Oracle Access Manager Integration
Oracle FLEXCUBE Payments
Release 14.2.0.0.0
[November] [2018]

ORACLE®
FINANCIAL SERVICES

ORACLE®

Table of Contents

ORACLE®

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	*Preface* gives information on the intended audience. It also lists the various chapters covered in this User Manual.
Chapter 2	*Enabling Single Sign-on (SSO) with Oracle Access Manager* 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

ORACLE

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)

ORACLE

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 7.3.0.0.0.0.0 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).

ORACLE®

2.3   Background of SSO Related Components

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.

ORACLE

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

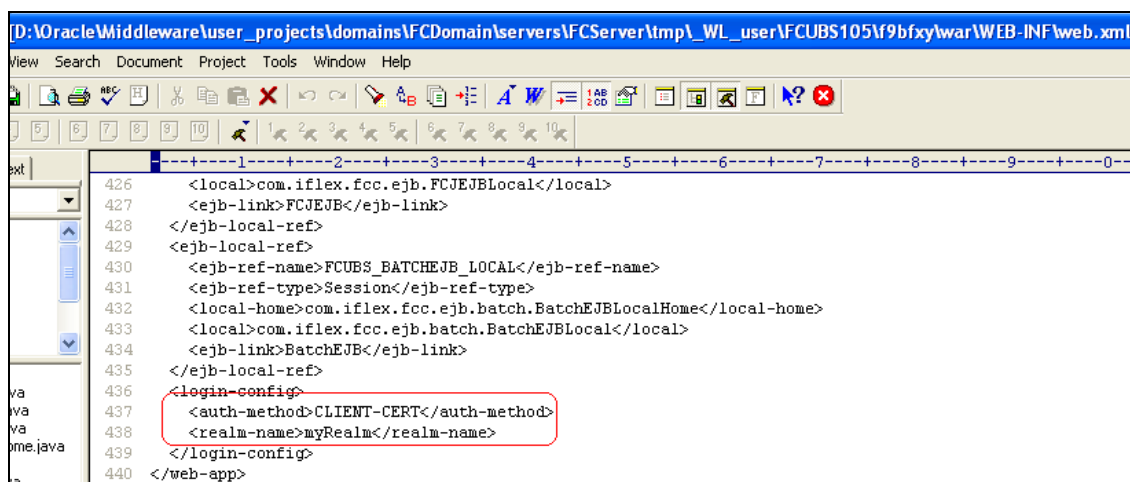Locate the file *web.xml* in the application (FCUBS) EAR file.

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*.
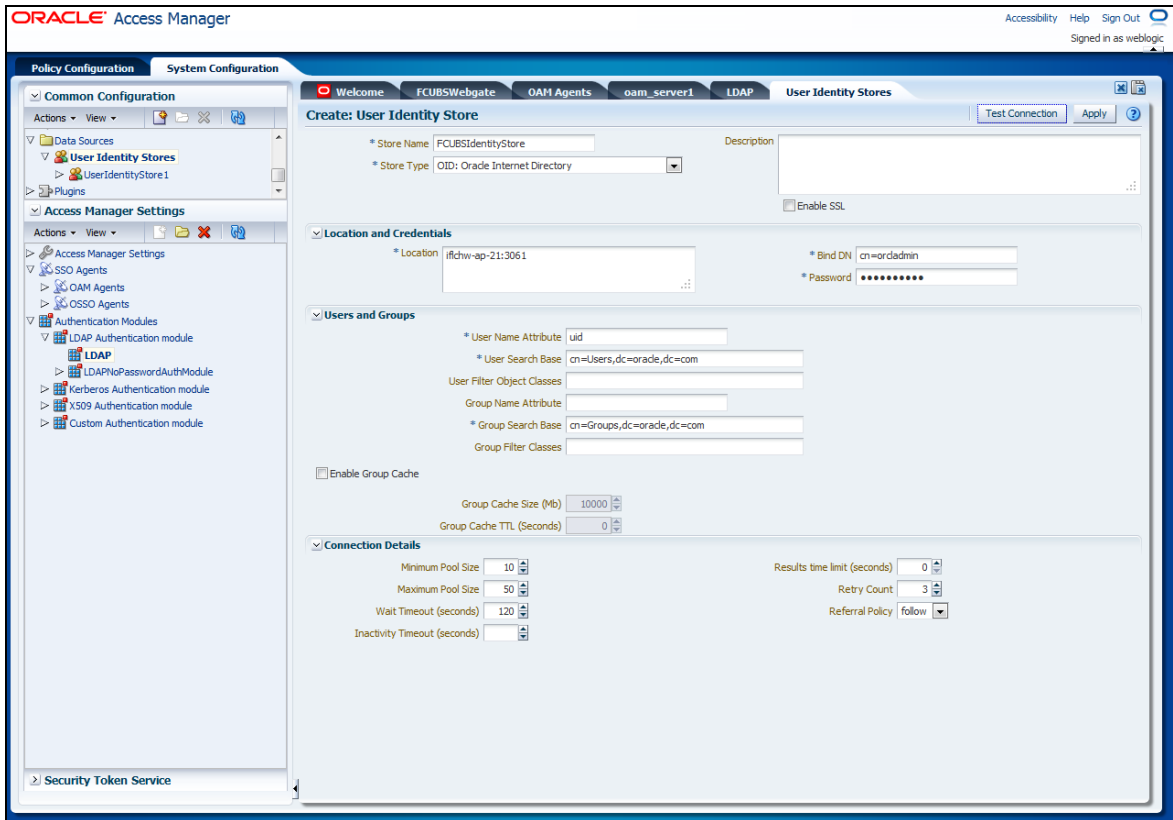
ORACLE

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.

ORACLE

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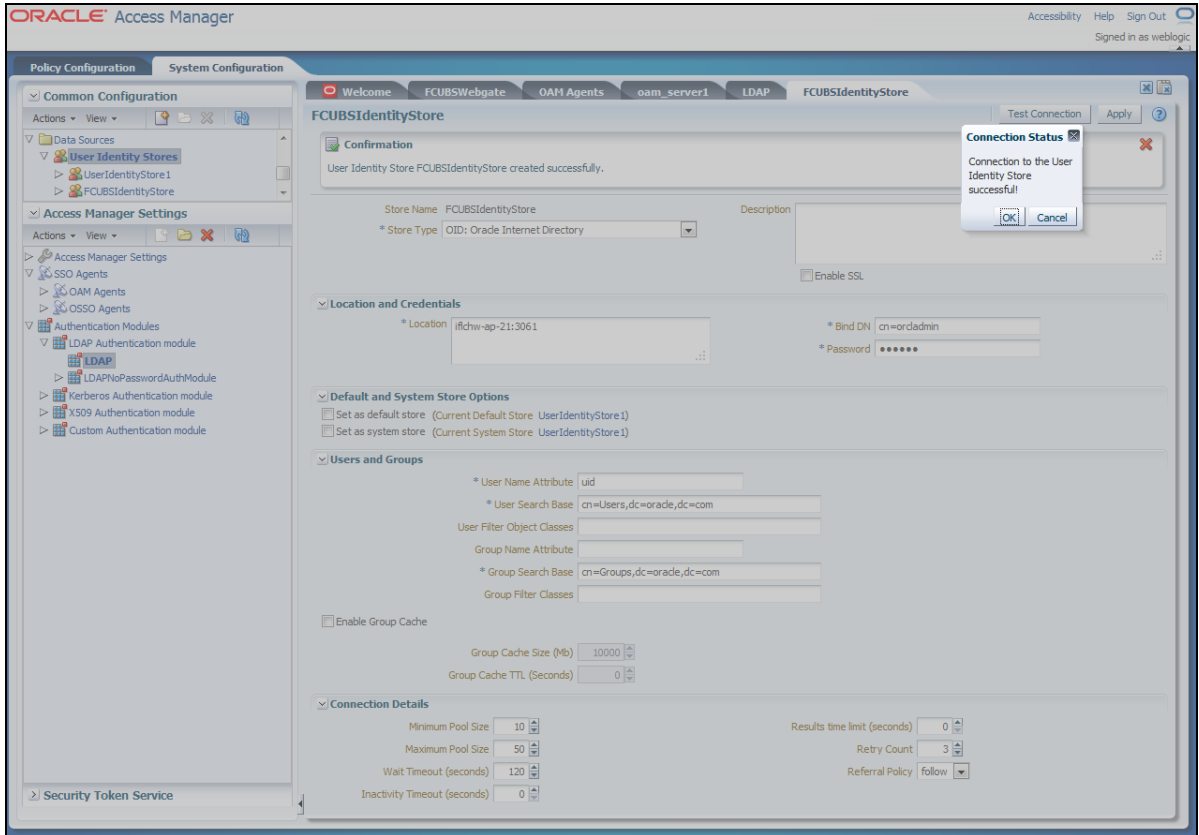
2.4.3.2 Creating Authentication Module

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

ORACLE
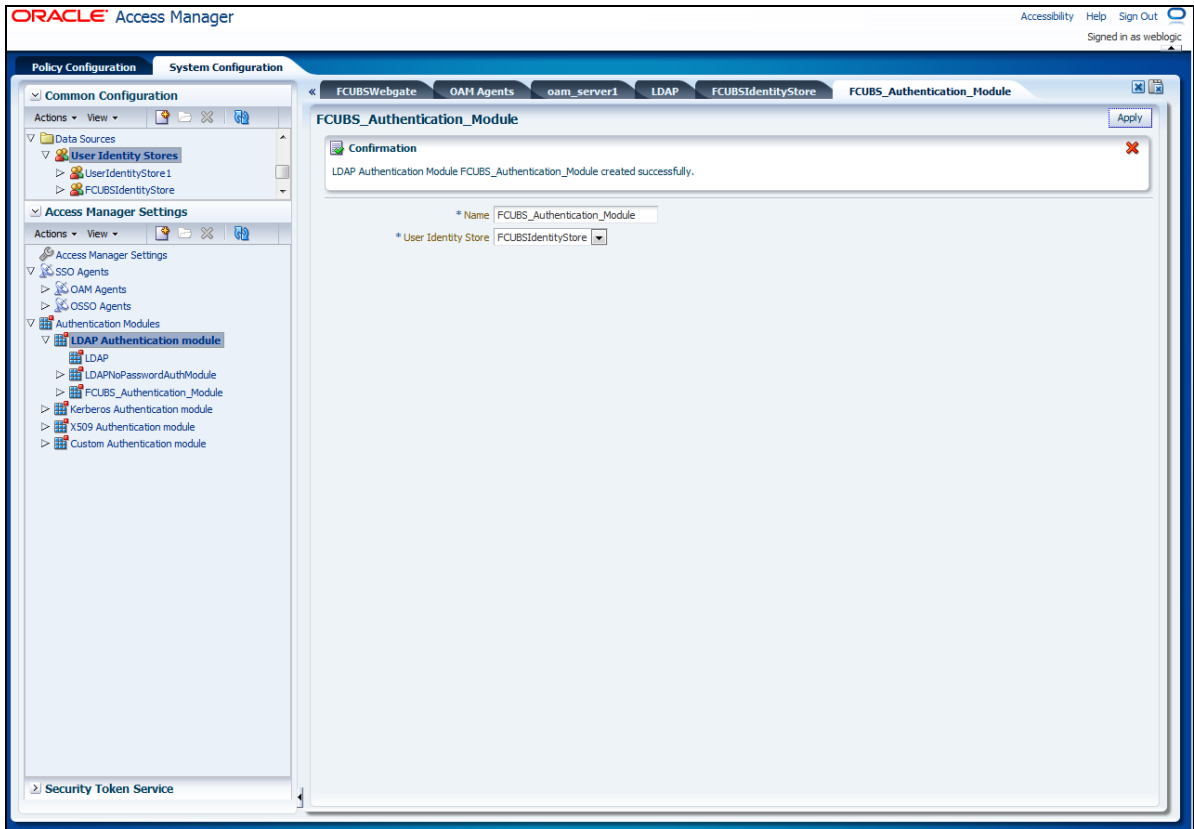
Click 'New' button to create new Authentication Module.

Name

Specify the name of the authentication module.

User Identity Store

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

ORACLE®

2.4.3.3 Creating OAM 11g Webgate

Navigate to *System Configuration>>Access Manager Settings>>SSo Agents>>OAM Agents*.
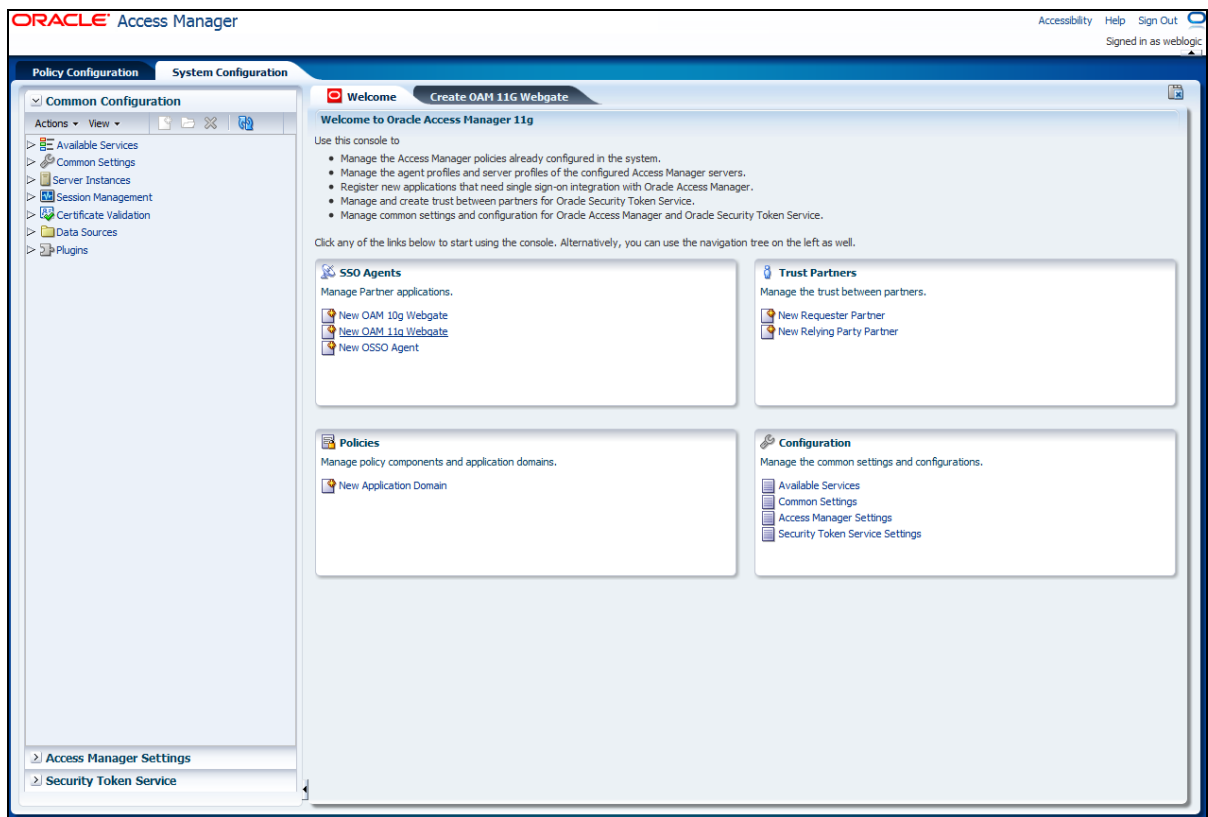
Click 'Create 11g webgate' button or 'New OAM 11g Webgate' link on the Welcome page.
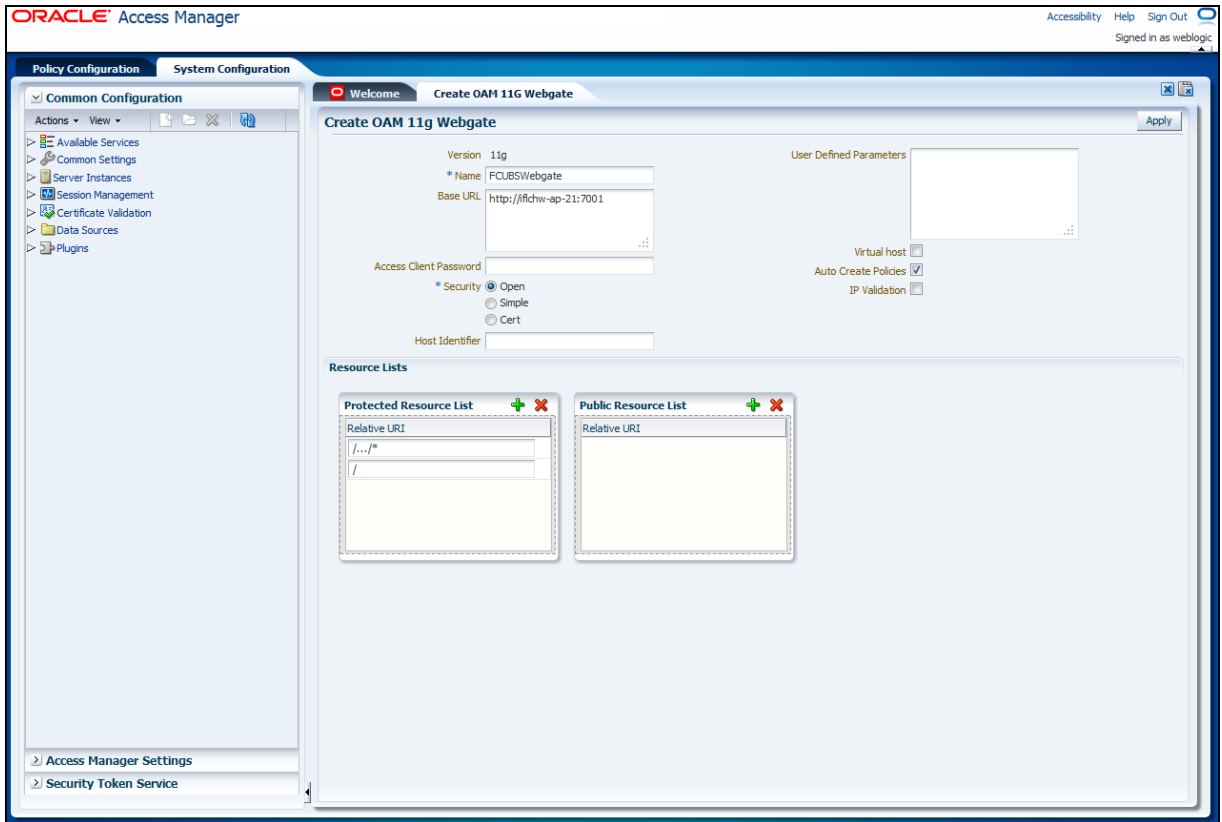
Specify a name for Webgate and the Base URL (the host and port of the computer on which the Web server for the Webgate is installed). Click 'Apply' button.

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.
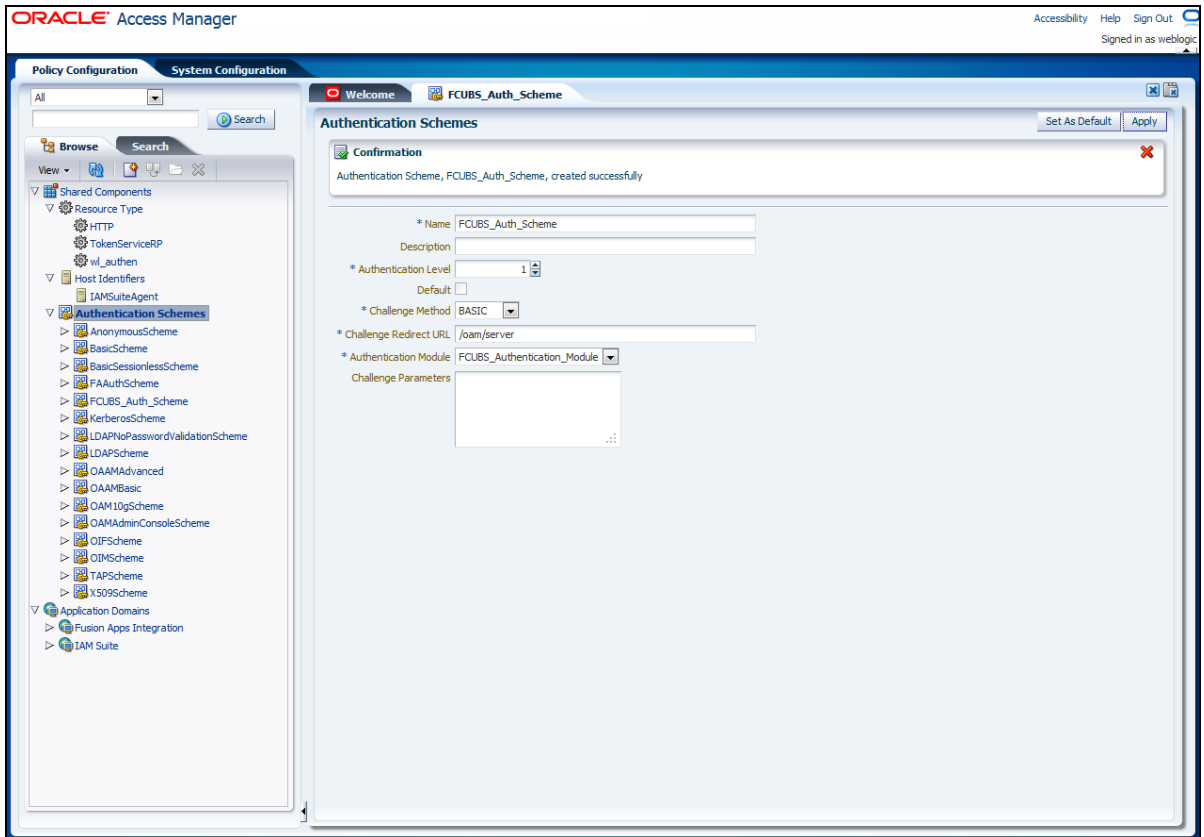
Name

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.
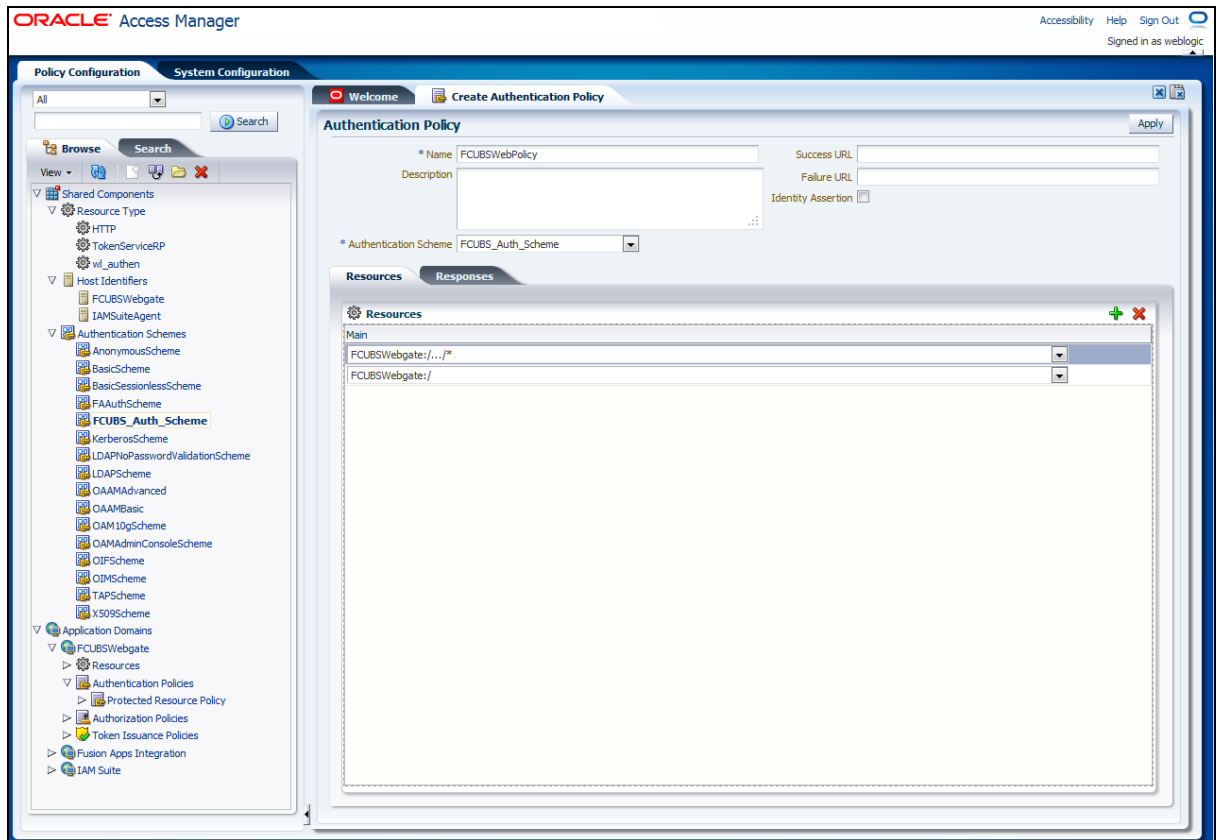
Name

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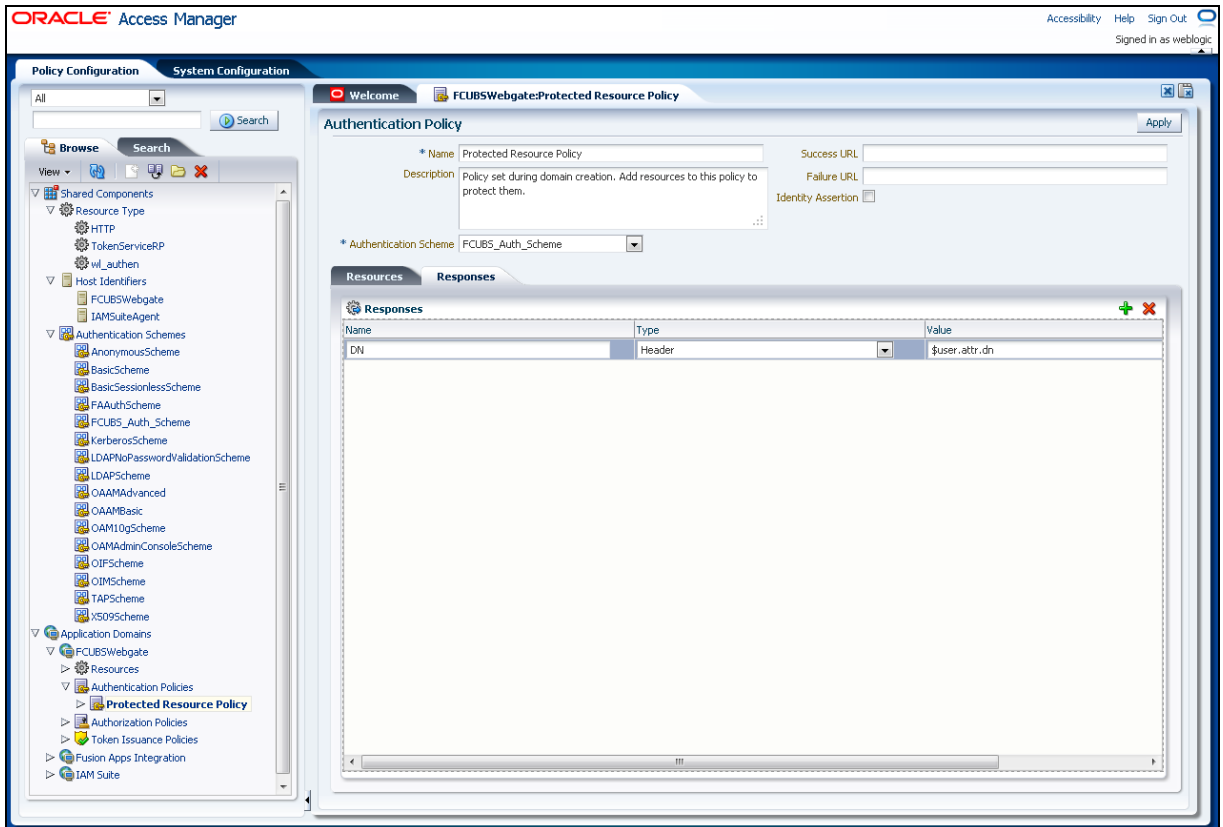
Enter the value as *$user.attr.dn*. The responses maintained in this tab will be added in the response header at the time of authentication.

2.4.3.7 Adding Resources

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

Click 'Create New Resource' button.

ORACLE®
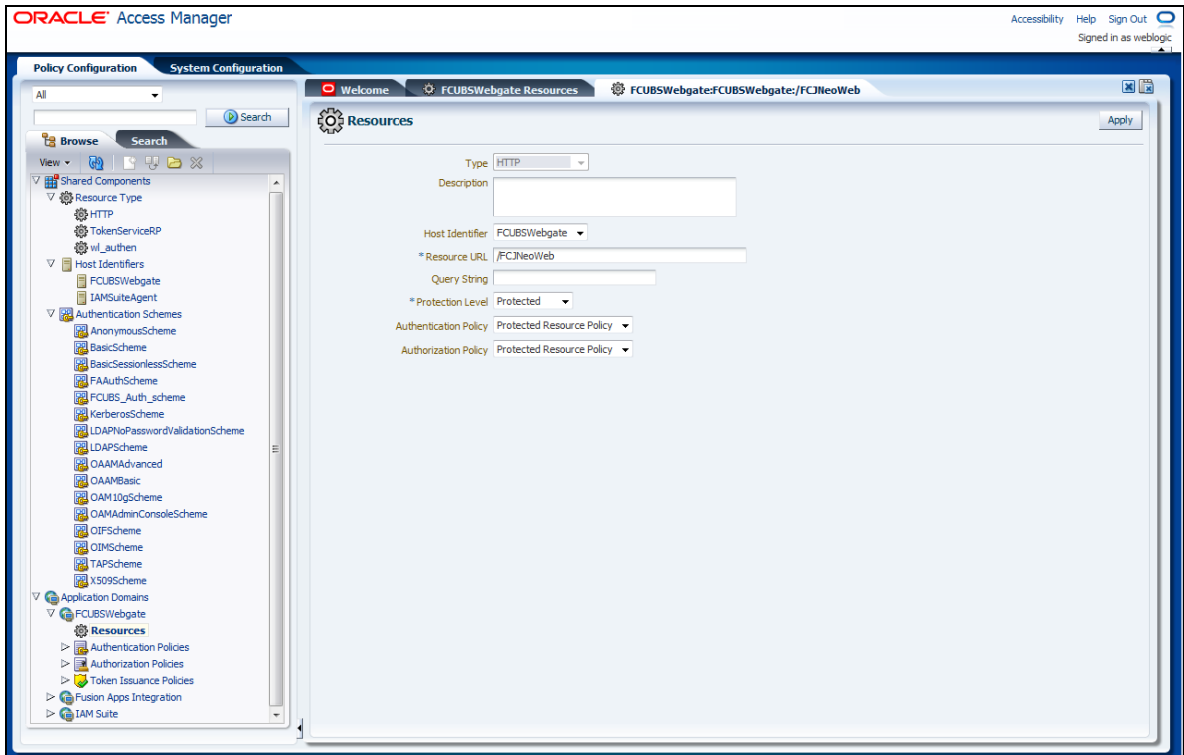
Type

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'.

2.4.3.8 Adding Authorization Policy

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

ORACLE®
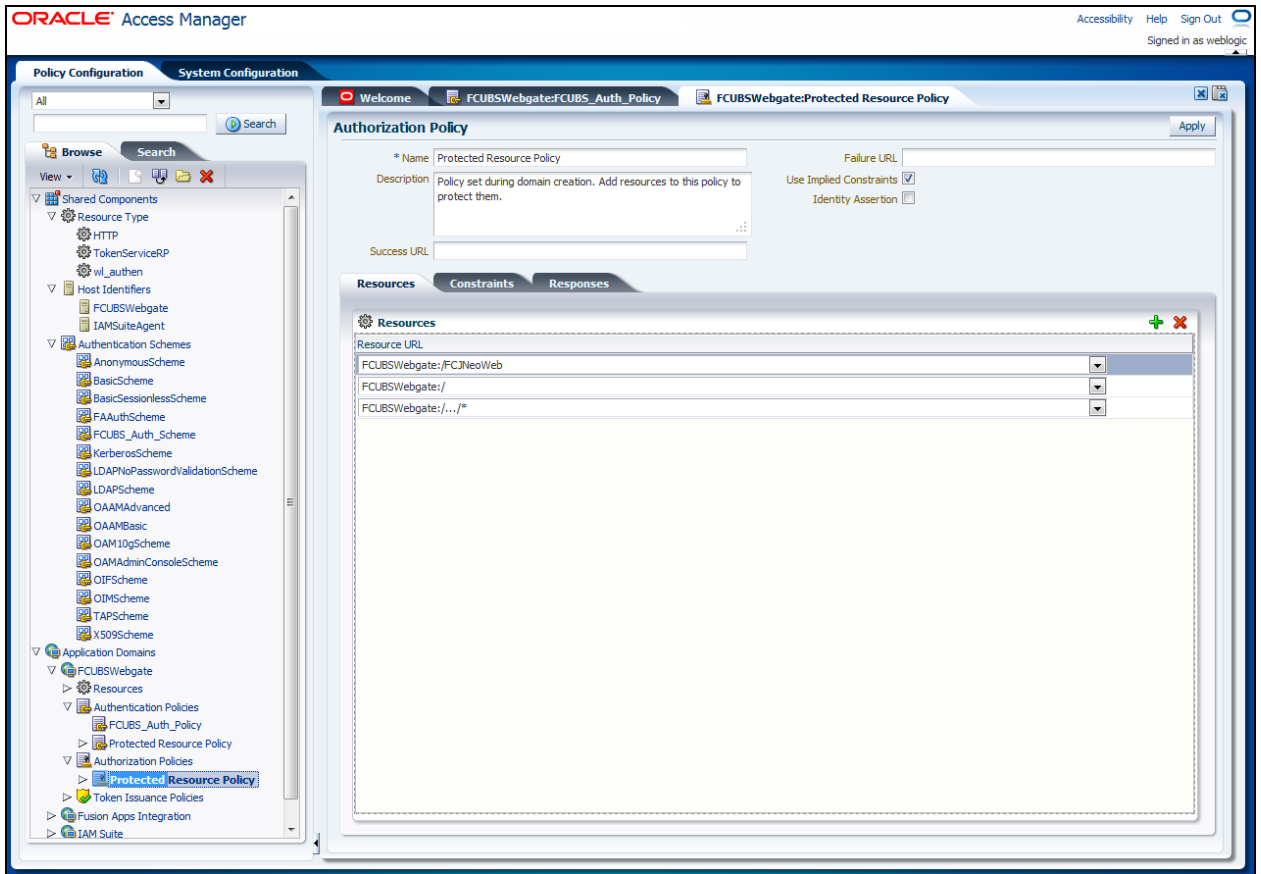
During web gate creation, these values are defaulted.
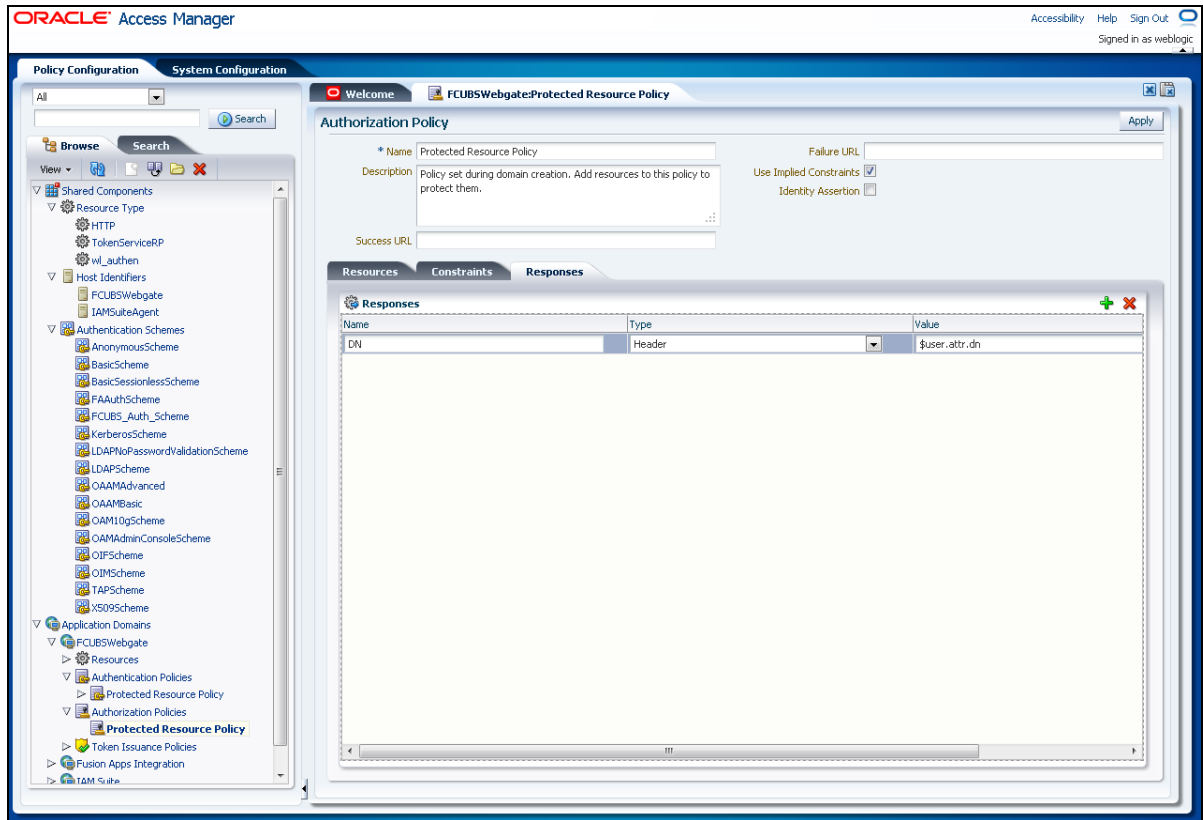
Add DN in the 'Responses' tab. Enter the value as *$user.attr.dn*.

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 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.

ORACLE®

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

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.
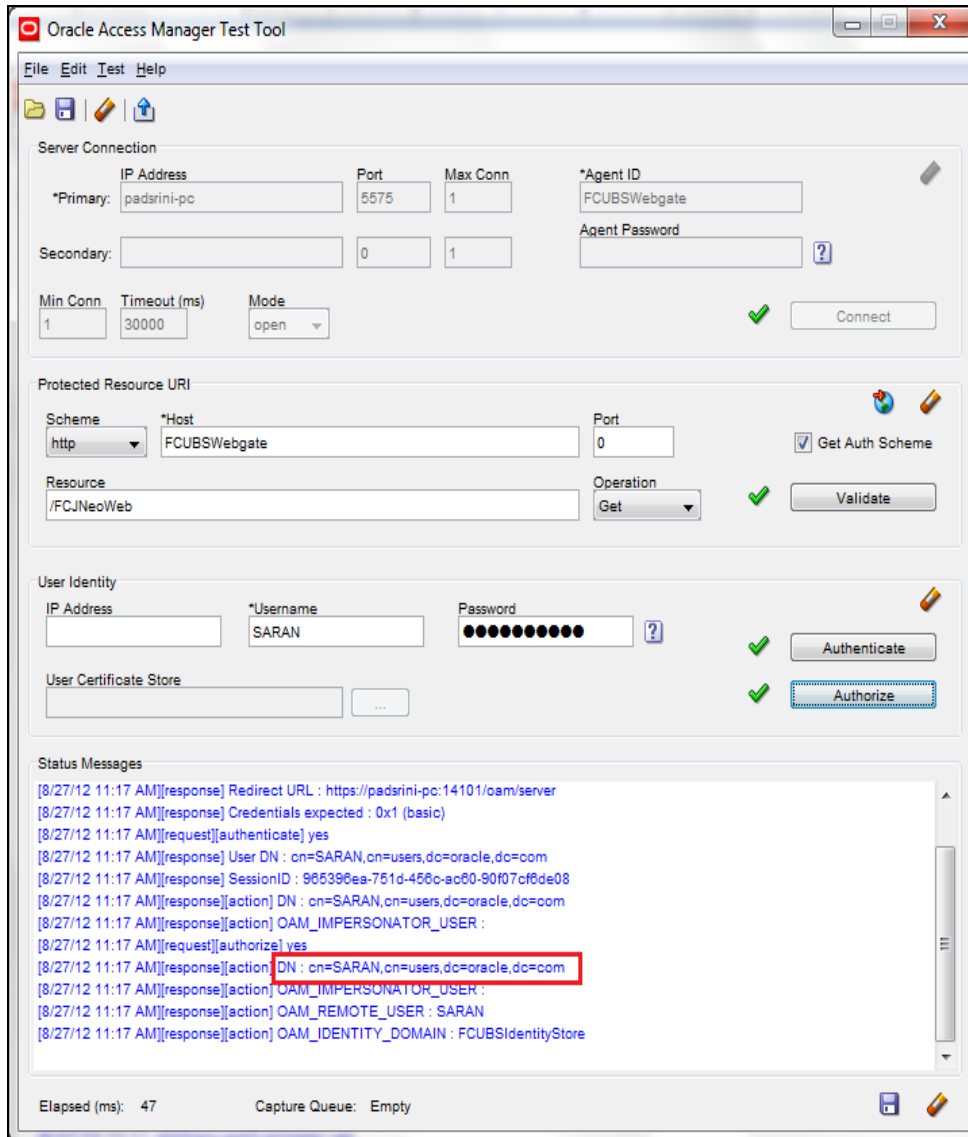
ORACLE

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.

ORACLE

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*'.

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.

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.

ORACLE

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.

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.
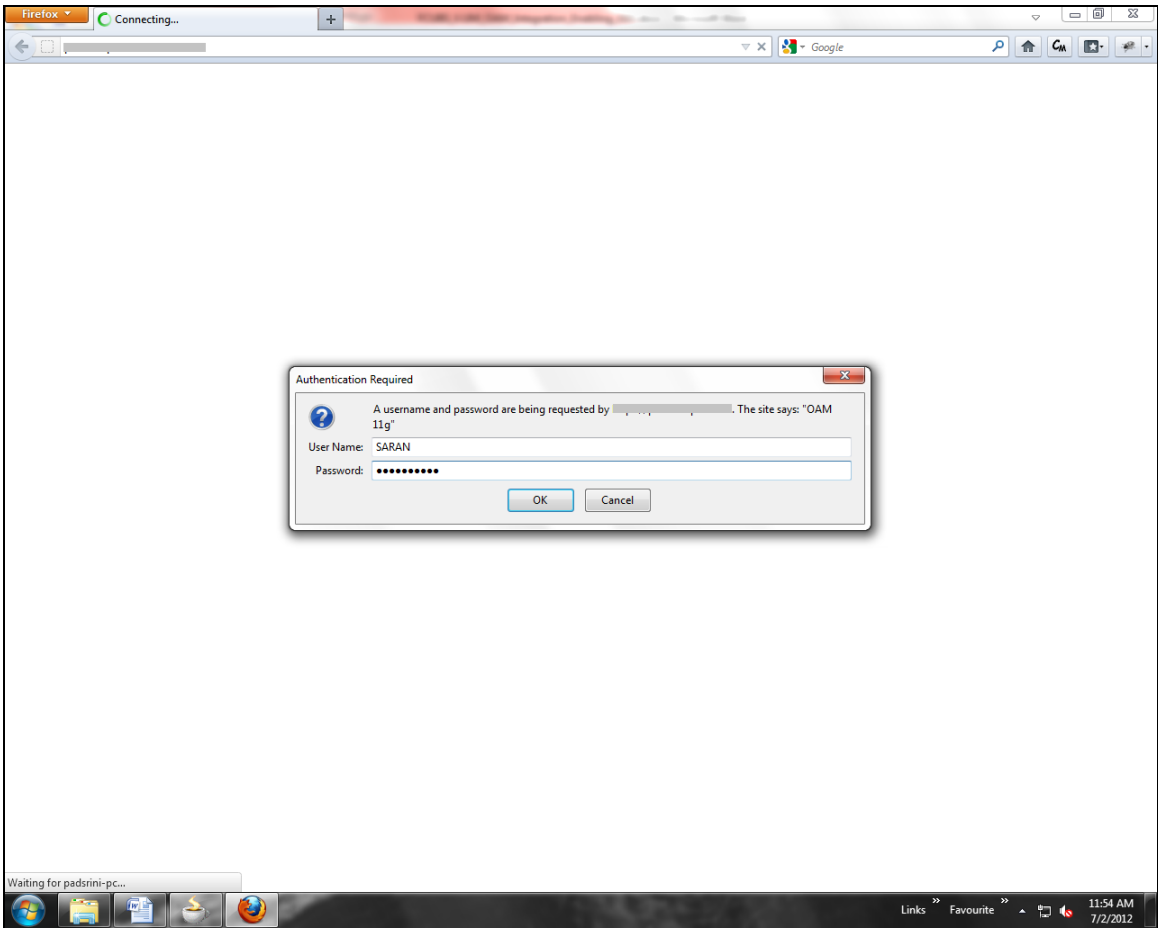
Once the user is authenticated and authorized to access the resource, the servlet gets redirected to Oracle Banking Payments application server URL. You can see the new sign-on screen. The application automatically redirects to Oracle Banking Payments home page.
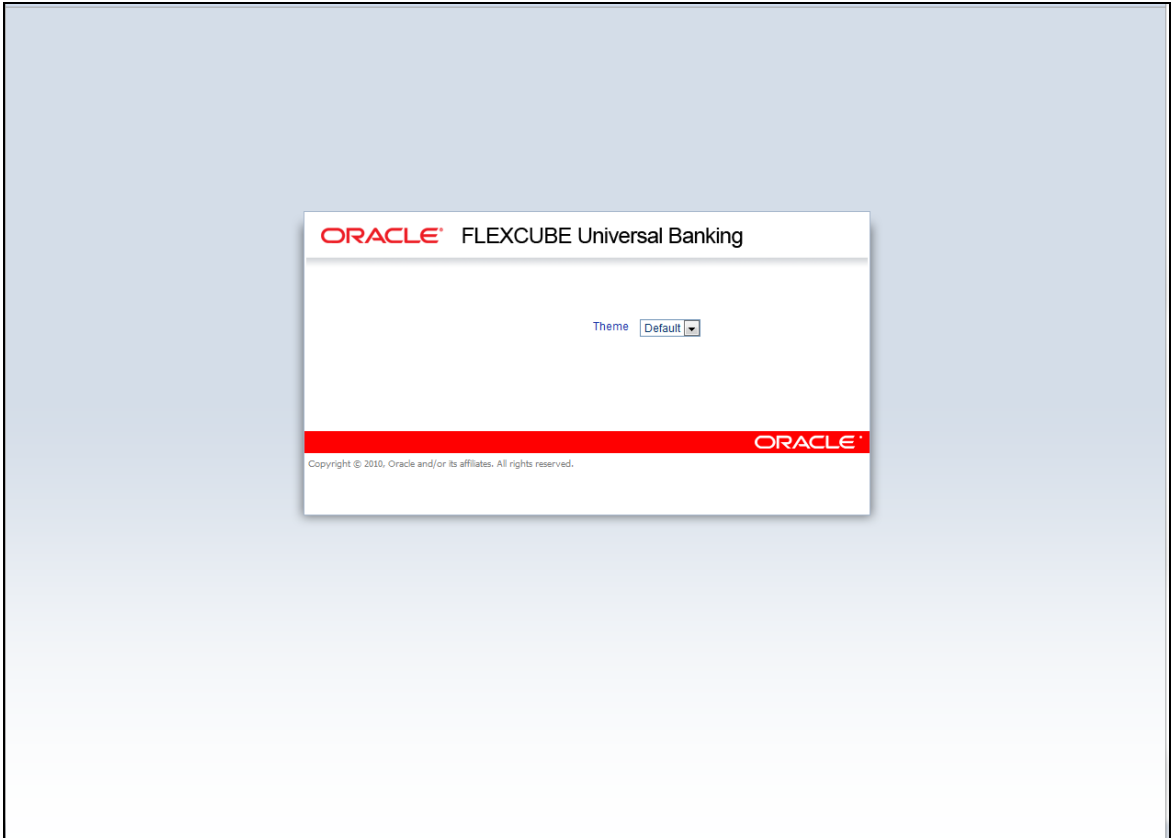
ORACLE®

2.4.4.6 <u>Signoff in a SSO Situation</u>

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®

ORACLE®

Oracle Banking Payments Oracle Access Manager Integration
[November] [2018]
Version 14.2.0.0.0

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/