Oracle Access Manager Integration Oracle FLEXCUBE Universal Banking Release 14.0.0.0.0 December 2017 Part No. E88855-01





Table of Contents

1. PRE	FACE	
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. ENA	BLING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER	
2.1	INTRODUCTION	
2.2	BACKGROUND AND PREREOUISITES	
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	
2.5.3	Configuring SSL Mode in Oracle Internet Directory	
2.6	CONFIGURING SSO IN OAM CONSOLE	
2.6.1	Identity Store Creation	
2.6.2	Creating Authentication Module	
2.6.3	Creating Authentication Scheme	
2.6.4	Creating OAM 11g Webgate	
2.6.5	Post OAM Webgate 11g Creation	
2.7	FIRST LAUNCH OF FLEXCUBE AFTER INSTALLATION	
2.7.1	Parameter Maintenance	
2.7.2	Maintaining LDAP DN for FLEXCUBE users	
2.7.3	Launching FLEXCUBE	
2.7.4	Signoff in a SSO Situation	



1. Preface

1.1 Introduction

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

1.2 <u>Audience</u>

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

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

1.3 Abbreviations

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

1.4 **Documentation Accessibility**

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

1.5 **Organization**

This manual is organized into the following chapters:

Chapter 1	<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
l	Delete row
Q	Option List

1.6.1 Related Documents

You may refer the following manual for more information

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



2. Enabling Single Sign-on with Oracle Access Manager

2.1 Introduction

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

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

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

2.2 **Background and Prerequisites**

2.2.1 Software Requirements

Oracle Identity and Access Management 11g R2 - 11.1.2.3.0

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

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

LDAP Directory Server

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

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

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



Oracle Weblogic (10.3.6)

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

2.3 Background of SSO related components

2.3.1 Oracle Access Manager (OAM)

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

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

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

2.3.2 LDAP Directory Server

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

2.3.3 WebGate/AccessGate

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

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

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

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



2.3.4 Oracle Adaptive Access Manager

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

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

2.4 Configuration

2.4.1 Pre-requisites

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

2.5 Enabling SSL for Weblogic and OAM Console

2.5.1 Self-signed Certificate Creation:

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

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

2.5.1.1 Keystore Creation

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

For example:

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



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

2.5.1.2 Export private key as certificate

keytool -export -v -alias <alias_name> -file <export_certificate_file_name_with_location.cer> -keystore <keystore_name.jks> > -keypass <Private key Password> -storepass <Store Password>

For example:

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

If successful the following message will be displayed :

Certificate stored in file < AdminFlexcubeCert.cer>

2.5.1.3 Import as trusted certificate

keytool -import -v -trustcacerts -alias rootcacert -file <export_certificate_file_name_with_location.cer> - keystore <keystore_name.jks> > -keypass <Private key Password> -storepass <Store Password>

For example:

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

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



2.5.2 Configuring Weblogic Console

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

2.5.2.1 Select Admin Server to enable SSL options

	Administration Console						Q				
Change Center	🔒 Home Log Out Preferences 🛃 Record	Help	<u>.</u>		Welcor	ne, weblogic Connected to: ia	ım_domaiı				
View changes and restarts	Home >Summary of Servers	Home >Summary of Servers									
Configuration editing is enabled. Future	g is enabled. Future Summary of Servers										
changes will automatically be activated as you modify, add or delete items in this domain.	Configuration Control										
Jomain Structure iam_domain ⊕ Environment ⊕ Environment ⊕ Servers −Outers −Outers −Outers −Coherence Servers −Outers −May and Shutdown Classes	A server is an instance of WebLogic Server This page summarizes each server that has C2 C3 C4 C4 C4 C4 C4 C4 C4 C4 C4 C4 C4 C4 C4	that runs in its own Java Virtual been configured in the current \	Machine (JVM) and has its o WebLogic Server domain.	own configuration.		Showing 1 to 4 of 4 Previous	: Next				
Deployments	🔲 Name 🏟	Cluster	Machine	State	Health	Listen Port					
Security Realms	AdminServer(admin)			RUNNING	≪ ok	7001					
How do I	oam_server1			RUNNING	✓ OK	14100					
Create Managed Servers	oim_server1			RUNNING	≪ ок	14000					
Clone Servers	soa_server1		LocalMachine	SHUTDOWN		8001					
Delete Managed Servers Delete the Administration Server Start and stop servers	New Clone Delete					Showing 1 to 4 of 4 Previous	Next				
System Status 🖃	j										
Health of Running Servers											
Failed (0) Critical (0) Overloaded (0) Warning (0)											

2.5.2.2 Follow the steps in General Tab as shown below:

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



Domain Structure	General Cluster Services Keys	tores SSL Federation Services	Deployment Migration	Tuning Overload	Health Monitoring	Server Start	Web Services		
lam_domain ▲ C-Environment Custers Custers Vironal Hosts Vironatable Targets Colenence Servers	Save Use this page to configure general feat View JNDI Tree @	ures of this server such as default net	twork communications.						
Coherence Clusters Machines Work Managers	Name:	Name: AdminServer			umeric name for this	server instance.	More Info		
Startup and Shutdown Classes	Machine:	(None)		The WebLogic Server host computer (machine) on which this server is a to run. More Info			on which this server is meant		
How do L	Cluster:	Cluster: (Standalone)			The duster, or group of WebLogic Server instances, to which this server belongs. More Info				
Configure default network connections Create and configure machines	🦺 Listen Address:	중 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 VII DE discounting volume	☑ Listen Port Enabled	Specifies v (non-SSL)	Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info						
System Status	Listen Port:		The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info			ten for regular (non-SSL)			
Health of Running Servers Failed (0)	SSL Listen Port Enabled			Indicates v port. Mo	whether the server c re Info	an be reached t	nrough the default SSL listen		
Critical (0) Overloaded (0)	SSL Listen Port:	7002		The TCP/IF requests.	P port at which this s More Info	erver listens for	SSL connection		
OK (3)	🔽 🦺 Client Cert Proxy Enabled			Specifies w special hea	whether the HttpClus ader. More Info	terServlet proxi	es the client certificate in a		
	Java Compiler:	javac	javac			The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info			
	Diagnostic Volume:	Low	×	Specifies t WebLogic 1 does not a controls th Info	he volume of diagnos Server at run time. N Iffect explicitly config le volume of events (stic data that is lote that the WL gured diagnostic generated for JF	utomatically produced by DF diagnostic volume setting modules. For example, this lockit Flight Recorder. More		
	- 🗢 Advanced								
	Virtual Machine Name:	iam_d	Iomain_AdminSe	When WLS running thi	is running on JRVE, is server More Info	this specifies th	e name of the virtual machine		
	🖉 🛃 WebLogic Plug-In Enabled			Specifies w header, wi from a pro	whether this server u hich is recommended xy plug-in. More In	ses the propriet if the server ins	ary WL-Proxy-Client-IP tance will receive requests		

2.5.2.3 Follow the steps in Keystores Tab as shown below:

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

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

	dministrati	ion Cons	ole												Õ
Change Center	🚹 Home	Log Out	Preference	s 📐 Record	Help		•	2					Welcome, w	eblogic Conne	cted to: iam_domain
View changes and restarts	Niew changes and restarts Home > Summary of Servers > AdminServer														
Configuration editing is enabled. Future	Settings for AdminServer														
modify, add or delete items in this domain.	Configur	ation P	rotocols	Logging D	ebug	Monitoring	Control	Deployments	Services	Security	Notes				
Domain Structure	General	Cluster	Services	Keystore	s SSI	L Federa	ation Services	Deployment	Migration	Tuning	Overload	Health Monitoring	Server Start	Web Services	
iam_domain	Save Keystore you to m Keystore Save	Cancel es ensure 4 aanage the es: Cancel	he secure : security o Dem Cust Cust Dem	storage and m f message tra- no Identity a com Identity com Identity com Identity to Identity a	anagem nsmission and Cc and Cc and Cl and Ja nd Der	ment of priv ns. mo Trust ommand ustom Tr ava Stanc mo Trust	ate keys and Line Trust Ist Jard Trust	Trusted certifica	te authoritie	s (CAs). Thi	s page lets yn Which t trust kr	ou view and define va configuration rules sh eystores? More Info	rious keystore o	nonfigurations. The	rese settings help
System Status															
Heatth of Running Servers Failed (0) Critical (0) Overloaded (0) Warning (0) OK (3)	ights reserved. and/or its affilis	ates, Other	names mav	be trademarks	of their:	respective o	wners.								



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 delate items in this domain	Settings for AdminServer Configuration Protocols Logaina Debua Monitorina Control Deployments Services Security Notes										
Domain Structure	General Cluster Services Keystores SSL Fed	eration Services Deployment Migratio	on Tuning Overload Health Monitorin	g Server Start Web Services							
Iam_domain → Environment → Guesters → Uritual Hosts → Wignatable Targets = Goherence Servers =	Save Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.										
Coherence Clusters Machines Work Managers Work Managers	Keystores: - Identity	Custom Identity and Custom Trust	Change Which configuration rules trust keystores? More In	should be used for finding the server's identity and fo							
	Custom Identity Keystore:	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	Custom Identity Keystore Passphrase:	•••••	The encrypted custom ide the keystore will be opene	ntity keystore's passphrase. If empty or null, then d without a passphrase. More Info							
Set up SSL	Confirm Custom Identity Keystore Passphrase:										
Health of Punning Servers	— Trust		/scratch/app/fmw115/oam1115/Ba	seKevStore/AdminFlexcubeKevStore.iks							
Failed (0)	Custom Trust Keystore:	nFlexcubeKeyStore.jks	me paur and me name or	are custom a ust keystore. More into							
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:	•••••	••••••••••••••••••••••••••••••••••••••								
	Confirm Custom Trust Keystore Passphrase:	•••••									
	Save										

2.5.2.5 Follow the steps in SSL Tab as shown below:

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



Change Center	🏠 Home Log Out Preferences 🚈 Recor	d Help		Welcome, weblogic Connected to: iam_domain
View changes and restarts	Home >Summary of Servers >AdminServer			
Configuration editing is enabled. Future	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 Security	Notes
Domain Structure	General Cluster Services Keystore	s SSL Federation Services Deployment	Migration Tuning	Overload Health Monitoring Server Start Web Services
iam_domain 🔶				
Environment	Save			
Servers Clusters Virtual Hosts	This page lets you view and define variou:	s Secure Sockets Layer (SSL) settings for this serve	r instance. These set	tings 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 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
Security Realms	Private Key Alias:	FlexcubeCert		The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info
How do I	🚝 Private Key Passphrase:	·····		The keystore attribute that defines the passphrase used to retrieve the
Set up SSL				server's private key. More Info
Verify host name verification is enabled Configure a custom host name verifier	Confirm Private Key Passphrase:			
Configure two-way SSL	Certificate Location:	from Custom Identity Keystore		The keystore attribute that defines the location of the trusted certificate. More Info
System Status	- Trust			
Health of Running Servers	Trusted Certificate Authorities:	from Custom Trust Keystore		The keystore attribute that defines the location of the certificate authorities. More Info
Critical (0)	— 🗢 Advanced —			
Overloaded (0) Warning (0)	Hostname Verification:	None Custom Hostname Verifier		Specifies whether to ignore the installed implementation of the weblogic.security.SSL.HostnameVerifier interface (when this server is acting as a client to another application server). More Info
OK (2)	🚝 Custom Hostname Verifier:	BEA Hostname Verifier None		The name of the class that implements the weblogic.security.SSL.HostnameVerifier interface. More Info
	Export Key Lifespan:	500		Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. More Info
	Use Server Certs			Sets whether the client should use the server certificates/key as the client
Warning (0) OK (2)	街 Custom Hostname Verifier:			client to another application server). More Info
				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 wark 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
	🛃 Cert Authenticator:			The name of the Java class that implements the weblogic.security.ad.Cer4u/thenticator 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	V	Indicates the server certificate validation rules for outbound SSL. More Info
	V 🗄 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



	Administration Console						Õ				
Change Center	🔒 Home Log Out Preferen	ces 📐 Record Help	Q			Welcome, w	eblogic Connected to: iam_domain				
View changes and restarts	Home >Summary of Servers >	AdminServer > Summar ุ	y of Servers								
Configuration editing is enabled. Future	Summary of Servers	Summary of Servers									
modify, add or delete items in this domain.	Configuration Control										
Domain Structure iam_domain ServersOustersVurbal HostsMigratable TargetsCoherence ServersCoherence ClustersMigratable ClustersMachinesMachines	A server is an instance of W This page summarizes each C2 © Customize this table Servers (Filtered - Mon	/eblogic Server that rur server that has been co e Columns Exist)	ns in its own Java Virtual M	achine (JVM) and has its own con	figuration.						
Work Managers	New Clone Dele	te				Shr	wing 1 to 4 of 4 Previous Next				
Deployments	🔲 Name 🐟		Cluster	Machine	State	Health	Listen Port				
Sen irity Realms	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 the Administration Server Student and the administration Server	New Clone Dele	te				Sho	wing 1 to 4 of 4 Previous Next				
Start and stop servers											
System Status											
Health of Running Servers											
Failed (0) Critical (0) Overloaded (0) Warning (0) OK (3)											

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

2.5.3 Configuring SSL Mode in Oracle Internet Directory

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

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



	anager 11g Fusion Middleware Contr	rol			Setup	• Help ↓ Log Out
👫 Farm 👻 💑 Topology						
∃ -	🔂 oid1 🕡				Logged in as well	logic 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 >		Load		Security	
O OAM	Control >) 121	Total LDAP Connections	0	Failed Bind Operations	0
	Logs >	220		2		•
O ovd1		220	Operations Completed	2	Falled Super User Logins	U
Metadata Repositories	Port Usage	65	Operations in progress	0	Sucessful Super User Logins	0
🗉 🛅 Web Tier	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/asi	nst_1/oid1
	5					
	100					
	80					
	60				Memory Utilization (%)	nst_1/oid1
	40				padsrini-pc	
	0 10 00 10 00 10				40.05 40.00	
	16:22 16:23 16 February 15 2013	5:24 16:25 16:26 16	527 16:28 16:29 16:30	16:31 16:32 16:33 16	34 16:35 16:36	Table Mary
	L					rable view

2. Click 'Create Self-Signed Wallet'.

	nager 11g Fusion Middleware Control	Setup → Help → Log Out
📑 Farm 👻 🔒 Topology		
Farm_base_domain Application Deployments	Orade Internet Directory	Logged in as weblogic Host padsminp; Page Refreshed Feb 15, 2013 4:39:54 PM IST 3 ⁴⁶
WebLogic Domain Generation Generation	Wallets A Vallet is a Keystore that stores X.509 certificates and private keys in industry-standard, PKCS #12 format. To cred Wallet. To manage the contents of a vallet, select a wallet and click Manage.	ate a wallet, dick Create. To create a wallet with a self-signed certificate, dick Create Self-Signed
OIM Ovd1	Create X Delete Create Self-Signed Wallet Import Export	6d Manage
	rame	Auto-logn
	Fetching Data	

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



	anager 11g Fusion M	liddleware Control		Setup Help Log Out
Farm - R Topology	5 5			
E 📲 Farm_base_domain	oid1 orade Internet Di	irectory 🕶		Logged in as weblogic Host padsrini-pc Page Refreshed Feb 15, 2013 4:40:45 PM IST €2
Application Deployments MebLogic Domain Identity and Access Ani OAni OM OIM OIM Ovd1	Wallets > Create Se Create Self-Sign A self signed wallet is or password-protecte PKCS#12 wallet that provide the necessar	Sf-Signed Wallet net Wallet not signed by a well known CA. A se ed. Passwords, if specified, have a m provides PKI-based access to service y security for Auto-login wallets.	of-signed wallet is not recommended in a production environment immun length of eight characters, and contan alphabetic character is and applications without requiring a password at runtime. Auto	CMC Cancel The walet name should be unique for a given component. The walet type can be auto-bojn ters combined with numeric or special characters. Auto-bojn walets an obfuscated form of dogn walet don't need a password to modify, or delete the walet. File system permissions
Metadata Repositories Web Tier	Self-Signed Wallet * Wallet Name Wallet Password Confirm Password	oidselfsigned]	
	Add Self-Signed Ce Add a self-signed cer * Common Name	ertificate tificate that becomes part of the wal	let.	
	Organizational Unit Organization	OFSS Orade		
	City State Country	Chennai TN India		
	Key Size	2048 💌		

4. Click 60 Manage...

	nager 11g Fusion Middleware Control	Setup → Help → Log Out
🕂 Farm 👻 🔒 Topology		
I ▼ Farm_base_domain Application Deployments	Entroprise Manager 11g Fusion Middleware Control Setup → Heb → Log Out Topology Logged in as webliogic (Host paddrin pc edomain Drade Internet Directory → Sato Deployment Drade Internet Directory → Walletis Kystore that stores X.590 certificates and private keys in industry-standard, PKCS #12 format. To create a wallet with a self-signed certificate, dick Create Self-Signed MM d1 d1 data Repositories If Mone Mate Q Create	
WebLogic Domain Control Lidentity and Access O OAM Control Lidentity O OAM Control Lidentity O OIM	Wallets A Vallet is a Keystore that stores X.509 certificates and private keys in industry-standard, PKCS #12 format. To Wallet. To manage the contents of a wallet, select a wallet and cick Manage. Yereate Yereate Yereate Yereate Self-Signed Wallet Yereate Yereate Self-Signed Wallet	o create a wallet, clck Create. To create a wallet with a self-signed certificate, click Create Self-Signed
📀 ovd1	Name	Auto-login
Metadata Repositories	oidselfsigned	✓
📾 🧰 Web Tier		

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

	nager 11g Fusion Middleware Control				Setu	p → Help → Log Out
Farm - 💦 Topology						
Farm_base_domain Application Deployments	<pre></pre>				Logged in as we Page Refreshed Feb 15	blogic Host padsrini-pc , 2013 4:45:58 PM IST €2
WebLogic Domain MethLogic Domain Identity and Access OAM OAM Odd1 Odd1 Odd1	Walets > Manage Certificates Manage Certificates: oldselfsigned To generate a certificate ginging request (CSR), dick 'Add Certificate Request'. After you create a CSR, send it to your certificate or trusted cert, dick Import. You can only import the CA-signed certificate into the same wallet from which the Add Certificate Request 	r CA who will verify your identii e CSR was generated.	ty and retu	im the signe	d certificate. To import	the CA signed
🗉 🚞 Metadata Repositories	Subject Name	Certificate Type	Status	Key Size	Start Date	Expiration Date
🗉 🛅 Web Tier	CN=padsrini-pc,OU=OFSS,O=Orade,L=Chennai,ST=TN,C=IN	Certificate Request		2048		
	CN=padsrini-pc, OU=OFSS, O=Orade, L=Chennai, ST=TN, C=IN	Certificate	Valid	2048	February 15, 2013	February 14, 2018
	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
	CN=GTE CyberTrust Global Root, OU="GTE CyberTrust Solutions, Inc.", O=GTE Corporation, C=US	Trusted Certificate	Valid	1024	August 13, 1998	August 14, 2018
	CN=padsrini-pc, OU=OFSS, O=Orade, L=Chennai, ST=TN, C=IN	Trusted Certificate	Valid	2048	February 15, 2013	February 14, 2018
	OU=Class 2 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2028
	OU=Class 1 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	Trusted Certificate	Valid	1024	January 29, 1996	January 8, 2020

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



	Anager 11g Fusion Middleware Control		Set	up 👻 Help 👻 Log Out
📲 Farm 👻 🔒 Topology				
	☆ oid1 @		Logged in as we	blogic Host padsrini-pc
Farm_base_domain Application Deployments	Crade Internet Directory -		Page Refreshed Feb 1	5, 2013 4:45:58 PM IST 🔇
WebLogic Doman Jentity and Access OAM Gold OM OM OM OM OM	Walets > Manage Certificates Manage Certificates: oidselfsign To generate a certificate signing request (certificate or trusted cert, click Import. Yo	erd Trusted Certificate The Trusted Certificate The Trusted Certificate with Subject Name Chi=padomi-pc, OU=OFSS, O=Orade, L=Chennal, ST=TN, C=TN is shown below. You can cut and paste the entrie text in the box from BEGIN CERTIFICATE to the IOECRITETATE to the Intended bedings or dot K_DoorTituted Certificate 'to encore the certificate to a fits.' Unany work to do this fit another party	certificate. To impor	t the CA signed
Metadata Repositories	Subject Name	wants to trust your certificate directly.	Start Date	Expiration Date
B 🦲 Web Ter	CH=padsrim-pc, CU=OFSS, O=Ors CH=padsrim-pc, CU=OFSS, O=Or CU=CasS Public Privary Certific CH=CTE CyberTrust Global Root, CH=CTE CyberTrust Global Root, CH=CTE CyberTrust Global Root, CU=Class 3 Public Privary Certific CU=Class 3 Public Privary Certific	MILDOCCALACQAUQUINGEINUNGAENAQAEEBQAUYIELMAKGAUEBBMUSU4AUGAUBANTAFARANGAAUBANTAFARANGAAU MULDOCCALACQAUQUINGEINUNGAE OptivuQUEAUGAUSUkabByQUGUQUINQUEAUFDEFSDUTALBANTAFARAGUINAFATARANGAU CabaDayaBelad yabBkuTtardolauttakUTtarbaNokuTtakuDauttakUtakUtakUtakUtakUtakUtakUtakUtakUtak	February 15, 2013 January 29, 1996 August 13, 1998 February 15, 2013 January 29, 1996 January 29, 1996	February 14, 2018 August 2, 2028 August 14, 2018 February 14, 2018 August 2, 2028 January 8, 2020
	1	Export Trusted Certificate Gose		

7. Click 'Server Properties'.

	anage	er 11g Fusion Middleware C	ont	rol						Setu	p → Help →	Log Out
👫 Farm 👻 🔒 Topology												_
∃ -		oid1 🕡								Logged in as we	blogic Host	padsrini-pc
🖻 📲 Farm_base_domain	2:	Oracle Internet Directory 🛩								Page Refreshed Feb 15	, 2013 4:45:58	PM IST 🗘
Application Deployments Deployments Deployments		Home										
Identity and Access OAM OIM OIM		Monitoring Control Logs	> > >	gned (CSR), dok "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 ou can only import the CA-signed certificate into the same wallet from which the CSR was generated.								
ovd1		Port I leage		Import 🕆 😭 Export	K Delete							
Metadata Repositories		Administration					Certificate Type	Status	Key Size	Start Date	Expiration D	ate
🗉 🚞 Web Tier		Auminise auon		Server Properties			Certificate Request		2048			
		Security	'	Shared Properties			Certificate	Valid	2048	February 15, 2013	February 1	4, 2018
		Directory Services Manager	>		.", C=US		Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2	028
				Replication Management	Inc.", O=GTE Corporation, C=US		Trusted Certificate	Valid	1024	August 13, 1998	August 14,	2018
		General Information		Tuning and Sizing			Trusted Certificate	Valid	2048	February 15, 2013	February 1	4, 2018
		OU=Class 2 Public Primary	Cer	tification Authority, O="VeriSign, I	ic.", C=US		Trusted Certificate	Valid	1024	January 29, 1996	August 2, 2	028
		OU=Class 1 Public Primary	Cer	tification Authority, O="VeriSign, I	nc.", C=US		Trusted Certificate	Valid	1024	January 29, 1996	January 8,	2020
	4											

8. Click 'Change SSL Settings'.

	Inager 11g Fusion Middleware Control	Setup → Help → Log Out
🕂 Farm 👻 👗 Topology		
□ -	☆ oid1 ₀	Logged in as weblogic Host padsrini-pc
🗉 📑 Farm_base_domain	E Orade Internet Directory -	Page Refreshed Feb 15, 2013 4:54:17 PM IST 🗘
E Application Deployments		
🗉 🚞 WebLogic Domain	Server Droperties	Apply Revert
Identity and Access	For an United the Contraction Contraction	Apply Revert
OAM	General Performance SASL Statistics Logging	
	Server Mode Read / Write 💌	
() CIM	* Maximum number of entries to be returned by a search 10000	
Metadata Repositories	* Maximum time allowed for a search to complete (sec) 3600	
Web Tier	Preserve Case of Required Attribute Name specified in Search Request	
_	Anonymous Bind Disallow except for Read Access on the root DSE	
	* Maximum time allowed in a Transaction (sec) 0	
	* Maximum Number of Operations allowed in a Transaction 0	
	Port Numbers	
	Non-SSL Port 3060	
	SSI Port	
	SISI Contraction of the second sister of the second	

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



\sim		
ORACLE Enterprise Ma	Inager 11g Fusion Middleware Control	Setup 👻 Help 👻 Log Out
Farm - 🔒 Topology		
	☆ oid1 0	Logged in as weblogic Host padsrini-pc
Farm_base_domain Application Deployments	T Orade Internet Directory -	Page Refreshed Feb 15, 2013 4:55:50 PM IST 🗘
WebLogic Domain Jidentity and Access	Information Al changes made in this page require a server restart to take effect.	
OAM E oidl	SSL Configuration ?	OK Cancel
	C Enable SSL	
🔄 ovd1	Server Wallet Name oidselfsigned	
Metadata Repositories	oidselfsigned tot required for no-auth mode but is needed in other modes.	
u i web nei	Advanced SSL setungs	
	Server SSL properties	
	SSL Authentication Server Authentication	
	II AI	
	SSL_RSA_WITH_RC4_128_MD5	
	Cipher Suite	
	V SSL_RSA_WITH_DES_EDE_CBC_SHA	
	VILS_RSA_WITH_AES_128_CBC_SHA +	
	* SSL Protocol Version All	

10. Click 'Apply'.

	anager 11g Fusion Middleware Control	Setup ▾ Help ▾ Log Out
📑 Farm 👻 🔒 Topology		
∃ -	☆ oid1 0	Logged in as weblogic Host padsrini-pc
🛿 🚟 Farm_base_domain	🖅 Oracle Internet Directory 🗸	Page Refreshed Feb 15, 2013 4:56:40 PM IST 🗘
Application Deployments		
WebLogic Domain Identity and Access OAM	Information SSL configuration updated for /Farm_base_domain/asinst_1/aid1. Restart component for this change to be effective.	×
OIM Ovd1 ovd1	Server Properties	Apply Revert
🗄 🚞 Metadata Repositories	General Performance SASL Statistics Logging	
🗉 🚞 Web Tier	Server Mode Read / Write 💌	
	* Maximum number of entries to be returned by a search 10000	
	* Maximum time allowed for a search to complete (sec) 3600	
	Preserve Case of Required Attribute Name specified in Search Request	
	Anonymous Bind Disallow except for Read Access on the root DSE	
	* Maximum time allowed in a Transaction (sec) 0	
	Maximum Number of Operations allowed in a Transaction	
	Port Numbers	
	Non-SSL Port 3060	
	SSL Port 3131 VChange 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)



2.6.1 Identity Store Creation

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

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





2. Click 'Create' under OAM ID Stores.



Configuration >				
User Identity Sto	ores			
Default and System	Store			App
* De	efault Store UserIdentityStore1	•		
* Sy	stem Store UserIdentityStore1	•		
				Sync IDS Profile
OAM ID Stores Manage local User Identii	ly Stores. This includes IDS Profile	s that are synchronized by using Sync ID	S Profiles button.	Sync IDS Profile
✓ OAM ID Stores Manage local User Identif	ty Stores. This includes IDS Profile	s that are synchronized by using Sync ID Delete	S Profiles button.	Sync IDS Profil
▲ OAM ID Stores Manage local User Identii View ▼ + Create Name	y Stores. This includes IDS Profile The Duplicate Control of the Directory Type	s that are synchronized by using Sync ID Delete Host Information	S Profiles button. Description	Sync IDS Profil Synched IDS Profiles
▲ OAM ID Stores Manage local User Identif View ▼ + Create Name UserIdentifyStore1	y Stores. This includes IDS Profile Duplicate Zelit X Directory Type EMBEDDED_LDAP	s that are synchronized by using Sync ID Delete Host Information Idap-host7001	S Profiles button. Description	Sync IDS Profile Synched IDS Profiles No

- 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	Dry	•		Use Native ID Store S	ettings	
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					
	User Password Attribute	userPassword					
	* User Search Base	cn=Users,dc=ofss,dc=	in,dc=oracle,dc=c				
	Jser Filter Object Classes						
	Group Name Attribute						
	* Group Search Base	cn=Groups,dc=ofss,dc	=in,dc=oracle,dc=				

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

Case of the second seco	create: user lue	anuty Sto X					
Create: User Ident	ity Store User Identity	Store Service				Test Connection	Apply
* Store Name	FLEXCUBEStore	Store Service			Connection Status	×	
* Store Type	OID: Oracle Internet Directo	bry	•		Connection to the User Ide	entity Store successful!	
Description			р	refetched Attribut	es	in the second se	
▲ Location and Crede	entials						
* Location	ofss220607.in.oracle.com	3131		* Passwo	ord ••••••		
* Bind DN	cn=orcladmin						
▲ Users and Groups							
	* Login ID Attribute	cn					
	User Password Attribute	userPassword					
	* User Search Base	cn=Users,dc=ofss,dc=in,dc	=oracle,dc=c				
l	Jser Filter Object Classes						
	Group Name Attribute						
	* Group Search Base	cn=Groups,dc=ofss,dc=in,d	c=oracle,dc=				

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



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

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

2.6.2 Creating Authentication Module

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



RACLE [®] Access Management	Application Security	Federation Mobile Security
Quick Start Wizards Perform common setup tasks Application Registration SSO Agent Registration	Access Manager + • Access Manager + •	Agents + • Manage Single Sign-On agents
Session Management	Password Policy	Plua-ins
Aanage Single Sign-On sessions	Manage Common Password Policy for Single Sign-On	Manage Authentic Create LDAP Authentication Module Authentication Modules Authentication Plug-ins Create X509 Authentication Module Create Curtors Authentication Module

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

	agement	Application Security	Sederation	Mobile Security	Configurati
Launch Pad FlexcubeAuthModule ×					C
Access Manager >					
FlexcubeAuthModule LDAP Authe	entication Module			D	uplicate Apply
Use the LDAP Authentication module for Basic definition stored in an LDAP directory server.	and Form challenge methods. It ma	tches the credentials (username an	id password) of the user	who requests a resou	irce to a user
Confirmation					×
LDAP Authentication Module FlexcubeAuthN	lodule created successfully.				
* Name Flexcub	eAuthModule				
* User Identity Store FLEXCU	JBEStore 💌				
opyright © 2000, 2015, Oracle and/or its affiliates. All r	rights reserved.				

2.6.3 Creating Authentication Scheme

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





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

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



Basic Style Authentication Scheme

Enter the below details and click 'Apply':

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

Launch Pad FlexcubeBasicOAMScheme × Access Manager > Set As Default Duplicate Apply Create Authentication Scheme Authentication Scheme An Authentication Scheme defines the challenge mechanism required to authenticate a user ust also include a defined Authentication Module Each Auth Confirmation × Authentication Scheme, FlexcubeBasicOAMScheme, created successfully * Name FlexcubeBasicOAMScheme Description Basic login screen * Authentication Level 1 ^ ~ Default * Challenge Method BASIC -Challenge Redirect URL /oam/server • * Authentication Module FlexcubeAuthModule SacCookie=Secure Context/ipge=default Challenge Parameters Context/sile_el_ean challenge_ui=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 Auth	entication Module 2.6.2' of this document.
Challenge URL	: /pages/login.jsp
Context Type	: default
Context Value	: /oam
Challenge Parameters	: ssoCookie=Secure

Launch Pad FlexcubeFo	rmOAMScheme ×				
Access Manager >					
Create Authentic	ation Scheme Authentication Scheme		Set As Default	Duplicate	Apply
An Authentication Scheme	defines the challenge mechanism required to authentic	cate a user. Each Authentication Scheme must also include a	defined Authentica	ation Module.	
Confirmation					×
Authentication Scheme	, FlexcubeFormOAMScheme, created successfully				
* Name	FlexcubeFormOAMScheme				
Description	Form based login page				
* Authentication Level	2 🔨 💙				
Default					
* Challenge Method	FORM				
Challenge Redirect URL	/oam/server				
* Authentication Module	FlexcubeAuthModule				
* Challenge URL	/pages/login.jsp				
* Context Type	default 👻				
* Context Value	/oam				
	ssoCookie=Secure				
Challenge Parameters					



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

Enter the Below Details and click 'Apply':

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

Set As Default Duplicate Apply Create Authentication Scheme Authentication Scheme An Authentication Scheme defines the challenge mechanism required to authenticate a user. Each Authentication Scheme must also include a defined Authentication Module Confirmation × Authentication Scheme, FlexcubeKBAOAAMScheme, created successfully * Name FlexcubeKBAOAAMScheme Description KBA Based login page * Authentication Level 2 ^ ~ Default 📃 * Challenge Method FORM 💌 Challenge Redirect URL /oam/server -* Authentication Module FlexcubeAuthModule * Challenge URL /pages/oaam/login.jsp * Context Type default 💌 * Context Value /oam Challenge Parameters

2.6.4 Creating OAM 11g Webgate

Follow the below steps to create a Webgate:

1. Click on 'Server Instances' under Configuration.



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



2. Click on 'Search'.

Configuration > Search OAM Servers	jic 🔻 🚥
Launch Pad Server Instances × Configuration > Search OAM Servers Search Name Search Results Actions ▼ View ▼ + Create @ Duplicate Edit Duplicate Edit Duplicate Duplicate Edit Edit	figuration
Configuration > Search OAM Servers	
Search OAM Servers	
Actions ▼ View ▼ + Create → Edit ★ Delete Monitor	erver
Actions ▼ View ▼ + Create → Edit ★ Delete Monitor	
Name Search Results Actions ▼ View ▼ + Create → Edit ★ Delete 🖼 Monitor 🚔 Detach	
Search Results	
Search Results Actions ▼ View ▼ + Create → Edit → Edit → Delete Image: Action → Create → Edit → Edit → Delete	Reset
Actions 🕶 View 💌 🕂 Create 🔿 Duplicate 🧪 Edit 💥 Delete 🔛 Monitor	
Row Name	
No data to display.	

3. Edit oam_server1.

	Applic	ation Socurity	Endoration		curity	Configuratio
	The Applic		S rederation	Mobile se	ç 🔅	configuration
aunch Pad Server Instances x						
Configuration >						
Search OAM Servers					+ Create OA	M Server
Search						
Name						
					Search	Reset
Search Results						
Actions 🔻 View 👻 🕂 Create 🔿 Duplicate 🧪 Edit 💥 Delet	e 1 Monitor	Detach				
Row Name						
1 oam_server1						

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

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



	Application Security	Sederation	obile Security
aunch Pad Server Instances x oam_server1 x			
Dam_server1 OAM Server Instance			Duplicate Apply
* Server Name oam_server1	* Host	ofss220607.in.oracle.	
* Port 14101 ^ v Confirm	Edit ×		
OAM Proxy OAM Serve	r instance oam_server1 might be in use.		
Proxy Server Id AccessServerConfigP	Yes No		
* Mode Simple -			
Coherence Configuration			
Log Level 3 🔨 🗸			
Local Port 9095 🔨 🗸			
* Log Limit 4096 A Y			

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



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

	Application Security	weblogic 🗸 🚥	
Launch Pad	Access Manager + • Manage Single Sign-On Application Domains Resource Types Host Identifiers Authentication Schemes	Agents Agents Create Webgate Create OpenSSO Agent Create OpenSSO Agent	

6. Enter the below and Click 'Apply':

Version	: 11g	
Name	: Custom Webg	ate Name
Base URL	: The host and Webgate is inst https://example	port of the computer on which the Web server for the alled. For example, http://example_host:port or _host:port. The port number is optional.
Security	: Simple	
Protected Resource List	: for FCUBS	: /FCJNeoWeb
	For FCIS	: /FCISNeoWeb
User Defined Parameters	: filterOAMAuth	nCookie=false



Access Manager >						
reate Webgate se the following screen to regi	ister an OAM Agent. Before yo	u register, ensure that at least one OAI	M Server is running in t	he same mo	de as the Agent to	Apply be registered.
* Version	11g 💌		* Security) Open		
* Name	FlexcubeWebgate) Simple) Cert		
Description	Flexcube 11g Webgate	Enter the Base URLs for Agent	Virtual host			
Base URL	https://ofss220607.in.oracle. com	Ai	uto Create Policies 😱			
Access Client Password						
Host Identifier	FlexcubeWebgate					
	filterOAMAuthnCookie=false					
User Defined Parameters						
source Lists	an Lint	Add Delete Dublic	Perourse List		Add	Delete
Fibiected Resource	Je List	Fubic	Resource List			
Relative URI		Relati	ve URI			
I CONEDITED						
- excubeWebgate Webg	ate				Apply Download	
Confirmation OAM Webgate FlexcubeWebga	ate created successfully.				×	
Version 11g	3	Logout Tar	get URL			
Version 11g Name Fle	g excubeWebgate	Logout Tar Deny On Not P	rotected			
Version 11s Name Fle Description Fle	g excubeWebgate excube 11g Webgate	Logout Tar Deny On Not P	get URL	terVar=IS_ ^		
Version 11t Name Fle Description Fle Access Client Password * Security	g xxxubeWebgate xxube 11g Webgate Open	Logout Tar Deny On Not P User Defined Par	get URL rotected movestleas ssi uRLINUTR8Fo dient_request mpt=1 mpt=1	erVar=IS_ ^ rmat=true _retry_atte figPeriod=		
Version 11 Name Fle Description Fle Access Client Password * Security @	a axcubeWebgate axcube 11g Webgate Open Simple Cert	Logout Tar Deny On Not P User Defined Par * Sleep for (S	get URL rotected ameters ameters get URLINUTFRFor dient-request inactiveResson econds) 60 A	figPeriod=		
Version 11t Name Fle Description Fle Access Client Password * Security @ * State @	g excubeWebgate excube 11g Webgate Open Simple Cert Enable Disable	Logout Tar Deny On Not P User Defined Par * Sleep for (S Cache Pragma	get URL rotected ameters dient_request mpts=1 inscliveRecord Header no-cache	ierVar=IS_ ^ rmat=true retry_atte figPeriod= _;;		
Version 11; Name Fie Description Fie Access Client Password * Security © * State © * Max Cache Elements	a excubeWebgate excube 11g Webgate Open Simple Cert Enable Disable	Logout Tar Deny On Not P User Defined Par [*] Sleep for (S Cache Pragma Cache Control	get URL rootected ameters	terVar=IS_		

- 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	
Configuration Security Application Security Application Security Application Security	ration
Launch Pad SSO Agents x FlexcubeWebgate x	
Access Manager > FlexcubeWebgate Webgate Apply Down	oad
Version 11g Logout Target URL	
Name FlexcubeWebgate Deny On Not Protected 📝	
Description Flexcube 11g Webgate	
Access Client Password User Defined Parameters User De	
Security Open Image: Simple Sleep for (Seconds) Image: Open Image: Open	
* State Enable Cache Pragma Header no-cache Cache Control Header no-cache	

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

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

	🕞 Application Security 🔥 Federation 🔲 Mobile Security 🥳 Configuration
aunch Pad Server Instances x oam_server1 x	
Configuration > Dam_server1 OAM Server Instance	Duplicate Apply
Confirmation OAM Server instance cam_server1 modified successfully.	×
* Server Name oam_server1 * Port 14101 • •	* Host ofsa220807.in.oracle.con
* Proxy Server Id AccessServerConfigProxy * Port 5575 ^ ~ * Mode Open	
Coherence Configuration Log Level 3 Votable 9095 Votable	
* Log Limit 4096 A M	



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.

aunon au	Applicati	on Domain ×					
Access	Manager >	tion Domains	Domoin or olio	r the Create Application	Domain button to create a no		- Create Application Domain
⊿ Sea	rch	id an existing Application	Domain or circi		Somall Bullon to create a ne	w one.	
Nam	Results						Search Reset
Actions 👻	View 🗸	🕂 Create 🧪 Edit	💥 Delete	Detach			
	Name				Description		
Row							
Row Io data to d	display.						



	CLE	Access Management		Application Security	& Federation	Mobile Security	¢ c	onfigurati
aunch Pad	Application	Domain ×						C
Access Ma	anager >							
Search A	pplicatio	on Domains				+ Create A	Application	Domain
Jse the search	h tool to find	an existing Application Domain or click	k the Create Application	on Domain button to create a new	one.			
Searce	ch							
Name								
Name							Search	Reset
Name	sults					[Search	Reset
Name Search Res Actions • 1	esults View v	🕂 Create 🧪 Edit 💥 Delete	Detach			[Search	Reset
Name Search Res Actions v	view ↓ Name	🕂 Create 🖌 Edit 💥 Delete	Detach	Description		(Search	Reset
Name Search Res Actions - N Row 1	view ▼ Name FlexcubeW	+ Create / Edit X Delete	Detach	Description Application Domain created	through Remote Re	egistration	Search	Reset
Name Search Res Actions ▼ 1 Row 1 2	View View View View View View View View	+ Create / Edit X Delete	Detach	Description Application Domain created Policy objects enabling inte	through Remote Re gration with Oracle R	egistration =usion Applications	Search	Reset

3. Click on 'Authentication Polices'.

					weblogic 🔻 🚥
	Management	Application Security	Federation	Mobile Security	Configuration
aunch Pad Application Domain 🗙	FlexcubeWebgate ×				
Access Manager >					
lexcubeWebgate Application	on Domain				
pplication Domain provides a logical c	container for resources or sets of resources, and th	ne associated policies that dictat	te who can access	s specific protected reso	urces.
Summary Resources Authentica	ation Policies Authorization Policies Token Is:	suance Policies Administratio	n		
					Apply
* Name	FlexcubeWebgate				
	Application Domain created through Remote				
1	Registration				
Description					
* Session Idle Timeout (minutes)	0 0 ~				
Allow OAuth Token					
Allow Session Impersonation					

4. Click on 'Protected Resource Policy'.



aunch Pad	Application I	oomain 🗙 FlexcubeWebgate 🗙		[
Access N	lanager >			
lexcube	Webgate	Application Domain		
pplication De	omain provide	s a logical container for resources or sets of resource	and the associated policies that dictate who can access specific protected r	esources.
Summary	Resources	Authentication Policies Authorization Policies	en Issuance Policies Administration	
Select an ex	disting Authen	ication Policy from the list or click the Create Authentic	on Policy button to create a new one.	
Actions -	View 🔻	🕂 Create 🔿 Duplicate 🧪 Edit 🗙 Delete	Detach	
Row	Name		Description	
	1 Public Re	source Policy	Policy set during domain creation. Add resources to this policy to a	allow anyone access.

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

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

aunch Pad Appl	ication Domain \times FlexcubeWebgate \times	Flexcub	eWebgate : Protect ×				[
Access Manag	er >						
Protected Re	Source Policy Authentication Po	licy				Duplicate	Appl
uthentication Polic single policy can be	y defines the type of verification that must e defined to protect one or more resources	oe perform in the Appl	ed to provide a sufficient level of trust for Acc ication Domain.	ess Manager to g	grant access to the user ma	aking the reque	est. A
* Name	Protected Resource Policy		Success URL				
Policy set during domain creation. A		sources	Failure URL				
Description	to this policy to protect them.	Selectauthe	t the challenge mechanism required to nticate the user.				
* Authentication Scheme	LDAPScheme]					
Resources Re	AdaptiveAuthenticationScheme AnonymousScheme BasicFAScheme BasicScheme BasicSessionlessScheme ESSOProvAuthnScheme						
Resources	FAAdminLocalScheme FAAuthScheme						
Resource T	FederationMTScheme	-	Query String				
This Policy o	FlexcubeBasicOAMScheme FlexcubeFormOAMScheme FlexcubeKBAOAAMScheme						
	LDAPNoPasswordValidationScheme LDAPScheme OAAMAdvanced OAAMBasic						
oyright © 2000, 2015,	OAM10gScheme OAMAdminConsoleScheme						

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



Access Manag	er >			
Protoctod Dr			Duplic	ate App
uthentication Polic ingle policy can be	cy defines the type of verification that must be e defined to protect one or more resources in	y performed to provide a sufficient level of trust for Acces the Application Domain.	ss Manager to grant access to the user making the	request. A
* Name	Protected Resource Policy	Success URL		
Description	Policy set during domain creation. Add reso to this policy to protect them.	urces Failure URL		
* Authentication Scheme	FlexcubeBasicOAMScheme			
Resources	Advanced Rules			
Identity As:	sertion			
This will cause	an assertion to be generated for the user, or	tionally containing any Asserted Attribute set below.		
Responses	s 🕂 Add 💉 Edit 💥 Delete			

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

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

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

Click on Add button

Access Manag	er >		
Protected Re Authentication Polic	Authentication Policy Authentication Policy defines the type of verification that must b	y performed to provide a sufficient level of trust for Access Man	Duplicate Applicate Applic
single policy can be Name	e defined to protect one or more resources i Protected Resource Policy	the Application Domain. Add Response ×	
Description	Policy set during domain creation. Add res to this policy to protect them.	*Type Header Name DN Value	
* Authentication Scheme	FlexcubeBasicOAMScheme	\$user. <u>attr</u> .dn	
— Identity Asi	sertion an assertion to be generated for the user, o	Identity Assertion has not been enabled for this policy. Enable Identity, Assertion in order Add Cancel	
Responses Name	s + Add / Edit X Delete	Type Val	ue

8. Click on Apply to Save the Changes

e policy can be	e defined to protect one or more resources in t	he Application Domain.	
Confirmat	ion		>
uthentication F	Policy, Protected Resource Policy, modified su	ccessfully	
* Name	Protected Resource Policy	Success URL	
Description	Policy set during domain creation. Add resol to this policy to protect them.	Failure URL	
uthentication Scheme	FlexcubeBasicOAMScheme		
sources Re	sponses Advanced Rules		
Identity Ass	sertion		

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

aunch Pad	Application Domain × FlexcubeWebgate ×	a.
Access	Manager >	
lexcub	eWebgate Application Domain	
pplication C	Domain provides a logical container for resources or sets of	of resources, and the associated policies that dictate who can access specific protected resources.
Summarv	Resources Authentication Policies Authorization F	Policies Token Issuance Policies Administration
Summary	Resources Authentication Policies Authorization	Policies Administration
Summary Select an e	Resources Authentication Policies Authorization f existing Authorization Policy from the list or click the Create	Policies Token Issuance Policies Administration Authorization Policy button to create a new one.
Summary Select an e	Resources Authentication Policies Authorization I existing Authorization Policy from the list or click the Create	Policies Token Issuance Policies Administration Authorization Policy button to create a new one.
Summary Select an e Actions	Resources Authentication Policies Authorization F existing Authorization Policy from the list or click the Create View + Create Duplicate Edit Name	Policies Token Issuance Policies Administration Authorization Policy button to create a new one. Image: Comparison
Summary Select an e Actions	Resources Authentication Policies Authorization I existing Authorization Policy from the list or click the Create view + Create Duplicate Edit Name 1 Public Resource Policy	Delicies Token Issuance Policies Administration Authorization Policy button to create a new one. Delicies Detach Description Policy set during domain greation. Add resources to this policy to allow appone access
Summary Select an e Actions • Row	Resources Authentication Policies Authorization I existing Authorization Policy from the list or click the Create View + Create Duplicate Name 1 Public Resource Policy 2 Description Policy	Delete Image: Content delete Administration Authorization Policy button to create a new one. Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete Image: Content delete
Summary Select an e Actions	Name Duplicate Edit 1 Public Resource Policy 2	Policies Token Issuance Policies Administration Authorization Policy button to create a new one. Image: Comparison of the policy button to create a new one. X Delete Description Description Policy set during domain creation. Add resources to this policy to allow anyone access. Policy set during domain creation. Add resources to this policy to protect them.
Select an e Actions • Row	Name Public Resource Policy 1 Public Resource Policy	Policies Token Issuance Policies Administration Authorization Policy button to create a new one. Image: Comparison of the policy button to create a new one. Image: Comparison of the policy button to create a new one. Image: Comparison of the policy button to create a new one. Image: Comparison of the policy button to create a new one. Image: Comparison of the policy button to create a new one. Image: Comparison of the policy button to create a new one. Image: Comparison of the policy of the poli
Select an e Actions • Row	Resources Authentication Policies Authorization I existing Authorization Policy from the list or click the Create View View View Protected Resource Policy Protected Resource Policy	Delete Image: Delete Detech Description Policy set during domain creation. Add resources to this policy to allow anyone access. Policy set during domain creation. Add resources to this policy to protect them.

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



unch Pad Application Domain	× FlexcubeWebgate × Flexcube	Webgate : Protect ×			(
Access Manager >					
rotected Resource P	olicy Authorization Policy		E	Ouplicate	Apply
Identity Assertion					
Identity Assertion This will cause an assertion to Identity of the second se	b be generated for the user, optionally co	ontaining any Asserted Attribute set below.			
Identity Assertion This will cause an assertion to Responses Add Name	b be generated for the user, optionally or Call & Delete	ontaining any Asserted Attribute set below. Value			

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

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

Click on Add button

ch Pad Application Domain x FlexcubeWebgate	FlexcubeWebgate : Protect x	
Access Manager > Detected Resource Policy Authorization Policy and	Add Response X	Duplicate Apply
ititions apply to all resources within a specific Authorizati mmary Resources Conditions Rules Respon	* Type Header	ization rules and
Identity Assertion	* Name DN	
This will cause an assertion to be generated for the use	Suser.attr.gg	
Responses + Add / Edit X Delete		
Name This Policy does not have any Responses	this policy. Enable Identity Assertion in order	
ht © 2000, 2015, Oracle and/or its affiliates. All rights reserved		

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



	ess Management	a A	oplication Security	Federation	Mobile Security	Configuratio
unch Pad Application Domain	× FlexcubeWebgate ×	FlexcubeWebgate : Protect ×				
Access Manager > rotected Resource Po uthorization policy contains a set o inditions apply to all resources with	DIICY Authorization Polic of conditions that define why ithin a specific Authorizatior	2ý ether a user should be permitted or c i policy.	lenied access to the re	sources protected	d by the policy. Authorizati	Duplicate Apply
Confirmation Authorization Policy, Protected R	Resource Policy, modified s	uccessfully				×
Summary Resources Condi	tions Rules Respons	es				
Identity Assertion						
Identity Assertion This will cause an assertion to	be generated for the user,	optionally containing any Asserted At	tribute set below.			
Identity Assertion This will cause an assertion to Responses + Add	be generated for the user,	optionally containing any Asserted At	tribute set below.			
Identity Assertion This will cause an assertion to Responses + Add Name	be generated for the user,	optionally containing any Asserted At Type	tribute set below.			

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: 5575, 1	Up	Friday, January 11, 2013 16:18:27			

Cache Name	State	Max	Curr	Timeout	Cache Stats	Memory
		Elems	Elems	(seconds)	(Hits:Misses:	Footprint
					Expired:Flushed)	(bytes)
Resource to	active	100000	100	1800	6451:273:61:0	5 9 750
Authentication						
Scheme						
Authentication	active	25	1	1800	15012:34:33:0	802
Scheme						
Resource to	active	100000	100	1800	381:127:27:0	43200
Authorization						
Policy						
Authorization	active	1000	5	15	372:9:3:0	10845
Result						

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 _ ×
File Edit Test Help
🔁 🖯 🖉 👘
- Server Connection
IP Addr Port Max C *Age /
*Prim[ss220028.in.oracle.com] 5575 1 [FlexcubeWebdate]
Secon
Min C Timeou Mo Global Passp 1 30000 Si Connect
Protected Resource URI
Sche *H Port
https ▼ FlexcubeWebdate
Resour Operat Validate
l Iser Identity
IP Address *Username Password
Authenti
User Certifica
Authonze
- 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 OKL : https://orss220028.in.oracle.com:14101/oam/server
[1/11/13 5:34 PM][request][authenticate] yes
[1/11/13 5:34 PM][response] User DN : cn=SARAN,cn=users,dc=oracle,dc=com
[1/11/13 5:34 PM][response] SessionID : 6e531a7f-460d-4db8-b872-a7da77999282
[1/11/13 5:34 PM][response][action] OAN_IMPERSONATOR_USER_
[1/11/13 5·34 PM][request][authorize] ves
Elapsed (🕫 Capture Q Empty 🗟 🧳

2.7 First launch of FLEXCUBE after installation

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

2.7.1 Parameter Maintenance

2.7.1.1 Bank Parameter maintenance - UBS

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



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

2.7.1.2 Parameters Maintenance – IS

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

2.7.2 Maintaining LDAP DN for FLEXCUBE users

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

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

LDAP DN value should be entered as complete DN value.

eg.

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



For FLEXCUBE – UBS

🔶 User Maintenance			-
💾 Save			
User Details		User Status	Enabled
User Identification * Name *	FCUBSUSER		 Hold Disabled Locked
Language * Home Branch *	ENG =	Classification	Staff● Branch
Customer No Department Code		Status Changed On Last Signed On	2011-01-04
Department Description Tax Identifier		EL CM Lloor ID	Staff Customer Restriction Required
LDAP DN		ELCM User ID	Multi Branch Access
Amount Format	LDAP DN		Restricted Show Dashboards
Date Format	Auto Authorization		Alerts on Home
Supervisor Identification Supervisor Name	E		 F10 Access Required F11 Access Required F12 Access Required
User Password		Start Date	* 2011-01-04 🕎
Password Password Changed On Email Reference No	2012-01-04	End Date	
Invalid Logins		Screen Saver Details	
No of Cumulative Logins No of Successive Logins	17 0	Screensaver Interval (in seconds)	3600
Restricted Password Role	s Rights Functions Tills	Account Classes Genera	al Ledgers Limits Branches

For FLEXCUBE - IS

🔶 User Admin					_ >
🗄 Save					
User Details					
User Identification * Name * Externel Identifier LDAP DN Number Format	FCISUSER FCIS User cn=FCUSR,cn=Users,d(Language * Home Branch * Home Module *	ENG 000 FMG Ø Debug Window Enal	Classification	 Staff Auto End Of Day Customer
Modules	Investments Corporate	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	MM/DD/YYYY	Auto Auth Amount Format	No 💌 Dot Comma 💌		
Restricted Passwords	Roles Functions Bran	ches Module Disallo	wed Functions		
Input by Authorized by	D; D;	ateTime ateTime	Mod No Open Authorized		Ok Cancel



2.7.3 Launching FLEXCUBE

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

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

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



2.7.3.1 Basic Style Challenge by Webgate





2.7.3.2 Form Style Challenge by Webgate



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







First Time Login











🏉 Register - Windows Internet Explorer	And the second sec	
C v E https://ofss220223.in.oracle.com:14101/oam/pages/oaam/handleRegisterImagePhrase.jsp	🔹 😵 Certificate Error 🔛 🍫 🔀 Google	+ م
<u>File Edit View Favorites Tools H</u> elp		
X O McAfee X		
🖕 Favorites 🛛 👍 🙋 Web Slice Gallery 🕶		
C Register	🚵 🔻 🖾 👻 🖶 🖕 Page 🕶 Saf	ety▼ T <u>o</u> ols▼ @▼ [≫]
ORACLE		~
Access Manager		
Select Your Security Questions/Answers		
1) Where did you get your first pet?		
OFSS		
2) What is the name of the first musical group you saw in concert? -		
OFSS		
2) What as to use some first and 2		
4) What was the first name of your first boss? ▼		
OFSS		
5) Who is your favorite athlete?		
OFSS		
Continue		
Oracle Access Management Version: 11.1.2.2.0 Convribit © 1996.2013. Oracle and/or its affiliates. All rinhts reserved.		
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.		
		-
/oam/pages/oaam/handleRegisterQuestions.jsp	👊 Local intranet Protected Mode: Off	🖓 🔻 🔍 100% 🔻 .

Post First Login









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





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

2.7.4 Signoff in a SSO Situation

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

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





Oracle Access Manager Integration [April] [2017] Version 12.4.0.0.0

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

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

Copyright © [2007], [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.

