# Oracle Banking Trade Finance Oracle Access Manager



Release 14.7.4.0.0 F99218-01 June 2024

ORACLE

Oracle Banking Trade Finance Oracle Access Manager, Release 14.7.4.0.0

F99218-01

Copyright © 2007, 2024, Oracle and/or its affiliates.

Primary Authors: (primary author), (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

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.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 fail-safe, 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.

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

## Contents

#### 1 Introduction

#### 2 BACKGROUND AND PREREQUISITES

Requisites	2-1
Software Requirements	2-1
kground of SSO related components	2-1
Oracle Access Manager (OAM	2-2
LDAP Directory Server	2-2
WebGate/AccessGate	2-2
Identity Asserter	2-2
	Software Requirements kground of SSO related components Oracle Access Manager (OAM LDAP Directory Server WebGate/AccessGate

### 3 Configuration

3.1	Pre-F	Requisites	3-1
3.2	Char	ige the web.xml file	3-1
3.3	Conf	guring SSO in OAM Console	3-1
3.4	First	launch of ORACLE BANKING TRADE FINANCE after Installation	3-13
	3.4.1	SSO Parameters	3-13
	3.4.2	Maintaining LDAP DN for OBTF Users	3-14
	3.4.3	Launching ORACLE BANKING TRADE FINANCE	3-14
	3.4.4	Signoff in a SSO Situation	3-15



# 1 Introduction

For the purpose of single sign-on ORACLE BANKING TRADE FINANCE is qualified with Oracle Identity Management 12.2.1.4.0 (Fusion Middleware 12c) – specifically using the Access Manager component of Oracle Identity Management. This feature is available in the releases OBTF\_14.4.0.0.0 and onwards of ORACLE BANKING TRADE FINANCE.

This document is expected to provide an understanding as to how single sign-on can be enabled for a ORACLE BANKING TRADE FINANCE deployment using Oracle Fusion Middleware 12c.

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



# 2 BACKGROUND AND PREREQUISITES

## 2.1 Pre-Requisites

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

Software Requirements

#### 2.1.1 Software Requirements

- 1. Oracle Access Manager OAM (12.2.1.4.0)
  - Access Server
  - Webtier Utilities 12.2.1.4.0
  - Web Gate 12.2.1.4.0
  - Http Server
- LDAP Directory Server Please make sure that the LDAP which is been used for ORACLE BANKING TRADE FINANCE 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 12.2.1.4.0

For the purpose of achieving single sign on for OBTF in FMW 12c, it is necessary for the weblogic instance to have an explicit Oracle HTTP server (OHS).

## 2.2 Background of SSO related components

- Oracle Access Manager (OAM
- LDAP Directory Server
- WebGate/AccessGate



Identity Asserter

#### 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 ORACLE BANKING TRADE FINANCE with OAM to achieve Single Sign-on feature, ORACLE BANKING TRADE FINANCE's password policy management, like password syntax and password7 expiry parameters can no longer be handled by ORACLE BANKING TRADE FINANCE. 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 ORACLE BANKING TRADE FINANCE 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 already-authenticated Oracle Access Manager Users through the ObSSOCookie and creates a WebLogic-authenticated session. It also provides single sign-on between WebGates and portals. We can get more details on Identity asserter https://docs.oracle.com/cd/E12839\_01/core.1111/e10043/osso.htm#CHDGCACF

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 ORACLE BANKING TRADE FINANCE 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 (OBTF) EAR file
- 2. Add the following lines under login-config. <a></a>login-config>

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

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

<th>-config&gt;</th>	-config>
[D:\Oracle	Widdleware\user_projects\domains\FCDomain\servers\FCServer\tmp\_WL_user\FCUBS105\f9bfxy\war\WEB-INF\web.xml]
View Search	h Document Project Tools Window Help
1 🖪 🔿	** 🗉 👃 🖻 🛍 🗶 🕫 🖓 🍇 🖲 🕸 🔏 🗰 🚮 🐨 🖬 🖬 🖬 🖬 🖉 😒
	[] [] [] <b>x</b>   x x x x x x x x x x x x x x x x x x
ext ]	+1
	426 <local>com.iflex.fcc.ejb.FCJEJBLocal</local> 427 <ejb-link>FCJEJBC/ejb-link&gt;         428          430       <ejb-ref-name>FCUBS_BATCHEJB_LOCAL</ejb-ref-name>         431       <ejb-ref-type>Session</ejb-ref-type>         432       <local-home>com.iflex.fcc.ejb.batch.BatchEJBLocal</local-home>         433       <local-home>com.iflex.fcc.ejb.batch.BatchEJBLocal         434       <ejb-link>BatchEJB         435       </ejb-link></local-home></ejb-link>
va iva va ime.java	<pre></pre>

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 https://docs.oracle.com/cd/E17904\_01/install.1111/e12002/webgate004.htm#INOIM75770

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 OBTF 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.

iflchw-ap-21:7001/oamconsole/faces/pages/PolicyN							oam agent 11g base url			-
ACLE' Access Manager								Accessibility	Help Si Signed in	
icy Configuration System Configuration										
Common Configuration	Welcome FCUB	SWebgate OAN A	pents oam_se	erver1	LDAP	User Identit	y Stores			
tons + View + 🏼 😫 🔄 🖸	eate: User Identity	Store						Test Connection	Apply	0
Data Sources	* Store Name	CUBSIdentityStore			Description					
Suser Identity Stores      SuserIdentityStore1      Plugins	* Store Type	ID: Oracle Internet Director	Y							
Access Manager Settings						Enable SSL				
tons • View • 🕒 🔛 🗶 🍓 📃	Location and Credentia	ds.								
Access Manager Settings	* Location	iffchw-ap-21:3061		_		* Bind DR	n=ordadmin			
ÚSSO Agents - 😥 OAM Agents						* Password				
COSSO Agents										
Augrenocadon Modules	Users and Groups									
LDAP Authentication module		* User Name Attribute								
IDAPNoPasswordAuthModule			cn=Users,dc=orade,	,dc=com		_				
E Kerberos Authentication module		User Filter Object Classes			-					
X509 Authentication module     Gustom Authentication module		Group Name Attribute								
		<ul> <li>Group Search Base Group Filter Classes</li> </ul>		e,oc=com		-				
		Group Prise Classes								
	Enable Group Cache									
		Group Cache Size (Mb)	10000							
		Group Cache TTL (Seconds)	0							
2	Connection Details									
	Minimum				R	esults time limit				
	Maximum						try Count 3			
	Wait Timeout (					Refe	erral Policy follow			
	Inactivity Timeout (	seconds)								
Security Token Service										

http://ifichw-ap-21:7001/oamconsole/faces/pages/Policy...x?\_adf.ctrl-state=kfr23iytk\_4&\_afrLoop=10370372111194#



**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.

	olicyManager.jspx?_adf.ctrl-state=kfr23iytk_48i_afrLoop=1i		☆ = C 🛃 - car		٩	
ACLE Access Manager					Accessibility	Help Sign
						Signed in as
licy Configuration System Configuration						
Common Configuration	Welcome FCUBSWebgate 0AM Age	ents oam_server1	LDAP FCUB5Identity5	itore		
tons - View - 📑 🖿 🕺 🍓	FCUBSIdentityStore			Tes	t Connection	Apply
Data Sources *	Confirmation			Connection	Status 🖾	2
Stores	User Identity Store FCUBSIdentityStore created success	hdv.		Connection		
SuperIdentityStore1     SuperIdentityStore				Identity Stor successful	e .	
Access Manager Settings	Store Name FCUBSIdentityStore		Description		Cancel	
tons - View - 😗 🗁 💥 🚱	* Store Type OID: Oracle Internet Directory			<u>lok</u>	Cance	
Access Manager Settings						
GSSO Agents			Enable SSL			
LC DAM Agents	-Location and Credentials					
gC OSSO Agents Authentication Modules	"Location ifichin-ap-21:3061		* Bind DN	n woordadaain		
EDAP Authentication module	non de stroot		* Password			
EDAP			- reserveru			
IDAPNoPasswordAuthModule     Kerberos Authentication module						
1509 Authentication module	Default and System Store Options     Set as default store (Current Default Store UserIdent					
Custom Authentication module	Set as system store (Current System Store UserIdent					
	Vusers and Groups					
	Lion Name Attribute	uid				
	User Search Base	cn=Users.dc=orade.dc=com				
	User Filter Object Classes					
	Group Name Attribute					
		cn=Groups,dc=orade.dc=com				
	Group Filter Classes					
	Enable Group Cache					
	E thate troup Cache					
	Group Cache Size (Mb)					
	Group Cache TTL (Seconds)					
	~ Connection Details					
	Minimum Pool Size 10		Results time limit (se	conds) 0		
	Maximum Pool Size 50			Count 3		
	Wait Timeout (seconds) 120			Policy follow		
Security Token Service	Inactivity Timeout (seconds) 0					

 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.

ifichw-ap-21:7001/oamconsole/faces/pages/Po	licvManager.ispy? adl.ctrl-state=kfr23ivtk 48c a	afr1.cop=10370372111194	- + + e	🛃 - oam agent 11g base url	٩	A 8	a-11
			H SI	•••••••••••••••••••••••••••••••••••••••	Accessibility		
Policy Configuration System Configuration						Signed in	1 as wel
Common Configuration	K FCUBSWebgate OAM Agents	oam_server1 LDAP FCUBSId	dentityStore	FCUBS_Authentication_Module			
Actions • View • 📑 🗁 🐹 🍓	FCUBS_Authentication_Module					A	oply
Contract Sources  Contract Stores  Contract Stores  Contract Stores  Contract Stores  Contract Store  Contrac	Confirmation	tication_Module created successfully.				2	×
Access Manager Settings	* Name FOUBS	_Authentication_Module					
	* User Identity Stare   PCJ853						
Security Token Service							

http://iflchw-ap-21:7001/oamconsole/faces/pages/Policy...x?\_adf.ctrl-state=kfr23iytk\_48c\_afrLoop=10370372111194#

 Creating OAM 12c Webgate Navigate to System Configuration>>Access Manager Settings>>SSo Agents>>OAM Agents.

Click on 'Create 12c webgate' button

			Signed in as
Policy Configuration System Configu	aration		
Common Configuration	Welcome Create 0AM 11G Webgate		
Actons • View • 💽 🗁 💥 🚱	Welcome to Oracle Access Manager 11g Use this console to		
Common Settings Server Instances Server Instances Certificate Validation Otati Sources	Manage the Access Manager policies already configured in the system.     Manage the agent profiles and server profiles of configured Access     Register new applications that need angle agrin-on integration with One     Manage and reate trust between partners for Oracle Security Talent     Manage common stetting and configuration for Oracle Access Manage     Dick any of the Inits below to start using the console. Alternatively, you can	de Access Manager. iervice. and Orade Security Token Service.	
2 Plugins	122		
	SSO Agents Manage Partner applications.	Trust Partners Manage the trust between partners.	
	New OAM 10g Webgate		
	Henr Oder Lag verbägter Henr Oder Lag Verbante	Yeen Requester Partner	
	Policies Manage policy components and application domains.	Configuration Manage the common settings and configurations.	
	New Application Domain	Available Services Common Settings Access Manager Settings Security Token Service Settings	
Access Manager Settings			
Security Token Service	1		

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.

	es/PolicyManager.jspx?_adf.ctrl-state=kfr23iytk_48c_afrLoop=10370372111194	🏫 호 C 🔡 - configuring sso 11.1.1.5	۹ 🕈 🖸
RACLE' Access Manager			Accessibility Help Sign ( Signed in as
olicy Configuration System Configuratio	a		
Common Configuration	G Welcome Create OAM 11G Webgate		
ictions • Wew • 📑 🗁 💥 🝓	Create OAM 11g Webgate		Apply
E Available Services P Common Settings Server Instances Server Instances Server Settings Server Instances Server Settings Server Settings Server Settings Server Settings Settin	Version 11g * Name PCUESWebgate Base URL https://fidme-ap-21:7001	User Defined Parameters	h.
2 Plugins	H.	Virtual host [[]]	
	Access Clent Password * Security @ Open © Simple © Cent Host Identifier	Auto Create Policies 🗹	
	Protected Resource List		
	_		
Access Manager Settings			

or Click on New OAM 12c Webgate link available in welcome page.



Once the OAM 12c Webgate created, add filterOAMAuthnCookie=false parameter along with default parameters in User Defined Parameters.

ifichw-ap-21:7001/oamconsole/faces/pages ACLE: Access Manager	1 111-			erOAMAuthnCookie parameter	Heb So	-0
Access Hanager				- Country	Signed in a	
olicy Configuration System Configuration						
Common Configuration	Welcome OAM Agents	FCUBSWebgate			1	×
ctons • View • 🕒 🗁 🐹 🝓	FCUBSWebgate				Apply	Į
Available Services	Confirmation				×	
Server Instances	OAM 11g Webgate FCUBSWebgate	modified successfully. Application (	Domain is FCUBSWebgate			
Access Manager Settings	Name	FCUBSWebgate	Logout Caliback URL	/oam_logout_success		
ctions • View • 🕒 🗁 💥 🝓	Access Client Password		Logout Redirect URL	https://10.180.196.158:14101/oan		
Access Manager Settings	* Security	Open     Simple	Logout Target URL			
COAM Agents		) Cert	User Defined Parameters	proxySSLHeaderVar=15_55		
> 🖟 OSSO Agents		Enable		URLINUTF8Format=true dient_request_retry_attempts=1		
Authentication Modules		) Disable		inactiveReconfigPeriod=10		
	* Max Cache Elements	100000		filter:OAMAuthoCookie=false		
	* Cache Timeout (Seconds)	1800 💼	* Sleep for	60 🔹		
	<ul> <li>Token Validity Period (Seconds)</li> </ul>	3600 💼	Cache Pragma Header			
	Max Connections	1	Cache Control Header			
	* Max Session Time	3600 🚖	Debug			
	* Falover Threshold	1	IP Valdation			
	<ul> <li>AAA Timeout Threshold</li> </ul>	-1 💭	Deny On Not Protected			
	Preferred Host	PCU8SWebgate	Allow Management Operations			
	Logout URL					
	Server Lists					
	Primary Server List	<b>+ X</b> Se	condary Server List 🕴	×		
	Server Name Host Name		erver Name Host Name Host Port Max N	lumber		
	oam_server 💌 ifidhw-ap-21	5575 1				
Security Token Service	1	-178 EL-				

Click 'Apply' button to save the changes

× Find: TitterOAMAuthnCook 🗸 Next 🛊 Previous 🖌 Highlight all 🔟 Match case 🐠 Phrase not found

- 6. Post OAM Webgate 12c 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:

12cWebgate\_instance\_dir/webgate/config/ObAccessClient.xml

(for instance WebTier\_Middleware\_Home/Oracle\_WT1/instances/instance1/config/

OHS/ohs1/webgate/config/ObAccessClient.xml)

 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 Scheme

Challenge Method : BASIC

Challenge Redirect URL : /oam/server

		Accessibility Help Sign ( Signed in as
olicy Configuration System Configuration		
Search	Welcome     FCUBS_Auth_Scheme     Authentication Schemes	Set As Default Apply
Browse Search	Confirmation	×
iew - 🔄 💽 😌 🖿 💥	Authentication Scheme, FOUBS_Auth_Scheme, created successfully	-
Jee Couponens     Jee Co	* Name (PCUIS Julh Scheme Decorption * Authentication Level 1 * Challinge Method BASIC • * Challinge Referet UR. (Journame ref * Authentication Module (PCUIS Julhentication Module • Challinge Parameters	

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

If it is a basic authentication scheme, we need to add the 'enforce-valid-basic-authcredentials' 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. OBTFWebPolicy)

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 (
			Signed in as
Configuration System Configuration	Welcome     Greate Authentication Policy		
() Search	Authentication Policy		Apph
Browse Search	* Name FOUBSWebPolicy	Success URL	
- 🝓 📑 😔 🔀	Description	Failure URL	
Bhared Components		Identity Assertion	
Resource Type		and the product over the a	
чтн 🚳			
TokenServiceRP	* Authentication Scheme   PCUBS_Auth_Scheme	•	
W_authen Host Identifiers	Resources Responses		
FCUBSWebgate			
IAMSuiteAgent	@ Resources		+ x
Authentication Schemes	Main		
AnonymousScheme	FCUBSWebgate://*		
BasicScheme	FCUBSWebgate:/		
BasicSessionlessScheme			
FAAuthScheme			
FCUBS_Auth_Scheme			
LDAPNoPasswordValdationScheme			
LDAPScheme			
OAAMAdvanced			
CAAMBasic			
CAM10gScheme			
B OAMAdminConsoleScheme			
OIFScheme			
OIMScheme			
TAPScheme			
K509Scheme Application Domains			
FCUBSWebgate			
> @ Resources			
7 Authentication Policies			
Protected Resource Policy			
> 🛃 Authorization Policies			
> 🥪 Token Issuance Policies			
Fusion Apps Integration			
IAM Suite			
	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.

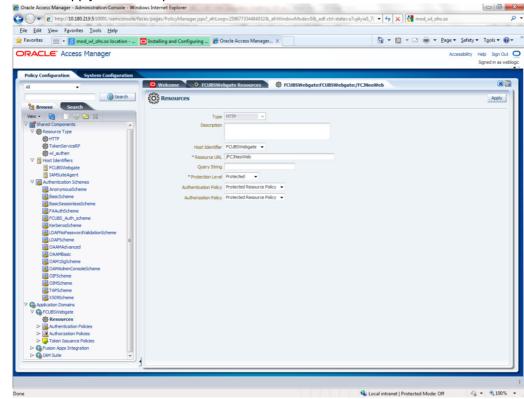
						3
	🖸 Welcome 🔜 Fi	CUBSWebgate:Protected	Resource Policy			
Search	Authentication Policy	r i				Apph
Browse Search	* Name	Protected Resource Policy		Success URL		
ew - 🍓 🕒 😲 😂 🗶	Description	Policy set during domain crea	ition. Add resources to this policy to	Failure URL		
Shared Components		protect them.	A 9	Identity Assertion		
/ @Resource Type						
@HTTP						
TokenServiceRP	Authentication Scheme	FCUBS_Auth_Scheme				
@wl_outhen	-					
Host Identifiers	Resources Resp	ponses				
FCUBSWebgate	Responses					+ x
IAMSuiteAgent	******************					<b>T A</b> ,
Authentication Schemes	Name		Type		Value	
AnonymousScheme	DN		Header	•	\$user.attr.dn	
Coll Barrel of the same						
BasicScheme						
BaskSessionlessScheme						
BasicSessionlessScheme						
BasicSessionlessScheme FAAuthScheme FCUBS_Auth_Scheme						
Bask/SessionlessScheme FAAuthScheme FCUBS_Auth_Scheme KerberosScheme						
Bask:SessionlessScheme FAuthScheme FOLBS_Auth_Scheme KorberosScheme LDAPNoPasswordValdationScheme						
BasicSessionlessScheme     FAuthScheme     FOBS_Auth_Scheme     KirberosScheme     LDAPNoPasswordValdstionScheme     LDAPNoPasswordValdstionScheme						
BasicSessionlessScheme FAUthScheme FOLBS_Auth_Scheme FoLBS_Auth_Scheme FoLDAPRoPasswordNaldstonScheme LDAPRoPasswordNaldstonScheme LDAPScheme FOLBAPScheme FOLBA						
BasiclessiversSchene     FAuthSchene     FAuthSchene     Kubhschene     LubPischene     LubPischene     LubPischene     LubPischene     GudPischene     GudPischene     GudPischene						
BasicSessorlessScheme  FAußScheme CSUBSUNCSCHEME CALISCHEME CALISCHEME CANPENSTERNORTHAIdationScheme CANPANAtoreced CANPEnst: COANPEnst: COANP						
BasiclessoflessSchene     FAuthSchene     FAuthSchene     Kobersoflene     LDAP4/Bisword/aldatorSchene     GAAMO-schene     GAAMO-schene     GAAMO-schene     GAAMO-schene     GAAMO-schene     GAAMO-schene     GAAMO-schene     GAAMO-schene     GAAMO-schene						
BacklessorlessScheme     FALLArbScheme     FAUBS.AuhScheme     KAUBS.AuhScheme     LAPAScheme     LAPAScheme     LAPAScheme     LAPAScheme     GAAMAdvarced     GAAMAdvarce						
BackCestoNestSchene     FAustOchme     FOLBS Auth_Schene     Kohnschene     LDAP405sword duldstorSchene     LDAP405sword duldstorSchene     GAAP40vacce     GAAP40vacce     GAAP40vacce     GAAP40vacce     GOStome     GOStome     GOStome						
Back/esion/esis5heme FAUS5.heme FAUS5.hem LOAP3.hem LDAP3.hem LDAP3.hem CANNAdvarced CANNAdvarc						
BackSestOrlesSAteme     FAuthOrbeme     FOUBS Auth_Scheme     KomesestationScheme     LDAPA95 serverd ValdatorScheme     LDAP495 serverd ValdatorScheme     GAAP40avice     GAAP40avice     GAAP40avice     GAAP40avice     GAAP40avice     GOStheme     GOStheme     GOStheme     GOStheme						
BackCestoNestSchene     FAubtochme     FCUBS Auth_Scheme     KuberosScheme     LDAPFeilsewordValdatorScheme     LDAPFeilsewordValdatorScheme     GAAVAvanced     GAAVAvan						
BacklessonkessShene     FAUHSchene     FAUHSchene     LD4F45chene     LD4F45chene     LD4F45chene     LD4F45chene     GAMMolysnoed     GA						
BasiclessOrlessSheme     FAuhtochme     FCUES_Auh_Scheme     FCUES_Auh_Scheme     LDAFraitwordMaldatorScheme     LDAFraitwordMaldatorScheme     LDAFraitwordMaldatorScheme     CAAMAdvanced						
BasiclessofiesSchene     FAubtschunne     FAubtschunne     Konsekungsschungsschung     Achungschung						
Besicless/sets/sets/ FAUE5/setme     FAUE5/setme     FAUE5/setme     LDAF45/setme     LDAF45/setme     LDAF45/setme     CLAMAQ4anced     DAF5/setme     CAAMBusc						
BasiclesionesSchme     FAuthochme     FOLES Auth_Schme     FOLES Auth_Schme     LDAPHoPseword/aldatorSchme     LDAPHoPseword/aldatorSchme     COMMAnanced     COMMAnance     COMMAna						
BisclessoriesSchene     FAUstSchene     FAUstSchene     FAUstAuftSchene     LDAPkinswordhaldstorSchene     LDAPkinswordhaldstorSchene     GAMAdvanced     GAMAdvancedde     GAMAdva						
BasclessoriesSchene     POUBS_Auth_Schene     POUBS_Auth_Schene     POUBS_Auth_Schene     LOAFlobswordbidstorSchene     LOAFlobswordbidstorSchene     CoAAMbasc						
BackSessoriesScheme FAubSchem FOUSS, Aub, Scheme FOUSS, Aub, Scheme FOUSS, Aub, Scheme FOUSScheme						
BascleristresSchne     POUBS, Auft Schnen     POUBS, Auft Schnen     POUBS, Auft Schnen     LofArlösswordfaldstorSchnen     LofArlösswordfaldstorSchnen     LofArlösswordfaldstorSchnen     OAAANbasc     OAANbasc     OAANbasc     OAANbasc     OAANbasc     OANbaschene     OASSchnene     OASSchnenee     OASSchnenee     OASSchnenee     OASSchnenee     OASSchnenee     OASSchnenee     OASSchnenee     OASSchnenee     OASSchnenee     OASSchneneee     OASSchneneeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee						
Bisiclesis/lesis/shene     FAUEA/Lh/Scheme     FAUEA/Lh/Scheme     LDAFis/shene     LDAFis/shene     LDAFis/shene     CAAMA/anced     CA						
BasiclessofiesSchene     FAustoches     FoustoresSchene     FoustoresSchene     FoustoresChene     LoAP4/0-sexedValdatorSchene     LoAP4/0-sexeValdatorSchene     CoAP4/0-sexeValdatorSchene     CoAP4/0-sexeValdat						
BasclessorbesSchene     FALMSchene     FALMSchene     FALMSchene     LDAP4/BiswordhaldstorSchene     LDAP4/BiswordhaldstorSchene     GAMBack     GAMMorene     GAMMorene     GAMMorene     GAMMorene     GAMMorenee     GAMMoreneee     GAMMoreneee     GAMMoreneee     GAMMoreneeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee						
Bis/Cesto/Res/Scheme       ■ FAuch/scheme       ■ FAuch/scheme       ■ FUBS /Auth_Scheme       ■ LDAP/Reiseword/aldator/Scheme       ■ LDAP/Reiseword/aldator/Scheme       ■ GAAAM/worded       ■ GAAM/worded       ■						
BisclessoriesSchene     FAUstSchene     FAUstSchene     FAUstAuftSchene     LDAPkinswordhaldstorSchene     LDAPkinswordhaldstorSchene     GAMAdvanced     GAMAdvancedde     GAMAdva	4					

9. Adding Resources

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

- Click on Create New Resource button.
- Select the type as HTTP.
- Select the Host Identifier as OBTFWebgate
- 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.

ACLE' Access Manager		Accessibility Help Sign 0 Signed in as v
icy Configuration System Configuration		
	Welcome     RecubsWebgatesfCUBS_Auth_Policy     E FCUBSWebgatesProtected Resource Policy	
Search	Authorization Policy	Apply
Browse Search	* Name Protected Resource Policy Falure URL	
w - 🚷 🕒 😲 😂 🗶	Description Policy set during domain creation. Add resources to this policy to Use Implied Constraints	
Shared Components	protect them.	
7 @Resource Type		
Флтр		
TokenServiceRP	Success URL	
🕸 wi_authen	Resources Constraints Responses	
7 Host Identifiers		
FCUBSWebgate	@ Resources	+ x )
Authentication Schemes	Resource LIRL	
AnonymousScheme	FCJ8SWebgate:/FCJNeoWeb	
BasicScheme	PC05Webgate:/	
BasicSessionlessScheme		•
BAAuthScheme	FCUBSWebgate://*	
FCUBS_Auth_Scheme		1
KerberosScheme		
LDAPNoPasswordValidationScheme		
LDAPScheme		1
CAAMAdvanced		
CAAMBasic CAM10gScheme		
CAMA sugscheme CAMAdminConsoleScheme		
OIFscheme		
OIMScheme		
TAPScheme		
X509Scheme		
Application Domains		
/ GFCUBSWebgate		
▷ @ Resources		
V Authentication Policies		
FCU85_Auth_Policy		
Protected Resource Policy     Authorization Policies		
Authorization Polices     Protected Resource Policy		
Token Issuance Policies		
Gen issuance Polices     Gen issuance Polices		
A IAM Sute		



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.

						Accessibility Help Sign O Signed in as v
cy Configuration System Configuration						signed in as in
	O Wekome	ECUBSWebgate:Protect	ed Resource Policy			
Search	Authorization P	olicy				Apply
Browse Search		Protected Resource Policy		Failure URL		
- 🔄 🖸 🔁 🗙				Use Implied Constraints		
Shared Components	Description	Policy set during domain creation. protect them.	Add resources to this policy to	Identity Assertion		
Shared Components     We Resource Type		provess orders		Identity Assertion		
@HTTP						
TokenServiceRP	Success URL					
@wl.authen						
Host Identifiers	Resources	Constraints Response				
FCUBSWebgate	10.0					
IAMSuiteAgent	Responses					+ X
Authentication Schemes	Name		Туре		Value	
AnonymousScheme	DN		Header		\$user.attr.dn	
BasicScheme						
Bask:SessionlessScheme						
FAAuthScheme						
FCUBS_Auth_Scheme						
KerberosScheme						
UDAPNoPasswordValidationScheme						
LDAPScheme E						
CAAMAdvanced						
GAAMBasic						
(19)						
GAM10gScheme						1
3 OAMAdminConsoleScheme						
OAMAdminConsoleScheme						
CAMAdminConsoleScheme CIFScheme CIMScheme						
CoMAdminConsoleScheme CIPScheme CIMScheme TAPScheme						
OFScheme OFScheme OFScheme OFScheme OFScheme OFScheme OFScheme S095Scheme						
CAMAdminConsoleScheme COPScheme CONScheme CAMScheme SofScheme Application Domains						
CMMdminConsoleScheme CMScheme CMScheme TAPScheme TAPScheme TAPScheme Application Domains CMSCHeme CUBSVedgate						
Consolestation Conso						
CAMAdminConsoleScheme 20 OBScheme 20 OBScheme 20 OBScheme 20 Streame 20						
CMMAdem/CrasoleScheme CMMAdem/CrasoleScheme CMMAdem/CrasoleScheme CMMAdem/CrasoleScheme Assistant Domains CMMAdem/CMMAdem CMMAdem/CMM						
CAMAdminConsoleScheme 20 OFScheme 21 OFScheme 21 OFScheme 21 APScheme 24 OPSCheme 24 OPSC						
CANAdain/ConsoleScheme ConsoleScheme ConsoleScheme ConsoleConsol						
CANAdosin/CansoleScheme ConsoleScheme ConsoleScheme Consoleme Con	*					
Constant ConsolesCheme ConsolesCheme ConsolesCheme Consoleme Cons						, ,

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>

 Checking the Webgate 12c Agent Creation After configuration of webgate 12c agent launch the URL

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

Access	1000	nection	Create		tion Num Of Dir	
Server padsrini-pc 5575, 1		late	Monda; August 27, 201 11:08:0	y, 2	ory [Threads]Info	rmation
Cache Name	State			Timeout (seconds)	Cache Stats (Hits:Misses: Expired:Flushed)	Memory Footprint (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

#### configuration is working fine.

**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



P Address padsrini-pc		Port				
IP Address						
IP Address						
			Max Conn	*Agent ID		1
[		5575	1	FCUBSWebgate		
				Agent Password		
		0	1	Agent Password	?	
Timeout (ms) 30000	Mode				Connect	Ĩ
30000	open 👻					_
					2	4
*Host				Port	_	
+ FCUBSW	ebgate			0	Get Auth Sche	me
				Operation		
eb				Get 👻	Validate	
	SARAN		••••••	•••	Authenticate	
cate Store					Authoriza	-
					Authorize	
	Redirect URL 1	nttos://padsrini-	oc:14101/oam/serv	er		
		SARAN, cn=us	ers,do=oracle,do=o	om		
17 AM][response]	[action] OAM_IN	PERSONATO	R_USER :			
17 AM][response]	[action] OAM_ID	ENTITY_DOM	AIN : FCUBSIdentit	yStore		
	FCUBSW      FCUBSW      b      b      c	"Host FCUBSWebgate Username SARAN ate Store ges 7 AM][response] Redirect URL :   7 AM][response] Credentials expr 7 AM][response] SessionID : 9657 7 AM][response] SessionID : 9657 7 AM][response][action] OAM_IN 7 AM][response][action] OAM_IN 7 AM][response][action] OAM_IN 7 AM][response][action] OAM_IN 7 AM][response][action] OAM_IN 7 AM][response][action] OAM_IN 7 AM][response][action] OAM_IN	"Host         FCUBSWebgate         ab         "Username         SARAN         ate Store         "T AM[response] Redirect URL : https://padsrini- 7 AM[response] Credentials expected : 0xt (ba 7 AM[response] User DN : cn=SARAN,cn=users 7 AM[response] SesionID : 965396ea-751d-45 AM[response] SesionID : 965396ea-751d-45 AM[response][action] OAM _IMPERSONATO 7 AM[response][action] OAM _IMPERSONATO 7 AM[response][action] OAM _IMPERSONATO 7 AM[response][action] OAM _IMPERSONATO 7 AM[response][action] OAM _IDENTITY_DOM	*Host FCUBSWebgate	Host       Port         FCUBSWebgate       0         ab       Operation         Get       Get         ab       Get         SARAN       Get         ate Store       2         AM[response] Redirect URL : https://padsrini-pc:14101/oam/server       ?         7 AM[response] Redirect URL : https://padsrini-pc:14101/oam/server       ?         7 AM[response] Credentials expected : 0x1 (basic)       ?         7 AM[response] SessionID : 9653996a-7516+4560-ac00-9007cr6de08       ?         7 AM[response] Isotion [ OAM_IMPERSONATOR_USER	Hot   Pott   Pott <

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

# 3.4 First launch of ORACLE BANKING TRADE FINANCE after Installation

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

- SSO Parameters
- Maintaining LDAP DN for OBTF Users
- Launching ORACLE BANKING TRADE FINANCE
- Signoff in a SSO Situation

#### 3.4.1 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).

#### 3.4.2 Maintaining LDAP DN for OBTF Users

For each user id in OBTF 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 creation form in OBTF. If the OBTF 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.

#### 3.4.3 Launching ORACLE BANKING TRADE FINANCE

After setting up ORACLE BANKING TRADE FINANCE 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



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

Waiting for padsrini-pc...

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



Oracle Financial Services - Google Chrome			-	
A Not secure   whf00fqn:7058/FCJNeoWeb/	LoginServlet			
ORACLE	Font Size: A A A	Theme: Cadet Green	Glaucous Dark	Sepia
		1 and a second		-
	Oracle FLEXCUBE Trade Finance			
	That Finance			
	User ID			
	-			
	Password			
	Sign In			
		and the second second		
	Copyright © 2017,2018, Oracle and/or its affiliates	All rights reserved.		

#### BANKING TRADE FINANCE home page

#### 3.4.4 Signoff in a SSO Situation

ORACLE BANKING TRADE FINANCE does not provide for single signoff currently, i.e., when a user signs off in ORACLE BANKING TRADE FINANCE, 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 ORACLE BANKING TRADE FINANCE will function as 'Exit', i.e., on clicking these, the user will 'exit' ORACLE BANKING TRADE FINANCE and will need to re-launch ORACLE BANKING TRADE FINANCE using the ORACLE BANKING TRADE FINANCE launch URL.

