Oracle Access Manager Integration Oracle Banking Payments Release 14.5.0.0.0 [May] [2021]

FINANCIAL SERVICES



Table of Contents

1. Pl	PREFACE	
1.1	INTRODUCTION	
1.2	AUDIENCE	
1.3	ABBREVIATIONS	
1.4	DOCUMENTATION ACCESSIBILITY	
1.5	ORGANIZATION	
1.6	GLOSSARY OF ICONS	
1.	.6.1 Related Documents	1-2
2. E	ENABLING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER	
2.1	INTRODUCTION	
2.2	Prerequisites	
2.3	BACKGROUND OF SSO RELATED COMPONENTS	
2.	2.3.1 Oracle Access Manager (OAM)	
2.	2.3.2 LDAP Directory Server	
2.	2.3.3 WebGate/AccessGate	
2.	3.4 Identity Asserter	
2.4	CONFIGURATION	
2.	2.4.1 Pre-requisites	
2.	2.4.2 Changing web.xml file	
2.	2.4.3 Configuring SSO in OAM Console	
2.	2.4.4 First Launch of Oracle Banking Payments after Installation	



1. Preface

1.1 Introduction

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

1.2 Audience

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

Role	Function
Back office data entry Clerks	Input functions for maintenance related to the interface.
Back office Managers/Officers	Authorization functions.

1.3 Abbreviations

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

1.4 **Documentation Accessibility**

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

1.5 **Organization**

This manual is organized into the following chapters:

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

1.6 Glossary of Icons

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

Icons Function



Icons	Function
×	Exit
+	Add row
-	Delete row
	Option List

1.6.1 Related Documents

You may refer the following manuals for more information

- Procedures User Manual
- Oracle Access Manager User Manual (not included with Oracle Banking Payments User Manuals)



2. Enabling Single Sign-on with Oracle Access Manager

2.1 Introduction

Single sign-on capability of Oracle Banking Payments is qualified with Oracle Identity Management 11.1.1 (Fusion Middleware 11gR1), specifically using the Access Manager component of Oracle Identity Management. This feature is available in the releases Oracle Banking Payments V.UM 7.3.0.0.0.0 and onwards.

This document explains the method to enable single sign-on for Oracle Banking Payments deployment using Oracle Fusion Middleware 11g. You will also find backgrounds of various components of deployment and the configurations in Oracle Banking Payments and Oracle Access Manager that enable single sign-on using Oracle Internet Directory as a LDAP server.

2.2 **Prerequisites**

2.2.1.1 Software Requirements

Oracle Access Manager – OAM (11.1.1.5)

- Access Server
- Webtier Utilities 11.1.1.5
- Web Gate 11.1.1.5
- Http Server

LDAP Directory Server

Ensure that the LDAP used for Oracle Banking Payments Single Sign-on deployment is certified to work with OAM.

Some of the LDAP directory servers supported as per OAM document are as follows.

Note: This is an indicative list. You can find the conclusive list in Oracle Access Manager Documentation.

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

WebLogic (10.3.5)

For achieving single sign-on for Oracle Banking Payments UBS in FMW 11gR1, the Weblogic instance must have an explicit Oracle HTTP server (OHS).



Background of SSO Related Components 2.3

2.3.1 Oracle Access Manager (OAM)

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

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

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

2.3.2 LDAP Directory Server

When Oracle Banking Payments is integrated with OAM to achieve Single Sign-on feature. Oracle FLEXCUBE password policy management, such as password syntax and password7 expiry parameters can no longer be handled in Oracle FLEXCUBE. Instead, the password policy management can be delegated to the Directory Server. All password policy enforcements will be based on LDAP user IDs and passwords.

2.3.3 WebGate/AccessGate

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

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

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

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

2.3.4 **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. You can get more details on Identity asserter at http://download.oracle.com/docs/cd/E12839 01/core.1111/e10043/osso.htm#CHDGCACF.

Note: This document contains the configuration of Oracle Internet Directory as LDAP server and its configuration in Weblogic. This document does not discuss the configuration and setup of OAM and LDAP directory server of other LDAP servers. Such details are provided by the corresponding Software provider.



2.4 Configuration

2.4.1 Pre-requisites

The configuration steps are provided in this section based on the following assumptions:

- Oracle FLEXCUBE has already been deployed and is working without single sign-on.
- Oracle Access Manager and the LDAP server are installed and the requisite setup for connecting them along Weblogic's Identity Asserter is completed.

2.4.2 Changing web.xml file

Locate the file *web.xml* in the application (FCUBS) EAR file.

Add the following lines under login-config.

<login-config>

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

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

</login-config>



Save the file and redeploy it. Restart the application.

2.4.3 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 explained in the page http://docs.oracle.com/cd/E17904_01/install.1111/e12002/webgate004.htm.

2.4.3.1 Identity Store Creation

Create a new User Identity Store. Login to OAM Console and navigate to System Configuration>>Common configuration>>Data Sources>>User Identity Store.



	Accessibility Help Sign U.	ut 🛌
Policy Configuration System Configuration		(PA)
✓ Common Configuration	Welcome FCUBSWebgate OAM Agents oam_server1 LDAP User Identity Stores	×
Actions 🕶 View 👻 📑 🗁 💥 🚱	Create: User Identity Store Test Connection Apply	2
♥	* Store Name FCUBSIdentityStore Description * Store Type OID: Orade Internet Directory .: Enable SSL	
Actions - View - 📑 🗁 💥 🔞	✓Location and Credentials	
	* Location Ifichw-ap-21:3061 * Bind DN on=oncladmin .:: * Password ******	
 > ⊒COSSU Agents > ∰ Cutherization Modules > ∰ LDAP Authentication module > ∰ LDAP > ∭ LDAPHOPassion duttModule > ∰ Korberos Authentication module > ∰ Cost Authentication module > ∰ Custom Authentication module 	Users and Groups * User Name Attribute ud * User Search Base Griu-Users,dc=orade,dc=com User Filter Object Classes Group Name Attribute * Group Search Base Group Cache Group Cache TRL (Seconds) O O Connection Details Minimum Pool Size O So Wait Timeout (seconds) D So Maximum Pool Size So So So Maximum Pool Size So So So Referral Policy follow Inactivity Timeout (seconds) O	
≥ Security Token Service	J	

Specify the following details in the User Identity Store.

Store Type

Select Oracle Internet Directory.

Location

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

Bind DN

Specify the user name to connect to the LDAP Server.

Password

Specify the password to connect to the LDAP Server.

User Name Attribute

Specify the attribute created in LDAP, which is the user name for the other application. in this example it is treated as the FCUBS Username.

User Search Base

Specify the container of the user name in the LDAP server.

Group Search Base

Specify the container of the group name in the LDAP server.



After entering the above details, click 'Apply' button. On Successful creation, click 'Test Connection' button to verify whether the LDAP connection is working fine.

ORACLE [®] Access Manager				Accessibility	Help Sign Out 🧲
					Signed in as weblogi
Policy Configuration System Configuration		_			
Common Configuration	Welcome FCUBSWebgate OAM Agents oam_server1 LI	LDAP FC	UBSIdentityStore		
Actions - View - 🎯 🗁 💥 🔞	FCUBSIdentityStore			Test Connection	Apply ?
V Data Sources	Confirmation			Connection Status	×
✓	User Identity Store FCUBSIdentityStore created successfully.			Connection to the User Identity Store successful!	
✓ Access Manager Settings	Store Name FCUBSIdentityStore De	escription		OK Cancel	
Actions 🗸 View 👻 🔄 🔀 🚱	* Store Type OID: Orade Internet Directory				
Access Manager Settings					
V SSO Agents			Enable SSL		
SOSSO Agents	✓ Location and Credentials				
V 🎬 Authentication Modules	* Location iffchw-ap-21:3061		* Bind DN cn=orcladmin		
DAP Authentication module			* Password •••••		
LDAP					
Erberos Authentication module	✓ 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=oracle,dc=com				
	User Filter Object Classes				
	Group Name Attribute				
	* Group Search Base cn=Groups,dc=oracle,dc=com				
	Group Filter Classes				
	Enable Group Cache				
	Group Cache Size (Mb) 10000 🖨				
	Group Cache TTL (Seconds)				
	✓ Connection Details				
	Minimum Pool Size 10 🚔	Resul	Its time limit (seconds) 0	k r	
	Maximum Pool Size 50 🚔		Retry Count 3	h F	
	Wait Timeout (seconds) 120 🚔		Referral Policy follow	•	
> Security Token Service	Inactivity Timeout (seconds) 0				
	1				

2.4.3.2 Creating Authentication Module

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



ORACLE Access Manager	Accessibili	ity Help Sign Out Ϙ
-		Signed in as weblogic
Policy Configuration System Configuration		
Sommon Configuration	FCUBSWebgate OAM Agents oam_server1 LDAP FCUBSIdentityStore FCUBS_Authentication_Module	
Actions - View - 📑 🗁 💥 🔯	FCUBS_Authentication_Module	Apply
Actors + View + Image: Second Seco	FCUBS_Authentication_Module Confirmation LDAP Authentication Module FCUBS_Authentication_Module * Name FCUBS_Authentication_Module * User Identity Store FCUBSIdentityStore	Apply
≥ Security Token Service	<u> </u>	

Click 'New' button to create new Authentication Module.

Name

Specify the name of the authentication module.

User Identity Store

Specify the user identity store you had created in the previous step.



2.4.3.3 Creating OAM 11g Webgate

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

ORACLE: Access Manager	Accessibility	Help Sign Out 🧲
-		Signed in as weblogic
Policy Configuration System Configuration		
	Welcome Create 0AM 11G Webgate	
Actions - View - R R X RS	Welcome to Oracle Access Manager 11g	
Actions v View v S S S S S S S S S S S S S S S S S S	Wetcome to Oracle Access Manager 11g Use this conside to Manage the Access Manager policies afteredly configured in the system. Manage the Access Manager profiles and envery profiles of the configured Access Manager servers. Manage and create trust between partners for Oracle Access Manager and Oracle Security Token Service. Manage common settings and configuration for Oracle Access Manager and Oracle Security Token Service. Click any of the links below to start using the console. Alternatively, you can use the navigation tree on the left as well. SSO Agents Mew OAM 10g Webgate Mew OAM 10g Webgate Mew OAM 10g Webgate New OASSO Agent Mew OSSO Agent Mew OSSO Agent Manage policy components and application domains. New Application Domain	
≥) Access Manager Settings ≥) Security Token Service		
[Ľ	2	

Click 'Create 11g webgate' button or 'New OAM 11g Webgate' link on the Welcome page.



ORACLE [®] Access Manager	Accessibility	Help Sign Out
Policy Configuration System Configuration		
Common Configuration	Welcome Create 0AM 11G Webgate	× 🖹
Actions • View • 📑 🗁 💥 🙀	Create OAM 11g Webgate	Apply
 ► Available Services ► Common Settings ► Service Instances ► Service Instances ► Obla Sources ► Plugins 	Version 11g Version 11g Version 11g User Defined Parameters Base URL http://ffctwi-op-21:7001 	
≥ Access Manager Settings		
≥ Security Token Service	4	

Specify a name for Webgate and the Base URL (the host and port of the computer on which the Web server for the Webgate is installed). Click 'Apply' button.

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.

2.4.3.4 Post OAM Webgate 11g Creation Steps

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

1. 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

2. On the OAM Agent host, copy artifacts (to the following Webgate directory path).

Example: 11gWebgate_instance_dir/webgate/config/ObAccessClient.xml

(for instance WebTier_Middleware_Home/Oracle_WT1/instances/instance1/config/

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

2.4.3.5 Creating Authentication Scheme

Navigate to *Policy Configuration >> Authentication Schemes*. Click 'Create' button to create a new Authentication Scheme.



ORACLE [®] Access Manager		Accessibility Help Sign Out 🧲
		Signed in as weblogic
		·
Policy Configuration System Configuration		
Al	Velcome BrCUBS_Auth_Scheme	
Search	Authentication Schemes	Set As Default Apply
Browse Search	Confirmation	×
View - 🚱 🕒 🕂 🗠	Authentication Scheme, FCUBS_Auth_Scheme, created successfully	
V H Shared Components		
V \$03 Resource Type	the property of a l	
SOS HTTP	Name PC0bs_Autr_screme	
Star Local ServiceRP	Description	
V Host Identifiers	* Authentication Level 1	
TAMS vite Acent	Default	
V Authentication Schemes	* Challenge Method BASIC	
AnonymousScheme	* Challenne Redirect I IRI / (nam/server	
▷ 🐻 BasicScheme		
BasicSessionlessScheme	* Authentication Module FCUBS_Authentication_Module 💌	
▷ 🞇 FAAuthScheme	Challenge Parameters	
FCUBS_Auth_Scheme		
▷ KerberosScheme		
LDAPNoPasswordValidationScheme		
D 200 LDAPScheme		
> C OAAMAdvanced		
> 🔀 TAPScheme		
> 🔀 X509Scheme		
√ @ Application Domains		
Fusion Apps Integration		
▷ 🌀 IAM Suite		

Name

Specify a name to identify Authentication Scheme.

Challenge Method

Select 'BASIC'.

Challenge Redirect URL

Specify '/oam/server'.

Authentication Module

Select the authentication module that you had created in an earlier step (Creating Authentication Module).

If it is a basic authentication scheme, you need to add the 'enforce-valid-basic-auth-credentials' tag to the *config.xml* file located under '/user_projects/domains/<MyDomain>/config/'.

Insert the tag before the end of the <security-configuration> tag as follows:

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

</security-configuration>



2.4.3.6 Creating Authentication Scheme

Navigate to Policy Configuration >> Application Domains >> [Webgate agent name] >> Authentication Policies.

Click 'New' button and specify the following information.

ORACLE: Access Manager		Accessibility Help Sign Out O
		Signed in as weblogic
Policy Configuration System Configuration		
All	🛛 Welcome 🛛 👼 Create Authentication Policy	×
Search	Authentication Policy	Apply
Browse Search	* Name FCUBSWebPolicy Success URL	
View 🗸 🔞 🕒 🖳 🔀	Description Failure URL	
V 🎬 Shared Components	Identity Assertion	
V SResource Type		
TokenServiceRP	* Authentication Scheme FCUBS_Auth_Scheme	
🐯 wl_authen	Recourses Recoonses	
Host Identifiers ECUBSWebgate	Resources Responses	
IAMSuiteAgent	🔅 Resources	+ ×
V 🚜 Authentication Schemes	Main	
AnonymousScheme	FCUBSWebgate://*	
BasicSessionlessScheme	FCUBSWebgate:/	
FAAuthScheme		
KerberosScheme		
LDAPNoPasswordValidationScheme		
LDAPScheme		
CAM 10gScheme		
OAMAdminConsoleScheme		
OINScheme		
TAPScheme		
X509Scheme		
Generation Domains Generation Committee		
▷ 戀 Resources		
✓ Authentication Policies		
Authorization Policies		
Distance Policies		
Existence in Fusion Apps Integration		
IAM Suite		i
J		

Name

Specify a name to identify the Authentication Policy (Eg: FCUBSWebPolicy).

Authentication Scheme

Select the authentication scheme you created in the previous step (Creating Authentication Scheme).

Resources

Add the resources which should be protected. If you add <WebgateName>:/.../ and <WebgateName>:/ in the resources, then all the sources are protected.

Add DN in the Responses section.





Enter the value as *\$user.attr.dn*. The responses maintained in this tab will be added in the response header at the time of authentication.

2.4.3.7 Adding Resources

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

Click 'Create New Resource' button.



ORACLE Access Manager		Accessi	ibility Help Sign Out 🧲
			Signed in as weblogi
Policy Configuration System Configuration			
All	🖸 Welcome 🚺 🌣 FCUBSWel	bgate Resources 🔅 FCUBSWebgate:FCUBSWebgate:/FCJNeoWeb	× 🖹
Search	Resources		Apply
Browse Search	CLUY .		
View 🗸 🔞 📑 🖳 🗁 %	Туре	HTTP V	
V 🔡 Shared Components	Description		
<pre>#TTP</pre>			
Contraction Contra	Host Identifier	FCUBSWebgate 💌	
🐯 wl_authen	* Desource I IRI	/EC1NeoWeb	
V 📑 Host Identifiers	Resource once	h muun	
FCUBSWebgate	Query String		
IAMSuiteAgent	* Protection Level	Protected	
V Mathematication Schemes	Authentication Policy	Protected Resource Policy -	
Anonymousscheme			
BasicScheme	Authorization Policy	Protected Resource Policy 👻	
Call EA AuthSchame			
B ECHES Auth schame			
WerberosScheme			
P I DAPNoPasswordValidationScheme			
B IDAPScheme =			
CAAMAdvanced			
CAAMBasic			
CAM 10gScheme			
CAMAdminConsoleScheme			
0IFScheme			
CIMScheme			
TAPScheme			
X509Scheme			
V G Application Domains			
V G FCUBSWebgate			
@ Resources			
Authentication Policies			
Authorization Policies			
I oken issuance Policies			
TAM Suite			
P			

Туре

Select 'HTTP'.

Host Identifier

Select 'FCUBSWebgate'.

Resource URL

Specify '/FCJNeoWeb'.

Protection Level

Select 'Protected'.

Click 'Apply' button to update the resource added.

Authentication Policy

Select the authentication policy and authorisation policy as 'Protected Resource Policy'.

2.4.3.8 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.



DRACLE: Access Manager						Accessibility Help Sign Out Signed in as web
Policy Configuration System Configuration						
Al	😐 Welcome	FCUBSWebgate:Protected Resource	Policy			×
Search	Authorization F	Policy				Apply
Browse Search	* Name	Protected Resource Policy		Failure URL		
View 🗸 🚱 🕒 🖳 🔀	Description	Policy set during domain creation. Add resources	s to this policy to	Use Implied Constraints 📝		
V 🎬 Shared Components		protect them.		Identity Assertion 📃		
\$PHTTP						
TokenServiceRP	Success URL					
🐼 wi_authen	Bocourcos	Fonstvaints Responses				
V Host Identifiers	Resources	constraints Responses				
FCUBSWebgate	🔞 Responses	5				+ ×
IAMSuiteAgent	Name	T	vne		Value	
V Mathematication Schemes	DAL		Joodor		dusor atte da	
Anonymous5cheme	Div		icauci	•	puser.aur.un	
Basicocheme						
BasicSessioniessScheme						
C AAUTHScheme						
CUBS_Auth_scheme						
Contraction of the second seco						
COLLECTION CONTRACTOR CONTRA						
LDAPScheme E						
CAAMAdvanced						
OAAMBasic						
OAM10gScheme						
OAMAdminConsoleScheme						
OIFScheme						
OIMScheme						
TAPScheme						
X509Scheme						
V C Application Domains						
▷ \$\$\$ Resources						
V a Authentication Policies						
Protected Resource Policy						
V 🛃 Authorization Policies						
Protected Resource Policy						
Token Issuance Policies	4					•
Fusion Apps Integration	L					
No Catam Suite						

Add DN in the 'Responses' tab. Enter the value as *\$user.attr.dn*.

The responses maintained in the tab will be added in the response header during authorization.

2.4.3.9 Configuring mod_wl_ohs for Oracle Weblogic Server Clusters

In order to enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server Clusters, add the below directive to the *mod_wl_ohs.sh* file in directory '<Weblogic Home> /Oracle_WT1/instances/instance1/config/OHS/ohs1'.

<Location /console> SetHandler weblogic-handler WebLogicHost idmhost1.mycompany.com WeblogicPort 7001

</Location>

2.4.3.10 Checking the Webgate 11g Agent Creation

After configuration of webgate 11g agent, go to the URL <u>http://<hostname>:<ohs_Port>/ohs/modules/webgate.cgi?progid=1</u> and verify whether the webgate configuration is fine. If the URL launches the following screen, then it indicates that the webgate configuration works fine.



Access Server	Conr St	ection tate	Create	d Installa Direct	tion Num Of Dir ory Threads Infor	ectory mation
padsrini-pc 5575, 1	Up		Monda <u>y</u> August 27, 201 11:08:0	y, 2 1		
Cache Name	State	Max Elems	Curr Elems	Timeout (seconds)	Cache Stats (Hits:Misses: Expired:Flushed)	Memory Footprin (bytes)
Resource to Authentication Scheme	active	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

2.4.3.11 Using OAM Test Tool

This step is not mandatory.

Oracle Access Manager Test Tool helps you check the response parameter values. The test tool is available in *<OAM Install Dir>\ oam\server\tester*.

Eg. D:\weblogic\Middleware\Oracle_IDM1\oam\server\tester

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



Oracle Access Manager T	est Tool				
le <u>E</u> dit <u>T</u> est <u>H</u> elp					
e 🗟 🥔 🔁					
Server Connection					
IP Address		Port Max C	onn *Agent	t ID	
Primary: padsrini-pc		5575 1	FCUB	SWebgate	
Secondary:		0 1	Agent	Password	?
Min Conn. Timonut (mr)	Mada				
1 30000	open 👻				Connect
Protected Resource URI					*
Scheme *Host			Port		V
http 🔻 FCUBSWe	ebgate		0		Get Auth Scheme
Resource			Ope	ration	Volidata
/FCJNeoWeb			Cat		validate
User Identity IP Address	*Username	Pass	word		•
Jser Identity IP Address User Certificate Store	*Username SARAN	Pass •••	word	. ?	Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages	*Username SARAN	Pass ••	word	. ?	Authenticate Authorize
Jser Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response]	*Username SARAN	Pass ●●	word oam/server	. ?	Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response] [8/27/12 11:17 AM][response]	*Username SARAN Redirect URL : https Credentials expecte	Pass ●● ://padsrini-pc:14101/ d : 0x1 (basic)	word oam/server	?	Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response] [8/27/12 11:17 AM][request] [8/27/12 11:17 AM][request]	*Username SARAN Redirect URL : https Credentials expecte uthenticate] yes User DN : on=SARAI	//padsrini-pc:14101/ d: 0x1 (basic)	oam/server		Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response] [8/27/12 11:17 AM][response] [8/27/12 11:17 AM][response] [8/27/12 11:17 AM][response]	Username SARAN Redirect URL : https Credentials expective User DN : on=SARAI SessionID : 9653964	Pass 	oam/server		Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response]	Username SARAN Redirect URL : https (Credentials expecte uthenticate] yes User DN : on=SARAI SessionID : 9653964 action] DN : on=SAF	Pass 	oam/server e.do=com 1007cf6de08 iole.do=com		Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response]	Username SARAN SARAN Credentials expecte uthenticate] yes User DN : on=SARAI SessionID : 965396 action] DN : cn=SAF action] OAM_IMPEI uthorize] yes	Pass //padsrini-pc:14101/ //padsrini-pc:14101/ d : 0x1 (basic) N,cn=users,dc=oracle sa-751d-456c-ac60-6 tAN,cn=users,dc=oracle RSONATOR_USER :	oam/server e,do=com 007ct6de08 icle,do=com		Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response] [8/27/12 1	Username SARAN SARAN Credentials expecte uthenticate] yes User DN : on=SARAI SessionID : 9653964 action] DN : on=SAFI uthorize] yes actioni DN : cn=SAFI	Pass //padsrini-pc:14101/ d:0x1 (basic) N.on=users,do=oraole: tAN, on=users,do=ora SONATOR_USER : tAN, on=users,do=ora	vord oam/server e,do=com 1007.cf8de08 icle,do=com icle,do=com	. ?	Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response] [8/27/12 1	*Username SARAN Redirect URL : https Credentials expecte uthenticate] yes User DN : on=SARAI SessionID : 965396 action] OAM_IMPEI uthorize] yes action [OAM_REM(action] OAM_REM(Pass 	word oam/server e,do=com 0007cf6de08 icle,do=com icle,do=com	. ?	Authenticate Authorize
User Identity IP Address User Certificate Store User Certificate Store [8/27/12 11:17 AM][response] [8/	Username SARAN Redirect URL : https Credentials expect User DN : on=SARAI SessionID : 965396 action] DN : on=SAI action] OAM_IMPEI uthorize] yes action] DN : on=SAI action] OAM_IMPEI action] OAM_IMPEI action] OAM_IDENT	Pass //padsrini-pc:14101/ //padsrini-pc:14101/ //on=users,do=oraol4 sa-751d-4560-ac60-5 tAN,on=users,do=ora tAN,on=users,do=ora tSONATOR_USER : tAN,on=users,do=ora tSONATOR_USER : tAN,on=users,do=ora tSONATOR_USER : table table	vord oam/server a,do=com 1007cf6de08 icle,do=com icle,do=com BSIdentityStore		Authenticate Authorize
User Identity IP Address User Certificate Store Status Messages [8/27/12 11:17 AM][response] [8/27/12 1	Username SARAN Redirect URL : https Credentials expecte uthenticate] yes User DN : on=SARAI SessionID : 9653964 action] DN : on=SAF action] OAM_IMPEI uthorize] yes action] OAM_IMPEI action] OAM_IMPEI action] OAM_IMPEI action] OAM_IDEN1	Pass //padsrini-pc:14101/ d: 0x1 (basic) N,cn=users,dc=oracle taa-751d-456c-ac60-6 tAN,cn=users,dc=ora RSONATOR_USER : RSONATOR_USER : RSONATOR_USER : STE_USER : SARAN TTE_USER : SARAN	word oam/server e,do=com 10f07cf6de08 icle,do=com Icle,do=com BSIdentityStore		Authenticate Authorize

2.4.4 First Launch of Oracle Banking Payments after Installation

After installing Oracle Banking Payments and launching it for the first time, you will see the Oracle Banking Payments login screen which prompts for user ID and password. This is because the parameter 'sso installed' is set to 'N' during installation.

2.4.4.1 Bank Parameter maintenance

In order to enable SSO for Oracle Banking Payments, login to the application and check 'SSO Enabled' check box in 'Bank Parameters Maintenance' screen.



Bank Parameters Maintenance	-	×
Bank Code * 000	Customer Name BANK FUTURA	
Head Office Branch Code * 000	Description BANK FUTURA	
Financial Preferences General Preferences		
Format Masks CIF Mask bbbnnnnn General Ledger Mask* nnnnnnnn	Year End Profit and Loss General Ledger * 241000801 Transaction Code * 000	III
Spread Application Both Leg Spool File Purge Days 90 Inter Pay Lead days 3	General Ledger Purge Days Auto Batch User Restriction For Batch Number SSO Enabled	
Cheque Numbering Details Scheme Cheque Numbers Unique for Branch	Checksum Algorithm	
TRS Details	Suspense Account	-
Account Mask Preferences Fields Input ByLC32702 Authorized ByLC32702A03 Date Time 2012-02-29 13:26:22 Date Time 2012-02-29	Modification 152 Authorized 15:20:45 Number Open Ok Exit	

2.4.4.2 SSO Parameters

After enabling SSO, you need to maintain the parameters required for SSO. Go to 'Security Maintenance -> Sys. Administration -> SSO Maintenance'.

🔷 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) *	600				
Fields					
Input BySARAN	Authorized By SAF	N Modification	1	Authorized	
Date Time 2012-01-06 12:3	3:04 Date Time 201	01-06 12:33:04 Number		V Onen	Exit

Specify all the details such as Directory Server Host Name, Port Number, LDAP Admin User ID, Admin Password, LDAP Base and Login Time Out Duration (in seconds).



2.4.4.3 Maintaining Branch Level DN Template (Branch Maintenance)

Go to the 'Branch Maintenance' screen of Oracle Banking Payments.

You need to maintain LDAP DN template for each branch. This is used in the Oracle FLEXCUBE user maintenance form to populate corresponding LDAP user ID automatically from this template. Go to 'Branch Parameters' screen and click 'Preferences' button.

Branch Parameters Prefere	ences		×
Netting Suspense General	233200804	Profit and Loss Adjustment	
Ledger			Track Previous Year Profit
Walk In Customer	000003171		And Loss Adjustment
Internal Swap Customer	0000031/1	Revaluation Split Details	
Clearing Account			Revoluction Split Required
Offset Clearing Account			
Weekly Holiday 1	Saturday 👻	Suspense Product Maintenand	ce
Weekly Holiday 2	Sunday 🚽	Debit Product	
Clearing Bank Code		Description	
MIS Group For Currency		Credit Product	
	Interdict Validation Required	Description	
Interdict Timeout Interval		International Banking Account	Number Masks
Status Processing Basis	Contract Level 📼	Bank Code	aaaann
Provisioning Frequency	Daily 👻	Account Number	aann
Uncollected Funds Basis		501 Jata (*	
Uncollected Funds	-	FGL Integration	
	Deferred Statement		FGL Handoff Required
	Generation	ELCM Integration	
Minor Age Limit (Vrs)	18		FLCM Replication
Notification Days			
Cheque Stale Days			
Limit Evpin/Advice Notification			
Days			
Back Value Details		LDAP DN Template	
	Back Valued Check	I DAP DN Template	cn= <fcclisr> cn=Liser</fcclisr>
	Required	LDAI DIV remplate	s,dc=oracle,dc=com
Back Value Days		L	
I CY Message Dreferences			
Lor mooduge Preferences			
			Ok Exit

Specify the LDAP DN Template.

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

In the above template *cn*=<*FCJUSR*> part must be there without alteration. However, the rest of the DN name can be changed based on the configuration.

2.4.4.4 Maintaining LDAP DN for FCUBS users

For each user ID in Oracle FCUBS, a user has to be created in the LDAP.



When creating the user in LDAP, ensure that the DN is same as the LDAP DN specified in 'User Maintenance'. Once the user is created in LDAP, go to the 'User Maintenance' in Oracle FCUBS. If the Oracle FCUBS user already exists, then unlock the user maintenance and update the LDAP DN value which was set while creating the user in LDAP. Click 'Validate' button to check whether any other user has the same LDAP DN value.

🔶 User Maintenance											_ ×
User Details						Us	er Status	OEnabl A Second secon	led		
User Identificatio Nan User Referen Languag Home Bran Customer N	on * FCUBS ne * FCUBS ce ge * ENG ch * 004	USER User			٤	Clas Status Cha Last S	sification anged On igned On	Hold Disat Locke Staff Branc	oled ed ch		
Department Coo Department Descriptio Tax Identifi LDAP D Time Lev Amount Form Date Form	de er N FCUBS rel * 9 at at Auto Validat	USER v Authorizatior	1]		ELCI	/I User ID	Staff Req	Customer F uired	Restriction	
User Password Passwo Password Changed C Ema	rd •••••• On 2012-0 ail	 1-06 11:01:3	3			5	Start Date [:] End Date	* 2012-0	1-06		
Invalid Logins Cumulati Successi	ve										
Restricted Password Ro	les Rights	Functions	Tills	Accoun	t Classes	General	Ledgers	Limits	Branches	Products	
Disallowed Functions Us	ers Holiday	Fields Gr	oup Re	striction	Centraliz	ed Role					
Maker KANN Checker SARA	AN1 N		Date ⁻ Date ⁻	Time: 20 [.] Time: 20 [.]	12-01-06 1: 12-01-06 1:	3:29:56 3:34:26	Reco Authorizati	Mod No ord Status on Status) 3 Closed Authorized		Exit

2.4.4.5 Launching Oracle Banking Payments

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

Eg.: 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 Oracle Banking Payments application server URL. You can see the new sign-on screen. The application automatically redirects to Oracle Banking Payments home page.



CRACLE' FLEXCUBE Universal Banking		
Theme Default		
	Theme Default .	
Copyright © 2010, Oracle and/or its affliates. All rights reserved.	Copyright © 2010, Oracle and/or its affiliates. All rights reserved.	

2.4.4.6 Signoff in a SSO Situation

Oracle Banking Payments does not provide for single signoff. When a user signs off from Oracle Banking Payments, the session established with Oracle Access Manager by the user will not be modified in any manner.

In an SSO situation the 'Signoff' action in Oracle Banking Payments functions as 'Exit'. On clicking 'Signoff', the user will exit Oracle Banking Payments. The user needs to re-launch Oracle Banking Payments using the Banking Payments launch URL to use it again.





Oracle Banking Payments Oracle Access Manager Integration [May] [2021] Version 14.5.0.0.0

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

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

Copyright © [2017], [2021], 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.