Oracle Access Manager Oracle FLEXCUBE Universal Banking Release 14.0.0.00 [February] [2018]



Table of Contents

2-1 2-1 2-1 2-1 2-1 2-2 2-2 2-2 2-2
2-1 2-1 2-1 2-2 2-2
2-1 2-1 2-2 2-2
2-1 2-1 2-2 2-2
2-1 2-2 2-2
2-2
2-2
2.2
3-1
3-1
3-1
3-1
3-17
3-17
3-17
3-18
3-19
3-20



1. Introduction

For the purpose of single sign-on FLEXCUBE UBS is qualified with Oracle Identity Management 11.1.2.2.0 (Fusion Middleware 11gR1) – specifically using the Access Manager component of Oracle Identity Management. This feature is available in the releases FC UBS V.UM 7.3.0.0.0.0 and onwards of FLEXCUBE UBS.

This document is expected to provide an understanding as to how single sign-on can be enabled for a FLEXCUBE UBS deployment using Oracle Fusion Middleware 11g.

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



2. Background and Prerequisites

2.1 <u>Pre-Requisites</u>

The following are the pre-requisites for Oracle Access Manager (OAM) and LDAP Directory Server.

2.1.1 Software Requirements

- 1. Oracle Access Manager OAM (11.1.2.2.0)
 - Access Server
 - Webtier Utilities 11.1.1.7.0
 - Web Gate 11.1.2.2.0
 - Http Server
- 2. LDAP Directory Server

Please make sure that the LDAP which is been used for FLEXCUBE Single Signon 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):

- Oracle Internet Directory
- Active Directory
- ADAM
- ADSI
- Data Anywhere (Oracle Virtual Directory)
- IBM Directory Server
- NDS
- Sun Directory Server
- 3. Web Logic(10.3.5)

For the purpose of achieving single sign on for FCUBS in FMW 11gR1, it is necessary for the weblogic instance to have an explicit Oracle HTTP server (OHS).

2.2 Background of SSO related components

2.2.1 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.

2.2.2 LDAP Directory Server

To integrate FLEXCUBE with OAM to achieve Single Sign-on feature, FLEXCUBE's password policy management, like password syntax and password7 expiry parameters can 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.

2.2.3 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.

2.2.4 Identity Asserter

Identity Asserter uses Oracle Access Manager Authentication services and also validates alreadyauthenticated Oracle Access Manager Users through the ObSSOCookie and creates a WebLogicauthenticated session. It also provides single sign-on between WebGates and portals. We can get more details on Identity asserter <u>HERE</u>

This document containts the configuration of Oracle Interner Directory as LDAP server and its configuration in weblogic. This document will not discuss the configuring and setting up of OAM and LDAP directory server of other LDAP servers. This will be provided by the corresponding Software provider.



3. Configuration

3.1 Pre-Requisites

The steps provided below assume that FLEXCUBE has already been deployed and is working (without single sign-on)

The provided below steps assume that Oracle Access Manager and the LDAP server have been installed already and the requisite setup already done with respect to connecting the two along Weblogic's Identity Asserter.

3.2 Change the web.xml file

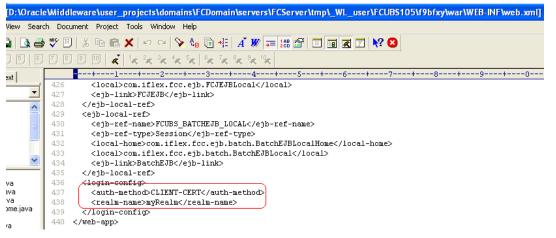
- 1. Locate the web.xml file in the application (FCUBS) EAR file
- 2. Add the following lines under login-config.

<login-config>

<auth-method>CLIENT-CERT</auth-method>

<realm-name>myRealm</realm-name>

</login-config>



3. Save the file and redeploy and restart the application.

3.3 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/E17904_01/install.1111/e12002/webgate004.htm



1. Identity Store Creation

To create new User Identity Store, Login to OAM Console and navigate to System Configuration>>Common configuration>>Data Sources>> User Identity Store.

2. Input below information in the User Identity Store.

Choose Store Type as Oracle Internet Directory.

Location:

LDAP server Host name and Port Number in <HOSTNAME>:PORT format

Bind DN:

User name to connect the LDAP Server

Password:

Password to connect the LDAP Server

User Name Attribute:

The attribute created in LDAP, which will be the User Name for the other application (here it will be treated as the FCUBS Username)

User Search Base:

The container of the User Name in the LDAP server.

Group Search Base:

The container of the Group Name in the LDAP server.



Firefox Oracle Access Manager - Administra	L × C Error 404Not Found × +	~ — 6 ×
iflchw-ap-21:7001/oamconsole/faces/pages/Pc	licyManager,jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop=10370372111194 😭 🔻 C 🚼 - oam agent 11g base url	ب 🖋 دی
ORACLE [®] Access Manager		Accessibility Help Sign Out O
Policy Configuration System Configuration		
Common Configuration	Velcome FCUB5Webgate 0AM Agents oam_server1 LDAP User Identity Stores Create: User Identity Store	Test Connection Apply (?)
Actions + View + P ≥ 26 400 V Data Sources V & User Identity Stores > @ User Identity Store1 > ⊇P Plugns ↓ Access Manager Settings	* Store Type OID: Oracle Internet Directory Type OID: Oracle Internet Directory Type OID: Oracle Internet Directory Type	.::
Actions - View - 📴 🗁 💥 🕅	⊻ Location and Credentials	
> & Access Manager Settings ▽ & SSO Agents > & OAM Agents > & OSO Agents	*Location ifchw-ap-21:3061 *Bind DN cn=ordadmin : *Password	
✓ M Luthentication module I Luthentication module I Luthentication module I Luthentication module I Retreme Authentication module	Users and Groups * User Name Attributs ud * User Search Base cn=Users,dc=orade,dc=com User Fitter Object Classes Group Name Attributs * Group Search Base cn=Groups,dc=orade,dc=com Group Fitter Classes Group Cache Size (Mb) 10000 @ Group Cache Size (Mb) 10000 @ Group Cache Size (Mb) 10000 @ Maximum Pool Size 10 @ Maximum Pool Size 10 @ Maximum Pool Size 10 @ Results time limit (seconds) 0 @ Retry Count 3 @ Maximum Pool Size 10 @ Maximum Pool Size 10 @ Maximum Pool Size 10 @ Retry Count 3 @ Referral Policy follow ♥ Inactivity Timeout (seconds) ①	
≥ Security Token Service	<u>.</u>	

3. After input of the above information click on Apply button. On Successful creation, click test connection button to verify whether the LDAP connection is working fine.



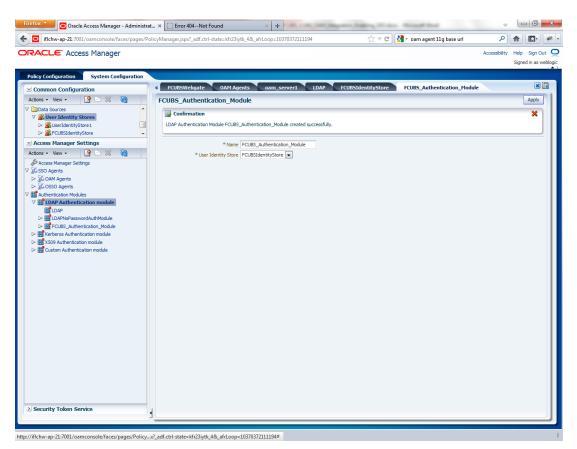
Firefox Oracle Access Manager - Administrat	× C Error 404Not Found × +	a second line		\bigtriangledown	_ 0	×
(iflchw-ap-21:7001/oamconsole/faces/pages/Po	icyManager.jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop=10370372111194	☆ ▼	C 👌 ar agent 11g base url	٩	ft 🗗	# •
ORACLE Access Manager				Accessibility	Help Sign C Signed in as r	
Policy Configuration System Configuration						
✓ Common Configuration	Welcome FCUBSWebgate OAM Agents oam_se	rver1 LDAP	FCUBSIdentityStore			
Actions - View - 📑 🗁 💥 🚮	FCUBSIdentityStore			Test Connection	Apply	3
♥ Data Sources	Confirmation			ection Status 🕅	×	11
▽ Loser Identity Stores ▷ LoserIdentityStore 1 ▷ LoserIdentityStore ↓	User Identity Store FCUBSIdentityStore created successfully.		Iden	nection to the User tity Store essful!		
Access Manager Settings	Store Name FCUBSIdentityStore	Description		OK Cancel		-11
Actions 🕶 View 👻 🔄 🔀	* Store Type OID: Oracle Internet Directory	×	_			
 ▷ Access Manager Settings ▽ SSO Agents ▷ SO Add Agents 			Enable SSL			.::
> 🕅 OSSO Agents	✓ Location and Credentials					
☑ ∰ Authentication Modules ☑ ∰ LDAP Authentication module	* Location iffchw-ap-21:3061		* Bind DN cn=orcladmin			
EDAP Authentication module EDAP LDAP LDAPNoPasswordAuthModule			*Password			
ECAPHOPASSWOTAAUMINOULE	✓ Default and System Store Options					
> # X509 Authentication module	Set as default store (Current Default Store UserIdentityStore1)					
Custom Authentication module	Set as system store (Current System Store UserIdentityStore1)					
	⊻ Users and Groups					
	* User Name Attribute uid					
	* User Search Base cn=Users,dc=orade,	dc=com				
	User Filter Object Classes Group Name Attribute					
	* Group Search Base cn=Groups,dc=orade	de=com				
	Group Filter Classes	Juc - com				
	Enable Group Cache					
	Group Cache Size (Mb) 10000					
	Group Cache TTL (Seconds)					
	✓ Connection Details					
	Minimum Pool Size 10	Re	sults time limit (seconds) 0			
	Maximum Pool Size 50 🛒		Retry Count 3 🚔			
	Wait Timeout (seconds) 120		Referral Policy follow 💌			
≥ Security Token Service	Inactivity Timeout (seconds)					
					_	

4. Creating Authentication Module

Navigate to System Configuration >> Access Manager Settings >> Authentication Modules >> LDAP Authentication Module.

Click New Button to create new Authentication Module. Input the Name of the authentication module and choose the User Identity Store we created in step 1.





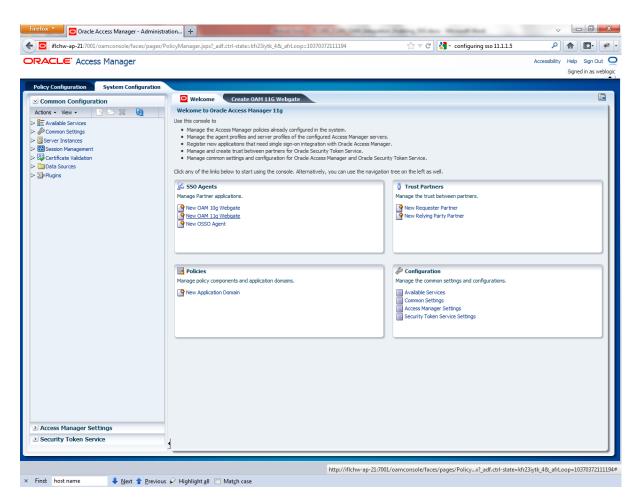
5. Creating OAM 11g Webgate

Navigate to System Configuration>>Access Manager Settings>>SSo Agents>>OAM Agents.

Click on Create 11g webgate button

or Click on New OAM 11g Webgate link available in welcome page.





Enter any name for Webgate and Base URL (The host and port of the computer on which the Web server for the Webgate is installed) and click on apply.



iflchw-ap-21:7001/oamconsole/faces/pages/Po	licyManager.jspx?_adf.ctrl-state=kfr23iytk_	4&_afrLoop=10370372111194	☆ マ C 🚼 - configuring sso 11.1.1.5	۴ 🗈 ۴
RACLE [®] Access Manager				Accessibility Help Sign Out Signed in as webl
Policy Configuration System Configuration				
✓ Common Configuration	• Welcome Create 0AM 11G	Webgate		× 🕱
Actions • View • 📑 🗁 💥 🔯	Create OAM 11g Webgate			Apply
E Avalable Services	Version 11g *Name FCUBS: Base UR: http:// Access Clent Password *Security @ Oper © Simp © Cert Host Identifier Resource List Relative URI //*	lfkhw+ap-21:7001 n ke	User Defined Parameters	
Access Manager Settings Security Token Service				

Once the OAM 11g Webgate created, add filterOAMAuthnCookie=false parameter along with default parameters in User Defined Parameters.

Click apply button to save the changes.



	st × OTN Discussion Forums : Responses i × OInt			
			Accessibility	
Policy Configuration System Configuration				
Common Configuration	Welcome OAM Agents FCUBSWebgate	e		×
Actions 🕶 View 👻 🔄 🖄 🔂	FCUBSWebgate			Apply
Available Services	Confirmation			×
Server Instances	OAM 11g Webgate FCUBSWebgate modified successfully. A	Application Domain is FCUBSWebgate		
Access Manager Settings	Name FCUBSWebgate	Logout Callback URL	/oam_logout_success	
tions 🗸 View 🖌 📑 🗁 💥 🔞	Access Client Password		https://10.180.196.158:14101/oan	
Access Manager Settings	* Security Open	Logout Target URL		
SSU Agents	Simple Cert	User Defined Parameters	proxySSLHeaderVar=IS_SSL	
SSO Agents	* State Enable		URLINUTF8Format=true client_request_retry_attempts=1	
Authentication Modules	Disable		inactiveReconfigPeriod=10	
	* Max Cache Elements 100000		filterOAMAuthnCookie=false	
	* Cache Timeout (Seconds) 1800 💂	* Sleep for	60 🖨	
	* Token Validity Period (Seconds) 3600 🚔	Cache Pragma Header		
	* Max Connections 1	Cache Control Header		
	* Max Session Time 3600 🚔	Debug		=
	* Failover Threshold 1	IP Validation		
	* AAA Timeout Threshold -1 🚔	Deny On Not Protected		
	* Preferred Host FCUBSWebgate	Allow Management Operations		
	Logout URL			
	Server Lists			
	Primary Server List 🕹 🛟	Secondary Server List	- ×	
	Server Name Host Name Host Port Max Numb	Server Name Host Name Host Port Max I	Number	
	oam_server infdrw-ap-21 5575	1		
Security Token Service				-
-	1			
	✓ Hichlight all ■ Match case ● Phrase not found			

6. Post OAM Webgate 11g Creation Steps

Perform the following steps to copy the artifacts to the Webgate installation directory:

• On the Oracle Access Manager Console host, locate the updated OAM Agent ObAccessClient.xml configuration file (and any certificate artifacts). For example:

\$DOMAIN_HOME/output/\$Agent_Name/ObAccessClient.xml

• On the OAM Agent host, copy artifacts (to the following Webgate directory path). For example:

11gWebgate_instance_dir/webgate/config/ObAccessClient.xml (for instance WebTier_Middleware_Home/Oracle_WT1/instances/instance1/config/ OHS/ohs1/webgate/config/ObAccessClient.xml)

7. Creating Authentication Scheme



To create Authentication Scheme navigate to Policy Configuration >> Authentication Schemes

Click on Create button to create new Authentication Scheme.

Name: Any name to identify Authentication SchemeChallenge Method: BASICChallenge Redirect URL: /oam/server

Authentication Module : Choose the authentication module created in step 2.

Firefox To Oracle Access Manager - Administr	rat × 🖸 Integrating OAM Security Provider wi × 🕂	
(iflchw-ap-21:7001/oamconsole/faces/pages/F	PolicyManager.jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop=10370372111194	☆ マ C 👌 authentication schema oam 11g 🛛 👂 🍙 💽 🖋 🔹
ORACLE [®] Access Manager		Accessibility Help Sign Out Q Signed in as weblogic
Policy Configuration System Configuration		
All	Welcome Bround FCUBS_Auth_Scheme	× 🖹
Search	Authentication Schemes	Set As Default Apply
Browse Search View ▼	Confirmation Authentication Scheme, FCUBS_Auth_Scheme, created successfully	×
▼	* Name FCU85 Auth_Scheme Description * Authentication Level 1 * Challenge Method [ASIC • * Challenge Redrect URI / Nam/server * Authentication Module FCU85 Authentication Module • Challenge Parameters	

If it is a basic authentication scheme, we need to add the 'enforce-valid-basic-auth-credentials' tag to the config.xml file located under /user_projects/domains/<MyDomain>/config/. The tag must be inserted within the <security-configuration> tag as follows: [Just before the end of security configuration tag]

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

</security-configuration>

8. Creating Authentication Scheme

To create authentication policy, navigate to Policy Configuration >> Application Domains >> [Webgate agent name] >> Authentication Policies.

Click new button and input the below information

Name: Enter any name to identify the Authentication Policy (eg. FCUBSWebPolicy)

Authentication Scheme: Choose the authentication scheme created in step 5.

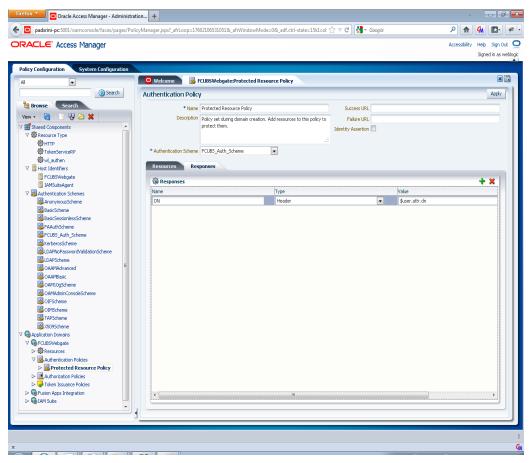
Resources:

Add the resources which are all need to be protected. If <WebgateName>:/.../ and <WebgateName>:/ are added in the resources then all the sources are protected.

	PolicyManager,jspx2_afrLoop=3227950810488558_afrWindowMode=08_adf.ctrl-state=sail189q1_ 🏫 🛡 C 🛛 🚷 - Goog	
ACLE' Access Manager		Accessibility Help Sign Ou Signed in as we
cy Configuration System Configuration		
	😐 Welcome 🛛 👼 Create Authentication Policy	X (
Search	Authentication Policy	Apply
Browse Search	* Name FCUBSWebPolicy Success URL	
w - 🔞 🕒 🖳 🛏	Description Failure URL	
Shared Components	Identity Assertion	
Resource Type		
袋 HTTP 袋 TokenServiceRP	* Authentication Scheme FCUBS_Auth_Scheme	
🔅 wl_authen		
/ Bost Identifiers	Resources Responses	
FCUBSWebgate		
IAMSuiteAgent	🔅 Resources	+ ×,
Authentication Schemes	Main	
AnonymousScheme	FCUBSWebgate://*	
BasicSessionlessScheme	FCUBSWebgate:/	
FAAuthScheme		
BFCUBS_Auth_Scheme		
KerberosScheme		
LDAPNoPasswordValidationScheme		
CAAMAdvanced		
OAAMBasic		
OAM 10gScheme		
CAMAdminConsoleScheme		
CIFScheme		
OIMScheme		
APScheme		
Application Domains		
G FCUBSWebgate		
▷ \$\$ Resources		
V Authentication Policies		
Protected Resource Policy		
Authorization Policies		
Generation		
 GIAM Suite 		
	L	
	1	

Add DN in the Responses section. Enter the value as *\$user.attr.dn.* The responses maintained in the tab will be added in the response header during the authentication.



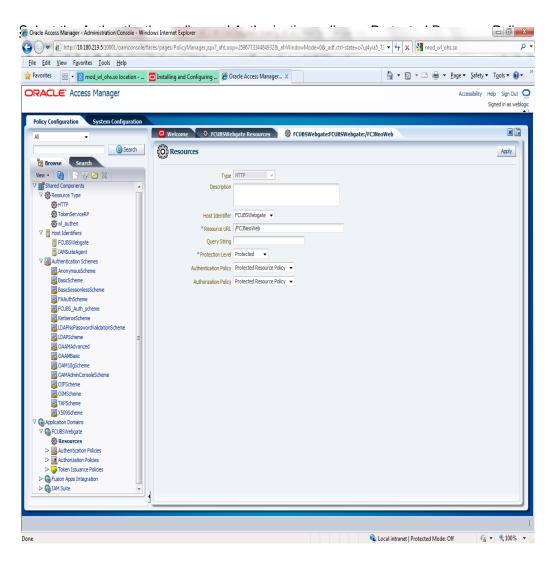


9. Adding Resources

Navigate to Policy Configuration >>Application Domains >>FCUBSWebgate >>Resources .

- Click on Create New Resource button .
- Select the type as HTTP.
- Select the Host Identifier as FCUBSWebgate
- Enter the resource URL as /FCJNeoWeb
- Select the protection level as Protected
- Click on apply button to update the resource added.

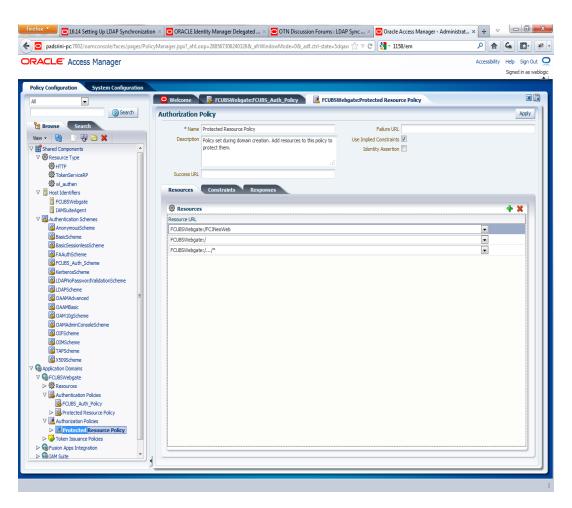




10. Adding Authorization Policy

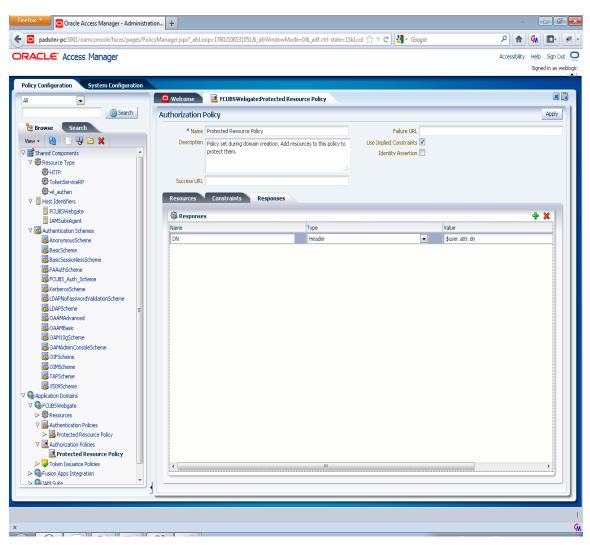
Check whether the resources available in the authentication policies are available in Authorization Policy. During web gate creation these values are defaulted.





Add DN in the Responses section. Enter the value as *\$user.attr.dn*. The responses maintained in the tab will be added in the response header during the authorization.





11. Configuring mod_wl_ohs for Oracle Weblogic server Clusters

To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server Clusters, add the directive shown below to the mod_wl_ohs.sh file available in <Weblogic Home> /Oracle_WT1/instances/instance1/config/OHS/ohs1.

<Location /console>

SetHandler weblogic-handler

WebLogicHost idmhost1.mycompany.com

WeblogicPort 7001

</Location>

12. Checking the Webgate 11g Agent Creation



After configuration of webgate 11g agent launch the URL

<u>http://<hostname>:<ohs_Port>/ohs/modules/webgate.cgi?progid=1</u> to verify whether the webgate configuration is fine. If the URL launches a screen as below then the webgate configuration is working fine.

Access		nection	Create	d		ectory
Server padsrini-pc 5575, 1			Monda <u>y</u> August 27, 201 11:08:0	y, 2	ory Threads Infor	mation
Cache Name	State			Timeout (seconds)		Memory Footprin (bytes)
Resource to Authentication Scheme		100000	60	1800	13979:416:139:1	33688
Authentication Scheme	active	25	1	1800	45629:140:138:1	710
Resource to Authorization Policy	active	100000	59	1800	183:59:0:1	25488
Authorization Result	active	1000	3	15	178:5:4:1	6507

13. 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		X
<u>File Edit Test H</u> elp		
🖻 🗟 🥔 🏦		
Server Connection		
IP Address Port Max Conn *Agent ID		
*Primary: padsrini-pc 5575 1 FCUBSWebgate Agent Password		
Secondary: 0 1	?	
Min Conn Timeout (ms) Mode 1 30000 open Image: Control open	Connect	
Protected Resource URI	4	
Scheme *Host Port		
http FCUBSWebgate 0	Get Auth Sche	me
Resource Operation	Validate	
User Certificate Store	Authenticate	
Status Messages		
[8/27/12 11:17 AM][response] Redirect URL : https://padsrini-pc:14101/oam/server		
[8/27/12 11:17 AM][response] Credentials expected : 0x1 (basic) [8/27/12 11:17 AM][request][authenticate] yes		
[8/27/12 11:17 AM][response] User DN : on=SARAN,on=users,do=oracle,do=com		
[8/27/12 11:17 AM][response] SessionID : 965396ea-751d-456c-ac60-90f07cf6de08 [8/27/12 11:17 AM][response][action] DN : cn=SARAN,cn=users,dc=oracle,dc=com		
[8/27/12 11:17 AM][response][action] OAM_IMPERSONATOR_USER :		E
[8/27/12 11:17 AM][request][authorize] yes [8/27/12 11:17 AM][response][action] DN : cn=SARAN,cn=users,dc=oracle,dc=com		-
[8/27/12 11:17 AM][response][action] OAM_IMPERSONATOR_USER : [8/27/12 11:17 AM][response][action] OAM_REMOTE_USER : SARAN		
[8/27/12 11:17 AM][response][action] OAM_IDENTITY_DOMAIN : FCUBSIdentityStore		_
Elapsed (ms): 47 Capture Queue: Empty		4



3.4 First launch of FLEXCUBE after Installation

After installing FLEXCUBE and while launching it for first time, the normal FCUBS login screen with userid and password will appear, this is because when installing the 'sso installed' parameter will be set to 'N'.

3.4.1 Bank Parameter Maintenance

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

Bank Parameters Ma	aintenance		_ ×
Bank	Code * 000	Customer Name	BANK FUTURA
Head Office Branch	Code * 000	Description	BANK FUTURA
Financial Preferences	General Preferences		
		 Year End Profit and Loss General Ledger * Transaction Code * General Ledger Purge Days 	
Inter Pay Lead Cheque Numbering Deta Sc		Checksum Algorithm	Number SSO Enabled Lodgment Numbers Unique For Branch
TRS Details		Suspense Account	.
Account Mask Prefere	ences Fields		
Input ByLC32702 Date Time 2012-02-		Number	2 ✓ Authorized ✓ Open Ok Exit

3.4.2 SSO Parameters

After enabling SSO, the parameters required for SSO should be maintained. Go to "Security Maintenance -> Sys. Administration -> SSO Maintenance". Provide all the details like Directory Server host name, Port number, LDAP admin Userid , admin Password, LDAP base and Login time out duration (in Sec).



🔶 Single Sign On Maintenance	;					_ ×
LDAP Host*	padsrini-pc					
LDAP Port *	3060					
LDAP Admin Id *	cn=orcladmin					
LDAP Password *	•••••					
LDAP Base *	cn=Users,dc=oracle,dc=c					
	om .::					
Time Out Duration(Seconds) *						
Fields			_		_	
Input BySARAN	Authorized By SAF		Modification Number	1	Authorized	Exit
Date Time 2012-01-06 12:3	3:04 Date Time 201	2-01-06 12:33:04			Open	LAIL

3.4.3 Maintaining Branch Level DN Template (Branch Maintenance)

Go to the "Branch Maintenance" of FLEXCUBE UBS.

For each branch LDAP DN template should be maintained, which is used in the FLEXCUBE user maintenance Form to populate corresponding LDAP userid automatically from this template. Go to branch level parameter screen and Click on Preferences Icon.

E.g.: LDAP DN Template: cn=<FCJUSR>,cn=Users,dc=i-flex,dc=com

Here in this above template **cn=<FCJUSR>** part preferably must be there and it should not be altered, but the rest of the DN name can change based on the configuration.



Branch Parameters Prefere	ences		
Netting Suspense General	233200804	Profit and Loss Adjustment	
Ledger			Track Previous Year Profit
Walk In Customer			And Loss Adjustment
Internal Swap Customer	000003171	Revaluation Split Details	
Clearing Account		•	Revaluation Split Required
Offset Clearing Account			Revaluation Split Required
Weekly Holiday 1	Saturday 👻	Suspense Product Maintena	ance
Weekly Holiday 2	Sunday 🚽	Debit Produ	ct
Clearing Bank Code		Descriptio	n
MIS Group For Currency		Credit Produ	
	Interdict Validation Required	Descriptio	on
Interdict Timeout Interval		International Banking Accou	unt Number Masks
Status Processing Basis	Contract Level 🚽	Bank Cod	le aaaann
Provisioning Frequency	Daily 👻	Account Numb	er aann
Uncollected Funds Basis	L		
Uncollected Funds	-	FGL Integration	
	Deferred Statement		FGL Handoff Required
	Generation	ELCM Integration	
Minor (an Limit (Vro)	Enterprise General Ledger		ELCM Replication
Minor Age Limit (Yrs)			ELOW Replication
Notification Days			
Cheque Stale Days			
Limit Expiry Advice Notification Days			
Back Value Details		LDAP DN Template	
	Parts Value of Obacili		te cn= <fccusr>,cn=User</fccusr>
	Back Valued Check Required	LDAP DN Templa	s,dc=oracle,dc=com
Back Value Days			
CY Message Preferences			
			Ok Exi

3.4.4 Maintaining LDAP DN for FCUBS Users

For each user id in FCUBS 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.



Vser Maintenance												_ ×
User Details							User	Status	Enable	led		
User Identifi	cation *	FCUBSU	JSER						⊖Hold			
	Name *	FCUBS	User						Olisab	oled		
User Refe	erence								Clocke	ed		
Lan	quage *	ENG					Classif	ication	Staff			
Home B	 Branch *	004					Status Chang	od On	Brand	'n		
Custom	ner No					`	Last Sign					
Department	Code						Last olyn	ieu Oli	Ctoff	f Customer F	Postriction	
Department Desc	ription									uired	Nesulcuon	
Tax Ide	entifier						ELCM U	Iser ID				
LD/	AP DN	FCUBSU	JSER						Multi	i Branch Acc	ess	
Time	Level *	9										
Amount F	ormat	-										
Date F	ormat		-									
		Auto	Authorizatio	n								
		Validate										
			-									
User Password						Start Date * 2012-01-06						
Password •••••		•••••					En	d Date				
Password Changed On 2012		2012-01	012-01-06 11:01:33									
	Email											
Invalid Logins												
Cum	ulative											
Succe	essive											
Restricted Password	Roles	Rights	Functions	Tills	Account	Classes	General Le	dgers	Limits	Branches	Products	
Disallowed Functions	Users	Holiday	Fields G	roup Re	striction	Centraliz	ed Role					
Maker KANNAN1 Date Time: 2012-01-06 13:29:56 Mod No 3												
Checker SARAN Date Time: 2012-01-06 13:34:26 Record Status Closed				Exit								
							Aut	horizati	on Status	Authorized		

3.4.5 Launching FLEXCUBE

After setting up FLEXCUBE to work on Single Sign on mode, navigate to the interim servlet URL from your browser.

For e.g.: http://<hostname>:[port]/FCJNeoWeb

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



Firefox Connecting	+ The Roll and the second string to an an at the	▽ □ □ \ \
padsrini-pc:7778/FCJNeoWeb	⊽ 🗙 🔤 Google	P 🚖 Cm 🖭 🥐 ·

Authentication Required						
0	A username and password are being requested by https://padsrini-pc:14101. The site says: "OAM 11g"					
User Name:	SARAN					
Password:	••••••					
	OK Cancel					



Once the user is authenticated and authorized to access the resource, the servlet gets redirected to normal FLEXCUBE application server URL and now the new signon form will appear as below. The application will automatically redirect FLEXCUBE home page.



Oracle FLEXCUBE UBS11.4Login - Mozilla Firefox	Temperature and the State of Street, S	
] padsrini-pc:7778/FCJNeoWeb/LoginServlet		☆ (
	ORACLE FLEXCUBE Universal Banking	
	Theme Default	
	Detault	
	ORACLE	
	Copyright © 2010, Oracle and/or its affiliates. All rights reserved.	

3.4.6 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 [February] [2018] Version 14.0.0.00

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 https://www.oracle.com/industries/financial-services/index.html

Copyright © [2007], [2018], 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.