Oracle Access Manager Integration Oracle FLEXCUBE Investor Servicing Release 12.0.4.7.1 June 2017 Part Number E57474-01 ORACLE FINANCIAL SERVICES



Table of Contents

1. PR	EFACE	
1.1	INTRODUCTION	
1.2	AUDIENCE	
1.3	ABBREVIATIONS	
1.4	DOCUMENTATION ACCESSIBILITY	
1.5	ORGANIZATION	
1.6	GLOSSARY OF ICONS	
1.6	1 Related Documents	
2. EN	ABLING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER	
2.1	INTRODUCTION	
2.2	BACKGROUND AND PREREQUISITES	
2.2		
2.3	BACKGROUND OF SSO RELATED COMPONENTS	
2.3	.1 Oracle Access Manager (OAM)	
2.3		
2.3	•	
2.3	.4 Oracle Adaptive Access Manager	
2.4	CONFIGURATION	
2.4	1 Pre-requisites	
2.5	ENABLING SSL FOR WEBLOGIC AND OAM CONSOLE	
2.5	.1 Self-signed Certificate Creation:	
2.5		
2.5	.3 Configuring SSL Mode in Oracle Internet Directory	
2.6		
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	
2.7	FIRST LAUNCH OF FLEXCUBE AFTER INSTALLATION	
2.7		
2.7	2 Maintaining LDAP DN for FLEXCUBE users	
2.7		
2.7	.4 Signoff in a SSO Situation	



1. Preface

1.1 Introduction

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

1.2 <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 Abbreviations

Abbreviation	Description
System	Unless specified, it shall always refer to Oracle FLECUBE
OAM	Oracle Access Manager
IS	Investor Servicing
SSO	Single Sign-on
LDAP	Lightweight Directory Access Protocol

1.4 **Documentation Accessibility**

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

1.5 Organization

This manual is organized into the following chapters:

Chapter 1	<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
1	Delete row
	Option List

1.6.1 Related Documents

You may refer the following manual for more information

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



2. Enabling Single Sign-on with Oracle Access Manager

2.1 Introduction

For the purpose of single sign-on FLEXCUBE is qualified with Oracle Identity Management 11.1.2 (Fusion Middleware 11gR2) – specifically using the Access Manager component of Oracle Identity Management. This feature is available in FLEXCUE since the release FC IS V.UM 7.3.0.0.0.0.

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						õ					
Change Center	🏠 Home Log Out Preferences 🔤 Record H	ielp	۹.		Welcon	me, weblogic Connected to: iam	n_domain					
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.domain	A server is an instance of WebLogic Server th This page summarizes each server that has be Customize this table Servers (Filtered - More Columns Exist) New Cone Delete	en configured in the current \		wm configuration.		Showing 1 to 4 of 4 Previous 1	Next					
Deployments Services	🔲 Name 🗇	Cluster	Machine	State	Health	Listen Port						
	AdminServer(admin)			RUNNING	🖋 ок	7001						
How do I 😑	oam_server1			RUNNING	🖋 ОК	14100						
Create Managed Servers	oim_server1			RUNNING	🖋 ок	14000						
Clone Servers Delete Managed 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 I	Next					
System Status 🗆	1											
Health of Running Servers												
Failed (0) Critical (0) Overloaded (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	Keystores	SSL	Federation Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services	
lam_domain ▲ D=Thirkomanit D=Thirkomanit - Clusters - Clusters - Clusters - Clusters - Clusters - Coherence Servers - Coherence Clusters - Machines		Save Use this page to configure general features of this server such as default network communications. Vew JNDI Tree IP												
	Name: AdminServi						erver An alphanumeric name for					server instance.	More Info	
Work Managers Startup and Shutdown Classes Deployments BI-Services	Machine:					(None)	(None)				The WebLogic Server host computer (machine) on which this server is meant to run. More Info			er is meant
How do I	Cluster:					(Standa	(Standalone)				The cluster, or group of WebLogic Server instances, to which this server belongs. More Info			
Configure default network connections Create and configure machines	街 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	☑ Listen Port Enabled							Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More ${\rm Info}\ldots$					plain-text
System Status	Listen Port:					7001	7001			The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info			n-SSL)	
Health of Running Servers Failed (0)	🗹 SSL Lis	ten Port I	Enabled							Indicates port. Mo	whether the server one Info	an be reached t	nrough the default	SSL listen
Critical (0) Cverloaded (0) Warning (0)	SSL Listen	Port:				7002					IP port at which this : More Info	erver listens for	SSL connection	
OK (3)	🗹 🕂 Che	ent Cert P	roxy Enat	oled							whether the HttpClus ader. More Info	terServlet proxi	es the client certific	ate in a
	Java Com	piler:				javad					compiler to use for a ava code. More 1		sted on this server	that need
	Diagnostic Volume:								Specifies the volume of diagnostic data that is automatically produced by WebLogic Server at run time. Note that the WLDF diagnostic volume setting does not affect exploitly conjugned diagnostic modules. For example, this controls the volume of events generated for 'Rodit Flight Recorder. More Info					
	— 🛡 Adva	nced —												
	Virtual Ma	chine Nar	ne:			iam_	iam_domain_AdminSe			When WLS is running on JRVE, this specifies the name of the virtual machine running this server More Info				al machine
	😰 🥵 WebLogic Plug-In Enabled								header, v	whether this server u which is recommended oxy plug-in. More In	l if the server ins			



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.

	Administrati	on Cons	ole												Õ
Change Center	🔒 Home	Log Out	Preferences	s 🔤 Record H	elp		۹						Welcome, w	eblogic Conne	ected 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	Protocols	Logging Deb	Jg M	Ionitoring Co	ontrol	Deployments	Services	Security	Notes				
Domain Structure	General	Cluster	Services	Keystores	SSL	Federation S	Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services	3
ion_domain ▲ ⊡-Environment Servers Ousters Virtual Hosts Virtual Hosts Virtual Hosts Coherence Envers Coherence Clusters	Keystore	anage the	e security of	storage and mar f message transr 10 Identity anc	nissions	•	eys and tru	-	e authorities	: (CAs). Thi	Which	you view and define va	ould be used for	-	
How do L	Save	Cancel	Cust Cust	om Identity ar om Identity ar om Identity ar io Identity and	d Cus d Jav	tom Trust a Standard					trust k	æystores? More Info			
Configure identity and trust Configure keystores Set up SSL															
System Status															
Health of Running Servers Failed (0) Critical (0) Overloaded (0) Warning (0) OK (3) WebLogic Server Westions 10.3.5.0 Copyroph (6) Strong Westions and/or its affiliates. All r Oracle a seglistered trademark of Oracle Corporation		ates. Other	names may	be trademarks of	their res	spective 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.

	dministration 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 modify, add or delete items in this domain.	Settings for AdminServer Configuration Protocols Logging Debug Monitor								
Domain Structure	General Cluster Services Keystores SSL Fee	deration Services Deployment Migr	ation Tuning Overload Health Monitorin	g Server Start Web Services					
Iam_domain ▲ Christmonnet -Servers -Clusters -Virtual Hosts -Migratable Targets -Coherence Servers -Coherence Servers	Save Keystores ensure the secure storage and management of p you to manage the security of message transmissions.	rivate keys and trusted certificate author		various keystore configurations. These settings help					
Order and Casters a Machines Work Managers Stephoyments D-Services Services	— Identity Custom Identity Keystore:	nFlexcubeKeyStore.jks	trust keystores? More Ir	seKeyStore/AdminFlexcubeKeyStore.jks					
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 Set up SSL	Custom Identity Keystore Passphrase: The encrypted custom identity keystore's passphrase. If empty or the keystore will be opened without a passphrase. If one for the keystore will be opened without a passphrase. More Info								
System Status	Confirm Custom Identity Keystore Passphrase:	•••••							
Health of Running Servers Failed (0)	Trust	nFlexcubeKeyStore.jks		/BaseKeyStore/AdminFlexcubeKeyStore.jks e or the custom stark eystore. Hoke stird					
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 will be opened without a p	's passphrase. If empty or null, then the keystore assphrase. 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	Home Log Out Preferences 🖂 Recor	rd Help	Welcome, weblogic Connected to: iam d												
-	Home >Summary of Servers >AdminServer														
View changes and restarts	Settings for AdminServer														
Configuration editing is enabled. Future changes will automatically be activated as you															
modify, add or delete items in this domain.	Configuration Protocols Logging	Debug Monitoring Control Deployments	Services Security Notes												
Domain Structure	General Cluster Services Keystore	s SSL Federation Services Deployment	Migration Tuning Overload Health Monitoring Server Start Web Services												
iam_domain	Save This page lets you view and define variou:	s Secure Sockets Layer (SSL) settings for this serve	er instance. These settings help you to manage the security of message transmissions.												
Migratable Targets Coherence Servers Coherence Clusters	Identity and Trust Locations:	Keystores Change	Indicates where SSL should find the server's identity (certificate and privat key) as well as the server's trust (trusted CAs). More Info												
Machines Work Managers	- Identity														
	Private Key Location:	The keystore attribute that defines the location of the private key file. Mo Info													
Security Realms	Private Key Alias:	The keystore attribute that defines the string alias used to store and retrie 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	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	Trusted Certificate Authorities:	from Custom Trust Keystore	The keystore attribute that defines the location of the certificate authorities. More Info												
Failed (0) Critical (0)	— ♥ 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.SSLHostnameVerfiler interface (when this server is actin 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 n key. The more secure you want WebLogic Server to be, the fewer times th 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						Q			
hange Center	🟦 Home Log Out Preferences 🔤 Record I	Help	Q		Welcor	ne, weblogic Connected to: iam	ı_doma			
liew changes and restarts	Home >Summary of Servers >AdminServer >Su	mmary of Servers								
onfiguration editing is enabled. Future	Summary of Servers									
hanges will automatically be activated as you nodify, add or delete items in this domain.	Configuration Control									
Domain Structure m_domain -Environment	A server is an instance of WebLogic Server th			own configuration.						
Servers	This page summarizes each server that has been configured in the current WebLogic Server domain.									
Virtual Hosts	22									
	Customize this table									
Wachines	Servers (Filtered - More Columns Exist	.)								
Startup and Shutdown Classes	New Clone Delete					Showing 1 to 4 of 4 Previous	Next			
Deployments Services	🔲 Name 🗞	Cluster	Machine	State	Health	Listen Port				
Security Realms	AdminServer(admin)			RUNNING	🖋 ОК	7001				
ow 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	New Clone Delete					Showing 1 to 4 of 4 Previous	Next			
Start and stop servers										
rstem Status 🖂										
ealth of Running Servers										
Failed (0) 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 M	anager 11g Fusion Middleware Contr	ol			Setup •	r Help → Log Out
📑 Farm 👻 🔒 Topology						
	<pre>分 oid1 ₀</pre>				Logged in as weble	ogic Host padsrini-pc
B 📴 Farm_base_domain	Cracle Internet Directory				Page Refreshed Feb 15, 2	013 4:35:59 PM IST 🗘
Application Deployments WebLogic Domain	Home					
Identity and Access	Monitoring >		Load		Security	
OAM	Control >) 121	Total LDAP Connections	0	Failed Bind Operations	0
	Logs >	000		-		
ovd1		220	Operations Completed	2	Failed Super User Logins	0
Metadata Repositories	Port Usage	65	Operations in progress	0	Sucessful Super User Logins	0
I Deb Tier	Administration >					
	Security >	Audit Policy				
	Directory Services Manager	Wallets			•	
	General Information					
					Server Response (ms)	
	40 20					
	0					
	8					
	6					
	4				Total Operations	
	2					
	0					
	20					
	15				07011077-0702 (7/1)	
	10				CPU Utilization (%) /Farm_base_domain/asins	st_1/oid1
	5				padsrini-pc	
	0				•	
	100					
	60				Memory Utilization (%)	4 4/-144
	40				padsrini-pc	st_mold i
	20					
	16:22 16:23 16 February 15 2013	24 16:25 16:26 16	27 16:28 16:29 16:30 1	6:31 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 O
📑 Farm 👻 🔒 Topology	
Farm_base_domain Application Deployments	û oid1 ₀ Logged in as weblogic (Host paderin- î) Oracle Internet Directory → î) Oracle Internet Directory → Page Refreshed Feb 15, 2013 4(39:54 PH 157
WebLogic Domain Identity and Access OAM OId OId	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	Oreate % Delete Create Self-Signed Walet Import 6 Manage Name Auto-boain
💽 ovd1 🗄 🦢 Metadata Repositories 🗷 🦢 Web Tier	Name Auto-login
	Fetding Data



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

ORACLE Enterprise Ma	nager 11g Fusion N	iddleware Control Setup + Help + Log Out
🕂 Farm 👻 🔒 Topology		
	🔂 oid1 🗿	Logged in as weblogic Host padsrini-pc
B 📑 Farm_base_domain	I Oracle Internet D	rectory 🕶 Page Refreshed Feb 15, 2013 4:40:45 PM IST 🖏
Application Deployments		
📧 🚞 WebLogic Domain	Wallets > Create Se	
Identity and Access	Create Self-Sig	
OAM E oid1 OIM OIM Over over 000000000000000000000000000000000000	or password-protect PKCS#12 wallet that	not signed by a well known C.A. A self-signed walet a not recommended in a production environment. The walet name should be unged for a given component. The walet type can be auto-login d. Passwords, "givesfield, have a minum length of eight harders; and contain alphabet characters combined with numeric or pseul characters. Auto-login wallet a nobfuscated from of provides FRG-based access to services and applications without requiring a password at runtime. Auto-login wallet don't need a password to modify, or idelet the wallet. File system permissions y security for Auto-login wallets.
Ovd1 Metadata Repositories	Self-Signed Wallet	Debrit
Web Tier	Self-Signed Wallet	Uctails
a web ner	* Wallet Name	oldselfsioned
	walleervalle	
		☑ Auta-login
	Wallet Password	
	Confirm Password	
	Add Self-Signed Ce	
		runcate Micate that becomes part of the wallet.
	Add a sell-signed cel	ancare diat becomes part of one water.
	* Common Name	hostname.in.orade.com
	Organizational Unit	OFSS
	Organization	Orade
	City	Chennai
	State	TN
	Country	India 💌
	Key Size	2048 -

4. Click 6d Manage...

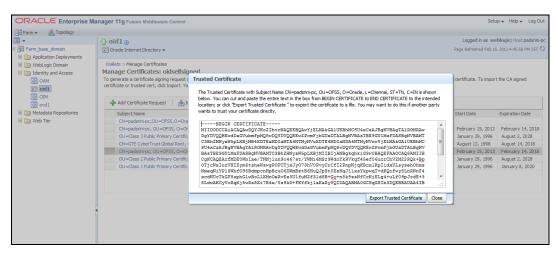
	nager 11g Fusion Middleware Control	Setup → Help → Log Out
🕂 Farm 👻 🔒 Topology		
↓ Farm_base_domain Farm_base_domain Farm_base_domain	<pre></pre>	Logged in as weblogic (Host padsrini-pc Page Refreshed Peb 15, 2013 4(44)27 PM 15T 🖏
WebLogic Domain Gentity and Access OAM Gentity	Wallets A Wallet is a Keystore 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 X Delete C Create Self-Signed Wallet M Import L Export Name	6x8 Manage Auto-login
 Metadata Repositories Web Tier 	isidselfsigned	v ✓

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

🖁 Farm 👻 🛛 💑 Topology						
•	<pre> oid1 o </pre>				Logged in as we	blogic Host padsrir
Farm_base_domain	Crade 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 you	ur CA who will verify your identit	ty and retu	rn the signe	d certificate. To import	the CA signed
i oid1	certificate or trusted cert, dick Import. You can only import the CA-signed certificate into the same wallet from which t	the CSR was generated.				
OIM						
ovd1	👍 Add Certificate Request 🔄 Import 😭 Export 💥 Delete					
🛅 Metadata Repositories	Subject Name	Certificate Type	Status	Key Size	Start Date	Expiration Date
-	Subject Name ON=padsrini-pc,OU=OFSS,O=Orade,L=Chennai,ST=TN,C=IN	Certificate Type Certificate Request	Status	Key Size 2048	Start Date	Expiration Date
-			Status Valid		Start Date February 15, 2013	
	CN=padsrini-pc,OU=OFSS,O=Orade,L=Chennai,ST=TN,C=IN	Certificate Request		2048		
	CN=padsrini-pc,OU=OFSS,O=Orade,L=Chennai,ST=TN,C=IN CN=padsrini-pc,OU=OFSS, O=Orade,L=Chennai,ST=TN,C=IN	Certificate Request Certificate	Valid	2048 2048	February 15, 2013	February 14, 20: August 2, 2028
Metadata Repositories Web Tier	ON-padsrin-pc, OU-OPSS, O-Orade, L-Chennal, ST-TN, C=N ON-padsrin-pc, OU-OPSS, O-Orade, L-Chennal, ST-TN, C=N OU-Class 3-Public-Primary Certification Authority, O="Versign, Inc.", C=US	Certificate Request Certificate Trusted Certificate	Valid Valid	2048 2048 1024	February 15, 2013 January 29, 1996	February 14, 201 August 2, 2028 August 14, 2018
-	Ot-padorni-pc,OU=OFS,O=Orade,L=Chemnal,ST=TN,C=IN Ot-padorni-pc,OU=OFS,O=Orade,L=Chemnal,ST=TN,C=IN OU=OSS 9-Phile/Pmany Certification Autority, o=Versign, Inc.*, C=US ON=GTE CyberTrust Global Root, OU="GTE CyberTrust Solutions, Inc.*, O=GTE Corporation, 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, 20: August 2, 2028 August 14, 2018



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



7. Click 'Server Properties'.

Farm 👻 💑 Topology										
•	1 û	oid1 🕦							Logged in as we	blogic Host padsrini
🖇 Farm_base_domain		Oracle Internet Directory 🛩							Page Refreshed Feb 15	, 2013 4:45:58 PM IST
Application Deployments MebLogic Domain		Home								
OAM OIN		Monitoring Control Logs	> st	signed st (CSR), clock "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.						
🔄 ovd 1		Port Usage	b):	Import 🖹 🏦 Export	🗙 Delete					
Web Tier		Administration	>	Server Properties		Certificate Type Certificate Request	Status	Key Size	Start Date	Expiration Date
i web her		Security	>	Shared Properties		Certificate Request	Valid	2048 2048	5 L	E 1 44 004
		Directory Services Manager	>	ondred rioperdes	L. C=US	Certificate Trusted Certificate	Valid		February 15, 2013	
		birectory bernees manager						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	
				cation Authority, O="VeriSign,		Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
		OU=Class 1 Public Primary C	ertific	ation Authority, O="VeriSign,	Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	January 8, 2020

8. Click 'Change SSL Settings'.

ORACLE Enterprise Ma	anager 11g Fusion Middleware Control	Setup ← Help ← Log Out
📑 Farm 👻 🛃 Topology		
∃ -	🗘 oid1 💿	Logged in as weblogic Host padsrini-pc
🗉 🚟 Farm_base_domain	Oracle Internet Directory	Page Refreshed Feb 15, 2013 4:54:17 PM IST €2
Application Deployments		
I Domain	Server Properties	Apply Revert
Identity and Access		index and a second s
OAM		
DIM	Server Mode Read / Write	
ovd1	* Maximum number of entries to be returned by a search 10000	
Metadata Repositories	Maximum time allowed for a search to complete (sec) 3600	
I Web Tier	Preserve Case of Required Attribute Name specified in Search Request	
_	Preserve Case of Required Attribute Name specified in Search Request Anonymous Bind Disalow except for Read Access on the root DSE	
	Maximum time allowed in a Transaction (sec)	
	* Maximum Number of Operations allowed in a Transaction	Server Mode Read / Write aximum number of entries to be returned by a saard Maximum time allowed for a search to complete (sec.) Required Attribute Name specified in Search Request Anonymous Bind Deallow except for Read Access on the root DSE * Maximum time allowed in a Transaction (sec.) 0
	Port Numbers	
	Non-SSL Port 3060	
	SSL Port 3131	



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

	nager 11g Fusion Middleware Control	Setup ← Help ← Log Out
📲 Farm 🔻 🔒 Topology		
	☆ oid1 @	Logged in as weblogic Host padsrini-pc
🛛 📲 Farm_base_domain	Orade Internet Directory	Page Refreshed Feb 15, 2013 4:55:50 PM IST 🗘
Application Deployments		
🗄 🛅 WebLogic Domain	1 Information	
Identity and Access	All changes made in this page require a server restart to take effect.	
OAM 2 oid1	SSL Configuration ③	OK Cancel
OIM	☑ Enable SSL	
🐼 ovd1	Server Wallet Name oldselfsigned	
🗉 🛅 Metadata Repositories	able SSL ver Walet Name oddselfagned ot required for no-auth mode but is needed in other modes. Advanced SSL Settings	
🖲 🛅 Web Tier	Advanced SSL Sectures	
	Server SSL properties	
	SSL Authentication Server Authentication	
	SSL_RSA_WITH_RC4_128_MD5	
	Opher Suite	
	SL_RSA_WITH_3DES_EDE_CBC_SHA ~	
	SSL_RSA_WITH_DES_CBC_SHA	
	VITLS_RSA_WITH_AES_128_CBC_SHA +	
	* SSL Protocol Version All	

10. Click 'Apply'.

	Ianager 11g Fusion Middleware Control	Setup ← Help ← Log Out
🕂 Farm 🗸 🔒 Topology		
□ •	<pre>介 oid1 ₀</pre>	Logged in as weblogic Host padsrini-pc
I 🕂 Farm_base_domain	Crade Internet Directory -	Page Refreshed Feb 15, 2013 4:56:40 PM IST ᢗ2
Application Deployments		
🗄 🤖 WebLogic Domain	(i) Information	×
Identity and Access OAM	SSL configuration updated for /Farm_base_domain/asinst_1/oid1. Restart component for this change to be effective.	
Did1		
OIM	Server Properties	Apply Revert
ovd1		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 Change SSL Settings	

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 Out weblogi
Launch Pad				
Welcome to Oracle Access Management				
		Host Identifiers	Ession Management Password Policy	
🕲 Identity Federation 🖉	+	▼ 📲 Security Token Service 🖉		+ -
Identity Provider Administration Service Provider Administration		👌 Partners 🎲 Partner Profiles 😙 Endpoints	₩ Token Validation Templates ₩ Token Issuance Templates ₩ Custom Tokens	
Mobile and Social O Mobile Services	🔀 OAuth Service	Access Portal Service O Credential Sharing Groups Password Generation Policies	🕵 Global Agent Settings	+ •
le Configuration				
E Available Services	Se Common Settings Se Access Manager Settings Se Mobile and Social Settings			
Certificate Validation	Severation Settings			
Server Instances	 Security Token Service Settings Access Portal Service Settings 			



2. Click 'Create' under OAM ID Stores.

	entity Stores ×			
Identity Stores				
efault and System Stor				Appl
	* Default Store UserIdentityStore 1 💌			
	* System Store UserIdentityStore 1			
AM ID Stores				Sync IDS Profile
	res. This includes IDS Profiles that are synchronize	d by using Sync IDS Profiles button.		
	Edit 💥 Delete			
ne	Directory Type	Host Information	Description	Synched IDS Pro
eridentityStore 1 Jentity Directory Servic titly Directory Service is a c IDS Profiles	EMBEDDED_LDAP ce common service used by Oracle Identity Managem	idap-host: 7001 ent products to access and manage Identity Directory. The IDS Pi	offles can be used within Orade Access Management after they	No are synchronized. Create Form-Fill Application IDS Prof
ne ridentityStore1 Hentity Directory Service tity Directory Service is a c IDS Profiles anage common Identity Directory	EMBEDDED_LDAP ce common service used by Oracle Identity Managem ectory Service Profiles. IDS Profiles created here v	ldap-host: 7001	offles can be used within Orade Access Management after they	No are synchronized. Create Form-Fill Application IDS Profi
ne ridentity Directory Service titly Directory Service is a c IDS Profiles anage common Identity Directory View V Create O	EMBEDDED_LDAP ce common service used by Orade Identity Managem ectory Service Profiles. IDS Profiles created here w 2 Edit X Delete	Idap-host: 7001 ent products to access and manage Identity Directory. The IDS Pr vill appear in OAM ID Stores table. You have to synchronize IDS P	ofiles can be used within Oracle Access Management after they ofiles created outside Oracle Access Management Console using	No are synchronized. Create Form-Fill Application IDS Prof
ne ridentity Directory Service tity Directory Service is a c IDS Profiles anage common Identity Direc View Create Name	EMBEDDED_LDAP ce common service used by Oracle Identity Managem ectory Service Profiles. IDS Profiles created here v Cedit X Delete Description	Idap-host: 7001 ent products to access and manage Identity Directory. The IDS P vill appear in OAM ID Stores table. You have to synchronize IDS P Repository Nu	offles can be used within Oracle Access Management after they offles created outside Oracle Access Management Console using me Created By	No are synchronized. Create Form-Fill Application IDS Prof
ne ridentity Directory Service titly Directory Service is a c IDS Profiles anage common Identity Directory View V Create O	EMBEDDED_LDAP ce common service used by Oracle Identity Managem ectory Service Profiles. IDS Profiles created here v 2 Edit 2 Delete Description User/Role entities in Def	Idap-host: 7001 ent products to access and manage Identity Directory. The IDS P vill appear in OAM ID Stores table. You have to synchronize IDS P Repository Nu	ofiles can be used within Oracle Access Management after they ofiles created outside Oracle Access Management Console using	No are synchronized. Create Form-Fill Application IDS Profi
ne elentity Directory Service tity Directory Service is a composition of the service of the serv	EMBEDDED_LDAP ce common service used by Oracle Identity Managem ectory Service Profiles. IDS Profiles created here v 2 Edit 2 Delete Description User/Role entities in Def	Idap-host: 7001 ent products to access and manage Identity Directory. The IDS P will appear in OAM ID Stores table. You have to synchronize IDS P ault Identity Directory ault Identity Directory in Default Identity Directory	offies can be used within Oracle Access Management after they offies created outside Oracle Access Management Console using me Created By OPSS	No are synchronized. Create Form-Fill Application IDS Profi
e enderstryStore 1 lentity Directory Service is a C IDS Profiles nange common Identity Directory Verwer Wew Wew Wer Wer Wert idsuserrole IDS Repositories nange Identity Directory Se	EMBEDDED_LDAP CE Common service used by Oracle Identity Manageme ectory Service Profiles. IDS Profiles created here v Cetory Service Profiles. IDS Profiles created here v Cetory Service Profiles. IDS Profiles or eated here v Cetory Service Profiles. IDS Profiles or eated here v Cetory Service Profiles. IDS Profiles or eated here v Cetory Service Repositories that are common across Oracle Cetory Delete	Idap-host: 7001 ent products to access and manage Identity Directory. The IDS P will appear in OAM ID Stores table. You have to synchronize IDS P ault Identity Directory ault Identity Directory in Default Identity Directory	offies can be used within Oracle Access Management after they offies created outside Oracle Access Management Console using me Created By OPSS	No are synchronized. Create Form-Fill Application IDS Profi

- 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.

eate: User Identity Store					1	est Connection	Apply
* Store Name	d La			Enable SSL			
	OID: Orade Internet Directory	•	Prefetched Attributes				
Description	OID: Oracle Internet Directory						
0000000							
Location and Credentials	ofss220223.in.oracle.com:3131		8 Rind Di	cn=orcladmin			
	0155220223.01.01808.0001.3131			••••••			
			Password				
Users and Groups							
	* Login ID Attribute	a					
	User Password Attribute	userPassword					
	* User Search Base	cn=Users,dc=in,dc=oracle,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							
6	Group Membership Cache Maximum Size	10000					
	pership Cache Time to Live (in seconds)	0					
Connection Details							
Minim	num Pool Size 10 🌻		Results time limit	t (in seconds) 👘 0 🛢			
Maxim	num Pool Size 50 🌻			Retry Count 3 🗘			
Wait Timeout	: (in seconds) 120 🌲		R	teferral Policy follow			
Inactivity Timeout	: (in seconds)						

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

	nagement					
reate: User Identity Store	ores × Create: User Identity Sto.	.×			Test Connection	Apply
	FlexcubeStore			Enable SSL	Connection Status ×	-obbit
	OID: Oracle Internet Directory	•	Prefetched Attributes		Connection to the User	
Description	Old: Ordice Internet Directory				Identity Store successful!	
					OK Cancel	
Location and Credentials						
	n ofss220223.in.orade.com:3131		* Bind DN	cn=orcladmin		
			* Password	•••••		
Users and Groups						
	* Login ID Attribute User Password Attribute					
		cn=Users,dc=in,dc=oracle,dc=com				
	User Filter Object Classes	ch-osersysc-enysc-onadeysc-com				
	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 Mem	bership Cache Time to Live (in seconds)	0 🗘				
Connection Details						
	mum Pool Size 10 🗘		Results time limi			
	mum Pool Size 50 C			Retry Count 3		
	it (in seconds) 120 🗘		R	eferral Policy follow		
Inactivity Timeou	it (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 Mar	nagement				Accessibility Help Sign Out weblogic 🧲
🖸 Launch Pad 🛛 🌋 User Identity St	ores × FlexcubeStore ×				
FlexcubeStore					Test Connection Apply
Generation					×
User Identity Store FlexcubeStore	created successfully.				
Store Name	FlexcubeStore			✓ Enable SSL	
	OID: Oracle Internet Directory	•	Prefetched Attributes		
Description					
⊿ Location and Credentials					
Locato	n ofss220223.in.orade.com:3131			cn=orcladmin	
			* Password	*****	
⊿ Users and Groups					
oscis una aroups	* 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 Cache					
	Group Membership Cache Maximum Size	10000 🗘			
Group Men	bership Cache Time to Live (in seconds)	0			
Connection Details					
Min	mum Pool Size 10 🗘		Results time limit	t (in seconds) 0 单	
Maxi	mum Pool Size 50 🗘			Retry Count 3 🗘	
Wait Timeou	it (in seconds) 120 🗘		R	eferral Policy follow	
Inactivity Timeou	ut (in seconds) 0 🗘				

2.6.2 Creating Authentication Module

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

RACLE' Access Management			Accessibility Help Sign Out we
Launch Pad			
elcome to Oracle Access Management			
🖗 Quick Start Wizards		G Access Manager	
C Application Registration		Image: Contract of Contracts Image: Contracts Image: Cont	Wather Create Application Domain Auther Create Application Son A Create Host Identifier Sessio Create Host Identifier Create Relearce Type Passor Create LDAP Authentication Module Create Kriberos Authentication Module Create Kriberos Authentication Module
 Identity Federation Identity Provider Administration Service Provider Administration 	+•	Security Token Service Image: Partners	Create Custom Auffentication Module Create Authentication Scheme Create 109 Webgate Create 109 Webgate Custom Tokens
🚦 Mobile and Social 🥝		🖥 Access Portal Service 🖉	+
📕 Mobile Services 🛛 🔞	(CAuth Service	 Credential Sharing Groups Password Generation Policies 	ිදුරු Global Agent Settings
& Configuration			
월드 Available Services	Common Settings		
🔏 User Identity Stores 🖇	Access Manager Settings		



- 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	Accessbility	Help	Sign Out	weblogic S
	C Launch Pad f Authentication Modules × 📑 FlexcubeAuthnHodule ×				×
ſ	FlexcubeAuthnModule				Apply
	Confirmation				×
	LDAP Authentication Module FlexcubeAuthnModule modified successfully.				
	* Name FlexcubeAuthmModule * User Identity Store FlexcubeStore				

2.6.3 Creating Authentication Scheme

1. Click 'Create Authentication Scheme' under Access Manager

Launch Pad		
Welcome to Oracle Access Management		
Weick Start Wizards	Cacess Hanager	Create Application Domain Create Application Create Application Create Application Create Host Identifier Sessio Create Resource Type Passw Create Ketheros Authentication Module Create X309 Authentication Create X309 Au
Identity Federation 	iff Security Token Service 🖉 라고 Arthers 03 Partner Profiles 1월 Endponts	Create Authentication Scheme Totan Trate 11g Webgate Totan
Hobile and Social Courter of the service Social Identity	Access Portal Service	+ -
Configuration Common Settings Common Settings Common Settings Common Settings Common Settings Common 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':

the Authentication Scheme
/er
ation Module
Module' of this document.
e=Secure
/pe=default
alue=/oam

challenge_url=/CredCollectServlet/BASIC

ORACLE' Acce	ss Management	Accessibility Help Sign (Out weblogic 📿
🖸 Launch Pad 🛛 🔀 Flexo	ubeBasic0AM5cheme ×		
Authentication Sche	emes	Set As Default Dup	olicate Apply
Confirmation			×
Authentication Scheme,	FlexcubeBasicOAMScheme, modified successfully		
* Name	FlexcubeBasicOAMScheme		
Description	Basic Style SSO Login for FLEXCUBE		
* Authentication Level	1 🗘		
Default			
* Challenge Method	BASIC		
Challenge Redirect URL	/oam/server		
* Authentication Module	FlexcubeAuthnModule		
Challenge Parameters	sscCookje -Secure sottest/Upgdefault extensive-losen challenge_upj= /CredicolectSeculet/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

thentication Scho	mes	Set As Default Duplicate
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		
Challenge Parameters	ssoCookie=Secure	

2.6.3.3 KBA Based Strong Authentication Scheme (Only in case OAAM is used)

Enter the Below Details and click 'Apply':

Name	: Name of the Authentication Scheme
Authentication Level	: 2
Challenge Method	: FORM
Challenge Redirect URL	: /oam/server
Authentication Module	: Authentication Module

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



Challenge URL	: /pages/oaam/login.jsp
Context Type	: default
Context Value	: /oam
Challenge Parameters	: ssoCookie=Secure
	oaamPostAuth=true
	oaamPreAuth=true

RACLE Acce	ss Management		Accessbility H	elp Sign Out weblo	ogic
Launch Pad 🛛 👪 Flexo	ubeKBAOAAMScheme ×				ľ
uthentication Sche	emes		Set As Defa	ult Duplicate A	Apply
Gamma Confirmation					×
Authentication Scheme,	, FlexcubeKBAOAAMScheme, created su	uccessfully			
* Name	FlexcubeKBAOAAMScheme				
Description	OAAM - KBA Based Strong SSO Login f	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	9aamPostAuth=true 9aamPreAuth=true				

ss Management	Accessibility Help Sign Out weblogic
ubeKBA0AAM5cheme ×	
mes	Set As Default Duplicate Appl
FlexcubeKBAOAAMScheme, modified successfully	×
FlexcubeKBAOAAMScheme	
OAAM - KBA Based Strong SSO Login for FLEXCUBE	
2 🗘	
FORM	
/oam/server	
FlexcubeAuthnModule	
/pages/oaam/login.jsp	
default 💌	
/oam	
gaamEreAuth=true sspCcookis=Secure	
	FORM Com/server FlexcubeAuthrModule (pages/oaam/login.jsp)



2.6.4 Creating OAM 11g Webgate

Follow the below steps to create a Webgate:

1. Click 'Server Instances' under Configuration.

			Accessibility Help S	i gn Out weblogi
Launch Pad				
Welcome to Oracle Access Management		Host Identifiers	- Session Management	
B Identity Federation Ø	+ -	Security Token Service 🖉		+ -
() Identity Provider Administration		ලි Partners මූබ Partner Profiles මී Endpoints	🛃 Token Valdation Templates Token Issuance Templates 醚 Custom Tokens	
Mobile and Social O Mobile Services	😭 OAuth Service	Access Portal Service	🕵 Global Agent Settings	+ •
Configuration	 Common Settings Access Manager Settings Mobile and Social Settings Federation Settings Security Token Service Settings Access Portal Service Settings 			

2. Click 'Search'.

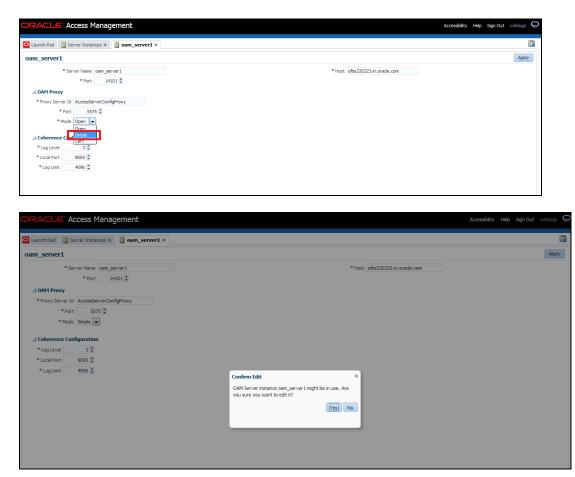
ORACLE Access Management	Accessibility	Help Sigr	Out	weblogic	Č
C Lauch Pad C Server Instances ×		Cri	eate OAI	M Server	
Name Search Results			Search	Reset	t
Actions + View + 💽 🔗 % ত Detach Row Name No data to display.					



3. Edit oam_server1.

Launch Pad 📱 Server Instances ×	
earch OAM Servers	Create OAM Server
∡ Search	
Name	
	Search
Search Results	
Actions 🔻 View 👻 📑 🖉 Detach	
Name 1 <u>gam server1</u>	

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





ORACLE' Access Management		Accessibility	Help Sign Out weblo	ogic 📿
Launch Pad Server Instances × Source of the server 1 ×				
oam_server1			A	Apply
Confirmation				×
OAM Server instance oam_server1 modified successfully.				
* Server Name oam_server1	* Host [ofss220223.in.orade.com			
* Port 14101 \$				
* Proxy Server Id AccessServerConfigProxy				
* Port 5575 🗘				
* Mode Simple 💌				
✓ Coherence Configuration				
*Log Level 3 🗘				
* Local Port 9095 \$				
* Log Limit 4096 🗘				

5. Click on Create 11g Webgate under Access Manager

Launch Pad					
elcome to Oracle Access Management					
🖗 Quick Start Wizards			G Access Manager		+ -
Application Registration			C Application Domains	🛗 Auther	Create Application Domain
K SSO Agent Registration			Applications	👸 Auther	Create Application
			Resource Type	🔊 SSO A	Create Host Identifier
			Host Identifiers	👪 Sessio	Create Resource Type
			De Plug-ins	📴 Passw	Create LDAP Authentication Module
					Create Kerberos Authentication Module
					Create X509 Authentication Module
					Create Custom Authentication Module
📆 Identity Federation 🥝		+ -	🛗 Security Token Service 🥝		Create Authentication Scheme
3 Identity Provider Administration			8 Partners	🛃 Token	Create 11g Webgate
Service Provider Administration			A Partner Profiles	Token	Create 10g Webgate
Service Provider Administration			Endpoints	Custor	*
📕 Mobile and Social ⊘			🗟 Access Portal Service 🖉		+ •
Mobile Services	CAuth Service		🙀 Credential Sharing Groups	🞉 Global	Agent Settings
Total Identity	_		- Password Generation Policies	-	
& Configuration			L		
Available Services	🖉 Common Settings				
🔏 User Identity Stores	S 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			

RACLE Access Managen	nent	Accessibility Help Sign Out weblogic
Launch Pad 🛛 🕸 SSO Agents × Creat	e 11g Webgate ×	
Create OAM 11g Webgate		Apply
	11g FlexcubeWebgate	User Defined Parameters Ster Q&MAUDOCapile =False
Description Base URL	https://ofss220223.in.orade.com	
		Virtual host 🗐 Auto Create Policies 🗹
	© Open © Smple © Cert FlexubeWebgate	IP Validation
esource Lists Protected Resource List	Public Resource List 🕂 🕂 🗙	
Relative URI /FCJNeoWeb	Relative URI	
/FCISNeoWeb		



cubeWebgate				App
Confirmation				×
OAM 11g Webgate FlexcubeWebgate crea	ated successfully.			
Artifacts are generated in following locatio	n : /scratch/app/sso1123/wl1036/Middle	ware/user_projects/domains/domain_two/output/FlexcubeWebgate		
Name	FlexcubeWebgate	Logout Redirect URL	https://ofss220223.in.oracle.com:1	
Description		Logout Target URL		
Access Client Password		User Defined Parameters	proxySSLHeaderVar=IS_SSL	
* Security			URLINUTF8Format=true dient_request_retry_attempts	
	 Simple Cert 		=1	
	Enable		inactiveReconfigPeriod=10 maxSessionTimeUnits=minutes	
	🔘 Disable			
* Max Cache Elements	100000 🗘	* Sleep for (Seconds)	60 🗘	
* Cache Timeout (Seconds)	1800 🗘	Cache Pragma Header		
* Token Validity Period (Seconds)	3600 \$	Cache Control Header		
* Max Connections	1	Debug IP Validation		
Max Session Time	60 🗘	IP Validation 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		
Lagout Callback UDI	/oam_logout_success			
	/oam_logout_success			
ver Lists				
Primary Server List	🕂 💥 Secondary Se	rver List 🕹 😤		

- 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'.

🖸 Launch Pad 🛛 🌋 SSO Agents 🗙 🛛 Flex	cubeWebgate ×						
FlexcubeWebgate							Apply
Confirmation OAM 11g Webgate FlexcubeWebgate mo	dified successfully.						×
	FlexcubeWebgate				Logout Redirect URL	https://ofss220223.in.orade.com:1	
Description					Logout Target URL		
Access Client Password * Security * State	 Open Simple Cert Enable 				User Defined Parameters	proxySSLHeaderVar=ssl URLInUTF8Format=true dient_request_retry_attempts=1 inactiveReconfigPeriod=10 maxSessionTimeUnits=minutes filterOAMAuthnCookie=false	
* Max Cache Elements	Disable 100000 \$				* Sleep for (Seconds)	60 🗘	
Max Cache Elements Cache Timeout (Seconds)					Cache Pragma Header	no-cache	
 Cache Timeout (Seconds) * Token Validity Period (Seconds) 					Cache Control Header	no-cache	
, , ,					Debug		
* Max Connections					IP Validation		
* Max Session Time					Deny On Not Protected		
* Failover Threshold					Allow Management Operations Allow Token Scope Operations		
* AAA Timeout Threshold	- (*)				Allow Master Token Retrieval		
* Preferred Host Logout URL	FlexcubeWebgate				Allow Credential Collector Operations		
	/oam_logout_success						
Primary Server List	+ ×	Secondary Ser					
	Port Max Number	Access Server	Host Name	Host Port Max Number			
oam_server ofss220223.in.o 5575		Access Server	HUSCHAINE	HOST POIL MAX NUMBER			



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.

ACLE Access Management	Accessbillty Help Sign Out weblogic
unch Pad 🔋 Server Instances × 🔋 oam_server1 ×	
_server1	Appl
Confirmation	×
DAM Server instance oam_server 1 modified successfully.	
* Server Name oam_server1	* Host ofss220223.in.orade.com
* Port 14101 🗘	
OAM Proxy	
Proxy Server Id AccessServerConfigProxy	
* Port 5575 🗘	
* Mode Open	
Coherence Conf Cert	
*Log Level 3 🗘	
* Local Port 9095 🗘	
* 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 'Application Domains' under Access Manager

DRACLE' Access Managemen	t			Accessibility Help	Sign Out weblogic
Launch Pad					
Welcome to Oracle Access Management					
Quick Start Wizards Quick Start Wizards Quick Store Registration SSO Agent Registration			Ceess Hanager Ceess	Authentication Modules Authentication Schemes Sol Agents Session Management ► Password Policy	+ •
Identity Federation Identity Frevider Administration Identity Frevider Administration Identity Frevider Administration		+-	Security Token Service ³ ³ Partners ³ ³ Partner Profiles ³ Endpoints	i⊒ Token Validation Templates ④ Token Issuance Templates ∰ Custom Tokens	+-
Hobile and Social Hobile Services Social Identity	n OAuth Service		Access Portal Service Co	🕵 Global Agent Settings	+ •
Configuration B ∃Available Services	ھ Common Settings				



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

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

ORACLE Access Management	Accessibility	Help Sign Out weblogic Q
Launch Pad Application Domain × Search Search	[Create Application Domain
Name Search Results Actions View V		Search Reset
Actions • View • Gall & Actions • View	Description	

ORACLE.	Access Management		Accessibility Help	Sign Out weblogic 🤉
🖸 Launch Pad 🛛 🧯	Application Domain ×			
Search Applicat	ion Domains		Crea	te Application Domain
⊿ Search				
Name				
				Search Reset
Search Results				
Actions • View •	📑 🧪 💥 🔛 Detach			
Row Name		Description		
1 Flexo	ubeWebgate_	Application Domain created through Remote Registration		
2 PUSIO	n Apps Integration	Policy objects enabling integration with Gracie Pusion Applications		
3 IAM 9	Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications		

3. Click 'Authentication Polices'.

ORACLE' Access Ma	inagement Access	lity Help	Sign Out	weblogic 🧲
Launch Pad 🛛 🍙 Application Dor	nan x 🛛 🍓 FlexcubeWebgate ×			
Application Domains				
Summary 🔅 Resources	🛃 Authentication Policies 🛛 🛃 Authorization Policies 🛛 🤯 Token Issuance Policies 🛛 Administration			
				Apply
* Name	FlexubeWebgate			
	Application Domain created through Remote Registration			
	Regulation			
Session Idle Timeout (minutes)	0			
Allow OAuth Token				
Allow Session Impersonation				
Policy Ordering				
Enable Policy Ordering				
View 🕶 💠 🖉 💥				
Resource Prefix	Resource Type Host Identifier			
No Data to Display				



4. Click 'Protected Resource Policy'.

plication Do	Application Domain × 🌀 FlexcubeWe		
	mains		
Summary 🔅 R	Resources Authentication Policies	🛃 Authorization Policies 🛛 🌙 Token Issuance Policies 🛛 Administration	
Authenticatio	on Policies		Create Authentication Policy
Actions - Vie	ew 🕶	🕒 🖤 🥒 💥	d Detach
Row I	Name	Description	
1	Protected Resource Policy	Policy set during domain creation. Add resources to this	s policy to protect them.
2	Public Resource Policy	Policy set during domain creation. Add resources to this	s policy to allow anyone access.

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

Access Management Accessibility Help Sign Out 🖸 Launch Pad 🛛 🌀 Appli Vebgate × 🛛 👼 FlexcubeWebgate : Protect... × nain × 🔞 Flexcube Authentication Policy Duplicate App * Name Protected Resource Policy Success URL Description Policy set during domain creation. Add resources to this policy to protect them. Failure URL -Re + × 戀R Query String Name Value list rce Type Operatio All нттр

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

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

nch Pad 🛛 🌀 Applica	ation Domain × 🌀 FlexcubeWebgate × 🐻 FlexcubeWebgate : Protect	×	
entication Polic	y		Dupicate
* Name	Protected Resource Policy	Success URL	
Description	Policy set during domain creation. Add resources to this policy to protect them.	Failure URL	
uthentication Scheme	FlexcubeBasicOAMSchme		
	tion to be generated for the user, optionally containing any Asserted Attribute set belo	w.	
Responses			+ / >
ame vis Policy does not have	Type e any Responses	Value	۵۲ ۵۲



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

Type : Header

Name : DN

Value : \$user.attr.dn

🖸 Launch Pad 🛛 🌀 Applica	ation Domain × 🌀 FlexcubeWebgate ×	📕 FlexcubeWebgate : Pi	otect ×						
Authentication Policy	y							Duplicate	Apply
* Name	Protected Resource Policy			s	uccess URL				
Description	Policy set during domain creation. Add resource protect them.	es to this policy to			Failure URL				
* Authentication Scheme Resources Responses	FlexcubeBasicOAMScheme								
Identity Assertion	tion to be generated for the user, optionally co	ntaining any Asserted Attribut			×	_		+	1 %
Name	Туре	* Type	Header						
This Policy does not have	e any Responses	* Name	DN		Value				
		* Value	\$user.attr.dn						
			policy. Enable I	on has not been ena dentity Assertion in o ute type responses (rder to collect				
				Ade	d Cancel				

8. Click on Apply to Save the Changes

	s Management		Accessibility Help Sign Out weblogic
Launch Pad 🛛 🏠 Applica	tion Domain × 🏾 🌀 FlexcubeWebgate × 🛛 😹 FlexcubeWebgate : Protect		
thentication Policy	,		Duplicate Apply
Confirmation			×
Authentication Policy, Pro	otected Resource Policy, modified successfully		
* Name	Protected Resource Policy	Success URL	
	Policy set during domain creation. Add resources to this policy to protect them.	Failure URL	
* Authentication Scheme	FlexcubeBasicOAMScheme		
Resources Responses	Advanced Rules		
Identity Assertion This will cause an assert	ion to be generated for the user, optionally containing any Asserted Attribute set belo	<i>i.</i>	
🖗 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 🖸
C Launch Pad	Application Domain ×	te ×	
Application	Domains		
Summary 📢	🔅 Resources 🛛 🗟 Authentication Policies 🔂 🗛	thorization Policies Voken Issuance Policies Administration	
Authoriza	tion Policies		Create Authorization Policy
Actions 👻	View 🕶	🕒 👎 🥒 🗶	Detach
Row	Name	Description	
	1 Public Resource Policy	Policy set during domain creation. Add resources to this	s policy to allow anyone access.
	2 Protected Resource Policy	Policy set during domain creation. Add resources to this	s policy to protect them.
_			



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

ORACLE: Access Management	Accessibility	Help	Sign Out	weblogic 🤉
🖸 Launch Pad 🛛 🌀 Application Domain 🛪 🛛 🌀 FlexcubeWebgate x				×
Authorization Policy			Duplicate	e Apply
Summary Resources Conditions Rules Responses				
* Name Protected Resource Policy Description Policy set during domain creation. Add resources to this policy to protect them.				
Success URL Falure URL				

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

Type : Header

Name : DN

Value : \$user.attr.dn

ORACLE' Access Management			Accessibility	Help	Sign Out	weblogic
Launch Pad Application Domain × G FlexcubeWebgat	te × 🛃 FlexcubeWebgate : Protect ×					C
Authorization Policy					Duplicate	e Apply
Summary Resources Conditions Rules Responses Identity Assertion This will cause an assertion to be generated for the user, option Identity Assertion Identity Assertion	nally containing any Asserted Attribute set below.					
🖗 Responses					+ /	/ %
Name	Туре	Value				
This Policy does not have any Responses						

ORACLE Access Manage	ement		Accessibility Help Sign Out weblogic 드
🖸 Launch Pad 🛛 🌀 Application Domain ×	G FlexcubeWebgate ×	otect ×	×
Authorization Policy			Duplicate Apply
Summary Resources Conditions Ru	les Responses		
Identity Assertion This will cause an assertion to be generated	ated for the user, optionally containing any Asserted Attribut	ie set below.	
Responses			+ / X
Name This Policy does not have any Responses	Туре	Value	
	* Name	Header	



12. Click 'Apply' to Save the changes.

	agement			Accessibility He	lp Sign Out	weblogic 🧲
Launch Pad 🛛 🌀 Application Domai	in × 🌀 FlexcubeWebgate × 🖪 FlexcubeWebgat	te : Protect ×				
Authorization Policy					Duplicat	te Apply
Confirmation Authorization Policy, Protected Res	source Policy, modified successfully					×
Summary Resources Conditions	Rules Responses					
	generated for the user, optionally containing any Asserted At	ttribute set below.				
🖗 Responses					+	/ %
Name	Туре	Value				
DN	Header	\$user.attr.dr	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	Num Of Threads	Directory Information
ofss220028.in.oracle.com: 5575, 1	Up	Friday, January 11, 2013 16:18:27			

Cache Name	State			Timeout (seconds)	Cache Stats (Hits:Misses: Expired:Flushed)	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 Manage	r Test Tool _ ×
<u>F</u> ile <u>E</u> dit <u>T</u> est <u>H</u> elp	
🔁 🗟 I 🥔 I 🏦	
Server Connection	
IP AddrPortMax C*Prim\$55751	*Age 🖉
Secon 1	Agent Pa
Min C Timeou Mo Global Passp 1 30000 Si ************************************	Connect
Protected Resource URI	• 4
Sche *H [https 💙 FlexcubeWebdate	Port Get Auth S
Resour //FCINeoWeb	Operat Get 🗸 🗸 Validate
User Identity IP Address *Username Password SARAN ********* User Certifica	** ? Authenti Authorize
Status Messages	
[1/11/13 5:33 PM][response] Connected to primary access [1/11/13 5:34 PM][request][validate] yes [1/11/13 5:34 PM][response] Authentication scheme : Flexe [1/11/13 5:34 PM][response] Redirect URL : https://ofss220 [1/11/13 5:34 PM][response] Credentials expected : 0x1 (b [1/11/13 5:34 PM][response] Credentials expected : 0x1 (b [1/11/13 5:34 PM][response] User DN : cn=SARAN,cn=user [1/11/13 5:34 PM][response] User DN : cn=SARAN,cn=user [1/11/13 5:34 PM][response] SessionID : 66531a7f-460d-46 [1/11/13 5:34 PM][response][action] DN : cn=SARAN,cn=user [1/11/13 5:34 PM][response][action] OAM_IMPERSONATOR_ [1/11/13 5:34 PM][response][action] VAM_IMPERSONATOR_ [1/11/13 5:34 PM][response][action] VAM_IMPERSONATOR_	cubeAuthnScheme, level : 1 028.in.oracle.com:14101/oam/server asic) rs.dc=oracle.dc=com db8-b872-a7da77999282 sers.dc=oracle.dc=com
Elapsed (86 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 - IS

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

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 FCIS. If the FCIS user already exists then unlock the user and update the LDAP DN value which was set when creating the user in LDAP. Click on Validate button to check whether any other user is having the same LDAP DN value.

LDAP DN value should be entered as complete DN value.

eg.

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



For FLEXCUBE - IS

🔷 User Admin							- 1
🗄 Save							
User Details							
Externel Identifier LDAP DN Number Format	FCISUSER FCIS User cn=FCUSR,cn=Users,d() ® XXX,XXX,XXX,XXX © XXX,XXX,XXX,XXX	Language * Home Branch * Home Module *	000	AI AI Died		● Staff Auto End Of Day Customer	
Modules		Status Description					
	 Investments Corporate 	User Status	 Enabled Hold Disabled Locked 	Sta	Time Level * tus 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 Brand	ches Module Disallo	wed Functions				
Input by Authorized by		ateTime ateTime	Mod No Open Authorized			0	k Cancel

2.7.3 Launching FLEXCUBE

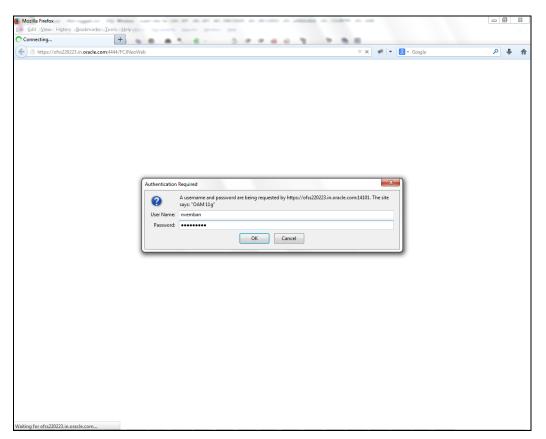
After setting up FLEXCUBE to work on Single Sign on mode, navigate to the URL <a href="https://<hostname>:<OHS">https://<hostname>:<OHS SSL Port>/<Context Root> from your browser

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

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

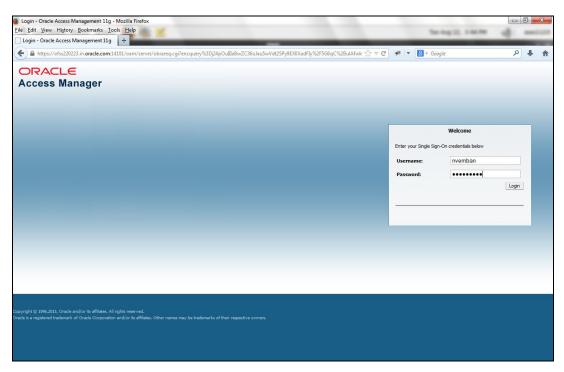


2.7.3.1 Basic Style Challenge by Webgate

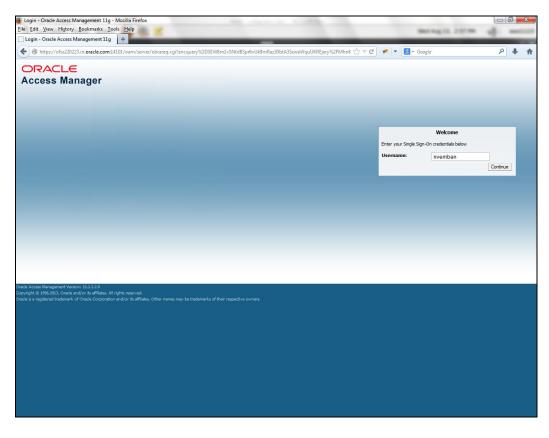




2.7.3.2 Form Style Challenge by Webgate

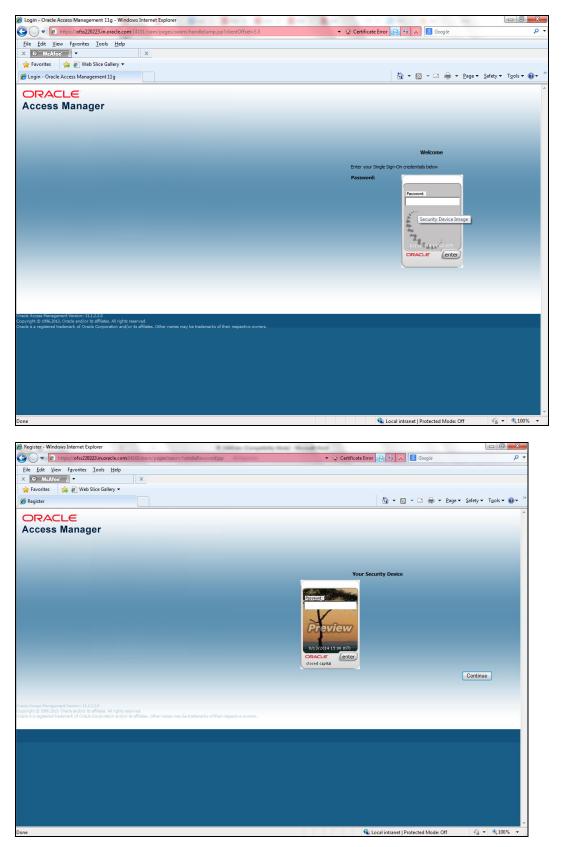


2.7.3.3 KBA Based Strong Authentication Challenge by Webgate(Only when OAAM is used)





First Time Login

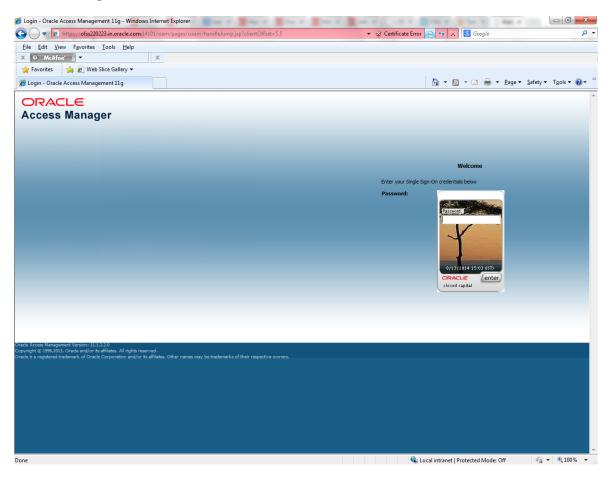




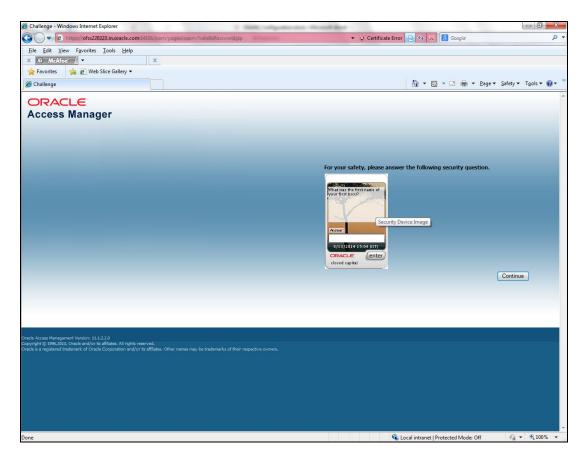
e Register - Windows Internet Explorer	Certificate Error C 42 X R Google P
C P I https://ofss220223.in.oracle.com:14101/oam/pages/oaam/handleRegisterImagePhrase.jsp	👻 Certificate Error 😥 🍫 💥 💈 Google 🖉
File Edit View Favorites Tools Help	
X O McAfee X	
🚖 Favorites 🛛 🚔 🖉 Web Slice Gallery ▼	
<i>€</i> Register	📩 🔹 🔂 👻 🖃 🖶 Page 👻 Safety 🕶 Tools 🕶 🔞 💌
ORACLE	
Access Manager	
Access Manager	
Select Your Security Questions/Answers	
1) Select One	
2) Select One	
3) Select One	
,	
N Print Pre	
) Select One	
i) Select One	
Continue	
vracle Access Management Version: 11.12.2.0 opyright © 1996,2013, Oracle and/or its affiliates. All rights reserved. racle is a registered trademark of Oracle Ocaporation and/or its affiliates. Other names may be trademarks of their respective owners.	
lone	💊 Local intranet Protected Mode: Off 🛛 🖓 💌 🔍 100% 💌
Register - Windows Internet Explorer	
🚱 🔵 💌 💈 https://ofss220223.in.oracle.com/14101/oam/pages/oaam/handleRegisterImagePhrase.jsp	✓ Certificate Error B 42 × S Google
Control of the second s	
Introvi/ofsz20223.in.orscle.com14101/osm/pages/osam/handleRegisterImagePhrise.jsp File Edit View Favorites Tools Help X O McAfect * X	
C Attps://ofss220223.in.oracle.com/14101/oam/page/oaam/handleRegisterImagePhrase.jap Eile Edit View Favorites Tools Help X Affect F X Affect X Affect X	 Certificate Error Image: Image: Image:
C Attps://ofsz20223.in.oracle.com/14101/oam/pages/oaam/handleRegisterImagePhrase.jap Eile Edit View Favorites Tools Help X MatArcor * K ge Favorites Se E Web Stice Gallery *	
C C	 Certificate Error Image: Image: Image:
Attps://ofsz20223.in.oracle.com/14101/cam/page/Joaam/handleRegisterlinagePhrase.jsp Elle Edit View Favorites Tools Help Tools Help Forontes Register	 Certificate Error Image: Image: Image:
C C	 Certificate Error Image: Image: Image:
Introv/ofsz222223 incracle.com 14101/com/ pages/coam/handleRegisterImagePhrise.jap Elie Edit View Favorites Tools Help MizArcor • X Favorites Access Manager	 Certificate Error Image: Image: Image:
Introv/ofsz222223 incracle.com 14101/com/ pages/coam/handleRegisterImagePhrise.jap Elie Edit View Favorites Tools Help MizArcor • X Favorites Access Manager	 Certificate Error Image: Image: Image:
Attps://ofsz20223.in.oracle.com/14/01/vem/pages/oaam/handleRegisterImagePhrase.pp Elie Edit View Favorites Tools Help Tools Help Favorites Register CRACLE Access Manager elect Your Security Questions/Answers	 Certificate Error Image: Image: Image:
Introvi/ofsz20223 in oracle.com 14101/com/ page/coam/handleRegisterImagePhrase.pp Ele Edit View Favorites Tools Help MacAccer Fororites Register Register CRACLE Access Manager elect Your Security Questions/Answers	 Certificate Error Image: Image: Image:
Https://ofsz20223.incracle.com/14101/4cm/pages/casm/handleRegistelImagePhrase.jap File Edit Yew File Edit Yew File Status Yew * * * * * * Foroites Foroites Foroites Foroites Foroites Foroites Foroites Foroites Foroites Foroites Foroites Foroites Foroites <td> Certificate Error Image: Image: Image:</td>	 Certificate Error Image: Image: Image:
i https://ofss220223.in.oracle.com/14101//cam/pages/oasm/handleRegistellmagePhrase.jap iie jaht View Favorites jools Help i dealer i Register CRACLEE Access Manager idect Your Security Questions/Answers i) Where did you get your first pet? OFSS	 Certificate Error Image: Image: Image:
introv/ofss220223.in.orscle.com 14101/vem/pagev/oasm/handlefkegistellmagePhrise.gp File Edit View Favorites Tools Help Favorites Favorites <td> Certificate Error Image: Image: Image:</td>	 Certificate Error Image: Image: Image:
Https://ofsz20223.incracle.com/14101/4cm/pages/casm/handleRegistellmagePhrase.gp File Edit View Favorites Image: Case of the phrase.gp File Edit View Favorites Image: Case of the phrase.gp For Fornites Image: Case of the phrase.gp Image: Case of the phrase.gp Fornites Image: Case of the phrase.gp Image: Case of the phrase.gp Fornites Image: Case of the phrase.gp Image: Case of the phrase.gp Fornites Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image: Case of the phrase.gp Image:	 Certificate Error Image: Image: Image:
introv/ofsz20223 increace.com 14101/sem/ pagev/osam / handlefkegistellmagePhrise.gp File Edit View Favorites Tools Help For Acace • Image:	 Certificate Error Image: Image: Image:
introv/ofss220223.in.oracle.com 14101/vent/pagev/oasm/handle/kegistellmagePhrase.gp File Edit View Favorites Tools Help Favorites Action (Contemported Factoria) Favorites Improve the State of the State	 Certificate Error Image: Image: Image:
introv/ofss220223.in.oracle.com 14101/vent/pagev/oasm/handle/kegistellmagePhrase.gp File Edit View Favorites Tools Help Favorites Action (Contemported Factoria) Favorites Improve the State of the State	 Certificate Error Image: Image: Image:
introv/ofsz20223 in oracle.com 14101/ven/pagev/oasm/handle/kegistel/magePhrise.gp File Edit Yiew Favorites Good Favorites Image: Comparison of the file Image: Comparison of the file Image: Comparison of the file Favorites Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you saw in concert? Image: Comparison of the first musical group you grou	 Certificate Error Image: Image: Image:
i https://ofss220223.in.oracle.com/14101//cmr/page/okam/handleflegited/magePhrate.gp iii i i it were sportes i ools Help iii i i i i i i i i i i i i i i i i i	 Certificate Error Image: Image: Image:
inters//ofss220223.increcle.com/14/01/vern/pages/okam/hundleflegited/magePhrase.gp iie gdit view Favorites Iools Help iii AcaCoe	 Certificate Error Image: Image: Image:
i https://ofss220223.in.oracle.com/14101//cmr/page/okam/handleflegited/magePhrate.gp iii i i it were sportes i ools Help iii i i i i i i i i i i i i i i i i i	 Certificate Error Image: Image: Image:
i https://ofsz22223.incracle.com/14101/4cm/pages/casm/thadleRegistelMasgePhrate.gp File Edit View Favorites Tools Help i Acadoe · · · · · · · · · · · · · · · · · · ·	 Certificate Error Image: Image: Image:
i https://ofsz22223.increde.com/14101/4cm/pages/clasm/thadleRegistellmagePhrate.gp File Edit View Favorites Tools Help i wadree • • • • • • • • • • • • • • • • • •	 Certificate Error Image: Image: Image:
i https://ofsz22223.increde.com/14101/4cm/pages/clasm/thadleRegistellmagePhrate.gp File Edit View Favorites Tools Help i wadree • • • • • • • • • • • • • • • • • •	 Certificate Error Image: Image: Image:
introv/ofsz20223.in.orscle.com 14101/vem/pageu/oasm/handleftegistellmagePhrase.gp File Edit Yew Favorites Image: Second Se	 Certificate Error Image: Image: Image:
i https://ofss220223.increde.com/14101/dom/page/dasm/handlelle-gistellinegePhrate.gp iii Edit View Favorites Tools Help i Acace • I × Favorites @ Web Site Gallery • i Favorites @ Web Site Gallery • i Register COCCLE 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 concet? • 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	 Certificate Error Image: Image: Image:
i https://ofss220223.increde.com/14101/dom/page/dasm/handlelle-gistellinegePhrate.gp iii Edit View Favorites Tools Help i Acace • I × Favorites @ Web Site Gallery • i Favorites @ Web Site Gallery • i Register COCCLE 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 concet? • 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	 Certificate Error Image: Image: Image:
The first musical group you saw in concert? OFSS What was the first name of your first boss? What was the first name of your first boss? OFSS What was the first name of your first boss? OFSS	 Certificate Error Image: Image: Image:
	 Certificate Error Image: Image: Image:
	 Certificate Error Image: Image: Image:
	 Certificate Error Image: Image: Image:
The first musical group you saw in concert? OFSS What was the first name of your first boss? What was the first name of your first boss? OFSS What was the first name of your first boss? OFSS	 Certificate Error Image: Image: Image:
	 Certificate Error Image: Image: Image:
	 Certificate Error Image: Image: Image:
	 Certificate Error Image: Image: Image:
P intps://ofs220223.in.orscle.com/14101/dom/paget/osam/hundeRegisterImagePhrase.pp File Edit View Favorites Iools Help MAAdee MAdee MAAdee MAAdee MAAdee MAAdee MAAdee	 Certificate Error Image: Image: Image:



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

https://shis220223.in.oracle.com/4444/FC8	esWeb/9MMC0FRM.pp	(1)	+
DRACLE	Baston Charge Module Date . 00/120214 Session Time . 0000.08 Working How Leoped Union	Connect Annual Asian 1 Star Off	-
Inne .			
leprch 单	💽 🕦 Information Message		
Edamal System Makilananos	Information Message		
Integration Schedule Datalis	1 LastLogin : 08/12/2014 15:56:50		
Security Maintenance			
	Current Time 16.15.36		
	OK		

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 [June] [2017] Version 12.0.4.7.1

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], [2017], 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.

