Oracle Access Manager Integration

Oracle Access Manager Integration Oracle FLEXCUBE Universal Banking Release 12.87.06.0.0

June 2020





Table of Contents

1. P	REFACE	
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. E	NABLING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER	
2.1	INTRODUCTION	
2.2	BACKGROUND AND PREREQUISITES	
2.	2.1 Software Requirements	
2.3	BACKGROUND OF SSO RELATED COMPONENTS	
2.	3.1 Oracle Access Manager (OAM)	
2.	3.2 LDAP Directory Server	
2.	3.3 WebGate/AccessGate	
2.	3.4 Oracle Adaptive Access Manager	
2.4	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 Configuring Weblogic Console	
	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	
	6.4 Creating OAM 11g Webgate	
2.	6.5 Post OAM Webgate 11g Creation	
2.7		
	7.1 Parameter Maintenance	
	7.2 Maintaining LDAP DN for FLEXCUBE users	
	7.3 Launching FLEXCUBE	
2.	7.4 Signoff in a SSO Situation	



1. Preface

1.1 Introduction

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

1.2 Audience

This manual is intended for the following User/User Roles:

Role	Function
Back office data entry Clerks	Input functions for maintenance related to the interface.
Implementation team	Implementation of Oracle FLEXCUBE Investor Servicing

1.3 <u>Abbreviations</u>

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

1.4 **Documentation Accessibility**

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

1.5 **Organization**

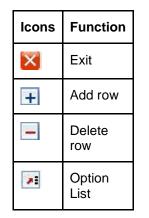
This manual is organized into the following chapters:

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

1.6 **Glossary of Icons**

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





1.6.1 Related Documents

You may refer the following manual for more information

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



2. Enabling Single Sign-on with Oracle Access Manager

2.1 Introduction

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

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

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

2.2 **Background and Prerequisites**

2.2.1 Software Requirements

Oracle Identity and Access Management 11g R2 - 11.1.2.3.0

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

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

Note: Refer Oracle Support Document: **1935703.1**, to have skip the escape sequence \ (slash) infront of, (comma) in Oracle 11gR2 OAM request header values

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									
Change Center	🔒 Home Log Out Preferences 🐼 Record Help									
View changes and restarts	Home >Summary of Servers	Home > Summary of Servers								
Configuration editing is enabled. Future	Summary of Servers	Summary of Servers								
changes will automatically be activated as you modify, add or delete items in this domain.	Configuration Control									
Domain Structure am.donain	A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JMM) and has its own configuration. This page summarizes each server that has been configured in the current WebLogic Server domain.									
-Services	🔲 Name 🐟	Cluster	Machine	State	Health	Listen Port				
How do I	AdminServer(admin)			RUNNING	🖋 ОК	7001				
	oam_server1			RUNNING	🖋 ОК	14100				
Create Managed Servers	oim_server1			RUNNING	🖋 ок	14000				
Clone Servers Delete Managed Servers	soa_server1		LocalMachine	SHUTDOWN		8001				
Delete the Administration Server Start and stop servers	New Clone Delete	New Cone Delete Showing 1 to 4 of 4 Previous Next								
System Status										
Health of Running Servers										
Failed (0)										
Critical (0)										
Overloaded (0)										
Warping (0)	1									

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 Service	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services	
iam_domain D-Environment	Save													
Servers Clusters Virtual Hosts Migratable Targets =	Use this pa View JNDI	-	gure gener	al features o	f this se	erver such as default r	etwork communie	ations.						
Coherence Clusters Machines	Name:	Name: AdminServer						An alphanumeric name for this server instance. More Info						
Work Managers Startup and Shutdown Classes Deployments BI-Services	Machine:					(None)					Logic Server host cor More Info	mputer (machine)	on which this serve	er is meant
How do I	Cluster:	Cluster: (Standalone)									er, or group of WebL More Info	ogic Server insta	nces, to which this	server
Configure default network connections Create and configure machines	👸 Listen	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 I	🖉 Listen Port Enabled					Specifies whether this server can be reached (non-SSL) listen port. More Info					hrough the default	plain-text	
System Status	Listen Por	t				7001					ult TCP port that this connections. More		sten for regular (no	n-SSL)
Health of Running Servers Failed (0)	🗹 SSL Lis	ten Port E	nabled								whether the server ore Info	can be reached t	hrough the default	SSL listen
Critical (0) Overloaded (0)	SSL Listen	Port:				7002					IP port at which this More Info	server listens for	SSL connection	
Warning (0) OK (3)	🗹 🐠 Che	nt Cert Pr	oxy Enab	led							whether the HttpClu eader. More Info		es the client certific	ate in a
	Java Com	piler:				java	•			The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info				that need
	Diagnostic	: Volume:				Low	•			WebLogic does not	the volume of diagno : Server at run time, affect explicitly conf he volume of events	Note that the Wi igured diagnostic	DF diagnostic volum modules. For exam	me setting nple, this
	— 🛡 Advar	nced —												
	Virtual Ma	chine Nan	ie:			iam	domain_Adm	inSe			.S is running on JRVE his server More Inf		e name of the virtu	al machine
	🗹 👍 We	bLogic Plu	g-In Enal	bled						header, v	whether this server which is recommende oxy plug-in. More I	d if the server in		

2.5.2.3 Follow the steps in Keystores Tab as shown below:

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

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

	Administration Con	sole									Õ
Change Center	🟦 Home Log Out Preferences 🔤 Record Help										
Tiew 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 Admin	iServer Protocols Logging Debu	ig Monitoring Con	trol Deployments	Services	Security	Notes				
Domain Structure	General Cluster	Services Keystores	SSL Federation Se	rvices Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services	
iam_domain	you to manage th	the secure storage and mana e security of message transm	issions.	and trusted certificat	te authorities	(CAs). This				-	
Coherence ClustersMachinesWark ManagersStartup and Shutdown ClassesDeployments B-ServicesSer	Keystores: Save Cancel	Demo Identity and Custom Identity an Custom Identity an Custom Identity an Demo Identity and	d Command Line T d Custom Trust d Java Standard Tr					configuration rules sho eystores? More Info.		finding the server's	identity and
How do I											
Configure identity and trust Configure keystores Set up SSL											
System Status											
Health of Running Servers											
Failed (0) Critical (0) Overloaded (0) Warning (0) OK (3)											
WebLogic Server Version: 10.3.5.0 Copyright © 1996,2010, Oracle and/or its affiliates. All r Oracle is a registered trademark of Oracle Corporation		names may be trademarks of t	heir respective owners.								



2.5.2.4 Follow the steps in Keystores Tab as shown below:

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

ORACLE WebLogic Server® A	Administration Console		Q								
Change Center	🔒 Home Log Out Preferences 🖂 Record Help	Q	Welcome, weblogic Connected to: iam_domain								
View changes and restarts	Home > Summary of Servers > AdminServer										
Configuration editing is enabled. Future changes will automatically be activated as you	Settings for AdminServer										
modify, add or delete items in this domain.	Configuration Protocols Logging Debug Monitori	ing Control Deployments Services Security	Notes								
Domain Structure	General Cluster Services Keystores SSL Fede	eration Services Deployment Migration Tuning	Overload Health Monitoring Server Start Web Services								
ian_donain ← Genvironment ← Genvironment ← Genvironment ← Genviron ← Wrubul floots ← Wrubul floots ← Gragetase ← Goherence Gusters ← → Work Managers ← → Gratup and Shutdoon Classes ← ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	Save Keystores ensure the secure storage and management of pr you to manage the security of message transmissions. Keystores: - Identity	page lets you view and define various keystore configurations. These settings help Which configuration rules should be used for finding the server's identity and trust keystores? More Info o/fmw115/oam1115/BaseKeyStore/AdminFlexcubeKeyStore.iks									
DeploymentsServicesServicesServicesServicesServicesServicesServicesServicesServicesServicesServicesServicesServicesServicesServicesServices	Custom Identity Keystore:	nFlexcubeKeyStore.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	Custom Identity Keystore Passphrase:	•••••	The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info								
Set up SSL System Status	Confirm Custom Identity Keystore Passphrase:	•••••									
Health of Running Servers Failed (0)	- Trust Custom Trust Keystore:	nFlexcubeKeyStore.jks	p/fmw115/oam1115/BaseKeyStore/AdminFlexcubeKeyStore.jks The path and the name of the custom attack Reystore. Hone and								
Critical (0) Overloaded (0)	Custom Trust Keystore Type:	jks	The type of the keystore. Generally, this is JKS. More Info								
Warning (0) OK (3)	Custom Trust Keystore Passphrase:	•••••	The custom trust keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. More Info								
	Confirm Custom Trust Keystore Passphrase:	•••••									
	Save										

2.5.2.5 Follow the steps in SSL Tab as shown below:

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

Note: For Weblogic 12c Server <DOMAIN_HOME>/bin setDomainEnv.cmd or setDomainEnv.sh update the JAVA_PROPERTIES from

JAVA_PROPERTIES=-Dwls.home=%WLS_HOME% -Dweblogic.home=%WLS_HOME%

To JAVA_PROPERTIES=-Dwls.home=%WLS_HOME% -Dweblogic.home=%WLS_HOME% -Dweblogic.security.SSL.minimumProtocolVersion=TLSv1



Change Center	🏠 Home Log Out Preferences 🖂 Recor	d Help	Welcome, weblogic Connected to: iam_domain
View changes and restarts	Home >Summary of Servers >AdminServer		
Configuration editing is enabled. Future	Settings for AdminServer		
changes will automatically be activated as you modify, add or delete items in this domain.	Configuration Protocols Logging	Debug Monitoring Control Deployments Services Securit	y Notes
Domain Structure	General Cluster Services Keystore	SSL Federation Services Deployment Migration Tuning	Overload Health Monitoring Server Start Web Services
iam_domain ▲	Save		
Servers			
Clusters Virtual Hosts Migratable Targets	This page lets you view and define various	Secure Sockets Layer (SSL) settings for this server instance. These se	ttings help you to manage the security of message transmissions.
Coherence ServersCoherence ClustersMachinesMachines	Identity and Trust Locations:	Keystores Change	Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CAs). More Info
Work Managers	- Identity		
LStartup and Shutdown Classes	Private Key Location:	from Custom Identity Keystore	The keystore attribute that defines the location of the private key file. More Info
How do I	Private Key Alias:	FlexcubeCert	The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info
Configure identity and trust	🚝 Private Key Passphrase:	•••••	The keystore attribute that defines the passphrase used to retrieve the server's private key. More Info
Set up SSL Verify host name verification is enabled	👸 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
	- Trust		
System Status 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)	— 🗢 Advanced —		
Critical (0) Overloaded (0) Warning (0) OK (2)	Hostname Verification:	None ▼ Custom Hostname Verifier BEA Hostname Verifier	Specifies whether to ignore the installed implementation of the weblogic.security.SSLHostnameVerifier interface (when this server is acting as a client to another application server). More Info
UN(L)	문 Custom Hostname Verifier:	None	The name of the class that implements the weblogic.security.SSLHostnameVerifier interface. More Info
	Export Key Lifespan:	500	Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. More Info
	Use Server Certs		Sets whether the client should use the server certificates/key as the client
Warning (0)			client to another application server). More Info
OK (2)	🎉 Custom Hostname Verifier:		The name of the class that implements the weblogic.security.SSL.HostnameVerifier interface. More Info
	Export Key Lifespan:	500	Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. More Info
	Use Server Certs		Sets whether the client should use the server certificates/key as the client identity when initiating an outbound connection over https. More Info
	Two Way Client Cert Behavior:	Client Certs Not Requested	The form of SSL that should be used. More Info
	街 Cert Authenticator:		The name of the Java class that implements the weblogic.escurity.aci.CertAuthenticator class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. More Info
	✓ SSLRejection Logging Enabled		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info
	🗌 👸 Allow Unencrypted Null Cipher		Test if the AllowUnEncryptedNullCipher is enabled More Info
	Inbound Certificate Validation:	Builtin SSL Validation Only	Indicates the client certificate validation rules for inbound SSL. More Info
	Outbound Certificate Validation:	Builtin SSL Validation Only	Indicates the server certificate validation rules for outbound SSL. More Info
	🗹 🎳 Use JSSE SSL		Select the JSSE SSL implementation to be used in Weblogic. More Info
	Save		

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



ORACLE WebLogic Server	Administration Console				Q						
Change Center	🔒 Home Log Out Preferences 🔤 Record	a Home Log Out Preferences 🐼 Record Help 🔍 🔍 Welcome, weblogic Connected to: iam_domain									
View changes and restarts	Home >Summary of Servers >AdminServer >Su	Home >Summary of Servers >AdminServer >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	Configuration Control									
Domain Structure	A server is an instance of Webl onis Converti	ank sums in its sum Taxa Vick of Marshine (1984) and have	ite euro configuration								
iam_domain		A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.									
E-Environment	This page summarizes each server that has b	een configured in the current WebLogic Server domain	n.								
Clusters	Q										
Virtual Hosts	C2										
Gigratable Targets Coherence Servers	Customize this table										
Coherence Clusters											
Machines	Servers (Filtered - More Columns Exist	.)									
Work Managers 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						
How do I			RUNNING	<pre>✓ OK</pre>	14100						
Create Managed Servers	oim server1		RUNNING	<pre>✓ OK</pre>	14000						
Clone Servers		LocalMachine	SHUTDOWN		8001						
Delete Managed Servers	soa_server1	Locaimachine	SHUIDOWN		8001						
Delete the Administration Server	New Clone Delete				Showing 1 to 4 of 4 Previous Next						
 Start and stop servers 											
System Status 🛛	3										
Health of Running Servers											
Failed (0)											
Critical (0)											
Overloaded (0)											
Warning (0)											
OK (3)											

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

2.5.3 Configuring SSL Mode in Oracle Internet Directory

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

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



	anager 11g Fusion Middleware Cont	rol						Setup 🗸 H	elp ✔ Log Out
🕂 Farm 👻 🔒 Topology									
	<pre> oid1 i </pre>							Logged in as weblogic	Host padsrini-pc
🛙 📲 Farm_base_domain	📧 Oracle Internet Directory 🛩							Page Refreshed Feb 15, 2013 4:	35:59 PM IST 🗘
Application Deployments	Home								
🗉 🚞 WebLogic Domain									
Identity and Access	Monitoring >		1	Load			Security		
OAM	Control >	. 1	121	Total LDAP Connections		0	Failed Bind Operation	ons	0
I OIM	Logs >								
ovd1		2	220	Operations Completed		2	Failed Super User Li	ogins	0
Metadata Repositories	Port Usage		65	Operations in progress		0	Sucessful Super Use	r Logins	0
Web Tier	Administration >								
	Security >	Audit Policy							
	Directory Services Manager >	Wallets							
	General Information							Server Response (ms)	
	40								
	20								
	8								
	6						•		
	4								
								Total Operations	
	2								
	0								
	20								
	15							CPU Utilization (%)	
	10							/Farm_base_domain/asinst_1/c padsrini-pc	id1
	5								
	100								
	80								
	60							Memory Utilization (%) /Farm_base_domain/asinst_1/c	id1
	40 20							padsrini-pc	
	0	6:24 16:25 16:26	16:27	16:28 16:29 16:30	16:31 16:32 16	5:33 16:	34 16:35 16:36		
	16:22 16:23 10 February 15 2013	0.24 10.25 10.20	10.27	10.20 10.25 10.30	10.51 10.52 10	5.55 10.	34 10.33 10.36		
									Table View

2. Click 'Create Self-Signed Wallet'.

	nager 11g Fusion Middleware Control	Setup → Help → Log Out
👫 Farm 👻 🔒 Topology		
Image: Second Secon	<pre> oid1 ₀ IOrade Internet Directory </pre>	لدوgged in as weblogic (Host padarini-pc Page Refreshed Feb 15, 2013 4(39):54 PM 157 الألية
WebLogic Domain Gottomain Constraints Gottomain Constraints Cons	Wallets A Wallet is a Keystore that stores X.509 certificates and private keys in industry-standard, PKCS #12 Wallet. To manage the contents of a wallet, select a wallet and click Manage.	format. To create a wallet, click Create. To create a wallet with a self-signed certificate, click Create Self-Signed
OIM	😭 Create 🛛 💥 Delete 🛛 🍞 Create Self-Signed Wallet 🔹 🎍 Import 😭	Export 6d Manage
ovd1	Name	Auto-login
H and the end of t		etdring Data
	<u>r</u>	

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



	anager 11g Fusion M	liddleware Control	Setup → Help → Log Out
Farm - A Topology			
□ •	🔂 oid1 🗿		Logged in as weblogic Host padsrini-pc
Farm_base_domain Application Deployments	Oracle Internet Di	irectory 🕶	Page Refreshed Feb 15, 2013 4:40:45 PM IST €2
WebLogic Domain	Wallets > Create Se		
Identity and Access	Create Self-Sig		OK Cancel
⊙ OAM 토 oid1 ⊙ OIM ⊙ ovd1	or password-protecte PKCS#12 wallet that	ed. Passwords, if specified, have a mi	If signed wallet is not recommended in a production environment. The wallet name should be unique for a given component. The wallet pipe can be auto-login timum length of eight characters, and contain alphabetic characters combined with numeir or special divarcters. Auto-login wallet is an obfiscated from of es and applications without requiring a password at runtime. Auto-login wallet don't need a password to modify, or delete the wallet. File system permissions
🗄 🚞 Metadata Repositories	Self-Signed Wallet	Details	
🗉 🚞 Web Tier			
	* Wallet Name	-	
	Wallet Password	V Auto-login	
	Confirm Password		
	Add Self-Signed Ce	ertificate	
	Add a self-signed cer	tificate that becomes part of the wall	let.
	* Common Name	hostname.in.orade.com	
	Organizational Unit	OFSS	
	 Organization 	Orade	
	City	Chennai	
	State	TN	
	Country	India 💌	
	Key Size	2048 💌	

4. Click 6d Manage...

ORACLE Enterprise Ma	nager 11g Fusion Middleware Control	Setup → Help → Log Out
🛱 Farm 👻 🔒 Topology		
Farm_base_domain Image: The second secon		Logged in as weblogic (Host padsrini-pc Page Refreshed Feb 15, 2013 4144127 PM IST 🖏
WebLogic Domain Gentity and Access OAM Gout	Wallets A Wallet is a Keystore that stores X.509 certificates and private keys in industry-standard, PKCS #12 format. To Wallet. To manage the contents of a wallet, select a wallet and dick Manage.	create a wallet, click Create. To create a wallet with a self-signed certificate, click Create Self-Signed
OIM Ovd1	Create 🗙 Delete 😭 Create Self-Signed Wallet 💁 Import 🏠 Export	6d Manage
	Name ioidselfsigned	Auto-login
	modular of plants	

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

Farm 👻 💑 Topology						
•	<pre>介 oid1 ₀</pre>				Logged in as we	blogic Host padsrir
Farm_base_domain	2 Orade Internet Directory -				Page Refreshed Feb 15	, 2013 4:45:58 PM IST
Application Deployments	,					
WebLogic Domain	Wallets > Manage Certificates					
Identity and Access	Manage Certificates: oidselfsigned					
OAM	To generate a certificate signing request (CSR), click "Add Certificate Request". After you create a CSR, send it to yo	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 the	the CSR was generated.				
101 OIN						
ovd1	🛉 🖶 Add Certificate Request 🔄 Import 😭 Export 💥 Delete					
💿 ovd1 🛅 Metadata Repositories	Add Certificate Request M Import Export Delete	Certificate Type	Status	Key Size	Start Date	Expiration Date
Contract of the second s		Certificate Type Certificate Request		Key Size 2048	Start Date	Expiration Date
Metadata Repositories	Subject Name				Start Date February 15, 2013	
Metadata Repositories	Subject Name CN=paderini-pc,OU=OFSS,O=Orade,L=Chernal,ST=TN,C=IN	Certificate Request		2048		
Metadata Repositories	Subject Name CN-padsrin-pc,OU=OFSS,O=Orade,L=Chernal,ST=TN,C=IN ON=padsrin-pc, OU=OFSS, O=Orade, L=Chernal, ST=TN, C=IN	Certificate Request Certificate	Valid	2048 2048	February 15, 2013	February 14, 20 August 2, 2028
Metadata Repositories	Subject Name CN=paddrnip-r_QOU=OPSS_0=Orade_L=Chernal_ST=TN,C=N CN=paddrnip-r_QOU=OPSS_0=Orade_L=Chernal_ST=TN,C=N CU=OPSS_0=OPAC_L=Chernal_ST=TN,C=N CU=class 3 Public Primary Certification Authority, 0="VeriSing, Inc.", C=US CU=CUS	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
Metadata Repositories	Subject Name ON=padsrini-pc, OU=OFSS, O=Orade, L=Chemal,ST=TN,C=N ON=padsrini-pc, OU=OFSS, O=Orade, L=Chemal,ST=TN,C=N OU=obass Public Primary Certification Autority, o=Versign, hc,**, 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.



	anager 11g Fusion Middleware Control			Setu	ip ∓ Help ∓ Log Out
Farm Topology Farm_base_domain Farm_base_domain Comparison C	<pre> oid1 @ E Oracle Internet Directory Wallets > Manage Certificates </pre>				blogic Host padsrini-pc , 2013 4:45:58 PM IST (것
Farm Farm Topology Form_base_domain Application Deployments WebLogic Domain Identity and Access OM	Manage Certificates: oidselfsign To generate a certificate signing request (certificate or trusted cert, cick Import. Yo 4 Add Certificate Request	certificate. To import the CA signed			
	Subject Name CNI=padirnin-pc,OU=OFSS, O=Ora CNI=padirnin-pc, OU=OFSS, O=Or OU=Class 3-Public Primary Certific CMI=DECyberTrust Global Rost, I CNI=padirnin-pc, OU=OFSS, O=O OU=Class 3-Public Primary Certific OU=Class 3-Public Primary Certific	<pre>wants to tust your certificate decdty.</pre>		Start Date February 15, 2013 January 29, 1996 August 13, 1998 February 15, 2013 January 29, 1996 January 29, 1996	Expiration Date February 14, 2018 August 2, 2028 August 14, 2018 February 14, 2018 August 2, 2028 January 8, 2020
	8	Export Trusted Certificate	Close]	

7. Click 'Server Properties'.

🙀 Farm 👻 🔒 Topology									
-	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 WebLogic Domain	Home								
Identity and Access OAM OIM	Monitoring Control Logs	'est	signed st (CSR), dx' Mdd 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.						the CA signed
ovd1	Port Usage	Þ	Import 🛉 😭 Export	🗙 Delete					
Metadata Repositories	Administration	>	Server Properties		Certificate Type	Status	Key Size	Start Date	Expiration Date
🗉 🚞 Web Tier	Security	>	Shared Properties		Certificate Request		2048		
	Directory Services Manager		Sildred Properdes		Certificate	Valid	2048	February 15, 2013	
	Directory del vices manager	1		. , C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
			Replication Management	Inc.", O=GTE Corporation, C=US	Trusted Certificate	Valid	1024	August 13, 1998	August 14, 2018
	General Information		Tuning and Sizing		Trusted Certificate	Valid	2048	February 15, 2013	
			cation Authority, O="VeriSign,		Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
	OU=Class 1 Public Primary 0	ertifi	cation Authority, O="VeriSign,	Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	January 8, 2020

8. Click 'Change SSL Settings'.

	anager 11g Fusion Middleware Control	Setup Help Log Out
📑 Farm 👻 🔒 Topology		
□ •	☆ oid1 0	Logged in as weblogic Host padsrini-pc
E 🛱 Farm_base_domain	E Orade Internet Directory -	Page Refreshed Feb 15, 2013 4:54:17 PM IST 🗘
Application Deployments		
🗉 🚞 WebLogic Domain	Server Properties	Apply Revert
Identity and Access	General Performance SASL Statistics Logging	index in the second sec
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	
III 📄 Web Tier	Preserve Case of Required Attribute Name specified in Search Request	
_	Anonymous Bind Disallow except for Read Access on the root DSE 💌	
	* Maximum time allowed in a Transaction (sec) 0	
	* Maximum Number of Operations allowed in a Transaction 0	
	Port Numbers	
	Non-SSL Port 3060	
	SSL Port 3131	
	3131 ULTRICE SLL Settings	

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



0			
	anager 11g Fusion Middleware Cont	lo	Setup
🕂 Farm 👻 🔒 Topology			
I •	<pre>分 oid1 ₀</pre>		Logged in as weblogic Host padsrini-pc
🗄 📲 Farm_base_domain	Crade Internet Directory -		Page Refreshed Feb 15, 2013 4:55:50 PM IST 🗘
🗉 🛅 Application Deployments			
🗄 🛅 WebLogic Domain	(i) Information		
Identity and Access	All changes made in this page req	uire a server restart to take effect.	
OAM	SSL Configuration (?)		OK Cancel
OIM	Enable SSL		
🐼 ovd1	Server Wallet Name	igned 🗸	
🗄 🛅 Metadata Repositories	oidself		
🗄 🛅 Web Tier	Advanced SSL Section	js	
	Server SSL properties		
	SSL Authentication	Server Authentication	
		A	
		SSL_RSA_WITH_RC4_128_MD5	
	Cipher Suite	SSL_RSA_WITH_RC4_128_SHA	
	Cipriei Suite	SSL_RSA_WITH_3DES_EDE_CBC_SHA	
		SSL_RSA_WITH_DES_CBC_SHA	
		TLS_RSA_WITH_AES_128_CBC_SHA +	
1	* SSL Protocol Version	All	
	1		

10. Click 'Apply'.

ORACLE Enterprise Ma	anager 11g Fusion Middleware Control	Setup ▾ Help ▾ Log Out
📑 Farm 👻 🔒 Topology		
□ •	☆ oid1 ₀	Logged in as weblogic Host padsrini-pc
1 📑 Farm_base_domain	E Orade Internet Directory -	Page Refreshed Feb 15, 2013 4:56:40 PM IST 🗘
Application Deployments		
🗄 🚞 WebLogic Domain	1 Information	×
Identity and Access OAM	SSL configuration updated for /Farm_base_domain/asinst_1/oid1. Restart component for this change to be effective.	
DI OAM		
	> oid1 ☐ Crade Internet Directory → Information Information Logged in as weblogic Host padorni-pc Page Refreshed Feb 15, 2013 4:56×00 PM IST (2) Information K	
Ø 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	

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)



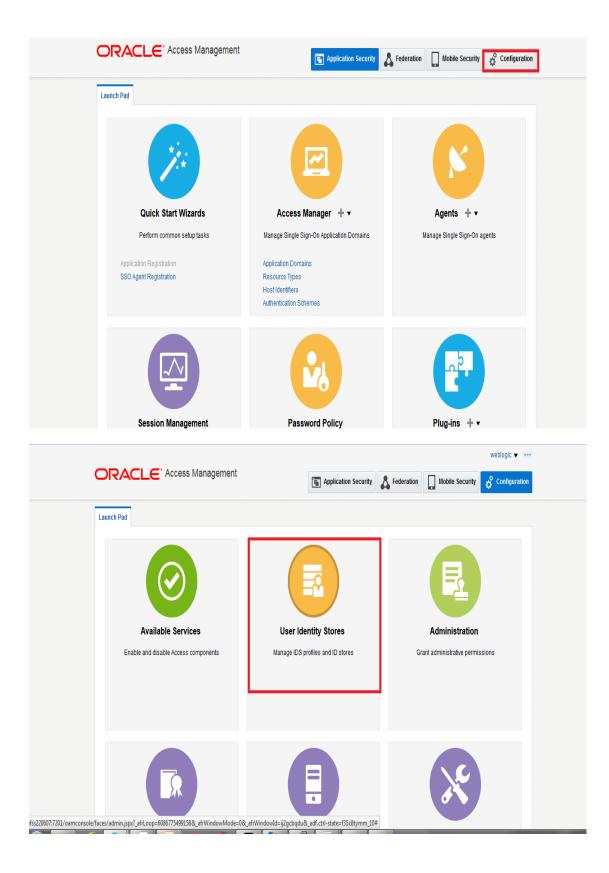
Note: Refer Oracle Support Document: **1935703.1**, to have skip the escape sequence \ (slash) infront of , (comma) in Oracle 11gR2 OAM request header values

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		About Orade ***
Sign In	Sign in to administer Oracle Access Management Username I Password Sign In	
Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.		





2. Click 'Create' under OAM ID Stores.



Configuration >				
User Identity Sto	pres			
Default and System	Store			Арр
* De	efault Store UserIdentityStore1	•		
* Sv	stem Store UserIdentityStore1	•		
5				
	,			
				Sync IDS Profile
▲ OAM ID Stores		is that are synchronized by using Sync ID:	S Profiles button.	Sync IDS Profile
▲ OAM ID Stores Manage local User Identit	ty Stores. This includes IDS Profile:		S Profiles button.	Sync IDS Profile
✓ OAM ID Stores Manage local User Identif View ▼ + Create	ty Stores. This includes IDS Profile: ○ Duplicate ✓ Edit 💥	Delete		
▲ OAM ID Stores Manage local User Identit	ty Stores. This includes IDS Profile:		S Profiles button.	Sync IDS Profile Synched IDS Profiles
✓ OAM ID Stores Manage local User Identif View ▼ + Create	ty Stores. This includes IDS Profile: ○ Duplicate ✓ Edit 💥	Delete		Synched IDS

- 3. Enter the below details in the Create User Identity Store Form
 - Store Name : FLEXCUBEStore
 - Choose Store Type as OID: Oracle Internet Directory.
 - Location: LDAP server Host name and Port Number in <HOSTNAME>:SSL PORT format
 - Select Enable SSL check box
 - Bind DN: Admin User name to connect the LDAP Server
 - Password: Admin Password to connect the LDAP Server
 - Login ID Attribute: Specify the LDAP attribute from which the login ID specifying the User will be extracted (cn).
 - User Search Base: Full DN for the node at which enterprise users are stored in the directory; for example, cn=Users,realm_DN.
 - Group Search Base: Currently only static groups are supported, with the uniquemember attribute. The node in the directory information tree (DIT) under which group data is stored, and the highest possible base for all group data searches.



Configuration >							
reate: User Ident	ity Store User Identity	Store Service				Test Connection	Apply
* Store Name	FLEXCUBEStore				Enable SSL		
* Store Type	OID: Oracle Internet Direct	ory	•		Use Native ID Store Sett	ings	
Description				Prefetched Attributes			
Location and Cred	entials						
* Location	ofss220607.in.oracle.com	:3131 .4		* Password	•••••		
* Bind DN	cn=orcladmin						
Users and Groups							
	* Login ID Attribute	cn					
	User Password Attribute	userPassword					
	* User Search Base	cn=Users,dc=ofss,dc=	in,dc=oracle,dc=c=				
	User Filter Object Classes						
	Group Name Attribute						
	* Group Search Base	on-Croups de-ofee de	-in do-oroolo do-				

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

Launch Pad User Identity S	Stores × Create: User Id	entity Sto ×					
Configuration >							
Create: User Ident	ty Store User Identity	Store Service				Test Connection	Apply
* Store Name	FLEXCUBEStore				Connection Status	×	
* Store Type	OID: Oracle Internet Direct	ory	•		Connection to the User Ide	ntity Store successful!	
Description				Prefetched Attribute	es		
▲ Location and Crede	entials						
* Location	ofss220607.in.oracle.com	:3131		* Passwo	rd ••••••		
* Bind DN	cn=orcladmin						
Users and Groups							
	* Login ID Attribute	cn					
	User Password Attribute	userPassword					
	* User Search Base	cn=Users,dc=ofss,dc=ir	n,dc=oracle,dc=c				
l	lser Filter Object Classes						
	Group Name Attribute						
	* Group Search Base	cn=Groups,dc=ofss,dc=	in,dc=oracle,dc=				

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



	User Identity Store Service				Dupl	icate Test Connectio	on App
Confirmation	CUBEStore created success	sfully.					×
Store Name	FLEXCUBEStore				Enable SSL		
* Store Type	OID: Oracle Internet Direct	ory	•		Use Native ID Stor	e Settings	
Description				Prefetched Attributes			
Location and Cred	entials						
* Location	ofss220607.in.oracle.com	:3131 .d		* Password	•••••		
* Bind DN	cn=orcladmin						
Users and Groups							
	* Login ID Attribute	cn					
	Login ID Attribute	on					

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

2.6.2 Creating Authentication Module

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



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

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

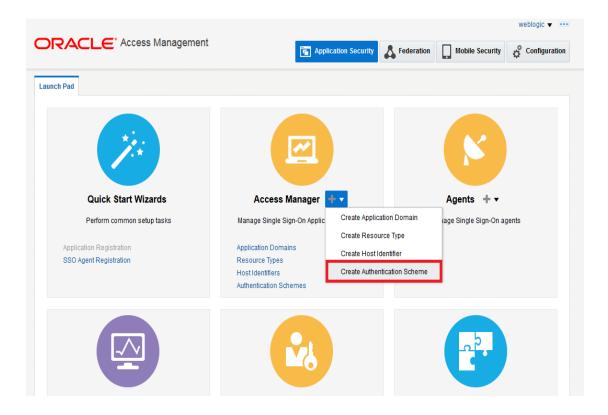
aunch Pad FlexcubeAuthModule	ĸ			
Access Manager >				
lexcubeAuthModule LD	AP Authentication Module			Duplicate Apply
se the LDAP Authentication module f efinition stored in an LDAP directory s		It matches the credentials (username and passw	ord) of the user who requests a res	source to a user
Confirmation				×
LDAP Authentication Module Flexor	ibeAuthModule created successfully.			
* Name	FlexcubeAuthModule			
* User Identity Store	FLEXCUBEStore -			

Module.

2.6.3 Creating Authentication Scheme

1. Click on **H** in Access Manager under Application Security to 'Create Authentication Scheme'.





Select any of the challenge method for creating an authentication Scheme as explained below and refer to OAM documentation for more details on the same.

2.6.3.1.1 https://docs.oracle.com/cd/E52734_01/oam/AIAAG/shared.htm#AIAAG488



Basic Style Authentication Scheme

Enter the below details and click 'Apply':

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

Launch Pad FlexcubeBa	asicOAMScheme x	
Access Manager >		
	Set As Defa	
An Authentication Scheme	defines the challenge mechanism required to authenticate a user. Each Authentication Scheme must also include a defined Auth	entication Module.
Confirmation		×
Authentication Scheme,	e, FlexcubeBasicOAMScheme, created successfully	
* Name	FlexcubeBasicOAMScheme	
Description	Basic login screen	
* Authentication Level	1 🔨 🖍	
Default		
* Challenge Method	BASIC -	
Challenge Redirect URL	/oam/server	
* Authentication Module	FlexcubeAuthModule	
Challenge Parameters	secCoolig=Secure conted/lipe=default conted/uliv=/oan challeng=_ut=?credCollectServlet/BASIC	

We need to add the 'enforce-valid-basic-auth-credentials' tag to the config.xml file ,located under <weblogic deployment path>/user_projects/domains/<MyDomain>/config/.

The tag must be inserted within the <security-configuration> tag as follows: [Just above </security-configuration> tag]

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



2.6.3.2 Form Style Authentication Scheme

Enter the below details and click 'Apply':

Name	: Name of the Authentication Scheme
Authentication Level	: 2
Challenge Method	: FORM
Challenge Redirect URL	: /oam/server
Authentication Module	: Authentication Module
Refer the section 'Creating Aut	hentication Module 2.6.2' of this document.
Challenge URL	: /pages/login.jsp
Context Type	: default
Context Value	: /oam
Challenge Parameters	: ssoCookie=Secure

Launch Pad F	lexcubeFor	mOAMScheme ×							
Access Mar	nager >								
Create Aut	thentica	tion Scheme	Authentication Scheme				Set As Default	Duplicate	Apply
An Authentication	n Scheme o	defines the challenge	e mechanism required to aut	henticate a use	er. Each Authentio	cation Scheme must also inc	lude a defined Authentic	ation Module.	
									×
Confirm	nation								~
Authenticatio	on Scheme,	FlexcubeFormOAMS	Scheme, created successfull	/					
	*	FlexcubeFormOAM							
	* Name	FlexcubeFormOAM	Scheme						
De	escription	Form based login p	age						
* Authentica	tion Level	2 ^	~						
	Default								
* Challeng	ge Method	FORM							
Challenge Red	direct URL	/oam/server							
* Authenticatio	on Module	FlexcubeAuthModul	e 💌						
* Chall	lenge URL	/pages/login.jsp							
* Cor	ntext Type	default 👻							
* Cont	text Value	/oam							
		ssoCookie=Secure							
Challenge Pa	arameters								



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

Enter the Below Details and clic	ck 'Apply':
Name	: Name of the Authentication Scheme
Authentication Level	:2
Challenge Method	: FORM
Challenge Redirect URL	: /oam/server
Authentication Module	: Authentication Module
Refer the section 'Creating Aut	nentication Module 2.6.2' of this document.
Challenge URL	: /pages/oaam/login.jsp
Context Type	: default
Context Value	:/oam
Challenge Parameters	: ssoCookie=Secure
	oaamPostAuth=true
	oaamPreAuth=true

reate Authentica	tion Scheme Authentication Scheme		Set As Default	Duplicate	App
Authentication Scheme	defines the challenge mechanism required to authenticate a u	ser. Each Authentication Scheme must also include a	defined Authentic	ation Module.	
Confirmation					×
Authentication Scheme,	FlexcubeKBAOAAMScheme, created successfully				
* Name	FlexcubeKBAOAAMScheme				
Description	KBA Based login page				
* Authentication Level	2 🔨 🗸				
Default					
* Challenge Method	FORM				
Challenge Redirect URL	/oam/server				
Authentication Module	FlexcubeAuthModule				
* Challenge URL	/pages/oaam/login.jsp				
* Context Type	default 💌				
* Context Value	/oam				
Challenge Parameters	ssoCookie=Secure oaamPosMuth=true oaamPreAuth=true				

2.6.4 Creating OAM 11g Webgate

Follow the below steps to create a Webgate:

1. Click on 'Server Instances' under Configuration.



		weblogic 👻 🚥
ORACLE [®] Access Management	The Application Security	Federation Mobile Security
Launch Pad		
		R
Available Services	User Identity Stores	Administration
Enable and disable Access components	Manage IDS profiles and ID stores	Grant administrative permissions
TR		×
Certificate Validation	Server Instances	Settings
Validate trust certificates	Manage and monitor OAM server instances	Manage configuration of Access components
		View 🕶



2. Click on 'Search'.

	* Access Manage	lient	The Applic	ation Security	A Federation	Mobile Se	ecurity 🥳 Configurati
aunch Pad Server Ins	stances ×						C
Configuration >							
Search OAM Ser	rvers						+ Create OAM Server
Search							
Name							
Name							Search Reset
Name Search Results							Search Reset
	+ Create 🔿 Duplic	ate 🧪 Edit 💥 Deleti	a Monitor	Detach			Search Reset
Search Results	+ Create 🔿 Duplic	ate 🖌 Edit 🗶 Delet	9 💽 Monitor	Detach			Search Reset
Search Results	- ∔- Create (?# Duplic	ate 🧪 Edit 💥 Delet	9 💽 Monitor	الله Detach			Search Reset
Search Results Actions ▼ View ▼ Row Name	- }- Create (?⊭ Duplic	ate 🥒 Edit 💥 Delet	9 Monitor	Detach			Search Reset

3. Edit oam_server1.

	weblogic 🔻 🚥
	The Application Security A Federation
Launch Pad Server Instances x	
Configuration > Search OAM Servers	Create OAM Server
⊿ Search	
Name Search Results	Search Reset
Actions ▼ View ▼ + Create	🖬 Monitor 🛛 🔐 Detach
Row Name 1 cam_server1	
Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.	

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

	weblogic 🔻
	🝙 Application Security 👗 Federation 🔲 Mobile Security 🥳 Configura
aunch Pad Server Instances x oam_server1 x	
Configuration >	
Dam_server1 OAM Server Instance	Duplicate Appl
* Server Name oam_server1	* Host ofss220607.in.oracle.
* Port 14101 ^ ~	
A OAM Proxy	
* Proxy Server Id AccessServerConfigP	
* Port 5575 🔨 🗸	
* Mode Simple 👻	
Coherence Coner	
* Log Level 3 ^ V	
* Local Port 9095 A V	



					weblog	ic 🔻
ORACLE [®] Access Management		Application Security	Sederation	Mobile Security	o ^o Conf	iguration
Launch Pad Server Instances x oam_server1 x						
Configuration >						
oam_server1 OAM Server Instance					Duplicate	Apply
* Server Name oam_server1		* Host	ofss220607.in.orac	le.		
* Port 14101 ^ ~	Confirm Edit	×				
A OAM Proxy	OAM Server instance oam Are you sure you want to e					
* Proxy Server Id AccessServerConfigP	Are you sure you want to e	Yes No				
* Port 5575 🔨 🗸		103 110				
* Mode Simple 💌						
Coherence Configuration						
* Log Level 3 🔨 🗸						
* Local Port 9095 🔨 🗸						
* Log Limit 4096 🔨 🗸						

Configuration >			
am_server1 OAM Server Instance		Duplicate	Apply
Onfirmation			×
OAM Server instance oam_server1 modified successfully.			
* Server Name oam_server1	* Host ofss220607.in.oracle.		
* Port 14101 ^ ~			
OAM Proxy			
Proxy Server Id essServerConfigProxy			
* Port 5575 ^ v			
* Mode Simple 💌			
Coherence Configuration			
Log Level 3 A V			
Local Port 9095 🔨 🗸			



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

	nt la		reblogic 🔻 🚥
	Application Security	Federation Mobile Security	Configuration
nch Pad			
1.			
Quick Start Wizards	Access Manager 🕂 🔻	Agents 🕂 🗸	
Perform common setup tasks	Manage Single Sign-On Application Domains	Manage Single S Create W	ebgate
r enorm common setup tasks	manage Single Sign-On Application Domains	manage onligie o	- SSO Agent
Application Registration	Application Domains	Create O	penSSO Agent
SSO Agent Registration	Resource Types Host Identifiers		
	Authentication Schemes		

6. Enter the below and Click 'Apply':

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



aunch Pad Create Webga	ite x				
Access Manager >					
Create Webgate					Ap
-	gister an OAM Agent. Before yo	ou register, ensure that at least one OAN	I Server is running in the same	mode as the Agent to	
			* Constitution of		
* Versio	n 11g 🔻		* Security 💮 Open i Simple	_	
* Name	e FlexcubeWebgate		Cert	-	
Description	Flexcube 11g Webgate	Enter the Base URLs for Agent	Virtual host		
	https://ofss220607.in.oracle.	Au	to Create Policies 📝		
Base URI			IP Validation		
Access Client Password					
Host Identifie	r FlexcubeWebgate				
	filterOAMAuthnCookie=false				
User Defined Parameters	à				
esource Lists					
Protected Resou	Irce List	Add Delete Public	Resource List	Add	Delete
Relative URI		Relativ	ve URI		
/FCJNeoWeb					
<u> </u>					
lexcubeWebgate we	bgate			Apply Download	
Confirmation				×	
OAM Webgate FlexcubeWeb	gate created successfully.				
Version	11g	Logout Targ	get URL		
Name	FlexcubeWebgate	Deny On Not Pr	otected 🔽		
Description	Flexcube 11g Webgate		proxySSLHeaderVar=IS		
Access Client Password		User Defined Para	URLINUTF8Format=true		
* Security	0000	over beineu Fala	client_request_retry_atte mpts=1	*	
) Simple		inactiveReconfigPeriod		
	Cert	* Sleep for (Se	econds) 60 ^ ¥		
	Enable	Cache Pragma	Header no-cache		
	Disable	Cache Control	Header no-cache		
* Max Cache Elements	100000				
	100000 ^ ~		Debug 🥅		
* Cache Timeout (Seconds)	1800 ^ *	10.14	Debug		

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



			weblogic 👻 🚥
ORACLE [®] Acc	ess Management	Application Security	urity
Launch Pad SSO Agents 🗙	FlexcubeWebgate ×		
Access Manager >			
FlexcubeWebgate we	bgate		Apply Download
Version	11g	Logout Target URL	
Name	FlexcubeWebgate	Deny On Not Protected	
Description	Flexcube 11g Webgate	prox/SSLHeader/Var=	
Access Client Password		User Defined Parameters ue	
* Security	Open	client_request_retry_ 👻 attempts=1	
	 Simple Cert 	* Sleep for (Seconds) 60 🔨 🗸	
* State	Enable	Cache Pragma Header no-cache	
	Disable	Cache Control Header no-cache	

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

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

		weblogic 👻 🚥
	The Application Security Application Security Application Security	ecurity 🗳 Configuration
unch Pad Server Instances x oam_server1 x		
Configuration >		
am_server1 OAM Server Instance		Duplicate Apply
 Confirmation OAM Server instance cam_server1 modified successfully. 		×
* Server Name oam_server1	* Host ofss220607.in.oracle.con	
* Port 14101 🔨 🗸		
A OAM Proxy		
Proxy Server Id AccessServerConfigProxy		
* Port 5575 ^ V		
* Mode Open		
Log Level 3 A ¥		
Local Port 9095 ^ v		
* Log Limit 4096 🔨 🗸		

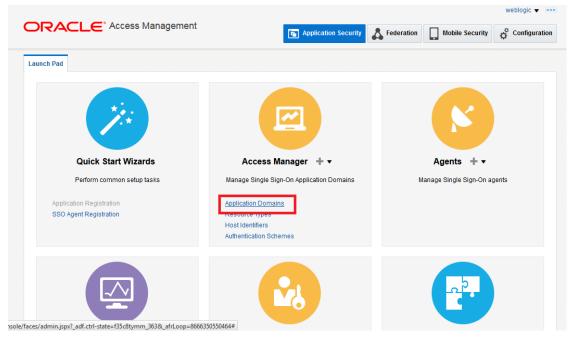


2.6.5 Post OAM Webgate 11g Creation

Follow the below steps to configure the webgate created .

2.6.5.1 Application Domains Changes

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



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

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

Access Manager > Create Application Domain Create Application Domain Create Application Domain Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one. Create Application Domain Search Name Create			* Access Management		Application Security	Sederation	Mobile Security	Configuration
Search Application Domains Cearch Application Domain or click the Create Application Domain button to create a new one. Cearch Name Cearch Results Cearch Result Cearch R	aunch Pad	Applicatio	on Domain 🗙					
se the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one. A Search Name Reset Actions v View + Create / Edit 2 Delete Row Name Description	Access	Manager >						
Actions view Actions Actions View Actions Actions Actions View Actions	earch /	Applicat	ion Domains				- Create Ap	plication Domain
Name Image: Control of the state Search Reset earch Results Image: Control of the state Image: Control of the state Reset Actions View V Image: Control of the state Image: Control of the state Image: Control of the state Reset Row Name Description Image: Control of the state Image:	se the sea	arch tool to fin	d an existing Application Domain or clic	k the Create Application	Domain button to create a new	one.		
Actions + View + + Create > Edit X Delete Search Reset ow Name Description Descrip								
Actions view view view view view view view view	Sea	rch						
Name Description								
	Nam	ie					s	earch Reset
lo data to display.	Name Search R	Results	+ Create ✓ Edit 💥 Delete	🔐 Detach			s	earch Reset
	Name Search R Actions V Row	Results View View View	+ Create ✓ Edit 💥 Delete	Detach	Description		S	Reset
	Name Search R Actions V Row	Results View View View	+ Create ✓ Edit 🗶 Delete	Detach	Description		s	Reset
	Name Search R Actions V Row	Results View View View	+ Create 🖉 Edit 💥 Dolete	Detach	Description		s	Reset



		ess manager	nent		F Application Security	A Federation	Mobile Sec	urity 🔅	Configurat
aunch Pad	Application Domain	×							[
Access Ma	anager >								
Search A	pplication Do	mains					+ Crea	ate Applicati	on Domain
				the Create Applic					
✓ Searce	:h								
	ch								
A Searce Name	ch								
	:h							Search	Reset
								Search	Reset
Name	sults	ate 🖉 Edit		Detach				Search	Reset
Name Search Re	sults	ate 🖉 Edit			Description			Search	Reset
Name Search Re Actions V	sults View ▼ ++ Cre	ate 🥒 Edit			Description Application Domain create	ed through Remote R	egistration	Search	Reset
Name Search Re Actions V Row	sults ^{View} ▼					2	-		Reset

3. Click on 'Authentication Polices'.

	weblogic 🔻 🖷
	Management 🔁 Application Security 👗 Federation 🔲 Mobile Security 🥳 Configuration
unch Pad Application Domain 🗙	FlexcubeWebgate x
Access Manager >	
lexcubeWebgate Applicat	on Domain
oplication Domain provides a logical	container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.
Summary Resources Authentic	ation Policies Authorization Policies Token Issuance Policies Administration
	Apply
	күрт
* Name	FlexcubeWebgate
	Application Domain created through Remote
Description	Registration
Description	
* Session Idle Timeout (minutes)	0 🔺 🗸
Allow OAuth Token	
Allow Session Impersonation	
Enable Policy Ordering	

4. Click on 'Protected Resource Policy'.



ORAC		🕞 Application Security 👗 Federation 🗌 Mobile Security 🥳 Configuration
aunch Pad Ap	pplication Domain x FlexcubeWebgate x	
Access Mana	ager >	
FlexcubeW	ebgate Application Domain	
Application Doma	ain provides a logical container for resources or sets of resources, and th	ne associated policies that dictate who can access specific protected resources.
Summary Re	esources Authentication Policies Authorization Policies Token Is	ssuance Policies Administration
Select on existi	ng Authentication Policy from the list or click the Create Authentication Po	Jicy button to create a new one
Seleci all'existi	ng Authentication Policy from the list of click the create Authentication Po	incy ballon to create a new one.
Actions V	fiew 🔻 🕂 Create 🔿 Duplicate 🧪 Edit 🗙 Delete 📰	Detach
Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	Protected Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.

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

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

aunch Pad Appl	ication Domain 🗙 FlexcubeWebgate	× Flexcub	eWebgate : Protect ×			
Access Manag	er >					
Protected Re	source Policy Authentication F	olicy			Duplica	te Apply
	y defines the type of verification that mus defined to protect one or more resource		ed to provide a sufficient level of trust for Acc ication Domain.	cess Manager to grant acc	ess to the user making the re	quest. A
* Name	Protected Resource Policy		Success URL			
Description			Failure URL			
			t the challenge mechanism required to nticate the user.			
Authentication Scheme	LDAPScheme	-				
Resources Re	AdaptiveAuthenticationScheme AnonymousScheme BasicFAScheme	*				
	BasicScheme BasicSessionlessScheme					
Resources	ESSOProvAuthnScheme FAAdminLocalScheme FAAuthScheme	=				
Resource	FederationMTScheme		Query String			
This Policy o						
	FlexcubeKBAOAAMScheme					
	LDAPNoPasswordValidationScheme LDAPScheme					
	OAAMAdvanced					

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



aunch Pad Appl	ication Domain 🗙 FlexcubeWebgate 🗙	FlexcubeWebgate : Protect ×		ſ
Access Manag	er >			
Protected Re	Source Policy Authentication Pol	icy		Duplicate Apply
	y defines the type of verification that must b e defined to protect one or more resources i	e performed to provide a sufficient level of trust for A n the Application Domain.	Access Manager to grant access to the user mak	ing the request. A
* Name	Protected Resource Policy	Success UR	RL	
Description	Policy set during domain creation. Add res to this policy to protect them.	sources Failure UF	RL	
* Authentication Scheme	FlexcubeBasicOAMScheme			
Resources	Advanced Rules			
Identity As:	sertion			
This will cause	an assertion to be generated for the user, o	optionally containing any Asserted Attribute set belo	W.	
Responses	Generation Add 🖍 Edit 💥 Delete			
Name		Туре	Value	
	es not have any Responses			

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

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

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

Click on Add button

Access Manage	er >		
Protected Re	SOURCE Policy Authentication Police	χ.	Duplicate Appl
	y defines the type of verification that must be defined to protect one or more resources in	performed to provide a sufficient level of trust for Access Manage the Application Domain.	ger to grant access to the user making the request. A
* Name	Protected Resource Policy	Add Response X	
Description	Policy set during domain creation. Add res to this policy to protect them.	* Type Header 💌	
Description		* Name DN Value	
* Authentication Scheme	FlexcubeBasicOAMScheme	\$user.attr.dn * Value	
Resources Res	sponses Advanced Rules	in.	
— Identity Ass	sertion	Identity Assertion has not been enabled for this policy. Enable Identity Assertion in order	
This will cause	an assertion to be generated for the user, o	Add Cancel	
Responses	🕂 Add 💉 Edit 💥 Delete		
Name		Type Value	e
This Policy do	es not have any Responses		

8. Click on Apply to Save the Changes



	icy defines the type of verification that must be e defined to protect one or more resources in		cess Manager to grant access to the user making the request. A
Confirmat	tion		×
uthentication	Policy, Protected Resource Policy, modified su	Iccessfully	
* Name	Protected Resource Policy	Success URL	
Description	Policy set during domain creation. Add reso to this policy to protect them.	Failure URL	
uthentication Scheme			
sources Re	esponses Advanced Rules		
Identity As This will cause		tionally containing any Asserted Attribute set below.	

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

		· Aaaaaa Managamant	weblogic 🔻 📼
		 Access Management 	Application Security A Federation
Launch Pad	Application	Domain x FlexcubeWebgate x	
Access I	Manager >		
Flexcub	eWebgat	e Application Domain	
Application D	omain provid	les a logical container for resources or sets of resource	es, and the associated policies that dictate who can access specific protected resources.
Summarv	Resources	Authentication Policies	Token Issuance Policies Administration
0.1			Ann Dellas hulles de secole e environ
Select an e	xisting Autro	rization Policy from the list or click the Create Authorizati	Ion Policy button to create a new one.
Actions •	✓ View ▼	🕂 Create 🔿 Duplicate 🧪 Edit 💥 Delete	e 📰 Detach
Row	Name		Description
	1 Public R	esource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
	2 Protecte	d Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.
opyright © 2000), 2015, Oracle	and/or its affiliates. All rights reserved.	

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



					weblogi	ic 🔻 🔳
	anagement	Application Security	Sederation	Mobile Security	¢ Confi	iguratio
Launch Pad Application Domain × Fle	xcubeWebgate × FlexcubeWebgat	e : Protect ×				
Access Manager >						
Protected Resource Policy	Authorization Policy				Duplicate	Apply
 Identity Assertion This will cause an assertion to be gen Responses + Add / Edit 	erated for the user, optionally containin	g any Asserted Attribute set below.				
Name	Туре	Value				
This Policy does not have any Respon	ISES					
opyright © 2000, 2015, Oracle and/or its affiliates.	All rights reserved.					

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

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

Click on Add button

unch Pad Application Domain x FlexcubeWebgate x	lexcubeWebgate : Protect ×	
Access Manager > rotected Resource Policy Authorization Polic	Add Response X	Duplicate Apply
Identity Assertion	 Type Header Name DN Suser.attr.dtd Identity Assertion has not been enabled for this policy. Enable Identity Assertion in order Add Cancel	

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



	Management	F Application	Security Federation	Mobile Security	Configura
nch Pad Application Domain 🗙	FlexcubeWebgate × Flexc	ubeWebgate : Protect ×			
Access Manager > Detected Resource Polic orization policy contains a set of co litions apply to all resources within	onditions that define whether a	user should be permitted or denied acc	ess to the resources protecte		Duplicate App
					×
	ource Policy, modified success	ully			
Authorization Policy, Protected Reso mmary Resources Condition	is Rules Responses				
Identity Assertion This will cause an assertion to be	is Rules Responses	ully Ily containing any Asserted Attribute set	below.		
uthorization Policy, Protected Reso mmary Resources Condition Identity Assertion This will cause an assertion to be	s Rules Responses				

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

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

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

ObAccessClient.xml

password.xml

cwallet.sso

cwallet.sso.lck

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

• Select the remaining 2 files

aaa_key.pem

aaa_cert.pem

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

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

Use the ORAPKI tool to import the Flexcube and OAM Server certificates to Oracle HTTP Server. Add <Oracle_MIDDLEWARE>/oracle_common/bin to PATH environment variable and also set JAVA_HOME environment variable. Execute the below command in the command line.



orapki wallet add -wallet

<Oracle_MIDDLEWARE>/<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1/keystore
s/default -trusted_cert -cert <export_certificate_file_name_with_location.cer> -auto_login_only

Note: Certificate has to be imported into OHS Wallet.

2.6.5.4 Configuring mod_wl_ohs for Oracle HTTP server Routing

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

<Location /FCJNeoWeb>

SetHandler weblogic-handler

WebLogicHost ofss00002.in.oracle.com

WeblogicPort 7002

WLProxySSL ON

SecureProxy ON

WLSSLWallet

"<ORACLE_MIDDLEWARE>/<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1/keystores/default"

</Location>

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

2.6.5.5 Verify the Webgate 11g Agent Created

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

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



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

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

2.6.5.6 Using OAM Test Tool (This step is not mandatory)

There is a test tool provided in OAM software which helps us to check the response parameter values. The test tool is available in <OAM Install Dir>\ oam\server\tester.

For eg. D:\weblogic\Middleware\Oracle_IDM1\oam\server\tester

Use *java -jar oamtest.jar* to launch the OAM test tool.



Oracle Access Manager Test Tool	_ ×
<u>F</u> ile <u>E</u> dit <u>T</u> est <u>H</u> elp	
ڬ 🗟 I 🥔 I 🏦	
Server Connection	
IP Addr Port Max C *Aαe *Primss220028.in.oracle.com 5575 1 FlexcubeWebgate	
*Prim[ss220028.in.oracle.com] [5575] [1 FlexcubeWebgate Agent Pa	
Secon 1	
Min C Timeou Mo Global Passp 1 30000 Si ✓ Conne	ect
Protected Resource URI	
Sche Port	S 🖉
(https) FlexcubeWebaate	uth S
Resour Operat //FCINeoWeb Get	ite
User Certifica User Certifica	
- Status Messages	
[1/11/13 5:33 PM][response] Connected to primary access server [1/11/13 5:34 PM][request][validate] yes [1/11/13 5:34 PM][response] Authentication scheme : FlexcubeAuthnScheme, level : 1 [1/11/13 5:34 PM][response] Redirect URL : https://ofss220028.in.oracle.com:14101/oam/server [1/11/13 5:34 PM][response] Credentials expected : 0x1 (basic) [1/11/13 5:34 PM][request][authenticate] yes [1/11/13 5:34 PM][response] Ser DN : cn=SARAN,cn=users,dc=oracle,dc=com [1/11/13 5:34 PM][response] Session]D : 6e531a7f-460d-4db8-b872-a7da77999282 [1/11/13 5:34 PM][response][action] DN : cn=SARAN,cn=users,dc=oracle,dc=com [1/11/13 5:34 PM][response][action] OAM_IMPERSONATOR_USER : [1/11/13 5:34 PM][request][authorize] ves	
Elapsed (86 Capture Q Empty	3

2.6.5.7 Fix for Escape sequence character back slash (\) infront of comma (,) in OAM Header Variable

cd <Oracle_IDM>/common/bin

./wlst.sh or wlst.cmd

wls:/offline> connect()

Please enter your username :Weblogic

Please enter your password :

Please enter your server URL [t3://localhost:7001] :t3://localhost:7201

Connecting to t3://vm34.sg.oracle.com:8001 with userid weblogic ...

Successfully connected to Admin Server 'AdminServer' that belongs to domain 'iam_domain'.

Warning: An insecure protocol was used to connect to the server. To ensure on-the-wire security, the SSL port or Admin port should be used instead.



wls:/base_domain/serverConfig> domainRuntime()

Location changed to domainRuntime tree. This is a read-only tree with DomainMBean as the root.

For more help, use help(domainRuntime)

wls:/base_domain/domainRuntime> configurePolicyResponses(responseSeparator=",", responseEscapeChar="")

Policy Responses configuration is updated.

wls:/base_domain/domainRuntime>

2.7 First launch of FLEXCUBE after installation

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

2.7.1 Parameter Maintenance

2.7.1.1 Bank Parameter maintenance - UBS

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

♦ Bank Parameters Maintenance	_ ×
🗄 Save	
Bank Code * 000	Bank Name Bank Futura
Head Office Branch	
Branch Code * 000	Branch Description Bank Futura
Financial Preferences General Preferences FATCA	
Format Mask	Year End Profit and Loss
Cif Mask bbbnnnn	General Ledger * 221000002
General Ledger Mask * nnnnnnnn	Transaction Code * YET
Spread	General Ledger Purge Days
Spread Application Both Legs 🔻	Auto Batch
Spoof Files Purge Days 90	
Inter Pay Lead Days 3	SSO Enabled
Cheque Numbering Details	Checksum Algorithm 🔹
Scheme Automatic 🔻	Checksum Algorithm
Cheque Number Mask NNNNNN	tor C.
	Unique For Branch
TRS Details	Suspense Account
Preferences Account Mask Field Properties	
Maker D)ate Time:
	Date Time:
	ord Status Open
Authorizati	ion Status



2.7.1.2 Parameters Maintenance – IS

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

2.7.2 Maintaining LDAP DN for FLEXCUBE users

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

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

LDAP DN value should be entered as complete DN value.

eg.

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



For FLEXCUBE – UBS

🔶 User Maintenance			-
E. Save			
User Details		User Status	Enabled
User Identification Name User Reference	* FCUBSUSER * FCUBSUSER		Hold Disabled Locked
User Reference Language Home Branch		Classification	Staff●Branch
Customer No		Status Changed On	2011-01-04
Department Code Department Description		Last Signed On	Staff Customer Restriction
Tax Identifier LDAP DN	cn=FCUBSUSER,cn=Us	ELCM User ID	Multi Branch Access
Time Level Amount Format	* 9 LDAP DN		Other RM Customer Access Restricted
Date Format	Auto Authorization Validate		Show Dashboards Alerts on Home
Supervisor Identification Supervisor Name	E		 F10 Access Required F11 Access Required F12 Access Required
User Password		Start Date *	* 2011-01-04 2
Password Password Changed On Email Reference No	2012-01-04	End Date	
Invalid Logins		Screen Saver Details	
No of Cumulative Logins No of Successive Logins	17	Screensaver Interval (in seconds)	3600
Restricted Password Role	s Rights Functions Tills	Account Classes Genera	al Ledgers Limits Branches

For FLEXCUBE - IS

🔶 User Admin					_ >
🗄 Save					
User Details					
Externel Identifier	FCISUSER FCIS User cn=FCUSR,cn=Users,d(XXX,XXX,XXXX XXX,XXX,XXXX XXX,XXX,XXXX	Language * Home Branch * Home Module *	000	Classification	 Staff Auto End Of Day Customer
Modules	Investments	Status Description User Status	 Enabled Hold Disabled Locked 	Time Level Status Changed On Last Signed On	* 9
Invalid Logins		User Passwords			
Cumulative Successive	0	Password Password Changed On Email		Start Date End Date	* 07/26/2014
Amount Limits					
Override Amount * Transaction Amount * Auth Amount * Date Format	٤	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		Ok Cancel



2.7.3 Launching FLEXCUBE

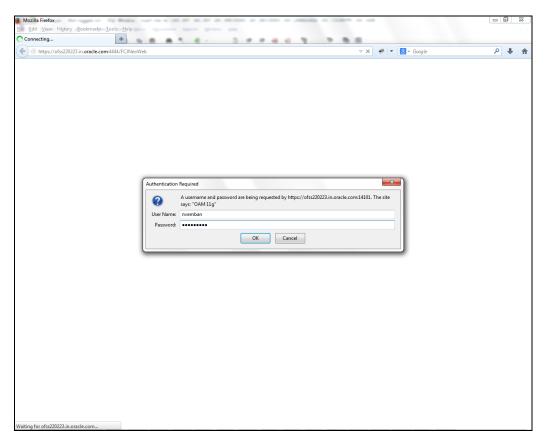
After setting up FLEXCUBE to work on Single Sign on mode, navigate to the URL <u>https://<hostname>:<OHS</u> SSL Port>/<Context Root> from your browser

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

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

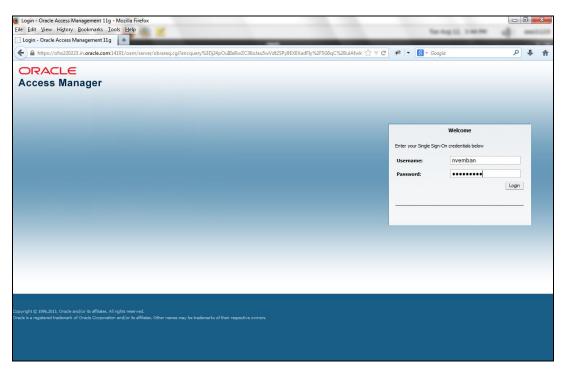


2.7.3.1 Basic Style Challenge by Webgate

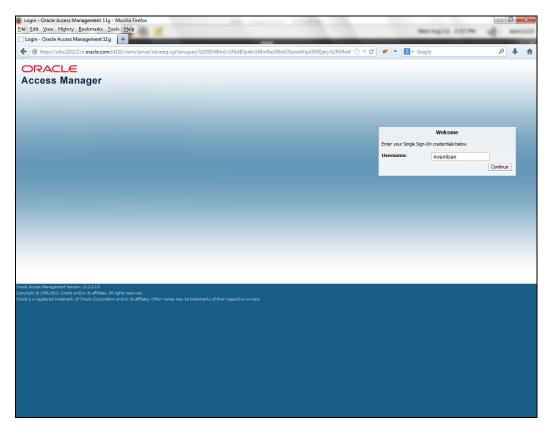




2.7.3.2 Form Style Challenge by Webgate

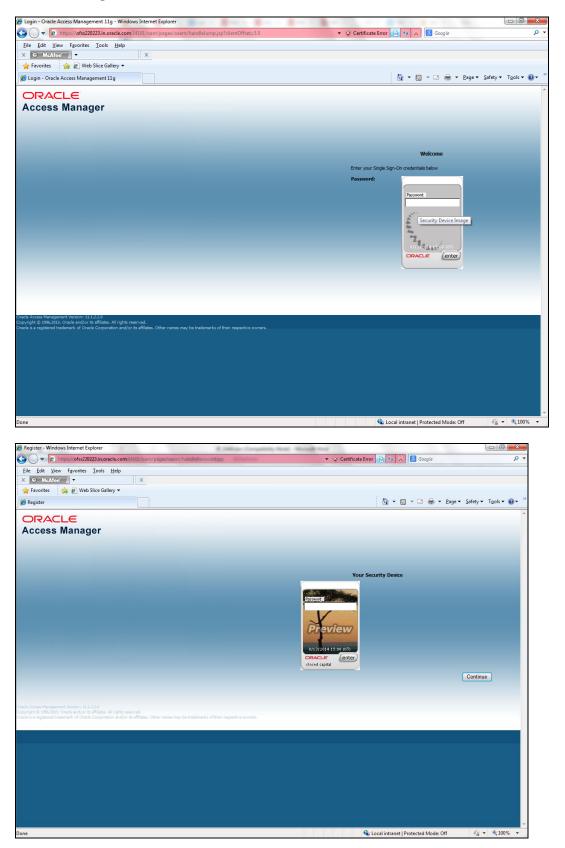


2.7.3.3 KBA Based Strong Authentication Challenge by Webgate(Only when OAAM is used)





First Time Login

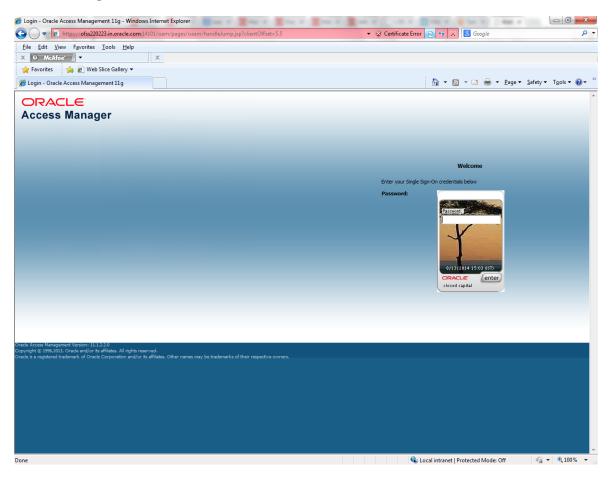




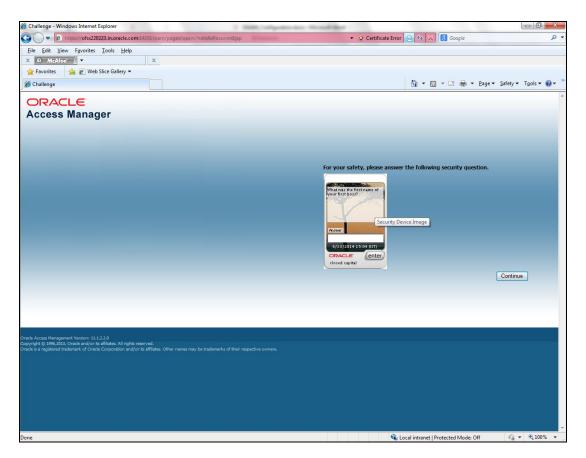
Register - Windows Internet Explorer	m:14101/oam/pages/oaam/handleRegisterImagePhrase.jsp		
	m 14101/0am/pages/0aam/nandiekegisterimagernraseljsp	👻 Certificate Error 🔛 🍫 🔀 Google	μ.
<u>F</u> ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp × ⊙ McAfoo* / ▼	x		
🖌 😈 McAree 🦼 🤄 Web Slice Gallery 🕶			
· · ·		🔓 🔻 🔝 👻 🖷 🖛 💌 <u>P</u> age	Safety = Tools = 🔊 = »
🏉 Register		🖬 · 🔤 · 📼 · 🔤	alety + Tools + W
ORACLE			^
Access Manager			
Select Your Security Questions/Answers			
1) Select One	-		
2) Select One	•		
2) 2000 200			
3) Select One	•		
S) Select One			
4) Select One	-		
5) Select One	•		
	Continue		
Oracle Accorr Management Version: 111.2.2.0			
Conduct Access Management Version: 11.1.2.2.0 Copyright © 1996,2013, Oracle and/or its affiliates. All rights	s reserved. /cr its affiliates. Other names may be trademarks of their respective owners.		
Oracle is a negistered trademark of Oracle Corporation and/	yor is annates. Other hames may be trademarks of their respective owners.		
		🗣 Local intranet Protected Mode: Off	
Done		Color intraffect Protected Wode. On	100.0
Register - Windows Internet Explorer	1,080 as Corp.		
G V Fittps://ofss220223.in.oracle.co	om 14101/oam/pages/oaam/handleRegisterImagePhrase.jsp	 Certificate Error S Google 	× ۵ ا
Image: Second state		 Certificate Error Coogle 	
C C ALARCE CONTRACTOR	x	- 2 Certificate Error 🕒 🧐 🗶 🕄 Coogle	
Image: Second	x		• م
C C ALARCE CONTRACTOR	x	 Cettificate Error Source So	• م
O O O O	x		• م
	x		• م
O O O O	x		- م
	x		- م
			٩
	x		٩
			٩
			- م
			٩
			٩
			٩
			٩
OFSS What is the name of the first musical grou OFSS	up you saw in concert? •		٩
OFSS What color was your first pet?	up you saw in concert? •		٩
Provides a second sec	up you saw in concer? •		- م
OFSS What color was your first pet?	up you saw in concer? •		- م
Access Manager Access Manager Access Manager What is the name of the first musical grou OFSS What color was your first pet? OFSS What was the first name of your first boss	up you saw in concer? •		- م
Access Manager Access M	up you saw in concert? •		- م
 What color was your first pet? OFSS What was the first name of your first boss OFSS Who is your favorite athlete? 	up you saw in concer? •		- م
Access Manager Access M	ap you saw in concert? •		- م
 What color was your first pet? OFSS What was the first name of your first boss OFSS Who is your favorite athlete? 	up you saw in concert? •		- م
 What color was your first pet? OFSS What was the first name of your first boss OFSS Who is your favorite athlete? 	ap you saw in concert? •		- م
 What color was your first pet? OFSS What was the first name of your first boss OFSS Who is your favorite athlete? 	ap you saw in concert? •		- م
 What color was your first pet? OFSS What was the first name of your first boss OFSS Who is your favorite athlete? 	ap you saw in concert? •		- م
 What color was your first pet? OFSS What was the first name of your first boss OFSS Who is your favorite athlete? 	ap you saw in concert? •		- م
 What color was your first pet? OFSS What was the first name of your first boss OFSS Who is your favorite athlete? 	ap you saw in concert? •		- م
 What color was your first pet? OFSS What was the first name of your first boss OFSS Who is your favorite athlete? 	ap you saw in concert? •		- م
Constant of the second sec	up you saw in concert? -		- م
Constant of the second sec	up you saw in concert? -		- م
Constant of the second sec	ap you saw in concert? •		- م



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.



https://sfaa?	220222 :		Web/SMMDIFRM.js			-							☆ •
		Com.4444/PCJNEO	Web/ SivilviDiPRIVI,js	p								-	
RACL						Branc	n : <u>000</u> Date .	Session Time : 0	0.00104 <u>Win</u>	tew Help	Logged User - Vinh	al I Sion Off	•
irrie Inlerad	tions Custom		sks Preferences										
earch		•	🦕 🕕 Informat	ion Message									
					Info	mation Morea							
				Information Message									
			-	🕩 Last Login :2011-01-04 16:22:27									
			Curren	Current Time :14:57:13									
			L										
									Ok				

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

2.7.4 Signoff in a SSO Situation

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

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





Oracle Access Manager Integration May 2020 Version 12.87.06.0.0

Oracle Financial Services Software Limited Oracle Park Off Western Express Highway Goregaon (East) Mumbai, Maharashtra 400 063 India

Worldwide Inquiries: Phone: +91 22 6718 3000 Fax:+91 22 6718 3001 www.oracle.com/financialservices/

Copyright © [2007], [2020], 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.

