Oracle Banking Trade Finance
Oracle Access Manager

Release 14.7.6.0.0

G32581-01

April 2025

ORACLE®

Oracle Banking Trade Finance Oracle Access Manager, Release 14.7.6.0.0

G32581-01

Contents

Preface

1   Introduction

2   BACKGROUND AND PREREQUISITES

3   Configuration

Preface

Purpose

This manual is designed to help acquaint you with the understanding how single sign-on can be enabled for a ORACLE BANKING TRADE FINANCE deployment using Oracle Fusion Middleware 12c.

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

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 ensure effective security, as strongly recommended by Oracle Software Security Assurance.

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.

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.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

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

2. 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.
   <login-config>

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

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

   </login-config>
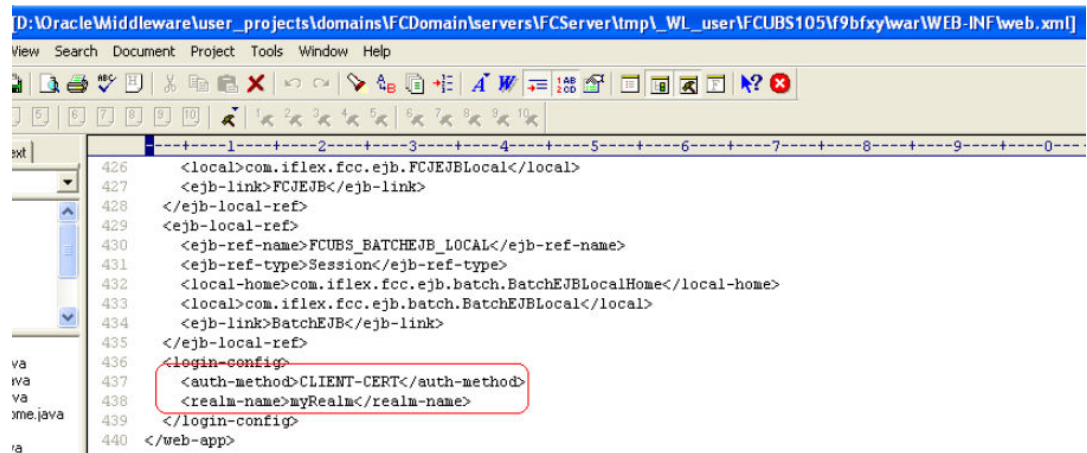
3. Save the file and redeploy and restart the application.

3.3 Configuring SSO in OAM Console

After installing OAM, Webtier Utilities and Webgate, extend the weblogic domain to create OAM server.

Follow the post installation scripts deployWebGate and EditHttpConf as provided in 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:

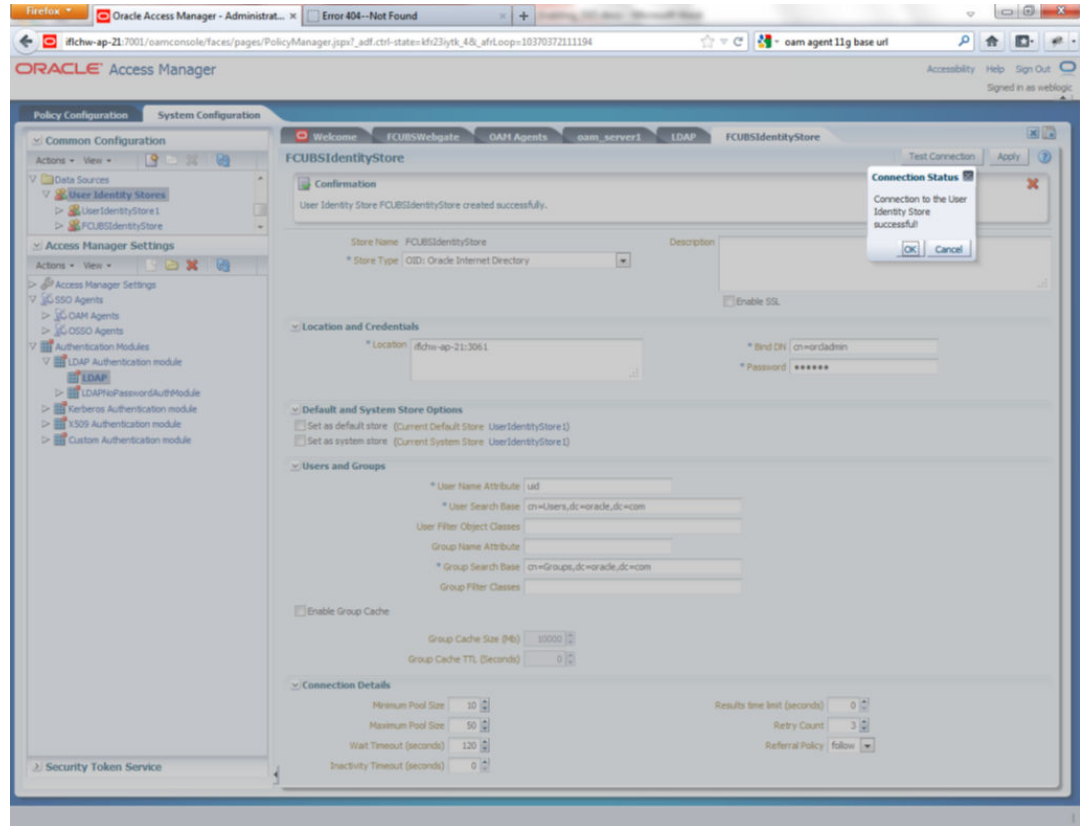   The container of the User Name in the LDAP server.

   Group Search Base:

   The container of the Group Name in the LDAP server.

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.

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

Click 'New' Button to create new Authentication Module. Input the Name of the authentication module and choose the User Identity Store we created in step 1.
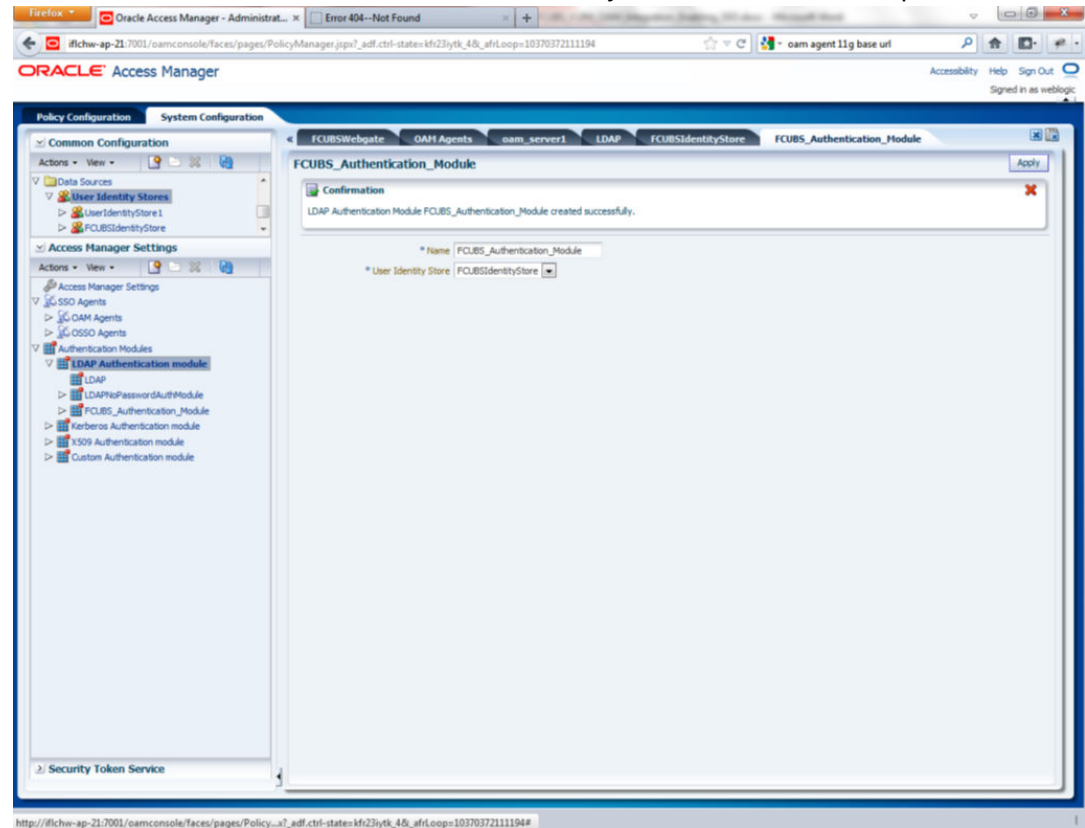
5. Creating OAM 12c Webgate
Navigate to System Configuration>>Access Manager Settings>>SSo Agents>>OAM Agents.

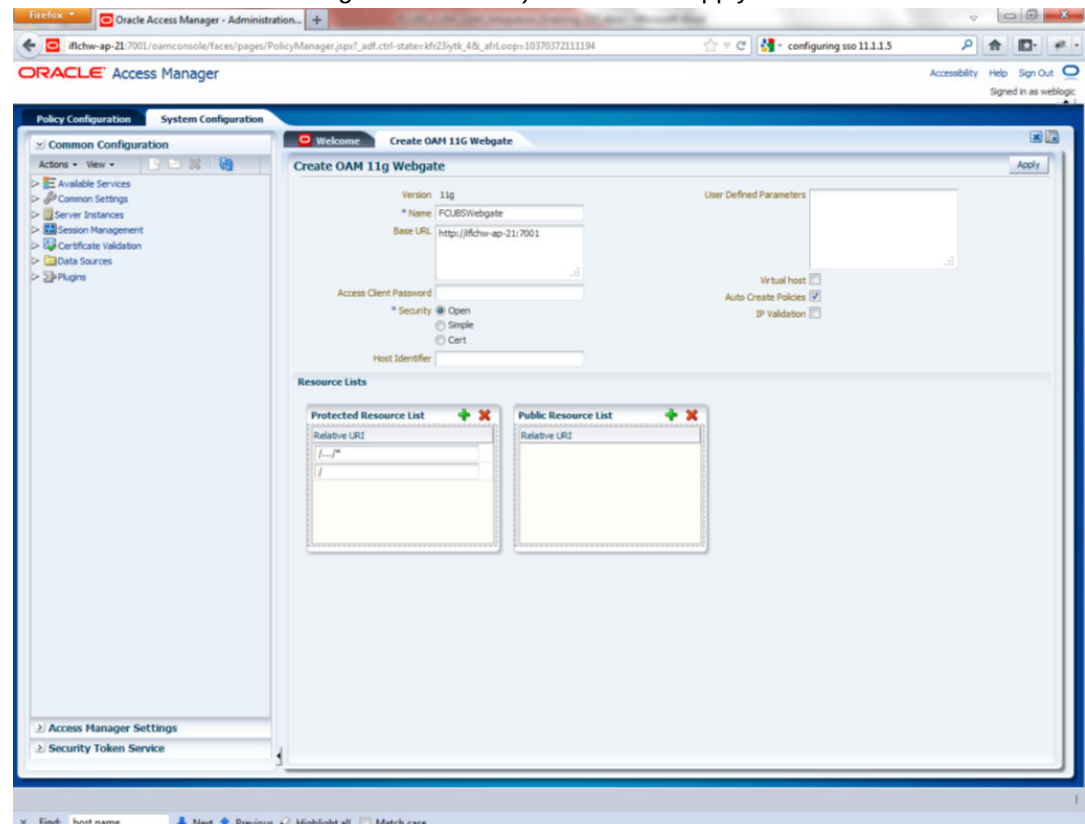Click on 'Create 12c webgate' button

or Click on New OAM 12c Webgate link available in welcome page.
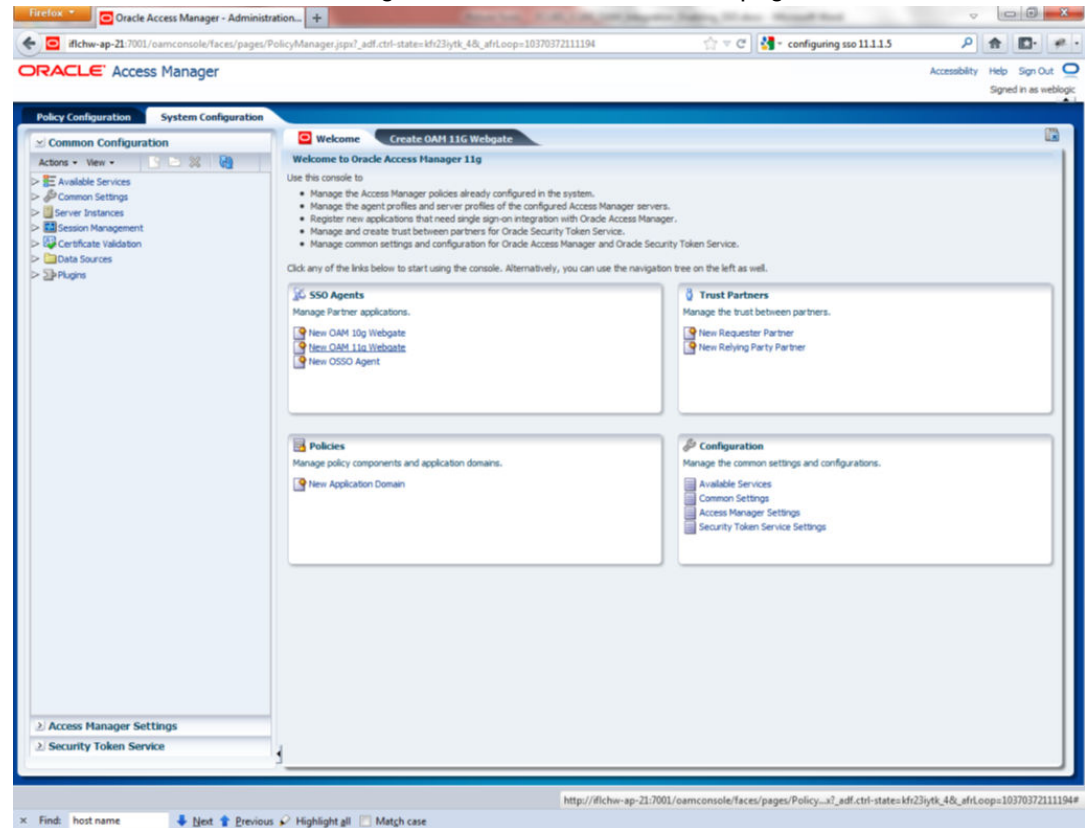
Enter any name for Webgate and Base URL (The host and port of the computer on which the Web server for the Webgate is installed) and click on apply.

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

Click 'Apply' button to save the changes.
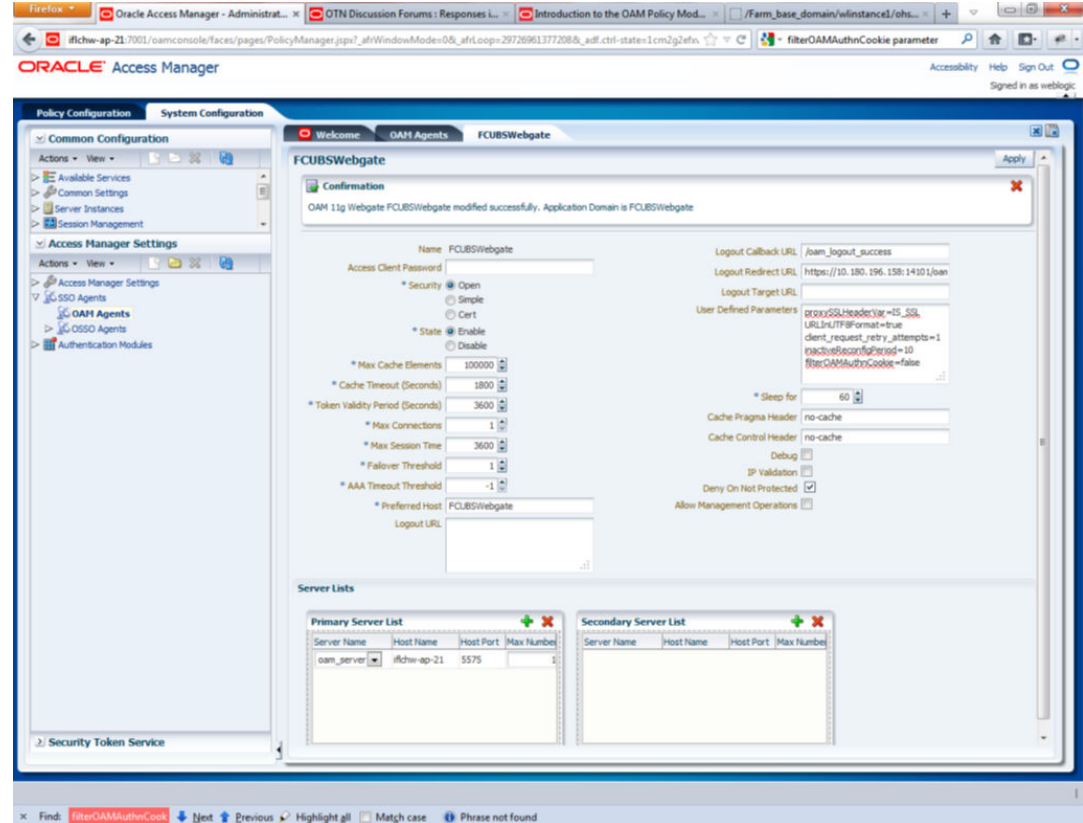
6. **Post OAM Webgate 12c Creation Steps**
   Perform the following steps to copy the artifacts to the Webgate installation directory

   • 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)

7. **Creating Authentication Scheme**
   To create Authentication Scheme navigate to Policy Configuration >> Authentication Schemes
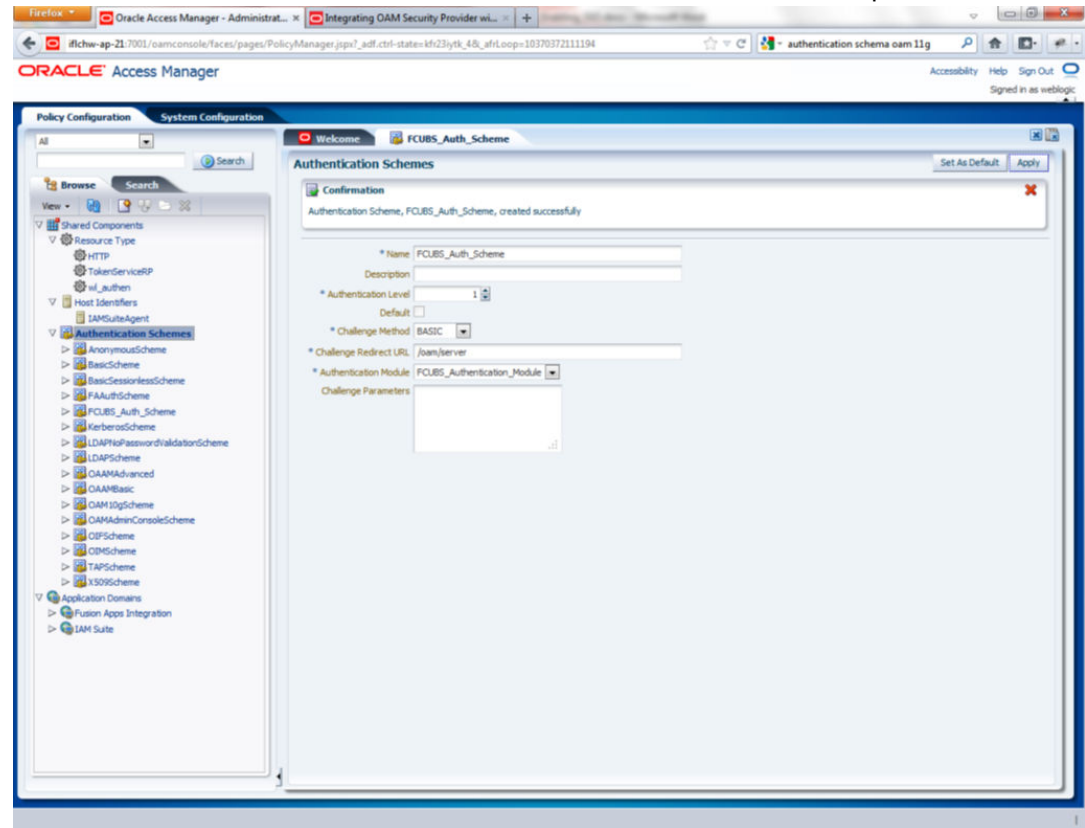
   Click on 'Create' button to create new Authentication Scheme.

   Name : Any name to identify Authentication Scheme

   Challenge Method : BASIC

   Challenge Redirect URL : /oam/server

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-auth-credentials' tag to the config.xml file located under /user_projects/domains/<MyDomain>/config/. The tag must be inserted within the <security-configuration> tag as follows: [Just before the end of security configuration tag]

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

</security-configuration>

8. Creating Authentication Scheme
    To create authentication policy, navigate to Policy Configuration >> Application Domains >> [Webgate agent name] >> Authentication Policies.
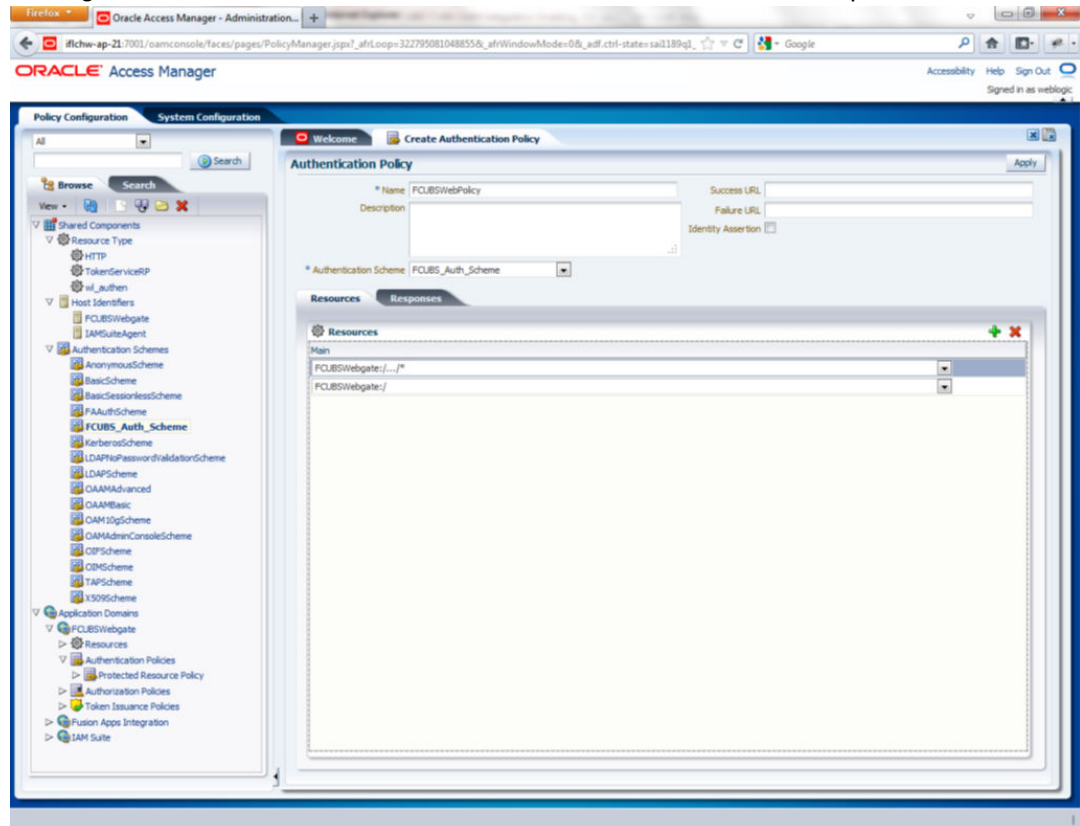
Click new button and input the below information

Name: Enter any name to identify the Authentication Policy (eg. 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.

Add DN in the Responses section. Enter the value as $user.attr.dn. The responses maintained in the tab will be added in the response header during the authentication.
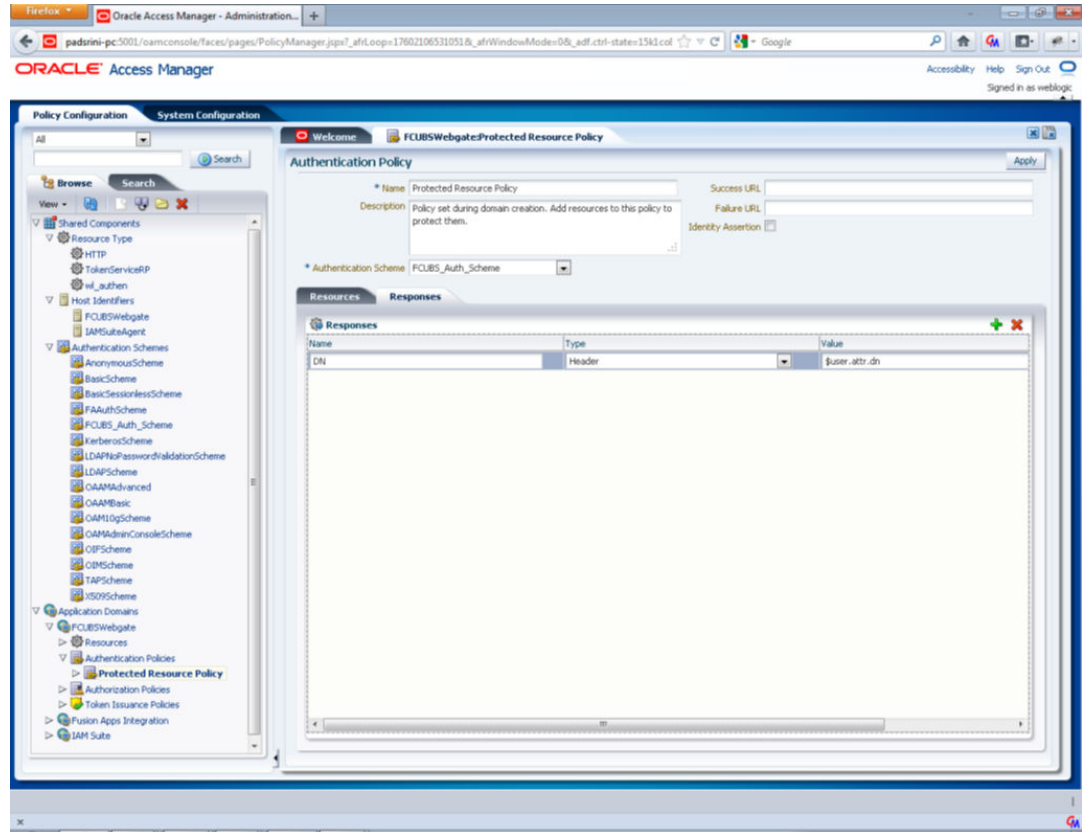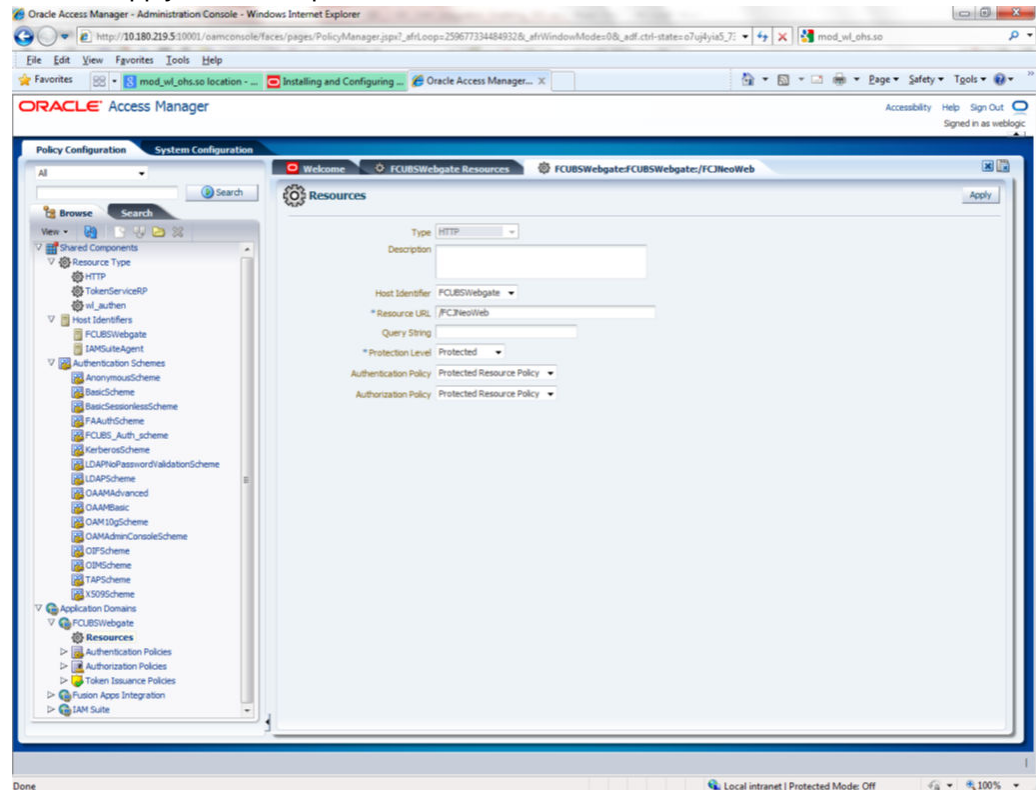

9. Adding Resources
   Navigate to Policy Configuration >>Application Domains >>OBTFWebgate >>Resources .

   • 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.
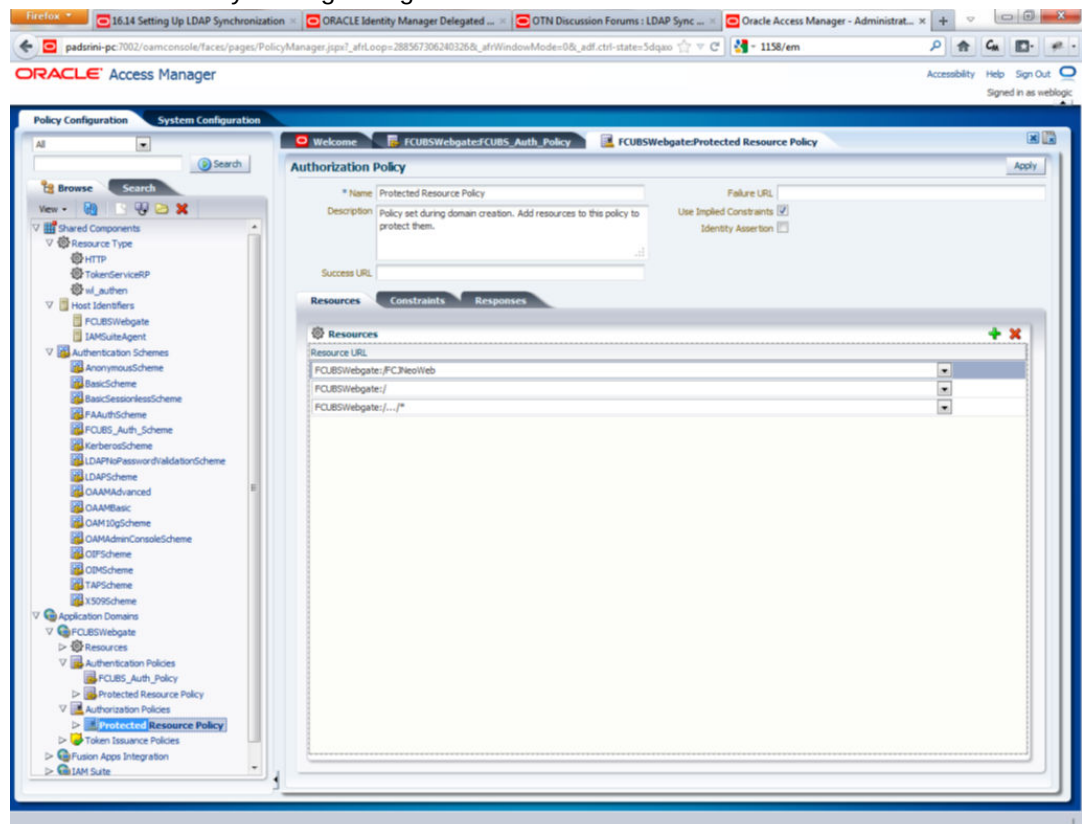
Add DN in the Responses section. Enter the value as $user.attr.dn. The responses maintained in the tab will be added in the response header during the authorization.
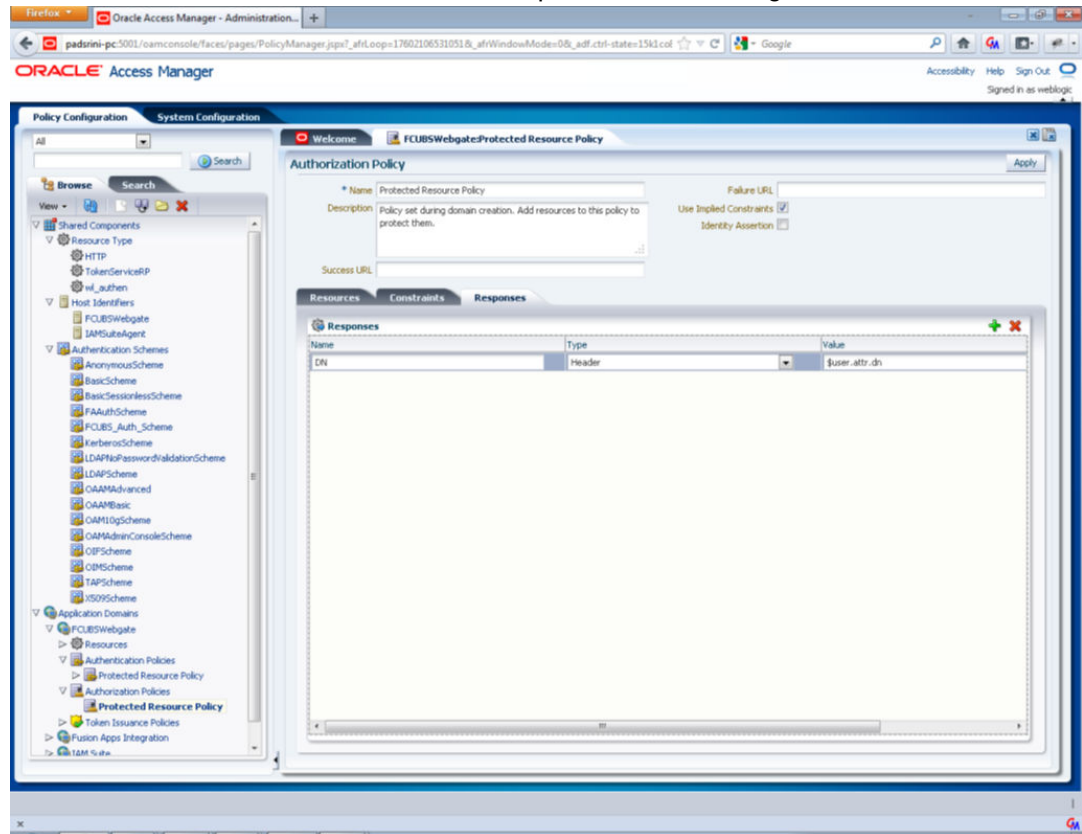
11. Configuring mod_wl_ohs for Oracle Weblogic server Clusters
    To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server Clusters, add the directive shown below to the mod_wl_ohs.sh file available in <Weblogic Home> /Oracle_WT1/instances/instance1/config/OHS/ohs1.

    <Location /console>

    SetHandler weblogic-handler

    WebLogicHost idmhost1.mycompany.com

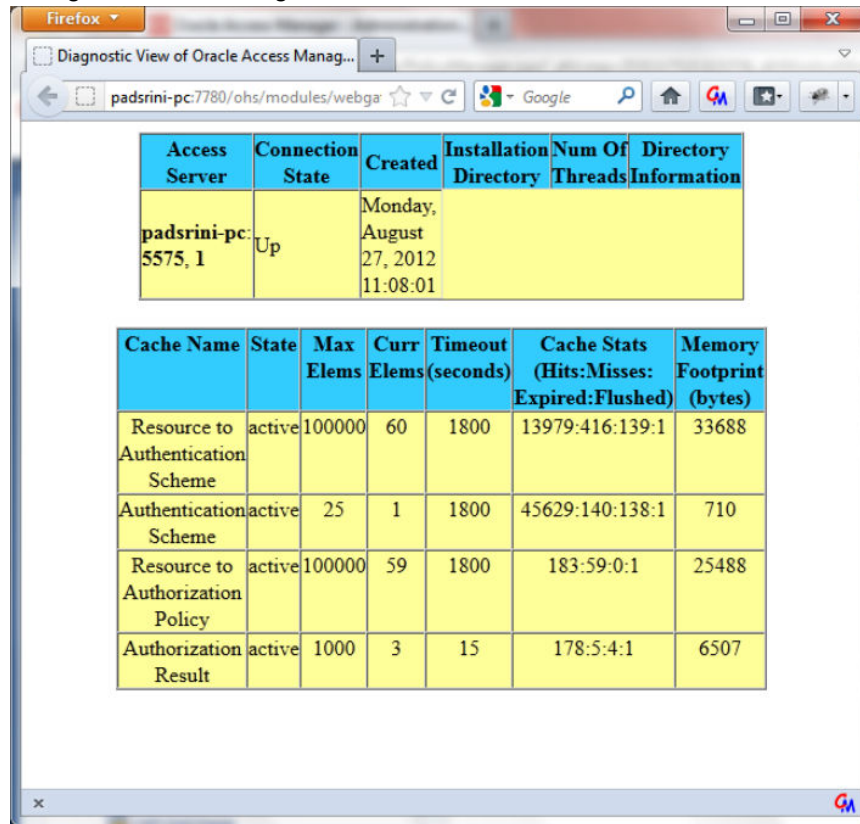   WeblogicPort 7001

    </Location>

12. Checking the Webgate 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
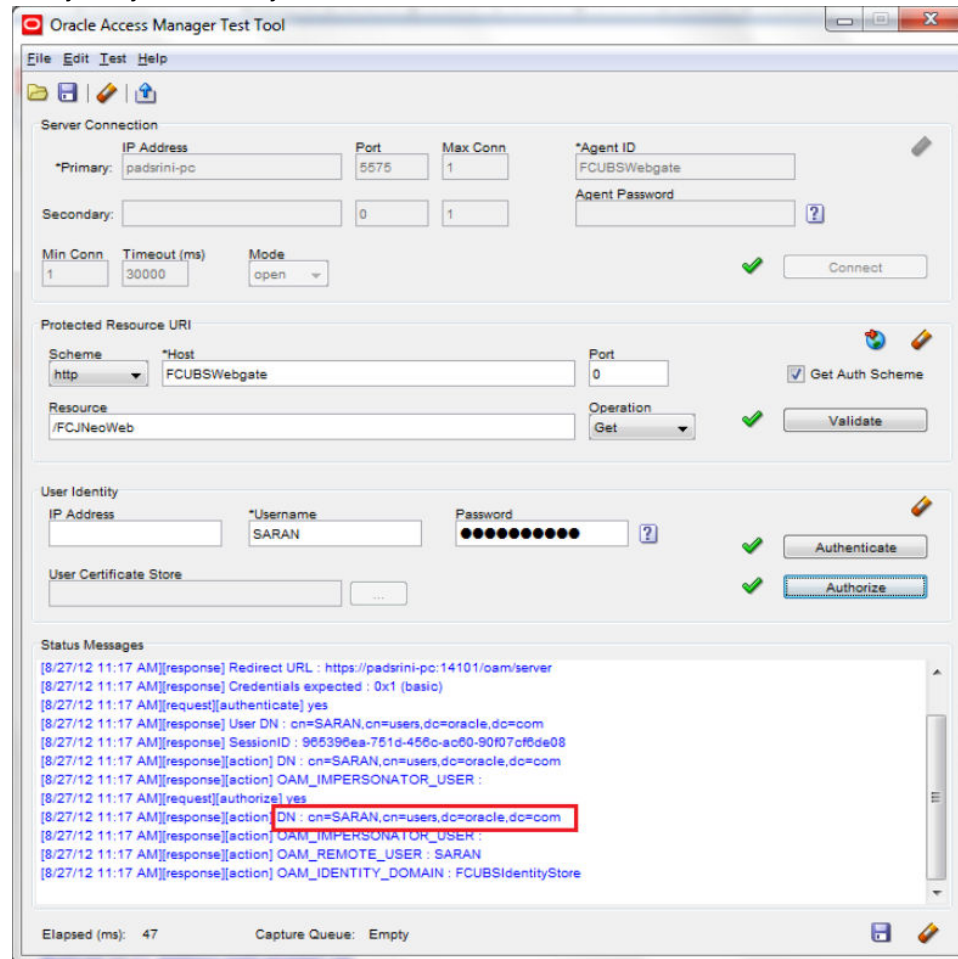
configuration is working fine.

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

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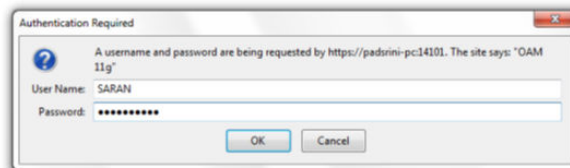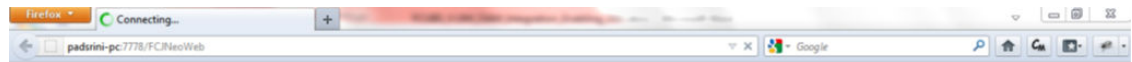
Once the user is authenticated and authorized to access the resource, the servlet gets redirected to normal ORACLE BANKING TRADE FINANCE application server URL and now the new signon form will appear as below. The application will automatically redirect ORACLE

BANKING TRADE FINANCE home page.
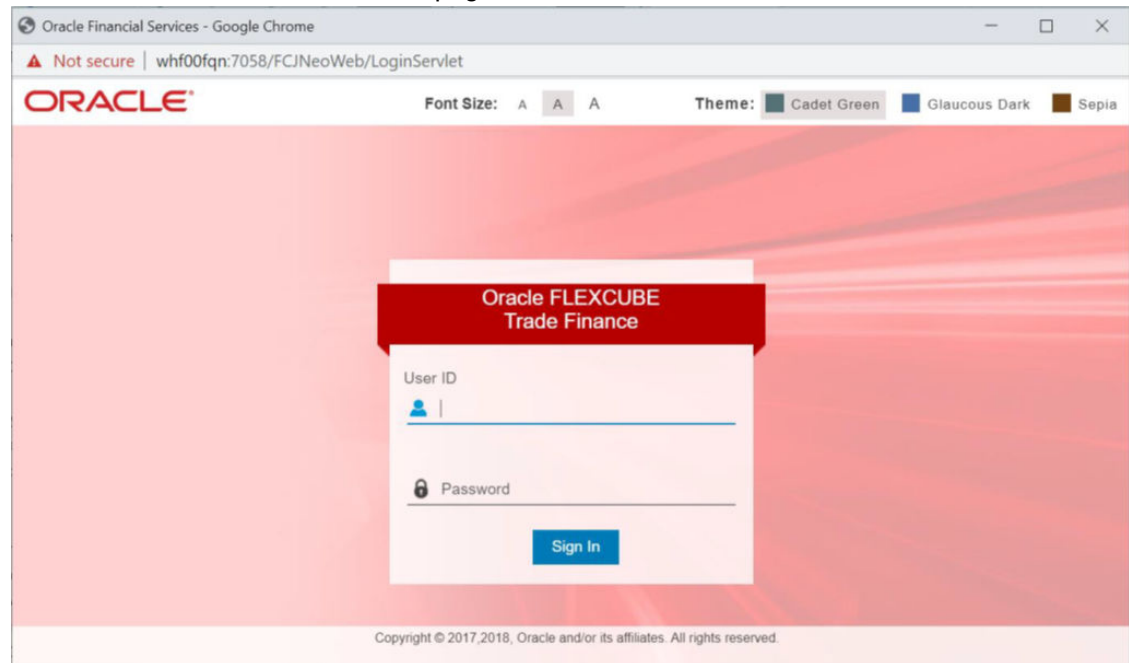
3.4.4 Signoff in a SSO Situation

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.