Oracle Access Manager Oracle Banking ELCM Release 14.4.0.0.0 [Apr] [2020]



Table of Contents

1.	. INTE	RODUCTION	1-1
2.	BACK	GROUND AND PREREQUISITES	2-1
		E-REQUISITES	
	2.1.1	Software Requirements	2-1
	2.2 BA	CKGROUND OF SSO RELATED COMPONENTS	
	2.2.1	Oracle Access Manager (OAM)	
	2.2.2	LDAP Directory Server	
	2.2.3	WebGate/AccessGate	
	2.2.4	Identity Asserter	2-2
3.	CON	FIGURATION	3-1
	3.1 PR	E-REQUISITES	3-1
	3.2 CH	IANGE THE WEB.XML FILE	3-1
	3.3 Co	NFIGURING SSO IN OAM CONSOLE	3-1
	3.4 Fif	RST LAUNCH OF FLEXCUBE AFTER INSTALLATION	
	3.4.1	Bank Parameter Maintenance	
	3.4.2	SSO Parameters	
	3.4.3	Maintaining Branch Level DN Template (Branch Maintenance)	3-18
	3.4.4	Maintaining LDAP DN for FCUBS Users	
	3.4.5	Launching FLEXCUBE	3-20
	3.4.6	Signoff in a SSO Situation	3-22



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

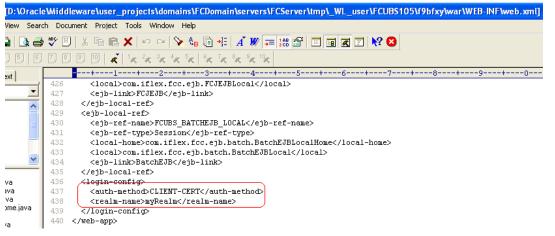
- 1. Locate the web.xml file in the application (FCUBS) EAR file
- 2. Add the following lines under login-config.

<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 (<u>http://docs.oracle.com/cd/E17904_01/install.1111/e12002/webgate004.htm</u>

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 - Administration	t × 🗍 Error 404Not Found × 🗍	+ barry til den bis-os	all these		▽ □ □ ×
iflchw-ap-21:7001/oamconsole/faces/pages/Po	licyManager.jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop=1	10370372111194	☆ ⊽ C 🚼 -	oam agent 11g base url	₽ 🟦 📴 🤗 י
ORACLE [®] Access Manager					Accessibility Help Sign Out Q Signed in as weblogic
Policy Configuration System Configuration					
Common Configuration	Welcome FCUBSWebgate OAM Ag	gents oam_server1	LDAP User Identit	-	
Actors - View - Data Sources V 20 Data Sources V 20 User Identity Stores > 20 User Identity Store 1 > 20 Plugns ✓ Access Manager Settings	Create: User Identity Store * Store Name FCUBSIdentityStore * Store Type OID: Oracle Internet Director	y 💌	Description	les	t Connection Apply (2)
Actions - View -	✓ Location and Credentials				
 ▷ Access Manager Settings ▽ SSO Agents ▷ SSO Agents 	*Location iffdhw-ap-21:3061	.:		I cn=orcladmin	
▷ SSO Agents ♥ # Authentication Modules	⊻ Users and Groups				
♥ ■ DAP Authentication module ■ ■ DAPNoPasswordAuthModule > ■ CDAPNoPasswordAuthModule > ■ Kenberos Authentication module > ■ Koson Authentication module > ■ Custom Authentication module	User Filter Object Classes Group Name Attribute	cn=Users,dc=orade,dc=com cn=Groups,dc=orade,dc=com		(seconds) 0 m try Count 3 m rral Policy follow ▼	
≥ Security Token Service					
	x2 adf.ctrl-state=kfr23ivtk 4& afrl oop=103703721111947				

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.



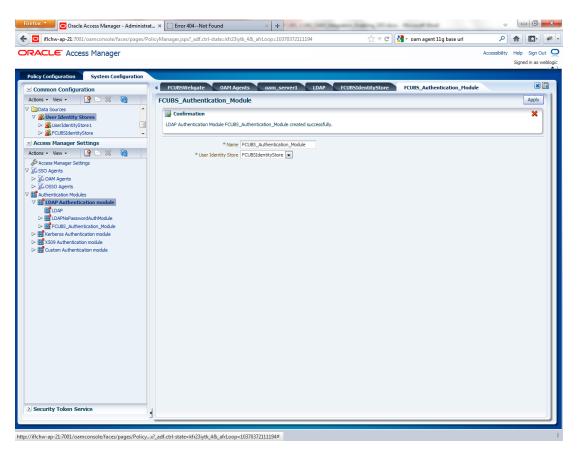
Firefox Oracle Access Manager - Administra	× C Error 404Not Found × +	▽ □ □ ►
(iflchw-ap-21:7001/oamconsole/faces/pages/Po	licyManager.jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop=10370372111194	🏠 マ C 🚼 マ oam agent 11g base url 🛛 🔎 🏫 💽 🦗
ORACLE [®] Access Manager		Accessibility Help Sign Out (Signed in as weblo
Policy Configuration System Configuration		
Common Configuration	Welcome FCUBSWebgate OAM Agents oam_server	
Actions - View - 📑 🗁 💥 🔂	FCUBSIdentityStore	Test Connection Apply (3)
 ✓ □Data Sources ✓ Super Identity Stores 	Confirmation	Connection Status 🕅 💥
Sover Identity Stores Sover Identity Store 1 Sover Identity Store	User Identity Store FCUBSIdentityStore created successfully.	Connection to the User Identity Store successful
Settings	Store Name FCUBSIdentityStore	Description OK Cancel
Actions 🗸 View 🖌 🔄 🗁 💥 🔞	* Store Type OID: Oracle Internet Directory	
▷		.::
▷ M Agents ▷ SSO Agents	✓Location and Credentials	
V H Authentication Modules	* Location iffchw-ap-21:3061	* Bind DN cn=orcladmin
IDAP Authentication module IDAP		Password •••••
▷ # LDAPNoPasswordAuthModule		
 Kerberos Authentication module X509 Authentication module 	Default and System Store Options Set as default store (Current Default Store UserIdentityStore 1)	
Custom Authentication module	Set as system store (Current System Store UserIdentityStore1)	
	⊻ Users and Groups	
	* User Name Attribute uid	
	* User Search Base on=Users,dc=orade,dc=co	com
	User Filter Object Classes	
	Group Name Attribute	
	* Group Search Base cn=Groups,dc=orade,dc=	=com
	Group Filter Classes	
	Enable Group Cache	
	Group Cache Size (Mb) 10000	
	Group Cache TTL (Seconds) 0	
	✓ Connection Details	
	Minimum Pool Size 10 🖤	Results time limit (seconds)
	Maximum Pool Size 50 🚔	Retry Count 3 🚔
	Wait Timeout (seconds) 120	Referral Policy follow 💌
Security Token Service	Inactivity Timeout (seconds) 0	

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.





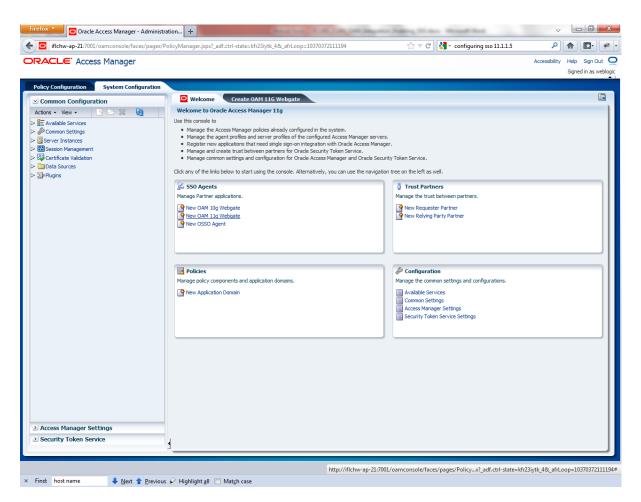
5. Creating OAM 11g Webgate

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.



inent up Exister ; builteonsole, races, pages, r	PolicyManager.jspx?_adf.ctrl-state=kfr23iytk_4&_afrLoop	=10370372111194 ☆ 🗸 🧟 🗸 configuring sso 11.1.1.5	P ★ ■
RACLE [®] Access Manager			Accessibility Help Sign Out Signed in as web
Policy Configuration System Configuration			
Common Configuration	• Welcome Create 0AM 11G Webgate		×
Actions 🗸 View 🖌 📑 🗁 💥 🔯	Create OAM 11g Webgate		Apply
E Avalable Services ∲ Common Settings ⊡ Serve Instances I Serve Instances I Serve Instances ⊡ Data Sources ⊇ Plugins	Version 11g *Name FCUBS/Vebgate Base URL http://fichw-op-21: Access Client Password *Security @ Open Smple Cert Host Identifier Resource List Relative URI //* /	Public Resource List	
2 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.



	× OTN Discussion Forums : Responses i × OIntroduct	•		
RACLE [®] Access Manager			Accessibility	Help Sign Out Signed in as web
Policy Configuration System Configuration				
Common Configuration	Welcome OAM Agents FCUBSWebgate			×
Actions 🗸 View 🖌 📑 🗁 💥 🛛 🔂	FCUBSWebgate			Apply 🔺
Available Services	Confirmation			×
Common Settings	OAM 11g Webgate FCUBSWebgate modified successfully. Applicat	on Domain is FCUBSWebgate		
Access Manager Settings	Name FCUBSWebgate	Logout Callback URL	/oam_logout_success	
Actions 🔹 View 👻 🔄 🗁 💥 🔯	Access Client Password	Logout Redirect URL	https://10.180.196.158:14101/oan	
Access Manager Settings	* Security Open	- Logout Target URL		
SSO Agents	Cert		proxySSLHeaderVar=IS_SSL	
▷ 🕅 OSSO Agents	* State @ Enable		URLInUTF8Format=true	
Authentication Modules	Disable		<pre>client_request_retry_attempts=1 inactiveReconfigPeriod=10</pre>	
	* Max Cache Elements 100000 🖨		filterOAMAuthnCookie=false	
	* Cache Timeout (Seconds) 1800 🚔			
	* Token Validity Period (Seconds) 3600 🚔	* Sleep for	60 荣	
	* Max Connections 1	Cache Pragma Header		
	* Max Session Time 3600 🖨	Cache Control Header		=
	* Failover Threshold 1	Debug		
	* AAA Timeout Threshold -1 🚔	IP Validation Deny On Not Protected		
	* Preferred Host FCUBSWebgate	Allow Management Operations		
	Logout URL	.il		
	Server Lists			
	Primary Server List 🕂 🐥 🗙	Secondary Server List	• 🗙	
	Server Name Host Name Host Port Max Number	Server Name Host Name Host Port Max N	lumber	
	oam_server 💌 iffctw-ap-21 5575 1			
Security Token Service				-

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 Contracter Access Manager - Administr	rat × 🖸 Integrating OAM Security Provider wi × 🕇 +	
(iflchw-ap-21:7001/oamconsole/faces/pages/P	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		
Al	Welcome Bround FCUBS_Auth_Scheme	
Search	Authentication Schemes	Set As Default Apply
Browse Search View ~ Image: Constraint of the search V Image: Shared Components	Confirmation Authentication Scheme, FCUBS_Auth_Scheme, created successfully	×
♥ Resurce Type ● ●	* Name FCUBS_Auth_Scheme Decrotion * Authentication Level Default * Challenge Method BASIC • * Challenge Redrect URI, Tolam/Rever * Authentication Module FCUBS_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.

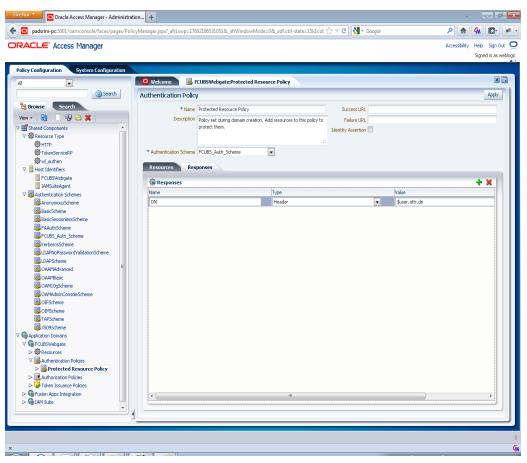
Resources:

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.

CLE [®] Access Manager		Accessibility Help Sign Ou Signed in as w
y Configuration System Configuration		
	O Welcome 🛛 🐻 Create Authentication Policy	×.
Search	Authentication Policy	Apply
Browse Search	* Name FCUBSWebPolicy Success URL	
🔹 🔞 🕒 🖳 🔺	Description Failure URL	
Shared Components	Identity Assertion	
Resource Type		
袋 HTTP 袋 TokenServiceRP	* Authentication Scheme FCUBS_Auth_Scheme	
號 I okenserviceRP 鄭 wl_authen		
Host Identifiers	Resources Responses	
FCUBSWebgate		
IAMSuiteAgent	🔅 Resources	+ 🗙
Authentication Schemes	Main	
AnonymousScheme	FCUBSWebgate://*	
BasicScheme	FCUBSWebgate:/	•
BasicSessionlessScheme		
FCUBS_Auth_Scheme		
KerberosScheme		
LDAPNoPasswordValidationScheme		
BLDAPScheme		
CAAMAdvanced		
OAAMBasic		
OAM10gScheme		
OAMAdminConsoleScheme		
🐻 OIFScheme 🐻 OIMScheme		
TAPScheme		
X509Scheme		
Application Domains		
G FCUBSWebgate		
Resources		
V Authentication Policies		
Protected Resource Policy		
Authorization Policies Value Token Issuance Policies		
Very Token Issuance Policies Fusion Apps Integration		
GIAM Suite		
All the band		

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.



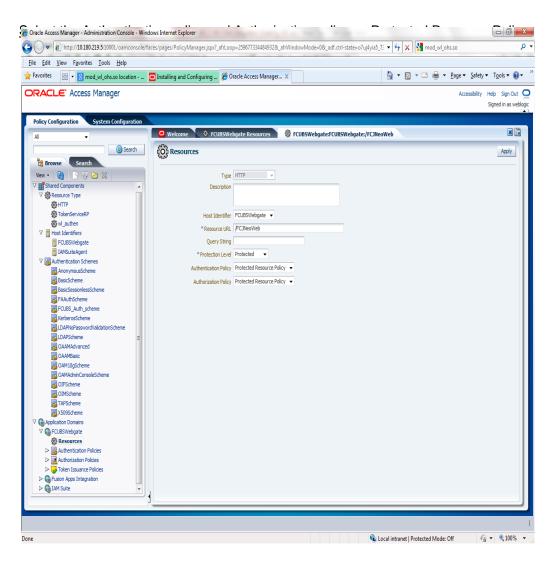


9. Adding Resources

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.

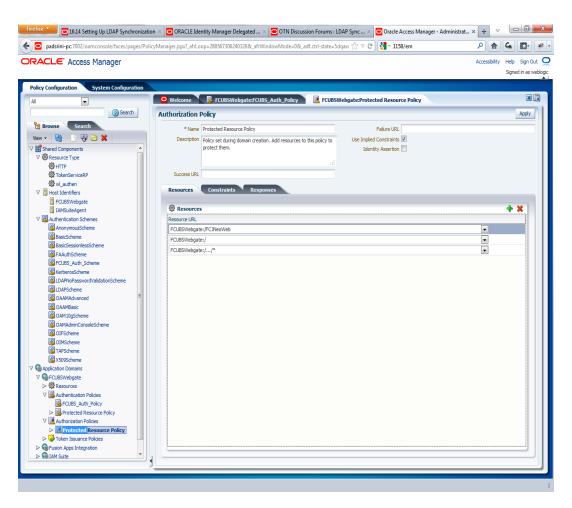




10. Adding Authorization Policy

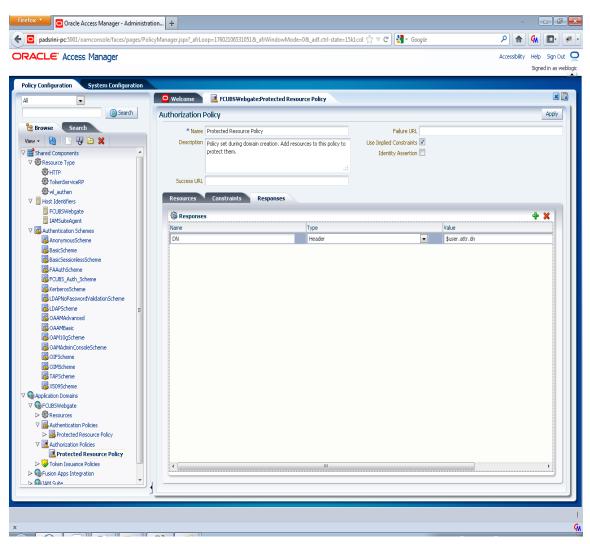
Check whether the resources available in the authentication policies are available in Authorization Policy. During web gate creation these values are defaulted.





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		ection	Create	d	tion Num Of Dir	
Server padsrini-pc 5575, 1			Monda <u>y</u> August 27, 201 11:08:0	y, 2	ory Threads Info	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	
<u>File Edit Test H</u> elp	
🖻 🗟 🥔 🏦	
Server Connection	
IP Address Port Max Conn *Agent ID	//
*Primary: padsrini-po 5575 1 FCUBSWebgate Agent Password	
Secondary: 0 1	?
Min Conn Timeout (ms) Mode 1 30000 open \nother	Connect
Protected Resource URI	a b
Scheme *Host Port	S 🖉
http	💟 Get Auth Scheme
Resource Operation	Validate
User Identity IP Address SARAN Password SARAN User Certificate Store	Authenticate Authorize
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 : cn=SARAN,cn=users,dc=oracle,dc=com [8/27/12 11:17 AM][response] SessionID : 965398ea-751d-456c-ac60-90f07cf6de08	
[8/27/12 11:17 AM][response][action] DN : on=SARAN,on=users,do=oracle,do=com	
[8/27/12 11:17 AM][response][action] OAM_IMPERSONATOR_USER : [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	E 🥠



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 *	•••••					
	cn=Users,dc=oracle,dc=c					
	om .::					
Time Out Duration(Seconds) *						
,						
				_		
Fields						
Input BySARAN	Authorized By SAF	RAN	Modification	1	Authorized	Exit
Date Time 2012-01-06 12:3	3:04 Date Time 201	2-01-06 12:33:04	Number		Open	EXIT

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 Walk In Customer	000003171			Track Previous Year Profit
Internal Swap Customer	000003171			And Loss Adjustment
Clearing Account		Revaluati	on Split Details	
Offset Clearing Account				Revaluation Split Required
Weekly Holiday 1	Saturday -	Sucnoned	Product Maintenand	ce
Weekly Holiday 2	Sunday V	Suspense		·c
	Sunday		Debit Product	
Clearing Bank Code MIS Group For Currency			Description	
MIS Group For Currency	Interdict Validation		Credit Product	
	Required		Description	
Interdict Timeout Interval		Internatio	nal Banking Account	Number Masks
Status Processing Basis	Contract Level 🚽		Bank Code	aaaann
Provisioning Frequency	Daily -		Account Number	
Uncollected Funds Basis				
Uncollected Funds		FGL Integ	ration	
	Deferred Statement			FGL Handoff Required
	Generation	ELCM Inte	gration	
Minor Age Limit (Yrs)	Enterprise General Ledger		2	ELCM Replication
Notification Days	18			ELCM Replication
Cheque Stale Days Limit Expiry Advice Notification				
Days				
Back Value Details		LDAP DN	Template	
	Back Valued Check	ſ	LDAP DN Template	cn= <fccusr>.cn=User</fccusr>
	Required		Cora on remplate	s,dc=oracle,dc=com
Back Value Days		L		
CY Message Preferences				
				Ok

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							Us	er Status	Enable	led		
User Identifica	ation *	FCUBSU	JSER						OHold			
		FCUBS							Olisat			
User Refere	ence								CLocke	ed		
Langu	iade *	ENG					Clas	sification	~			
Home Bra	-								Brand	ch		
Custome	r No						Status Cha	-				
Department C	Code						Last S	igned On	01-6			
Department Descrip										f Customer I juired	Restriction	
Tax Iden							ELCI	User ID	1104	anoa		
LDAP	P DN	FCUBSU	JSER		1				Multi	i Branch Aco	ess	
Time L	evel *	9			1							
Amount For	rmat	-										
Date For	rmat											
Dateroi	mat	Auto	Line Authorization									
		Validate	1	1								
		Validate										
User Password							5	Start Date	* 2012-0	1-06		
Passv	word						I	End Date				
Password Changed	d On	2012-01	-06 11:01:3	3								
E	mail											
Invalid Logins												
Cumula	ative											
Succes	sive											
Restricted Password F	Roles	Rights	Functions	Tills	Accoun	Classes	General	Ledgers	Limits	Branches	Products	
Disallowed Functions L	Users I	Holiday	Fields Gr	oup Re	striction	Centraliz	ed Role					
Maker KAN	NAN1			Date	Time: 201	2-01-06 1	3:29:56		Mod No	o 3		
Checker SAF	RAN			Date 1	Time: 201	2-01-06 1	3:34:26	Reco	ord Status	Closed		Exit
							,	Authorizati	on Status	s Authorized		
	_											

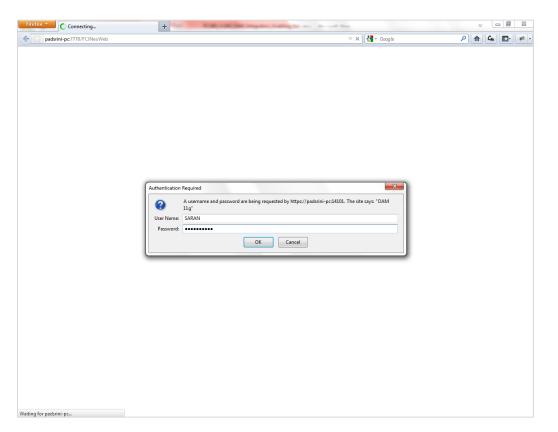
3.4.5 Launching FLEXCUBE

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.





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.



There Universal Banking There Universal Banking There Universal Banking Correcte	Oracle FLEXCUBE UBS11.4Login - Mozilla Firefox	Tonyman on sense. Succession of the	
	padsrini-pc:7778/FCJNeoWeb/LoginServlet		☆
		ORACLE FLEXCUBE Universal Banking	
ORACLE		;	
ORACLE			
ORACLE		Theme Default	
		ORACLE	

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 [Apr] [2020] Version 14.4.0.0.0

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

Copyright © [2007], [2020], Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.