Oracle® Banking Payments

Oracle Access Manager Integration

Release 14.8.0.0.0
G32383-01
April 2025

Oracle Banking Payments Oracle Access Manager Integration, Release 14.8.0.0.0

G32383-01

Copyright © 2017, 2025, Oracle and/or its affiliates.

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 Preface

1.1 Purpose 1-1
1.2 Audience 1-1
1.3 Documentation Accessibility 1-1
1.4 Critical Patches 1-1
1.5 Diversity and Inclusion 1-2
1.6 Conventions 1-2

2 Enabling Single Sign-on with Oracle Access Manager

2.1 Introduction 2-1
2.2 Prerequisites 2-1
2.3 Background of SSO Related Components 2-2
2.3.1 Oracle Access Manager (OAM) 2-2
2.3.2 LDAP Directory Server 2-2
2.3.3 WebGate/AccessGate 2-2
2.3.4 Identity Asserter 2-3

3 Configuration

3.1 Pre-requisites 3-1
3.2 Changing web.xml file 3-1
3.3 Configuring SSO in OAM Console 3-2
3.3.1 Identity Store Creation 3-2
3.3.2 Creating Authentication Module 3-4
3.3.3 Creating OAM 11g Webgate 3-5
3.3.4 Post OAM Webgate 11g Creation Steps 3-7
3.3.5 Creating Authentication Scheme 3-7
3.3.6 Creating Authentication Scheme 3-8
3.3.7 Adding Resources 3-9
3.3.8 Adding Authorization Policy 3-10
3.3.9 Configuring mod_wl_ohs for Oracle Weblogic Server Clusters 3-12
3.3.10 Checking the Webgate 11g Agent Creation 3-12
3.3.11 Using OAM Test Tool 3-13

3.4 First Launch of Oracle Banking Payments after Installation 3-14
3.4.1 Bank Parameter Maintenance 3-15
3.4.2 SSO Parameters 3-15
3.4.3 Maintaining Branch Level DN Template (Branch Maintenance) 3-16
3.4.4 Maintaining LDAP DN for FCUBS users 3-17
3.4.5 Launching Oracle Banking Payments 3-18
3.4.6 Signoff in a SSO Situation 3-20

1
Preface

- Purpose
- Audience
  This manual is intended for the following User/User Roles:
- Documentation Accessibility
- Critical Patches
- Diversity and Inclusion
- Conventions

1.1 Purpose

This guide is designed to help acquaint you with the Oracle Banking Payments application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

1.2 Audience

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

Table 1-1 User Roles

Role	Function
Implementation & IT Staff	Implementation & Maintenance of the Software

1.3 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.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1.4 Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to make sure effective security, as strongly recommended by Oracle Software Security Assurance.

1.5 Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1.6 Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

2

Enabling Single Sign-on with Oracle Access Manager

- Introduction
- Prerequisites
- Background of SSO Related Components

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

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 Directoryr

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

WebLogic (10.3.5)P

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

2.3 Background of SSO Related Components

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

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

https://docs.oracle.com/cd/E12839_01/core.1111/e10043/osso.htm

> **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.

3
Configuration

- Pre-requisites
- Changing web.xml file
- Configuring SSO in OAM Console
- First Launch of Oracle Banking Payments after Installation

3.1 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.

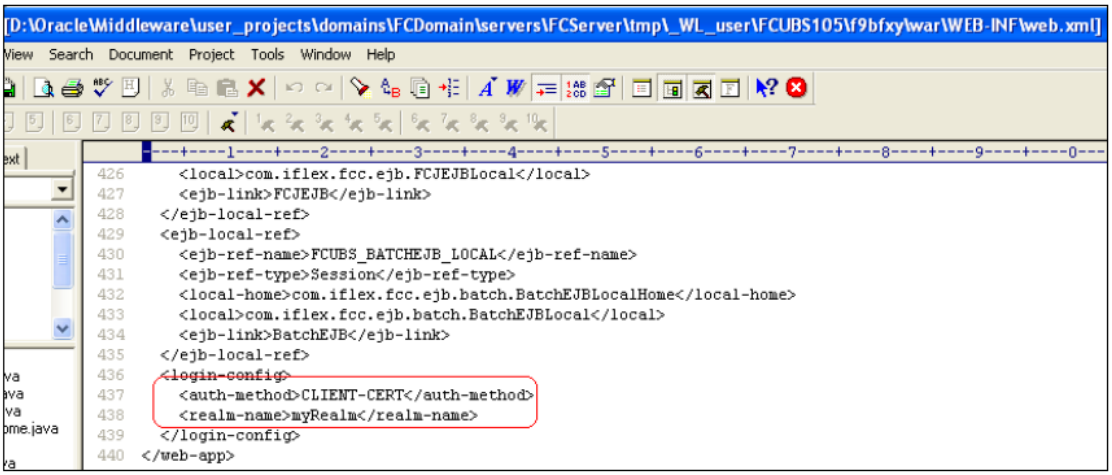
3.2 Changing web.xml file

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

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

```
<login-config>
<auth-method>CLIENT-CERT</auth-method>
<realm-name>myRealm</realm-name>
 </login-config>
```

Figure 3-1 login-config



Save the file and redeploy it. 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 explained in the page

https://docs.oracle.com/cd/E17904_01/install.1111/e12002/webgate004.htm

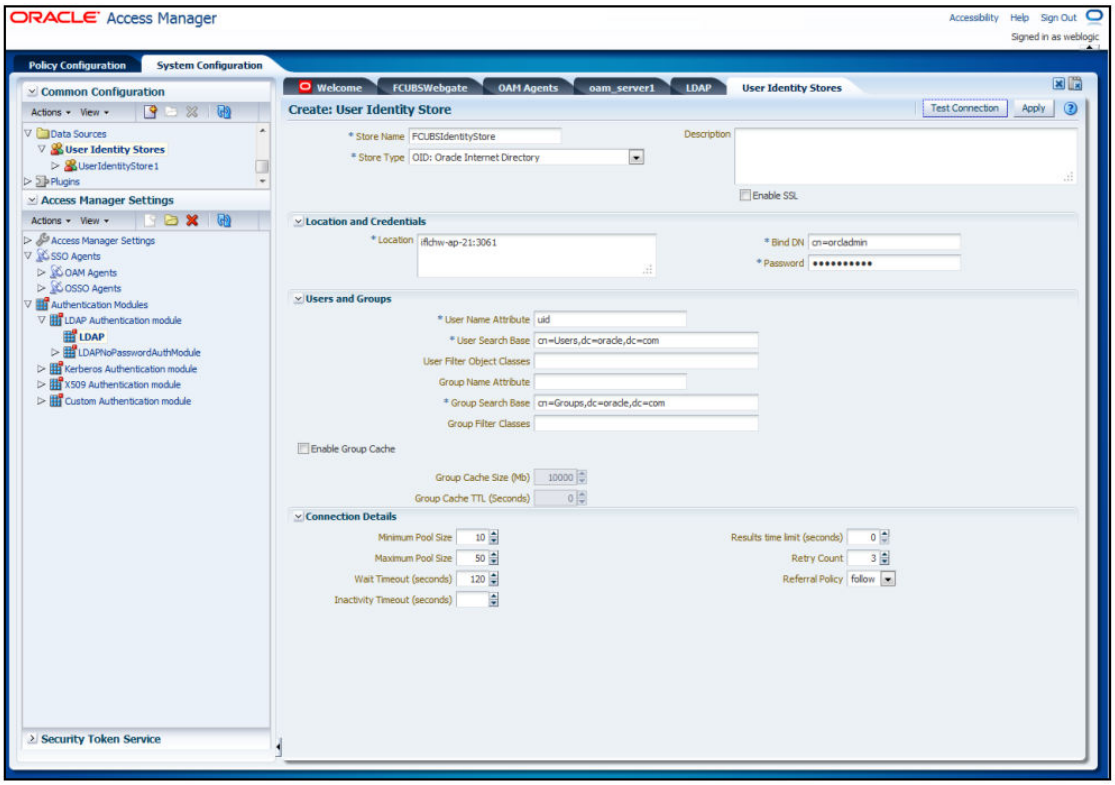
- Identity Store Creation
- Creating Authentication Module
- Creating OAM 11g Webgate
- Post OAM Webgate 11g Creation Steps
- Creating Authentication Scheme
- Creating Authentication Scheme
- Adding Resources
- Adding Authorization Policy
- Configuring mod_wl_ohs for Oracle Weblogic Server Clusters
- Checking the Webgate 11g Agent Creation
- Using OAM Test Tool

3.3.1 Identity Store Creation

Create a new User Identity Store.

1. Login to OAM Console.
2. Go to System Configuration, then Common configuration and click Data Sources to select User Identity Store.

Figure 3-2 Create User Identity Store

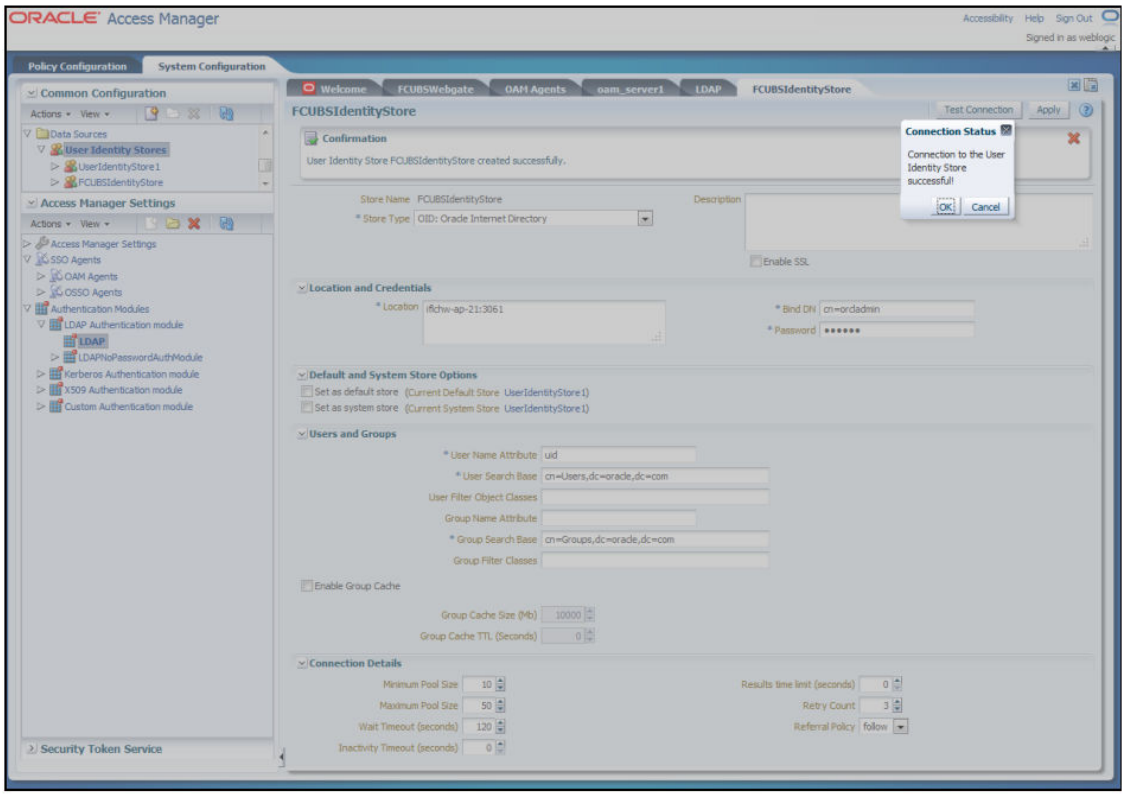


Specify the following details in the User Identity Store.

Field	Description
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.

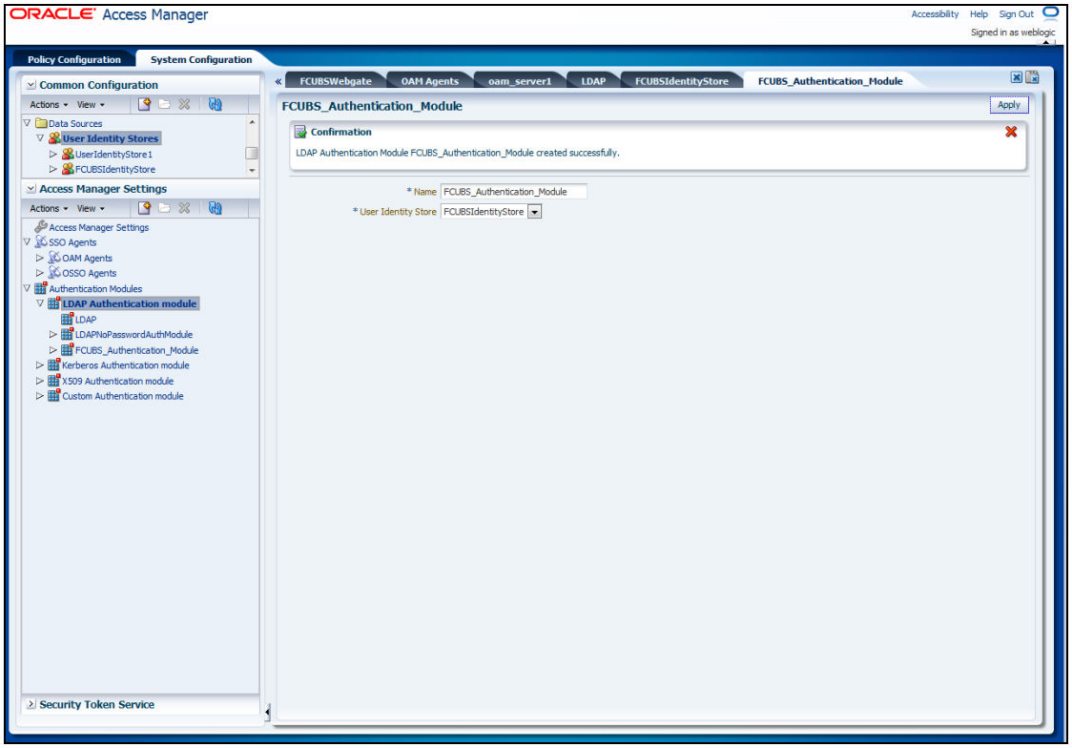
Figure 3-3 FCUBSIdentityStore



3.3.2 Creating Authentication Module

1. Go to System Configuration, then Access Manager Settings and click Authentication Modules to select LDAP Authentication Module.

Figure 3-4 FCUBS_ Authentication Module



2. Click **New** button to create new Authentication Module.

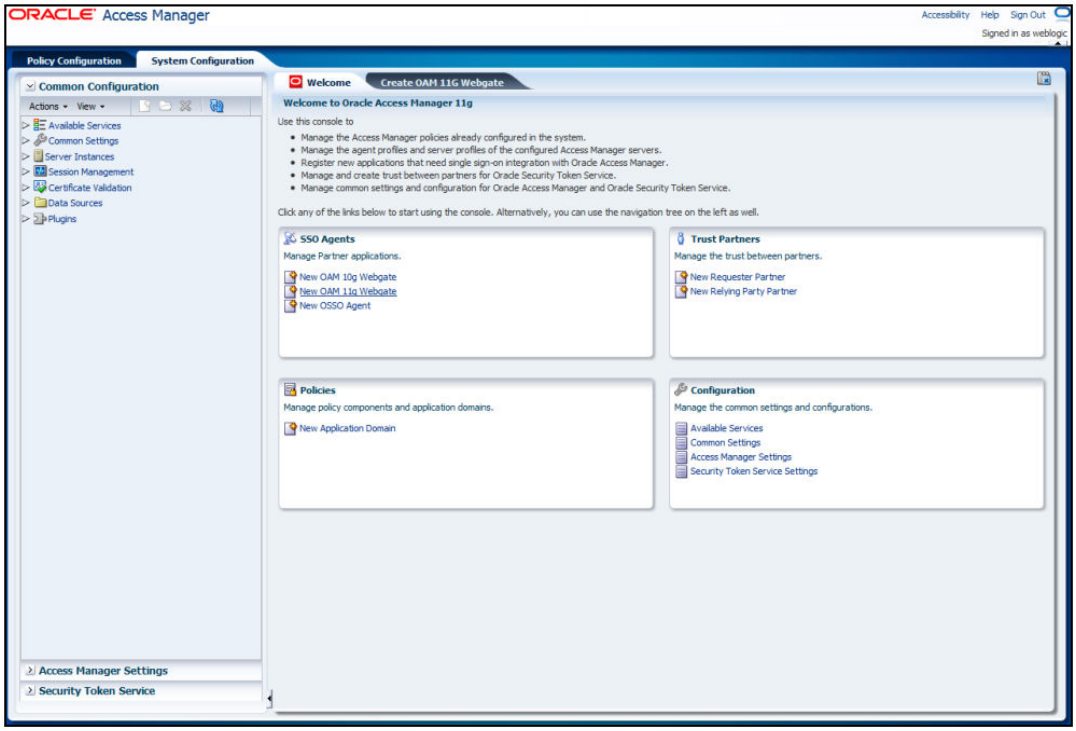
Specify the following details in the User Identity Store.

Field	Description
Name	Specify the name of the authentication module.
User Identity Store	Specify the user identity store you had created in the previous step.

3.3.3 Creating OAM 11g Webgate

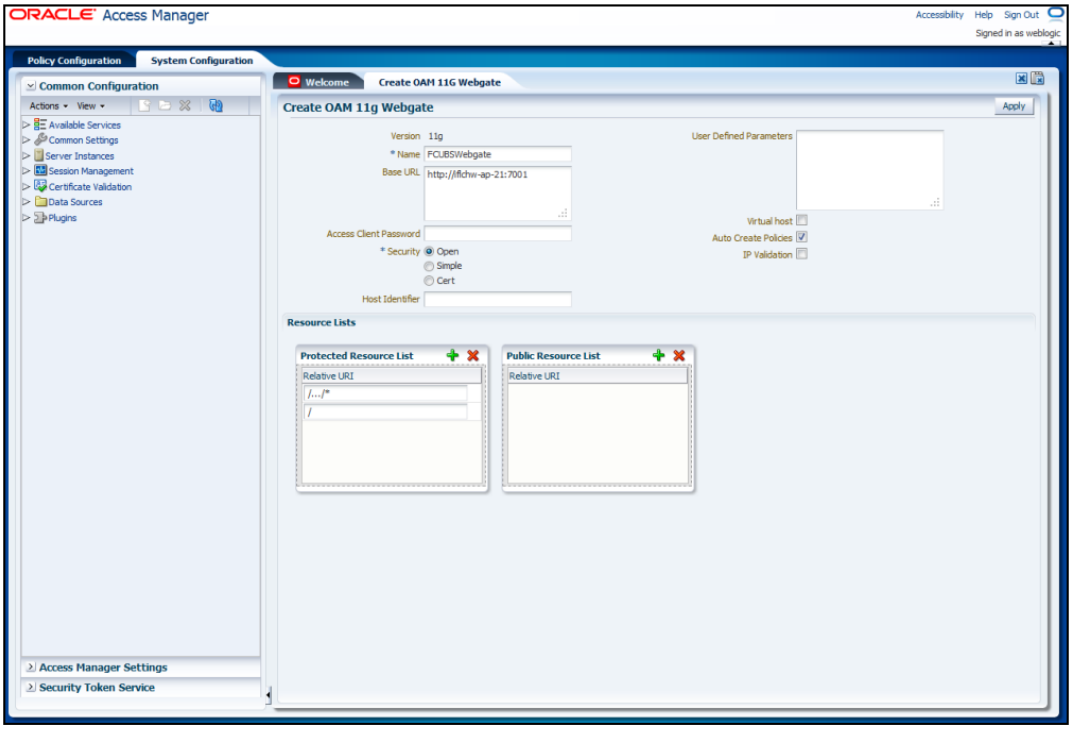
1. Go to System Configuration, then Access Manager Settings and click SSo Agents to OAM Agents.

Figure 3-5 Create OAM 11g Webgate



2. Click **Create 11g webgate** button or **New OAM 11g Webgate** link on the Welcome page **New** button to create new Authentication Module.

Figure 3-6 Create OAM 11g Webgate



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.

3.3.4 Post OAM Webgate 11g Creation Steps

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

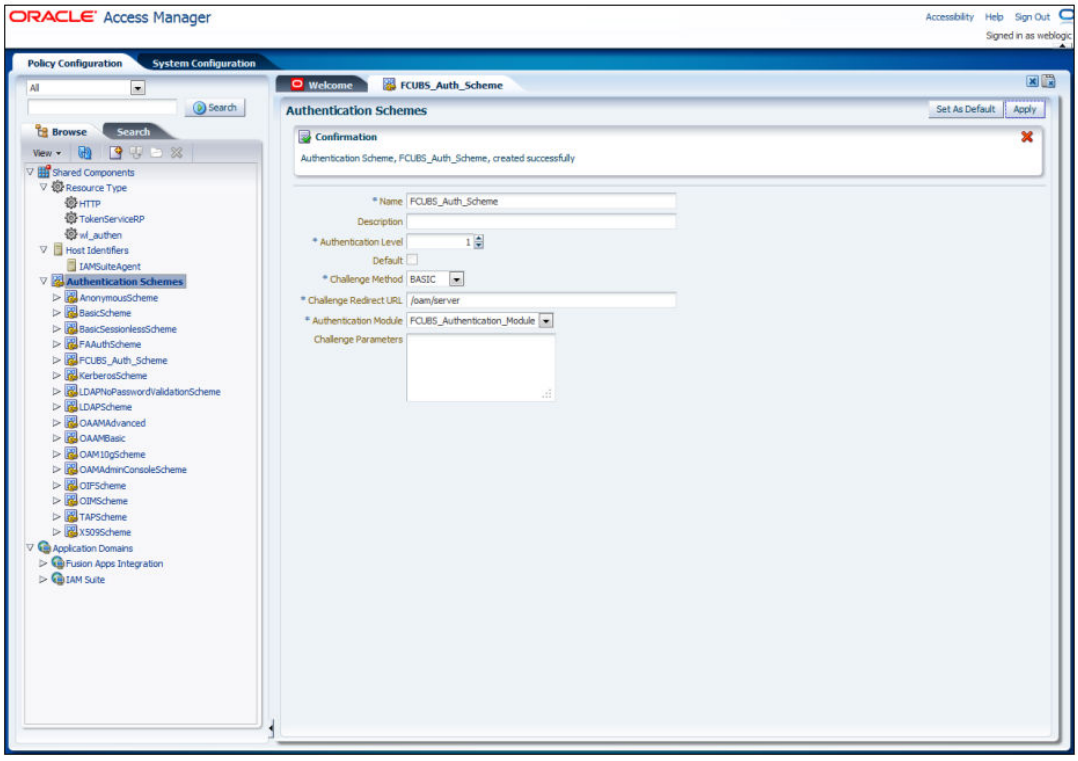
1. On the Oracle Access Manager Console host, locate the updated OAM Agent ObAccessClient.xml configuration file and any certificate artifacts.
   For example: $DOMAIN_HOME/output/$Agent_Name/ObAccessClient.xml
2. On the OAM Agent host, copy artifacts (to the following Webgate directory path). Example: 11gWebgate_instance_dir/webgate/config/ObAccessClient.xml

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

3.3.5 Creating Authentication Scheme

1. Go to Policy Configuration, then Authentication Schemes.
2. Click **Create** button to create a new Authentication Scheme.

Figure 3-7 FCUBS_ Authentication Scheme



Specify the following details in the User Identity Store.

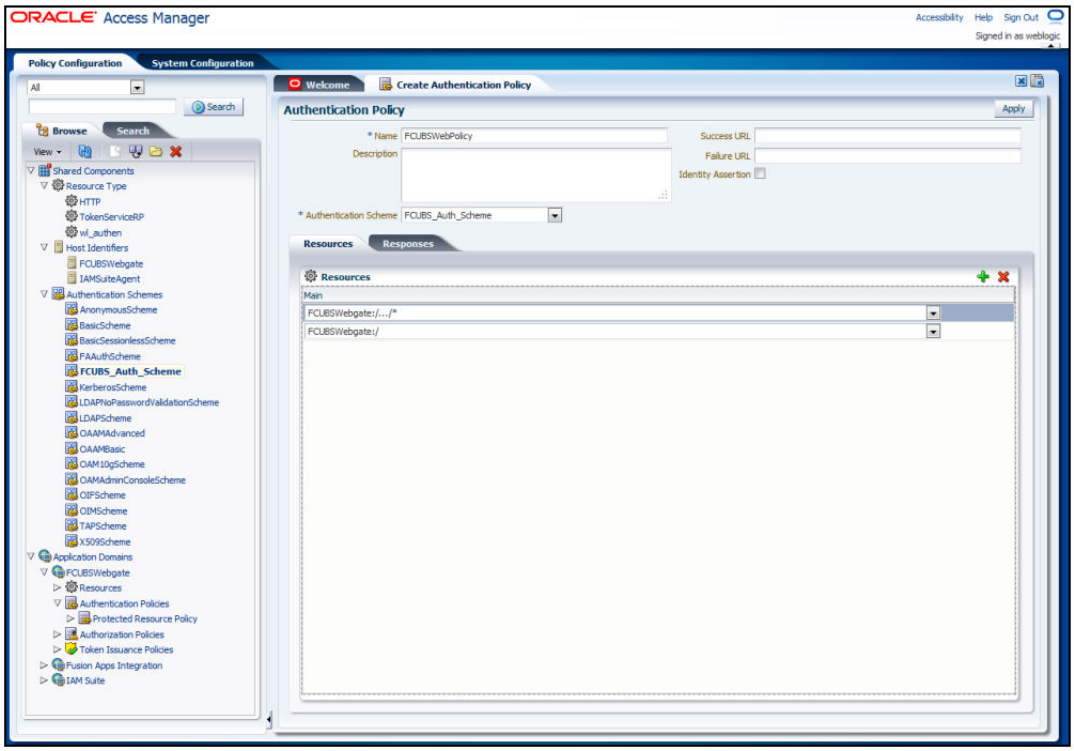
Field	Description
Name	Specify a name to identify Authentication Scheme.

Field	Description
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-authcredentials> </security-configuration>

3.3.6 Creating Authentication Scheme

1. Go to Policy Configuration, then Application Domains.
2. Select **[Webgate agent name]** under **Authentication Policies**
3. Click **New** button and specify the following information.

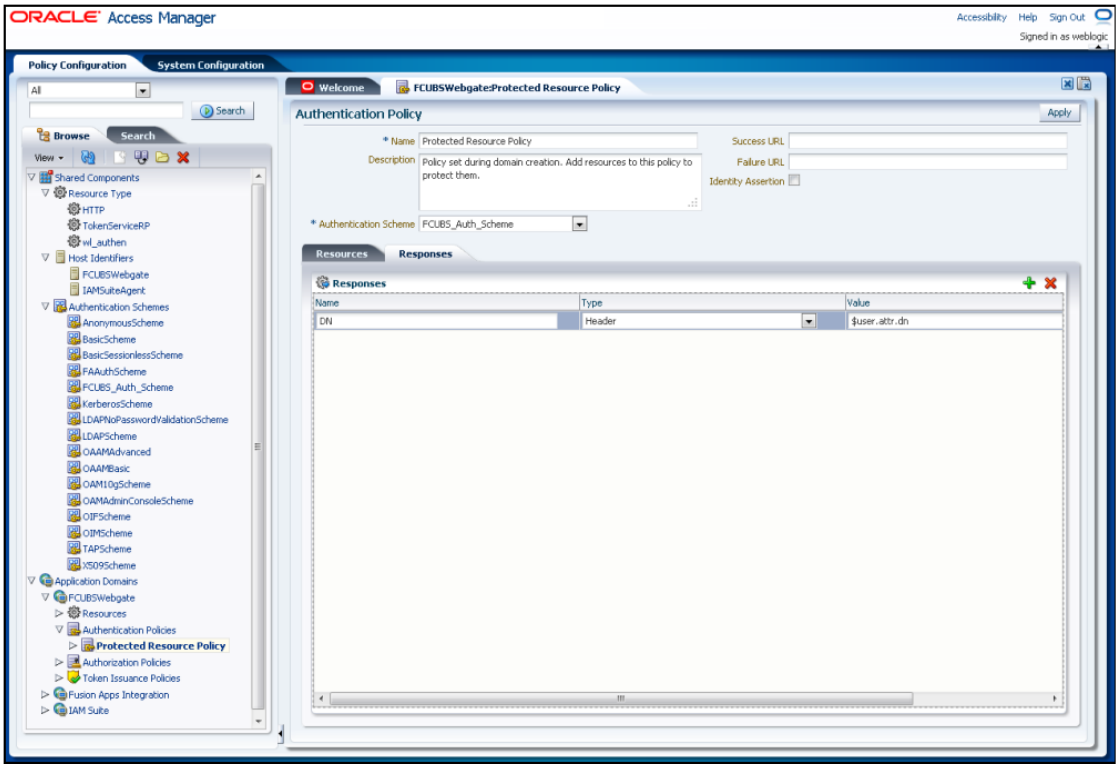
Figure 3-8 Authentication Policy



Specify the following details.

Field	Description
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.

Figure 3-9 Authentication Policy

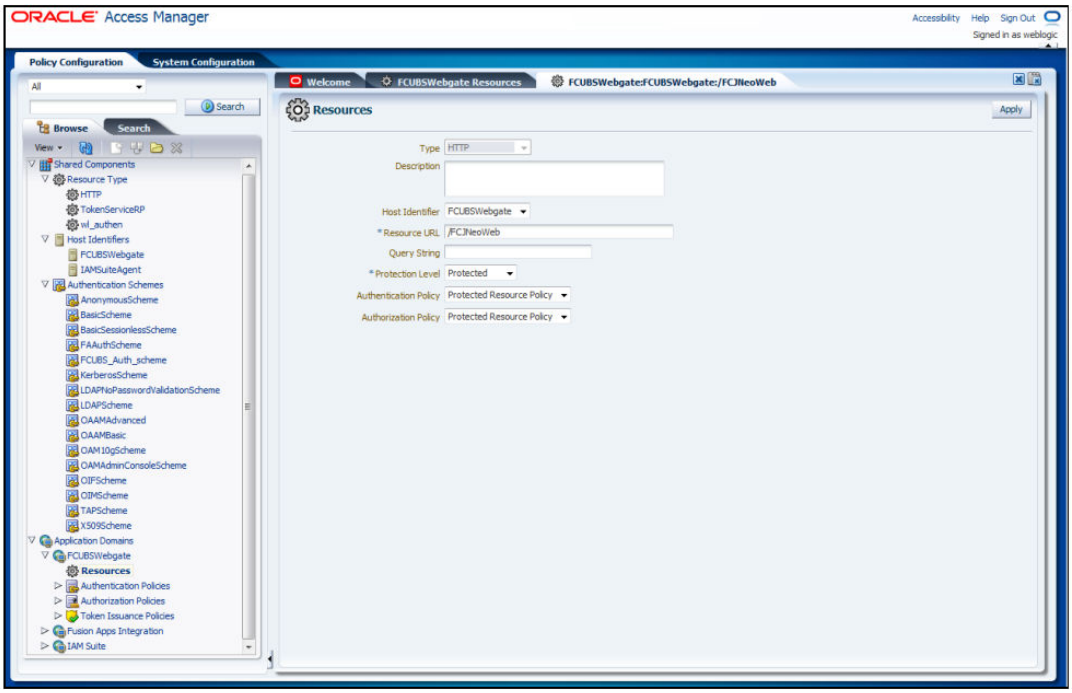


Enter the value as $user.attr.dn. The responses maintained in this tab will be added in the response header at the time of authentication.

3.3.7 Adding Resources

1. Go to Policy Configuration, then Application Domains.
2. Select **FCUBSWebgate** and click **Resources**.
3. Click **Create New Resource** button.

Figure 3-10 Resources



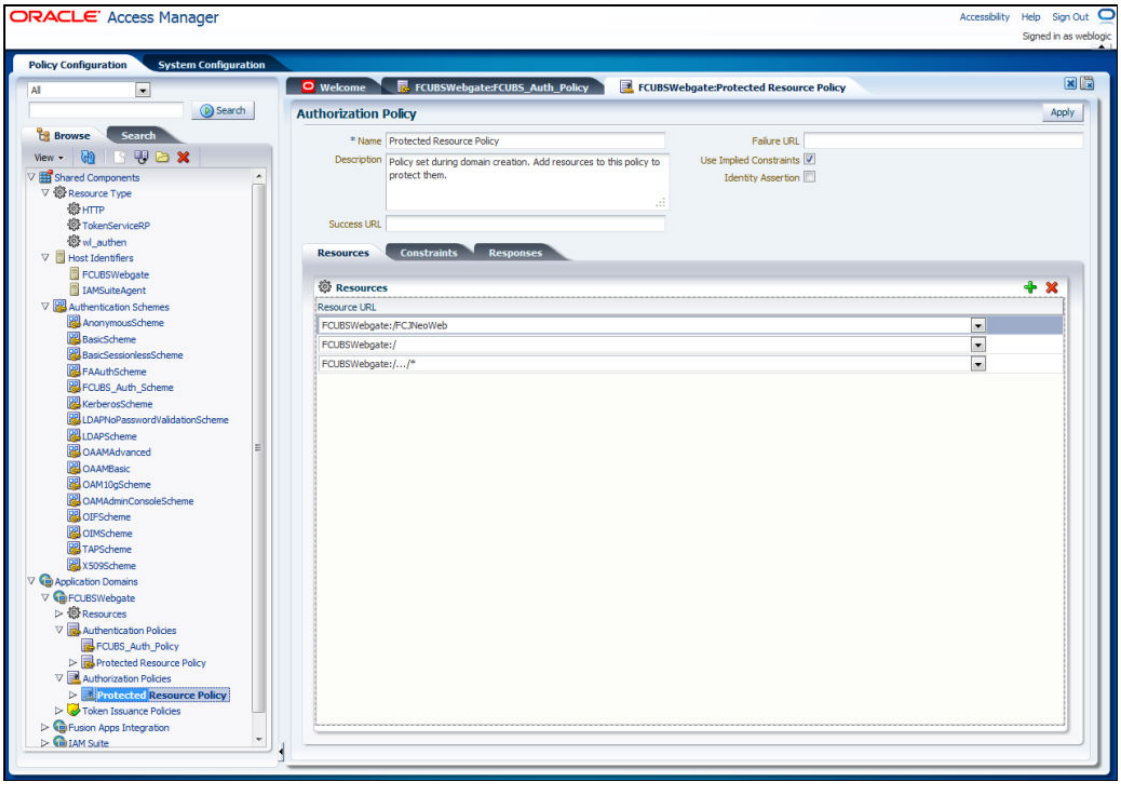
Specify the following details.

Field	Description
Type	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’.

3.3.8 Adding Authorization Policy

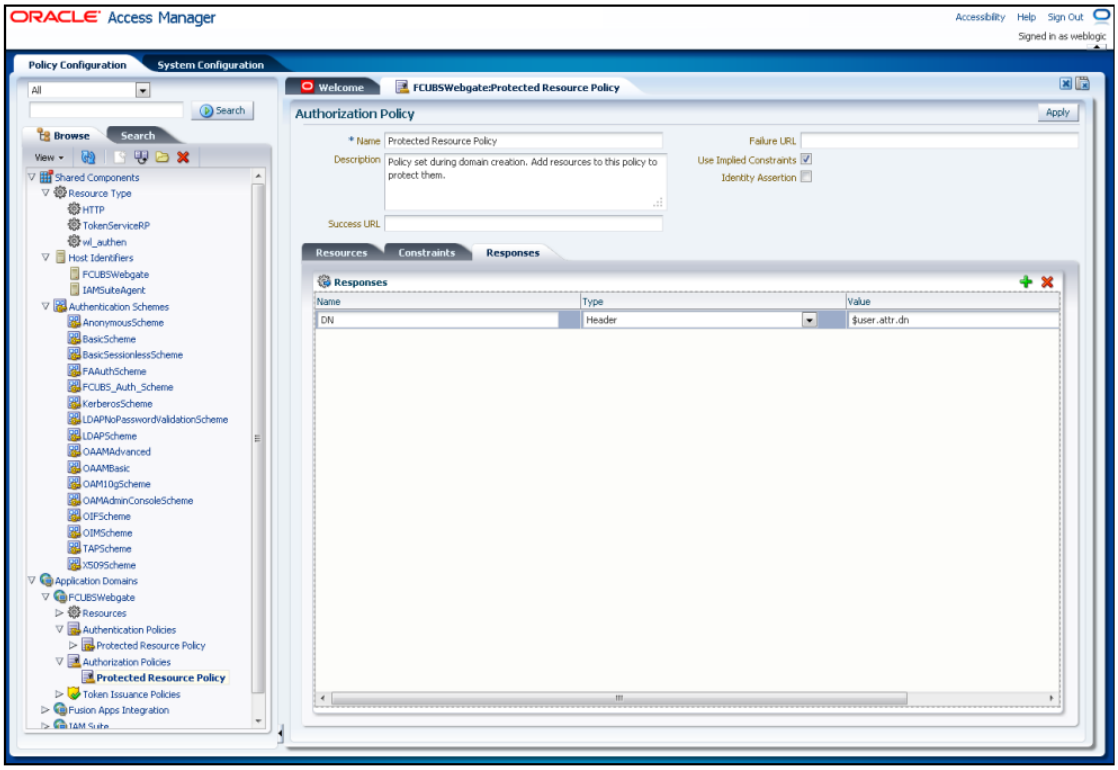
Check whether the resources available in the authentication policies are available in Authorization Policy.

Figure 3-11 Authorization Policy



During web gate creation, these values are defaulted.

Figure 3-12 Authorization Policy



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.

3.3.9 Configuring mod_wl_ohs for Oracle Weblogic Server Clusters

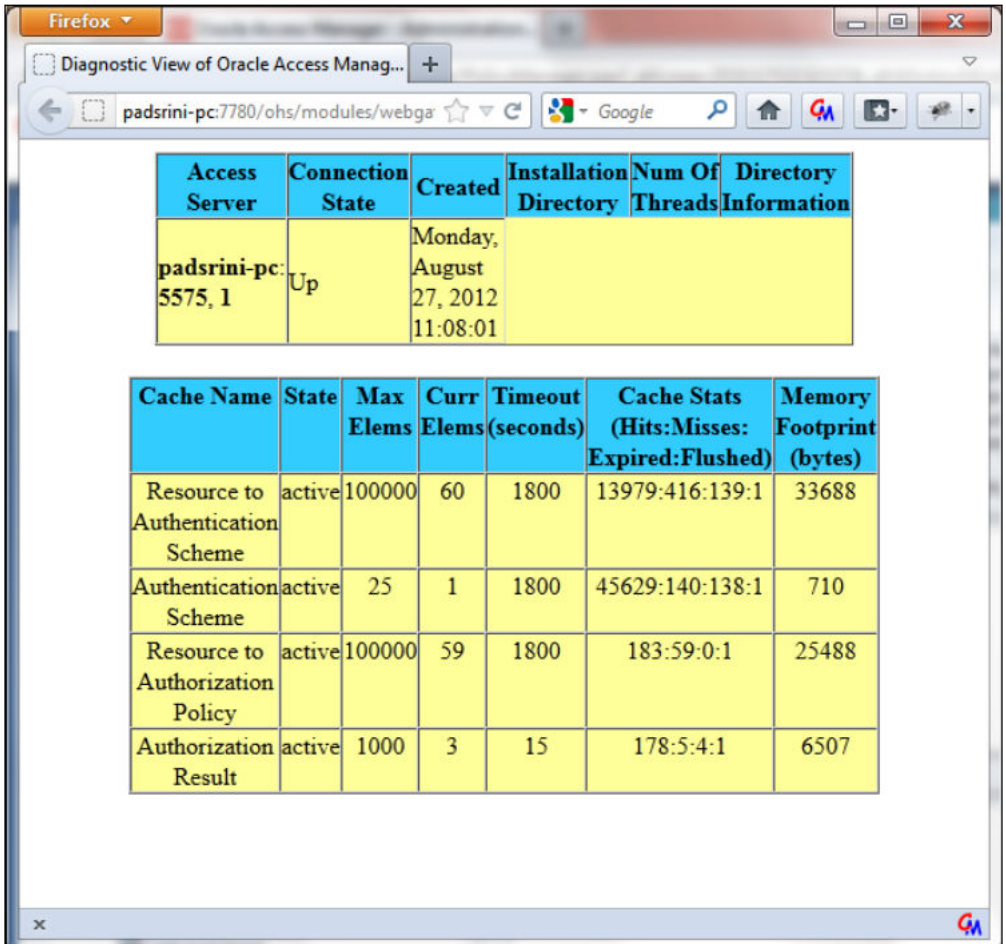
In order to enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server Clusters, add the below directive to the mod_wl_ohs.sh file in directory ‘<Weblogic Home> /Oracle_WT1/instances/instance1/config/OHS/ohs1’.

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

3.3.10 Checking the Webgate 11g Agent Creation

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

Figure 3-13 Firefox



Access Server	Connection State	Created	Installation Directory	Num Of Threads	Directory Information
padsrini-pc: 5575, 1	Up	Monday, August 27, 2012 11:08:01			

Cache Name	State	Max Elems	Curr Elems	Timeout (seconds)	Cache Stats (Hits:Misses: Expired:Flushed)	Memory Footprint (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

3.3.11 Using OAM Test Tool

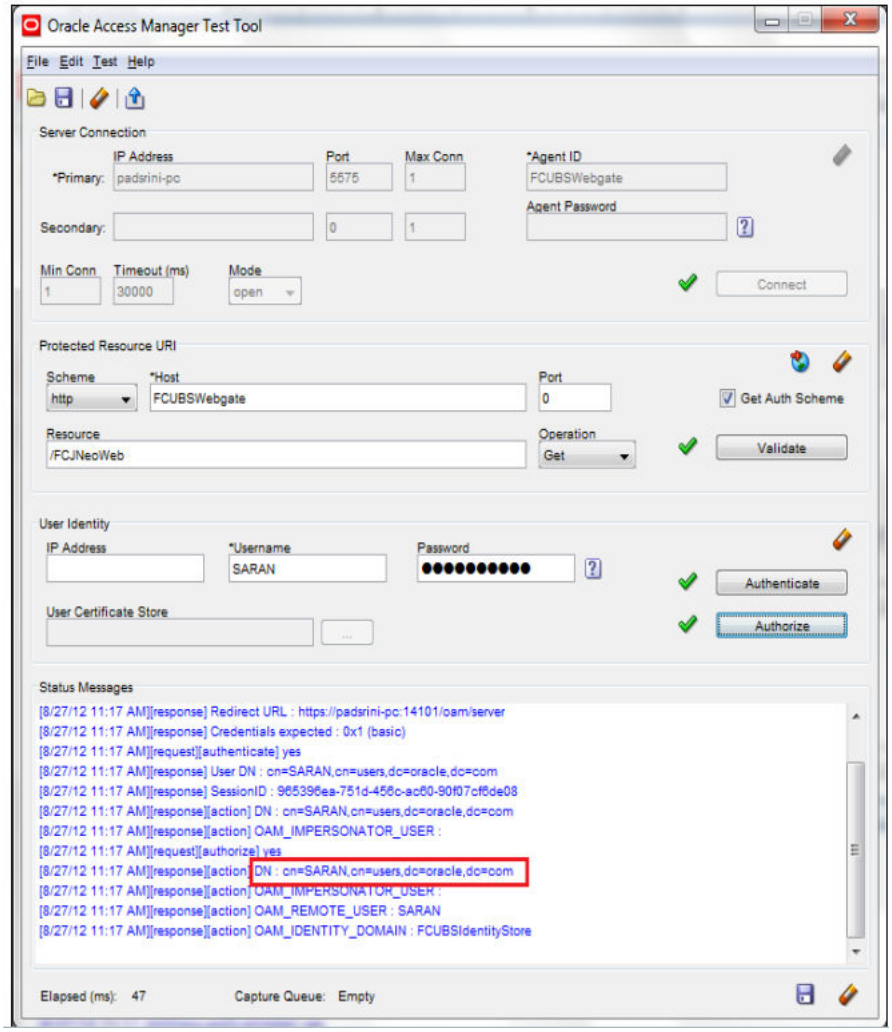
This step is not mandatory.

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.

Figure 3-14 Oracle Access Manager Test Tool



3.4 First Launch of Oracle Banking Payments after Installation

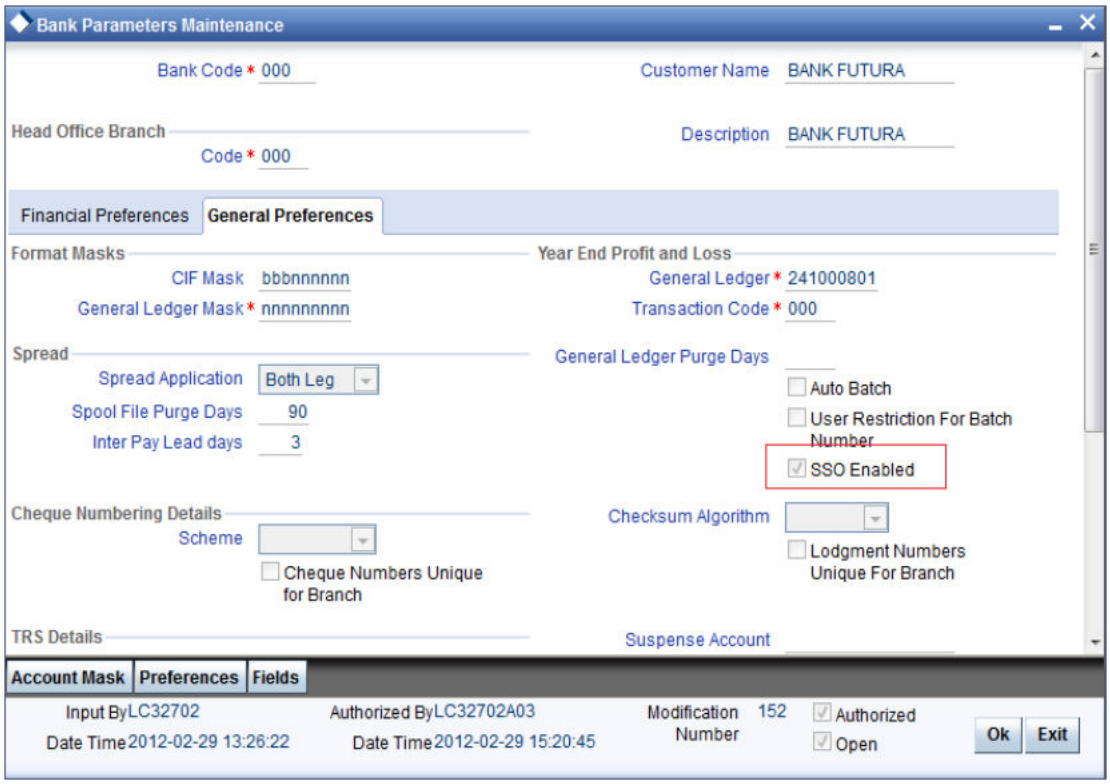
After installing Oracle Banking Payments and launching it for the first time, you will see the Oracle Banking Payments login screen which prompts for user ID and password. This is because the parameter ‘sso installed’ is set to ‘N’ during installation.

- Bank Parameter Maintenance
- SSO Parameters
- Maintaining Branch Level DN Template (Branch Maintenance)
- Maintaining LDAP DN for FCUBS users
- Launching Oracle Banking Payments
- Signoff in a SSO Situation

3.4.1 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.

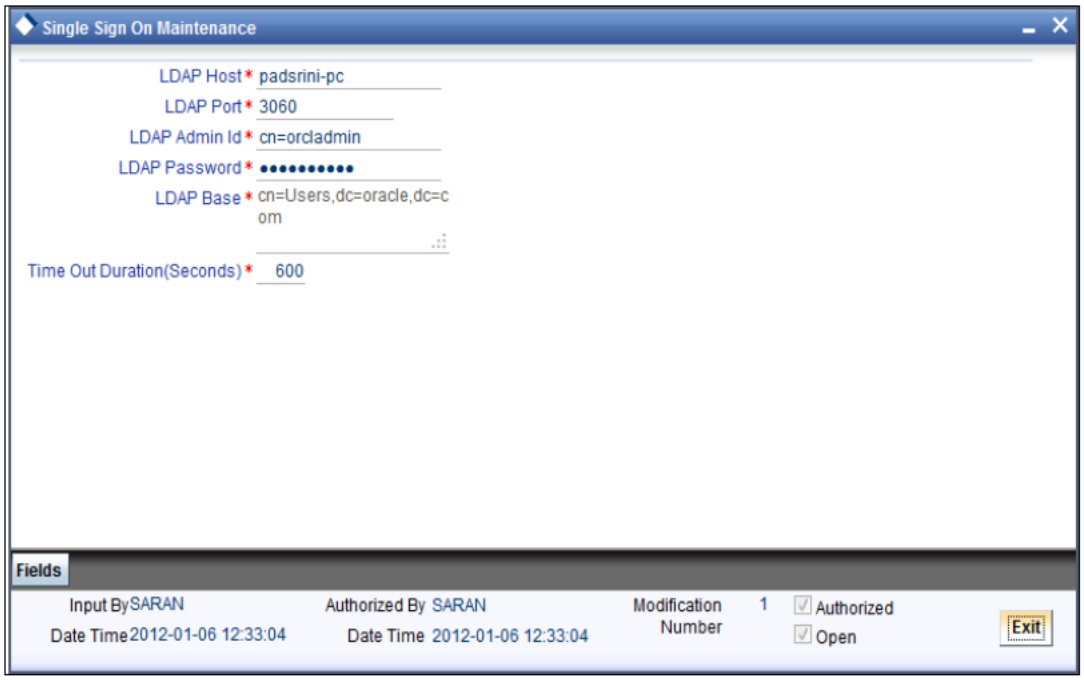
Figure 3-15 FCUBS_ Authentication Module



3.4.2 SSO Parameters

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

Figure 3-16 Single Sign On Maintenance



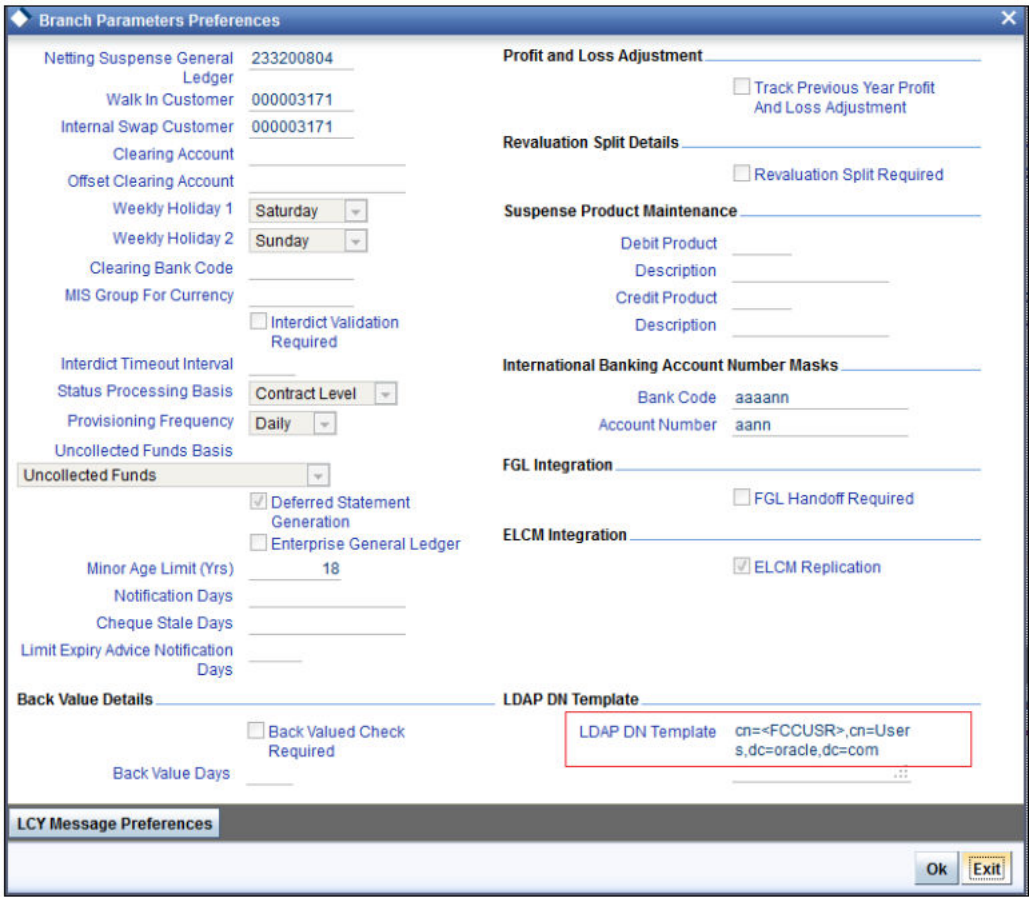
Specify all the details such as Directory Server Host Name, Port Number, LDAP Admin User ID, Admin Password, LDAP Base and Login Time Out Duration (in seconds).

3.4.3 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.

Figure 3-17 Bank Parameter Preferences



Specify the LDAP DN Template.

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

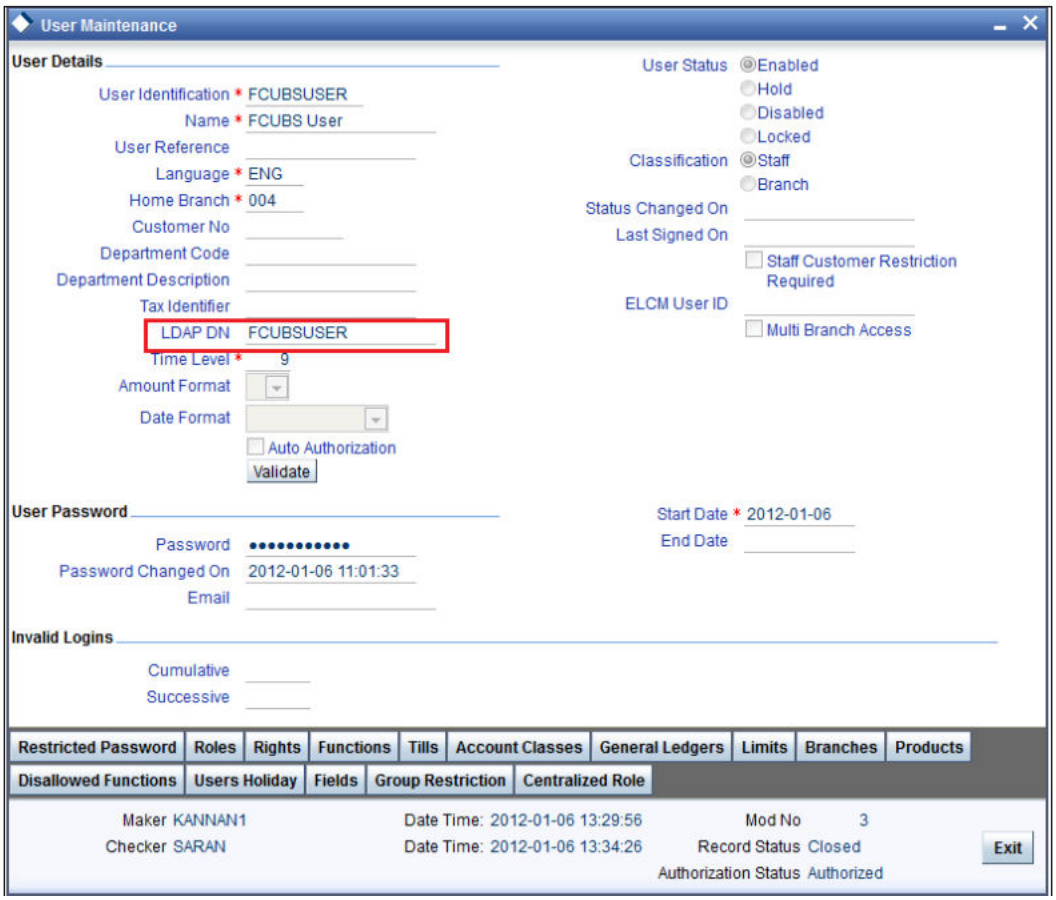
In the above template cn=<FCJUSR> part must be there without alteration. However, the rest of the DN name can be changed based on the configuration.

3.4.4 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.

Figure 3-18 User Maintenance



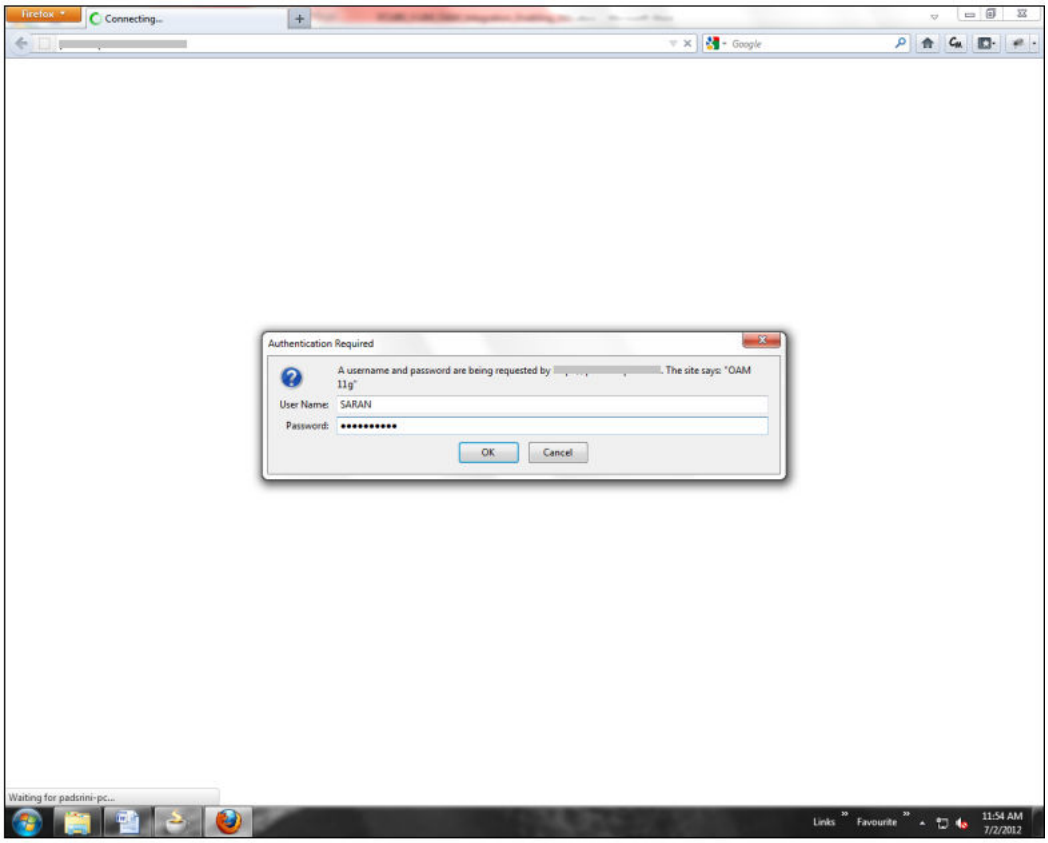
3.4.5 Launching Oracle Banking Payments

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

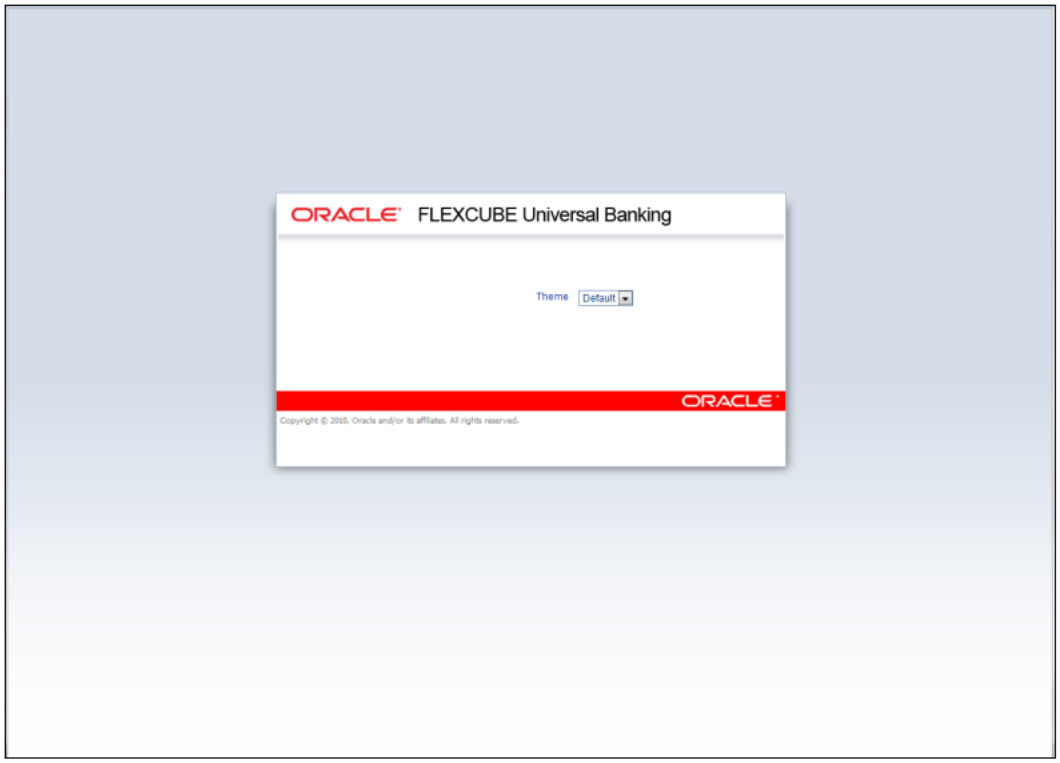
Since the resource is protected, the WebGate challenges the user for credentials as shown below.

Figure 3-19 Connecting



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.

Figure 3-20 Oracle Flexcube Universal Banking



3.4.6 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.