
nable Policy Ordening				
View 🔻 💠 🧷 💥				
esource Prefix	Resource Type Host Identifier			

4. Click 'Protected Resource Policy'.

ORAC	LE Access Management		Accessibility Help Sign Out weblogic 드
🖸 Launch A	Pad 🌀 Application Domain × 🌀 FlexcubeWe	bgate ×	
Applicat	ion Domains		
Summary	Authentication Policies	Authorization Policies 😺 Token Issuance Policies Administration	
Authe	ntication Policies		Create Authentication Policy
Actio	ns • View •		letach
Row	Name	Description	
	1 Protected Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.	
	2 Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.	

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

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



	tion Domain × 🧐 FlexcubeWebgat	te × 🛛 👼 FlexcubeWebgate : Pro	tect ×		
uthentication Policy	1				Duplicate App
* Name	Protected Resource Policy		Suc	cess URL	
	Policy set during domain creation. Add protect them.	resources to this policy to	Fai	llure URL	
* Authentication Scheme	LDAPScheme -]			
Resources	BasicScheme BasicSessionlessScheme ESSOProvAuthnScheme FAAuthScheme	Query String	Name Value list	Operations	+ x
LITTO EL	FederationMTScheme			Al	
HTTP F	FlexcubeBasicOAMScheme			All	
	Flexzube/FormOAMScheme Flexzube/RAOAMScheme IbaPScheme DAPKofeme OAAMAdvanced OAAMA				

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

unch Pad 🛛 🍙 Applic	ation Domain × 🌀 FlexcubeWebgate × 🐻 FlexcubeWebgate : Protect	×		
- hentication Polic	y		Duplicate	e Ap
* Name	Protected Resource Policy	Success URL		
Description	Policy set during domain creation. Add resources to this policy to protect them.	Failure URL		
	FlexcubeBasicOAMSchme Advanced Rules			
sources Kesponse				
Identity Assertion	tion to be generated for the user, optionally containing any Asserted Attribute set bel	DW.		
Identity Assertion	ton to be generated for the user, optionally containing any Asserted Attribute set bel	JW.	÷	1 >
Identity Assertion This will cause an asser	Туре	uw. Value	 +	

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

Type : Header

Name : DN

Value : \$user.attr.dn

ORACLE Acces	ss Manage	ement			Accessibility	Help Si	ign Out 🛛 🗤	reblogic 🧲
🖸 Launch Pad 🏾 🌀 Applica	ation Domain ×	G FlexcubeWebgate ×	B FlexcubeWebgate : Pro	otect ×				
Authentication Polic	у						Duplicate	Apply
* Name	Protected Reso	urce Policy		Success URL				
Description	Policy set during protect them.	g domain creation. Add resour	ces to this policy to	Failure URL				
* Authentication Scheme	FlexcubeBasicC	AMScheme						
Lidentity Assertion This will cause an asser Responses This Policy does not have	-	Туре		Header ×			+	×



8. Click on Apply to Save the Changes

unch Pad 🛛 🌀 Applica	ation Domain × 🏾 🌀 FlexcubeWebgate × 🛛 🙀 FlexcubeWebgate : F	Protect ×	
hentication Policy			Duplicate
Confirmation	rotected Resource Policy, modified successfully		8
* Name	Protected Resource Policy	Success URL	
	Policy set during domain creation. Add resources to this policy to protect them.	Failure URL	
Authentication Scheme	FlexcubeBasicOAMScheme		
sources Responses	Advanced Rules		
Identity Assertion This will cause an assert	tion to be generated for the user, optionally containing any Asserted Attribu	te set below.	
🖗 Responses			+/×
Name	Туре	Value	
DN	Header	\$user.attr.dn	

9. Click 'Authorization Policies' and 'Protected Resource Policy'.

ORACLE	🖬 Access Management		Accessibility Help Sign Out weblogic 📿
O Launch Pad	Application Domain × G FlexcubeWebgate	×	×.
Application	Domains		
Summary 🔮	Resources 🛛 Resources 🔂 Authentication Policies 🔂 Auth	orization Policies 🛛 🍛 Token Issuance Policies 🛛 Administration	
Authorizat	tion Policies		Create Authorization Policy
Actions 👻	View 👻	🕒 🕂 🥒 🖉	Detach
Row	Name	Description	
	1 Public Resource Policy	Policy set during domain creation. Add resources to t	this policy to allow anyone access.
	2 Protected Resource Policy	Policy set during domain creation. Add resources to t	his policy to protect them.

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

-									
OR	ACL	E Acce	ss Mana	gement	t	Accessibility	Help	Sign Out	weblogic 🧲
🖸 La	unch Pad	G Applic	ation Domain	× 🌀 FI	excubeWebgate × 🛛 🔀 FlexcubeWebgate : Protect ×				
Aut	horizati	ion Policy	1					Duplicate	e Apply
5	immary	Resources	Conditions	Rules	Responses				
				* Name	Protected Resource Policy				
				Description	Policy set during domain creation. Add resources to this policy to protect them.				
			S	uccess URL					
				Failure URL					

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

Type : Header

Name : DN

Value : \$user.attr.dn



DRACLE Access Mar	nagement			Accessibility	Help	Sign Out	weblogic
Launch Pad Application Doma	ain × 🌘 FlexcubeWebgate × 📃 FlexcubeWebga	te : Protect ×					C
Authorization Policy						Duplicate	Apply
Summary Resources Conditions	Rules Responses						
	generated for the user, optionally containing any Asserted A	Attribute set below.					
Responses						+ /	/ %
Name	Type	Valu	e				
This Policy does not have any Res	sponses						

ORACLE: Access Manag	jement		Accessibility Help Sign Out weblogic						
O Launch Pad G Application Domain ×	🖸 Launch Pad 🛛 🍓 Application Domain X 🛛 🍓 FlexcubeWebgate X 📃 FlexcubeWebgate : Protect X								
Authorization Policy			Duplicate Apply						
Summary Resources Conditions F	Rules Responses								
Identity Assertion This will cause an assertion to be gene	erated for the user, optionally containing any Asserted Attribute	e set below.							
Responses			+/%						
Name	Type	Value							
	* Name * Value	Header							

12. Click 'Apply' to Save the changes.

DRACLE Access Manage	ement		Accessibility Help Sign Out	weblogic 🧕
🖸 Launch Pad 🛛 🌀 Application Domain 🗙	G FlexcubeWebgate × 🔀 FlexcubeWebgate	: Protect ×		
Authorization Policy			Duplicate	e Apply
Confirmation				×
Authorization Policy, Protected Resource	e Policy, modified successfully			
Summary Resources Conditions R	tules Responses			
Identity Assertion This will cause an assertion to be gene	rated for the user, optionally containing any Asserted Att	ribute set below.		
🖗 Responses			+ /	/ %
Name	Туре	Value		
DN	Header	\$user.attr.dn		1

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



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	Directory Information
ofss220028.in.oracle.com: 5575, 1	Up	Friday, January 11, 2013 16:18:27		

Cache Name	State			Timeout (seconds)		Memory Footprint (bytes)
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 Tool	×
<u>File Edit Test H</u> elp	
🔁 🗟 I 🥔 I 🏦	
Server Connection	-
IP Addr Port Max C *Aαe *Prim[ss220028.in.oracle.com] 5575 1 FlexcubeWebgate	
Agent Pa	
Secon 1	
Min C Timeou Mo Global Passo 1 30000 Si **********	
Protected Resource URI	
Sche *H Port 🖏 🖉	
https ♥ FlexcubeWebαate	
Resour Operat Validate	
- User Identity	
IP Address *Username Password 🖉	
SARAN ******** ? Authenti	
User Certifica	
_ Status Messages	5
[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] ves	-
Elapsed (🕫 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.



🔶 Bank Parameters Maintenance		. ×
🛃 Save		
Bank Code * 000	Bank Name Bank Futura	*
Head Office Branch		
Branch Code * 000	Branch Description Bank Futura	
Financial Preferences General Preferences FAT	CA	
Format Mask	Year End Profit and Loss	
Cif Mask bbbnnnn	General Ledger * 221000002	
General Ledger Mask * nnnnnnnn	Transaction Code * YET	
Spread	General Ledger Purge Days	
Spread Application Both Legs 🔻	Auto Batch	
Spoof Files Purge Days	90 User Batch Restriction	
Inter Pay Lead Days	3 SSO Enabled	
Cheque Numbering Details	Checksum Algorithm 🔹	
Scheme Automatic 🔻	Checksum Algorithm	
Cheque Number Mask NNNNNN	for L	
	Lodgement Numbers Unique For Branch	
TRS Details	Suspense Account	-
Preferences Account Mask Field Propert	ies	
Maker	Date Time:	
Checker	Date Time:	col
Mod No 229	Record Status Open	Cer
Auti	horization 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			
Jser Details		User Status	Enabled
User Identification	* FCUBSUSER		Hold
Name	* FCUBSUSER		Olisabled
User Reference			OLocked
Language	* ENG 🚬	Classification	OStaff
Home Branch	* 000 🗾		Branch
Customer No	Z	Status Changed On	2011-01-04
Department Code	7	Last Signed On	
Department Description			Staff Customer Restriction Required
Tax Identifier		ELCM User ID	
LDAP DN	cn=FCUBSUSER,cn=Us 🖓		Multi Branch Access
Time Level	* 9		Other RM Customer Access
Amount Format	T LOAP DIN		Restricted
Date Format	•		Show Dashboards
	Auto Authorization		Alerts on Home
	Validate		MFI User
Supervisor Identification	===		F10 Access Required
Supervisor Name			✓F11 Access Required
			✓F12 Access Required
ser Password		Start Date 3	* 2011-01-04 🔤
Password	•••••	End Date	2
Password Changed On	2012-01-04		
Email			
Reference No			
valid Logins		Screen Saver Details	
No of Cumulative Logins	17	Screensaver Interval (in	3600
No of Successive Logins	0	seconds)	
Restricted Password Role	s Rights Functions Tills	Account Classes Genera	al Ledgers Limits Branches

For FLEXCUBE - IS

🔶 User Admin					_ >
🗄 Save					
User Details					
Externel Identifier	FCISUSER FCIS User cn=FCUSR,cn=Users,d(Language * Home Branch * Home Module *	000	Classification	 Staff Auto End Of Day Customer
Modules		Status Description			
	Corporate	User Status	 Enabled Hold Disabled Locked 	Time Level Status Changed On Last Signed On	* 9
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

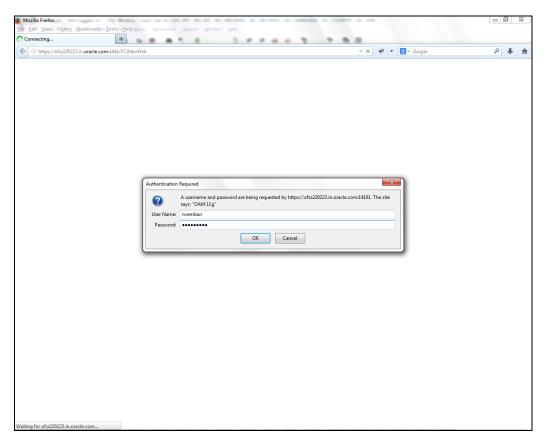
After setting up FLEXCUBE to work on Single Sign on mode, navigate to the URL <u>https://<hostname>:<OHS</u> SSL Port>/<Context Root> from your browser

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

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

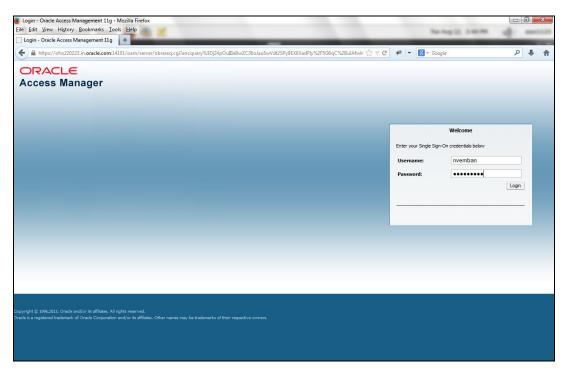


2.7.3.1 Basic Style Challenge by Webgate

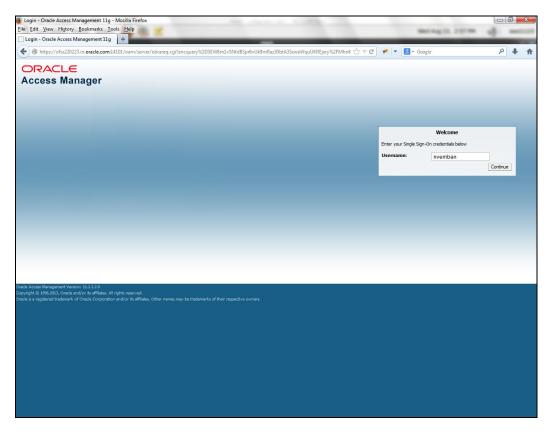




2.7.3.2 Form Style Challenge by Webgate

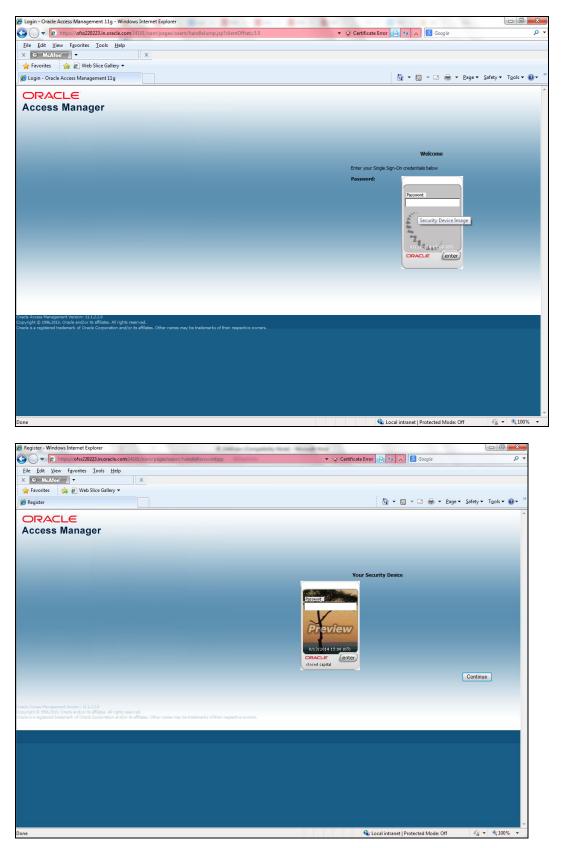


2.7.3.3 KBA Based Strong Authentication Challenge by Webgate(Only when OAAM is used)





First Time Login

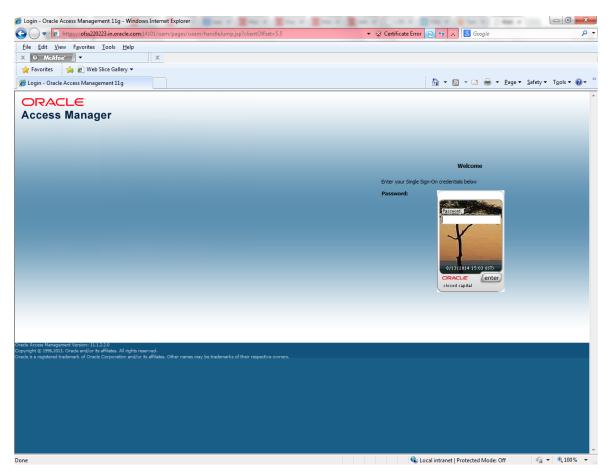




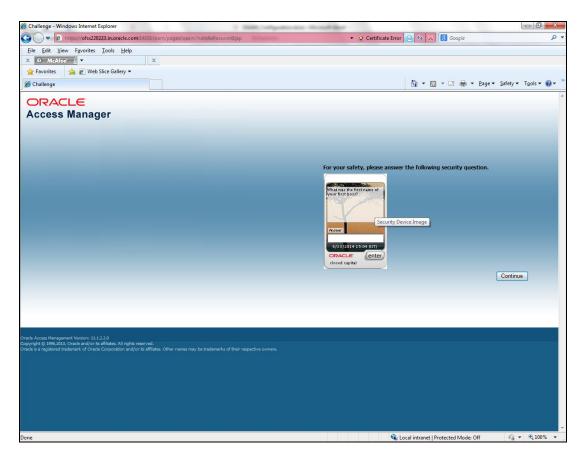
	R. (Million Competition)	the thread the	
	/oam/pages/oaam/handleRegisterImagePhrase.jsp	👻 🤇 Certificate Error 🔛 🍫 🔀 Google	• م
File Edit View Favorites Tools Help			
	x		
🖉 Register		🚹 🔻 🖾 🖛 💌 <u>P</u> age 🕶 <u>S</u> afe	ety ▼ T <u>o</u> ols ▼ @ ▼ ´
			4
Access Manager			
Select Your Security Questions/Answers			
1) Select One			
2) Select One	-		
3) Select One	•		
1) Select One			
Ty Select One	•		
5) Select One	~		
	Continue		
Pracle Access Management Version: 11.1.2.2.0			
opyright @ 1996,2013, Oracle and/or its affiliates. All rights reserved)racle is a registered trademark of Oracle Corporation and/or its affil			
Jone		🔦 Local intranet Protected Mode: Off 🛛 🚽	
	R. Stillar Compilia		
🚱 🔵 🗢 😢 https://ofss220223.in.oracle.com:1410	1/oam/pages/oaam/handleRegisterImagePhrase.jsp	🗸 😧 Certificate Error 🔛 49 🗙 🔂 Google	
Image: Second state		🗸 🖌 Cettificate Error 🕒 😚 🗙 🔀 Google	
Image: State	1/oam/pages/oaam/handleftegisteritmagePhrase.jsp X	👻 🗶 Certificate Error 🔛 🖓 🔀 Google	
Ittps://ofss220223.in.oracle.com1410 Eile Edit Yiew Favorites Tools Help			ر
Image: Second			ر
Comparing the second seco			ر
Constant of the second se			ر
Comparing the second seco			ر
Properties 20223 increace.com 210 File Edit View Favorites Icols Help MAAfee w Favorites Register ORACLE Access Manager			L
Properties 20223 increace.com 210 File Edit View Favorites Icols Help MAAfee w Favorites Register ORACLE Access Manager			
	×		
	×		
	×		
Constant Section 2002 Sect	×		
	×		
	×		
	×		
	x		
	x		
	saw in concert? •		
	x		
	saw in concert? •		
	saw in concert? •		L
P Provides 22023 incoracte.com 110 File Edit View Favorites Iools Help MoAtee Web Slice Gallery Provides P	saw in concert? •		L
 	saw in concert? •		L
	x		
Control of a low of parts Control Contro Contro Control Control Control			
 	x		L
P Pitter // of sector 2022 increace.com 1210 Elle Edit View Favorites Icols Help MAAce MAAcee MAAce MAAce MAAce MAAcee MAAcee MAAce	saw in concert? •		L
Constant and the set of the first musical group you so of the set of the	saw in concert? •		
Elie Edit View Favorites Tools Help X Mextee Y Repister CRACLE Access Manager Select Your Security Questions/Answers 1) Where did you get your first pet? 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?	saw in concert? •		L



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.



	_	XCUBE UBS12.0.3.0.5	-	put molinaritetox								- 0
https://ofss22	20223.in.oracle	.com:4444/FCJNeoW	/eb/SMMDIFRM.jsp									;
RACLE	E.			-	Branc	ti : <u>000</u> Date : S	ession Time : 00.00.04	i Window i He	<u>Ma</u> Logged (iser : <u>Visha</u> l I	Sion Off	
rne Inleracti	ons Custon	er Workflow Tasl	ks Preferences									
earch			- () Information M	essage								
					Information Messa	100						
				2011-01-04 16:22:27	mormation messa	ige						
			-									
			Current Time	14:57:13								
							Ok					
			L									

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 [February] [2016] Version 12.0.3.1.4

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], [2014], 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.

