Oracle® Banking Corporate Lending

Oracle Access Manager

Release 14.8.1.0.0
G43310-01
October 2025

Oracle Banking Corporate Lending Oracle Access Manager, Release 14.8.1.0.0

G43310-01

Contents

Preface

This topic contains the following sub-topics:

Purpose

This guide helps the user to understand single sign-on can be enabled for a Oracle Banking Corporate Lending deployment using Oracle Fusion Middleware 12c.

In addition, it describes Configuration of Oracle Banking Corporate Lending and Oracle Access Manager to enable single sign-on using Oracle Internet Directory as a LDAP server.

Acronyms and Abbreviations

The listed below acronyms and abbreviations are used in this document.

Table 1 Acronyms and Abbreviations

Abbreviations or Acronyms	Definition
EAR	Enterprise Archive file
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OAM	Oracle Access Manager
OBCL	Oracle Banking Corporate Lending
OHS	Oracle HTTP server
SSO	Single sign-on

Audience

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

Table 2 Audience

Role	Function
Administrator	Who controls the system and application parameters and ensures smooth functionality and flexibility of the banking application.
Implementation team	Implementation of Oracle Banking Corporate Lending Solution
Pre-sales team	Install Oracle Banking Corporate Lending for demo purpose
Bank personnel	Who installs Oracle Banking Corporate Lending

The user of this manual is expected to have basic understanding of Oracle Banking Application installation.

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.

Conventions

The following text conventions are used in this document:

Table 3 Conventions

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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.

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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

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.

Related Resources

For more information on any related features, refer to the following documents:

- Oracle Banking Corporate Lending User Guides.
- Oracle Banking Corporate Lending Installation Guides.

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

Pre-Requisites

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

This topic has the following sub-topics:

- Software Requirements
  This topic provides the detailed information on Software Requirement for OAM setup.
- Background of SSO related components
  This topic describes the SSO related component.

1.1 Software Requirements

This topic provides the detailed information on Software Requirement for OAM setup.

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
   Make sure that the LDAP which is been used for Oracle Banking Corporate Lending Single Sign-on 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 Oracle Banking Corporate Lending in Fusion MiddleWare 12c, it is necessary for the weblogic instance to have an explicit Oracle HTTP server (OHS).

1.2 Background of SSO related components

This topic describes the SSO related component.

The SSO related components are listed below:

- Oracle Access Manager
  This topic provides the overview of Oracle Access Manager (OAM) to enable Single Sign-On (SSO).
- LDAP Directory Server
  This topic describes the integration of Oracle Banking Corporate Lending with OAM using Single Sign-on feature.
- WebGate/AccessGate
  This topic provides detailed information on WebGate/AccessGate.
- Identity Asserter
  This topic provides the detailed information on Identity Asserter.

1.2.1 Oracle Access Manager

This topic provides the overview of Oracle Access Manager (OAM) to enable Single Sign-On (SSO).

Oracle Access Manager (OAM) 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 selfregistration 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

1.2.2 LDAP Directory Server

This topic describes the integration of Oracle Banking Corporate Lending with OAM using Single Sign-on feature.

To integrate Oracle Banking Corporate Lending with OAM to achieve Single Sign-on feature, Oracle Banking Corporate Lending’s password policy management, like password syntax and password7 expiry parameters can no longer be handled by Oracle Banking Corporate Lending.

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 Corporate Lending application users’ passwords.

1.2.3 WebGate/AccessGate

This topic provides detailed information on 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. Make sure that the Access Management Service is On.
- **Authenticator or Oracle Web Services Manager**: Requires a separate AccessGate and configuration profile for each application. Make sure that the Access Management Service is On.

1.2.4 Identity Asserter

This topic provides the detailed information on 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 WebLogicauthenticated session. It also provides single sign-on between WebGates and portals. Refer to *Fusion Middleware Security Guide* to get more details on Identity asserter

> **Note**
>
> This document contains the configuration of Oracle Internet 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.

2
Configuration

This topic explains the configuration of Oracle Access Manager to enable single sign-on using Oracle Internet Directory as a LDAP server.

This topic has the following sub-topics:

- Pre-Requisites
  This topic provides pre-requisites information to configure Oracle Access Manager to enable Single Sign-on.
- Change the web.xml file
  This topic provides the systematic information to change the web.xml filein the EAR file.
- Configure SSO in OAM Console
  This topic provides the systematic instructions to configure SSO in OAM console.
- Launch Oracle Banking Corporate Lending after Installation
  This topic describes information on first launch of Oracle Banking Corporate Lending after installation.

2.1 Pre-Requisites

This topic provides pre-requisites information to configure Oracle Access Manager to enable Single Sign-on.

The steps provided below assume that Oracle Banking Corporate Lending 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.

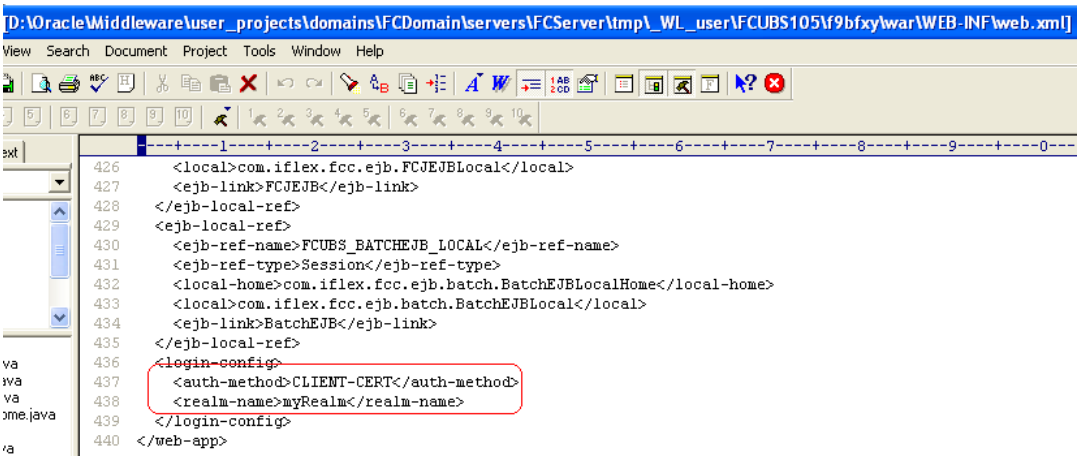
2.2 Change the web.xml file

This topic provides the systematic information to change the web.xml filein the EAR file.

1. Locate the web.xml file in the application (OBCL) 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>
```

Figure 2-1 web.xml file



3. Save the file and redeploy and restart the application.

2.3 Configure SSO in OAM Console

This topic provides the systematic instructions to configure SSO in OAM console.

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

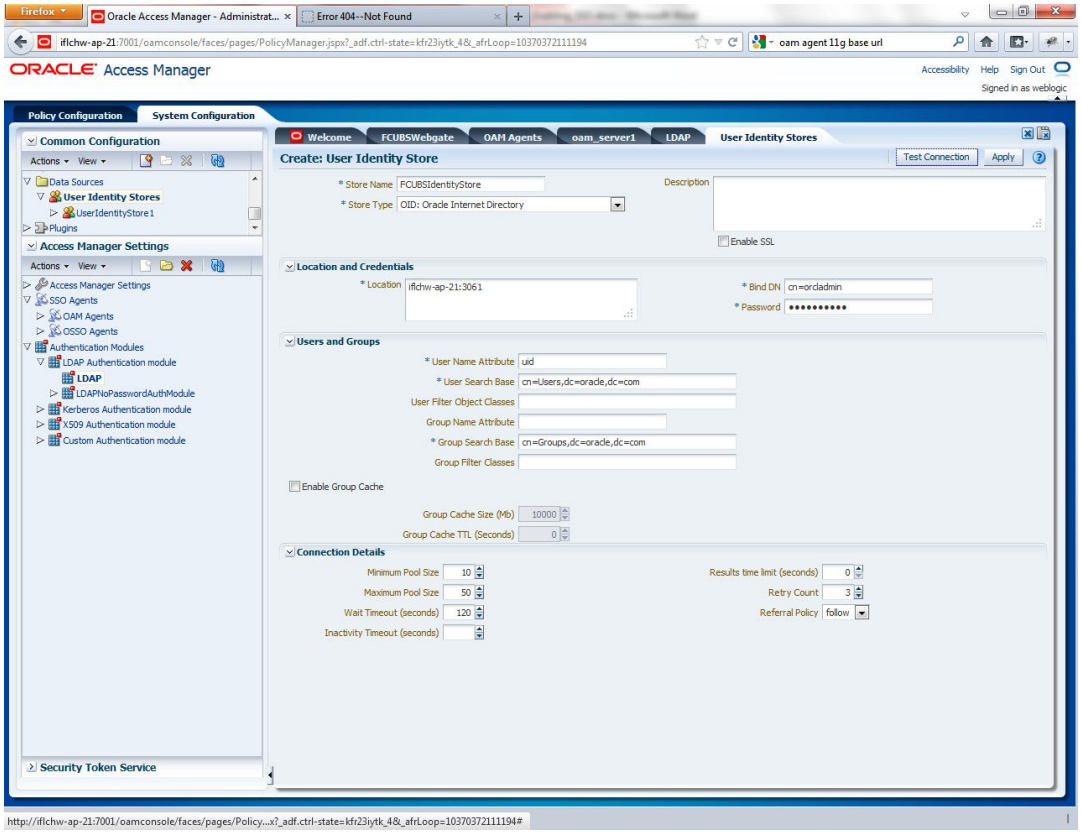
Follow the post installation scripts deployWebGate and EditHttpConf as provided in the *Post Installation Steps* topic in the *Fusion Middleware Installation Guide for Oracle Identity Management*.

1. Identity Store Creation.
2. To create new user identity store, login to OAM Console.
3. Navigate to **System Configuration** click **Common configuration**, and click**Data Sources** and select **User Identity Store**.
4. Specify the below information in the User Identity Store.

Table 2-1 User Identity Store

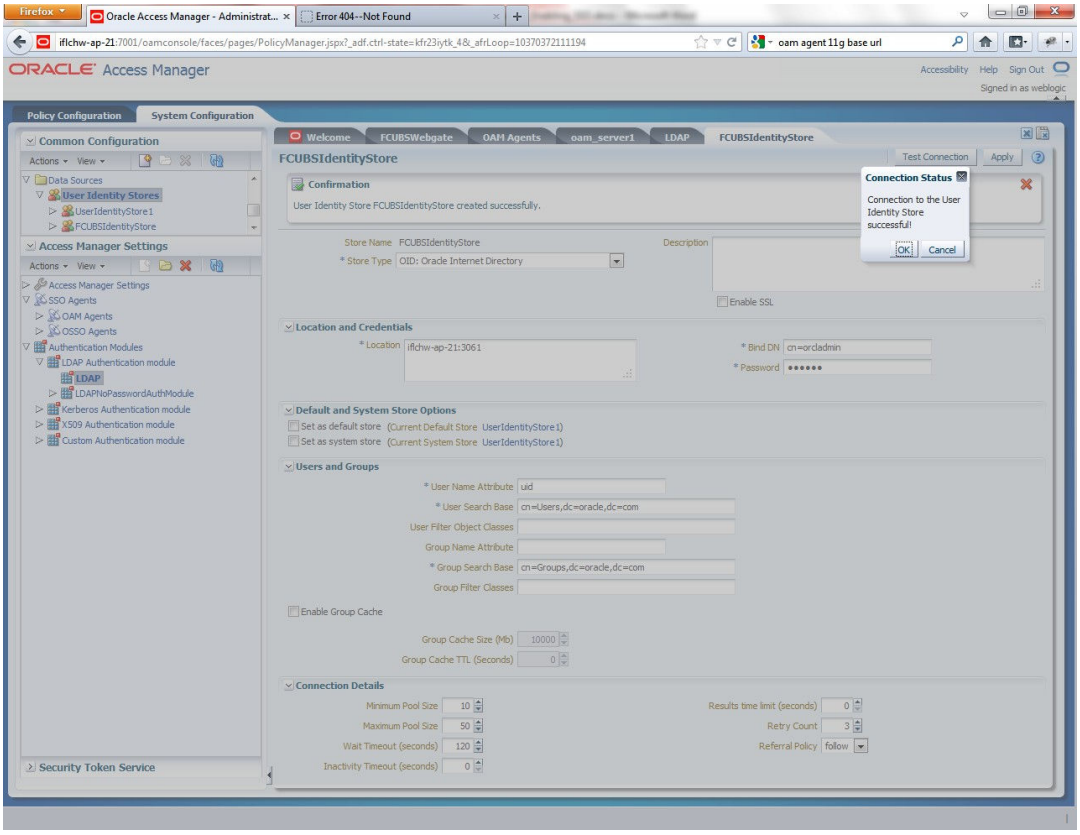
Field	Description
Store type	Select Store Type as Oracle Internet Directory.
Location	Specify LDAP server Host name and Port Number. For example: <HOSTNAME>:<PORT number>
Bind DN	Specify user name to connect the LDAP Server.
Password	Specify password to connect the LDAP Server.
User Name Attribute	The attribute created in LDAP, which will be the User Name for the other application (here it will be treated as the Oracle Banking Corporate Lending 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.

Figure 2-2 Oracle Access Manager- System Configuration



5. Click the **Apply** button after entering the above information.
6. On successful creation, click the **Test connection** button to verify whether the LDAP connection is working fine.

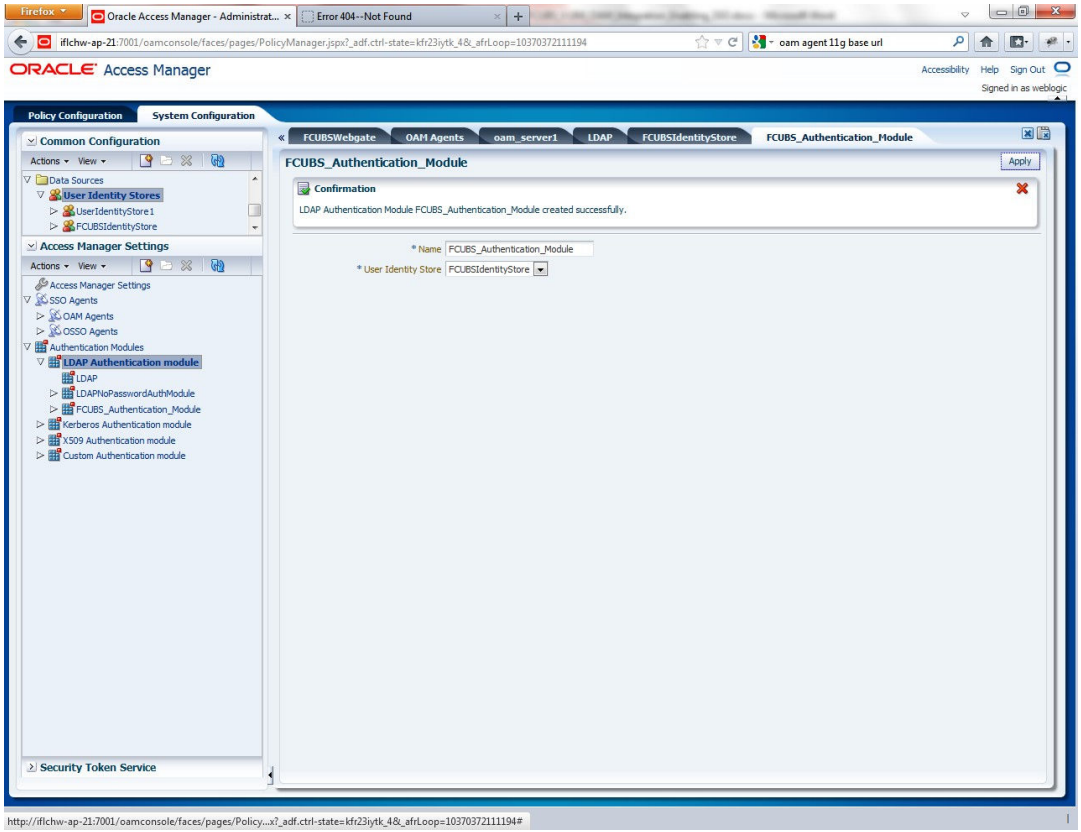
Figure 2-3 Oracle Access Manager- System Configuration - Test Connection



7. To create Authentication Module, navigate to **System Configuration** click **Access Manager Settings**, and click **Authentication Modules**, and then click **LDAP Authentication Module**.

   The **LDAP Authentication Module** screen displays.

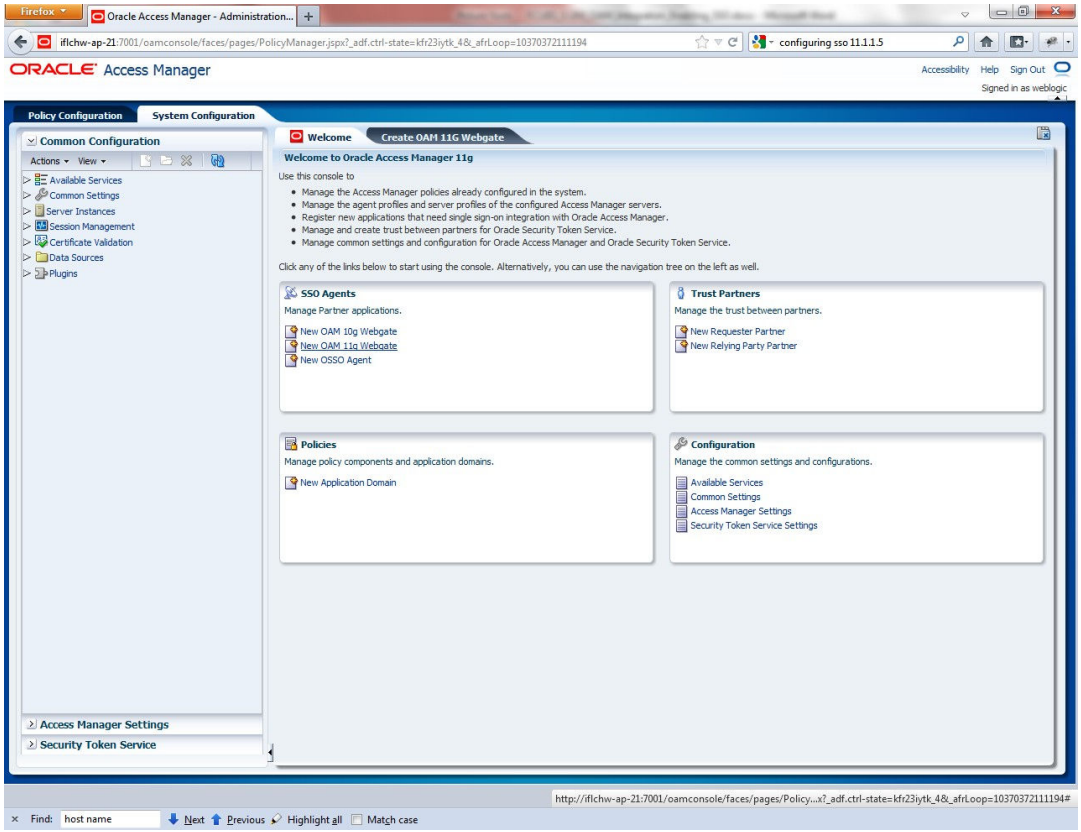
Figure 2-4 LDAP Authentication Module



8. Click the **New** button to create new Authentication Module.
9. Specify **Name** of the authentication module and choose the **User Identity Store**.
10. To create OAM 12c Webgate, navigate to **System Configuration**, click **Access Manager Settings**, and click **SSO Agents**, and then click **OAM Agents**.

    The **OAM Agents** screen displays.

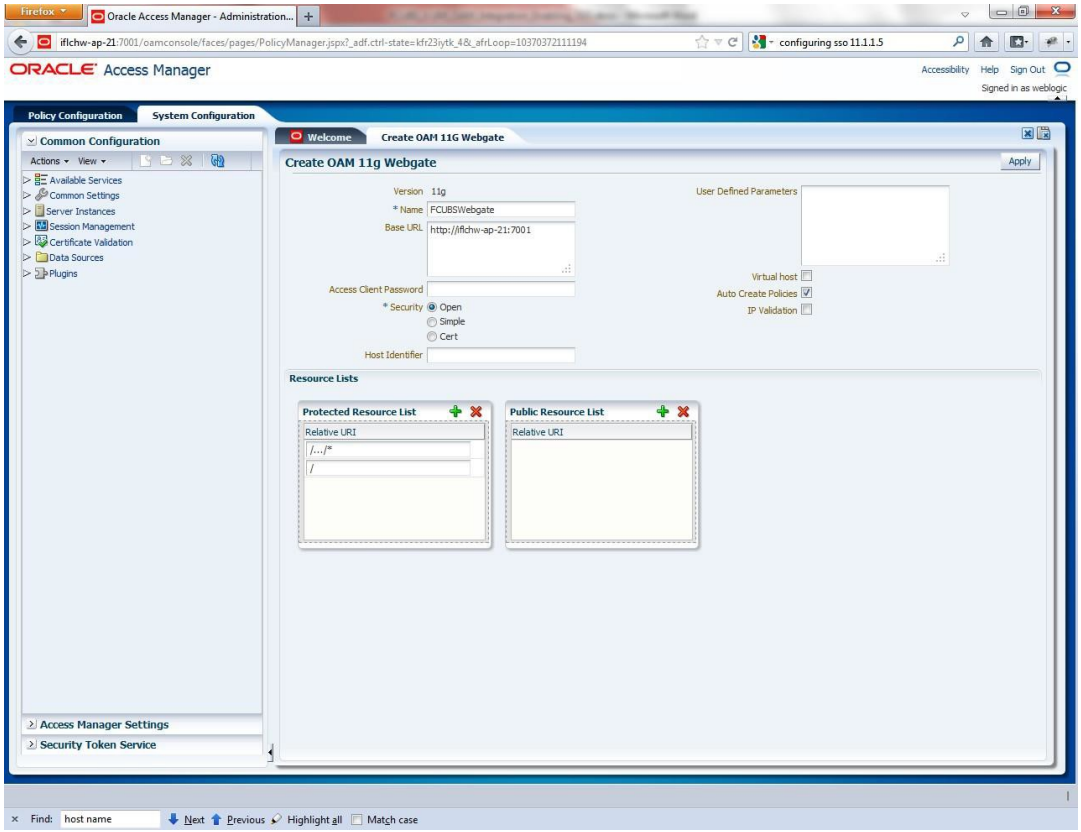
Figure 2-5 Welcome to Oracle Access Manager



11. Click the **Create 12c webgate** button or Click new **OAM 12c Webgate** link available in welcome page.

    The **Create OAM 12c Webgate** screen displays.

Figure 2-6 Create OAM 12c Webgate



12. Specify **Name** for Webgate and **Base URL** (The host and port of the computer on which the Web server for the Webgate is installed).

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

13. Click the **Apply** button to save the changes.

    A confirmation message displays on the **FCUBSWebgate** screen.

14. Perform the following steps to copy the artifacts to the Webgate installation directory after OAM Webgate 12c is created:

    - 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)`

15. To create Authentication Scheme, navigate to **Policy Configuration**, click **Authentication Schemes**.

    The **Authentication Schemes** screen displays.

16. Click **Create** button to create new Authentication Scheme and specify the following details:

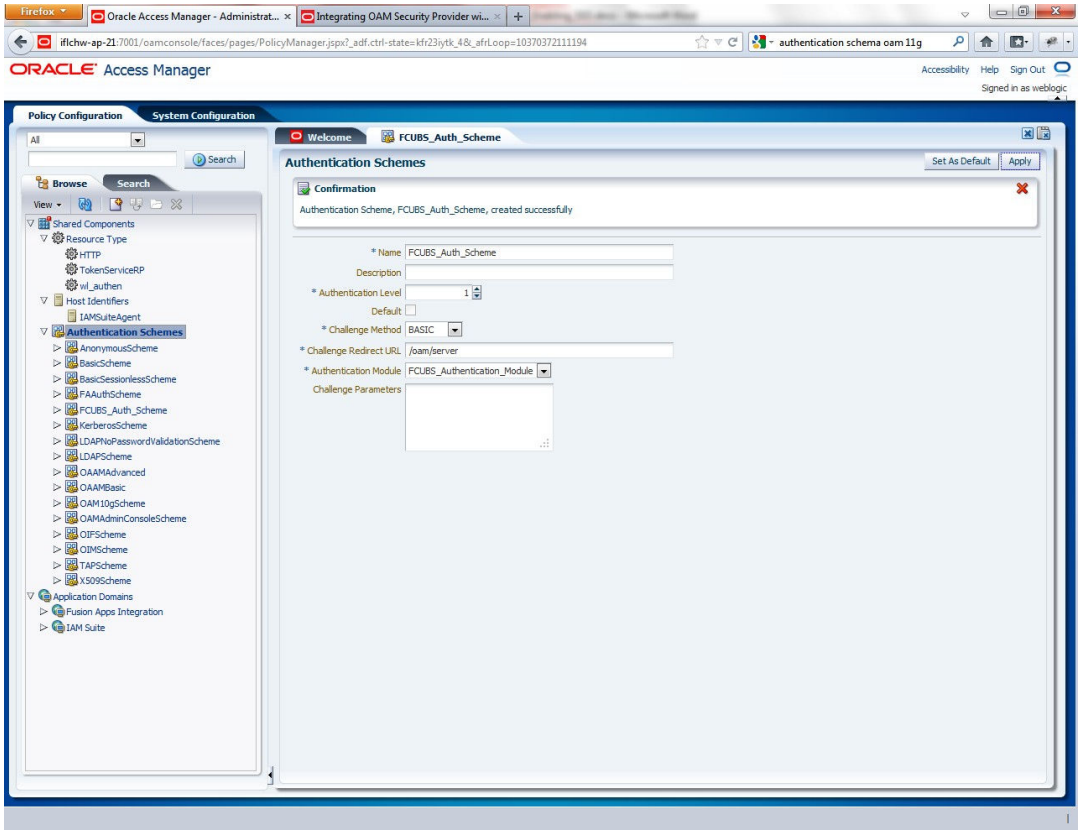
Table 2-2 Authentication Schemes

Field	Description
Name	Specify name to identify Authentication Scheme.
Authentication Level	Set the authentication level to 1.
Challenge Method	Select challenge method as **BASIC** from the drop-down.
Challenge Redirect URL	Specify URL as /oam/server
Authentication Module	Select the authentication module as OBCL_Authentication_Module from the drop-down.

If it is a basic authentication scheme, user 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>`

The new authentication scheme is created.

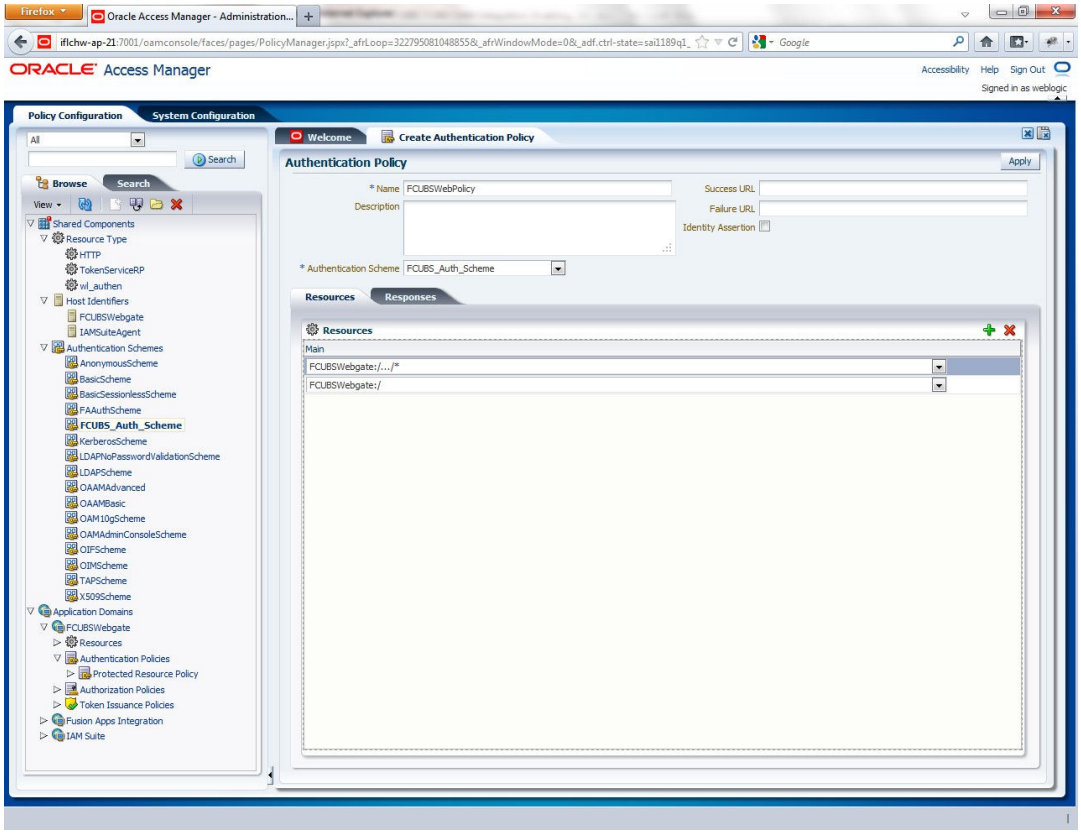
Figure 2-7 Authentication Schemes



17. To create authentication policy, navigate to **Policy Configuration**, click **Application Domains**, and click **[Webgate agent name]**, and then click**Authentication Policies**.

    The **Authentication Policies** screen displays.

Figure 2-8 Authentication Policies



18. Click **New** and specify the below information:

Table 2-3 Authentication Policies

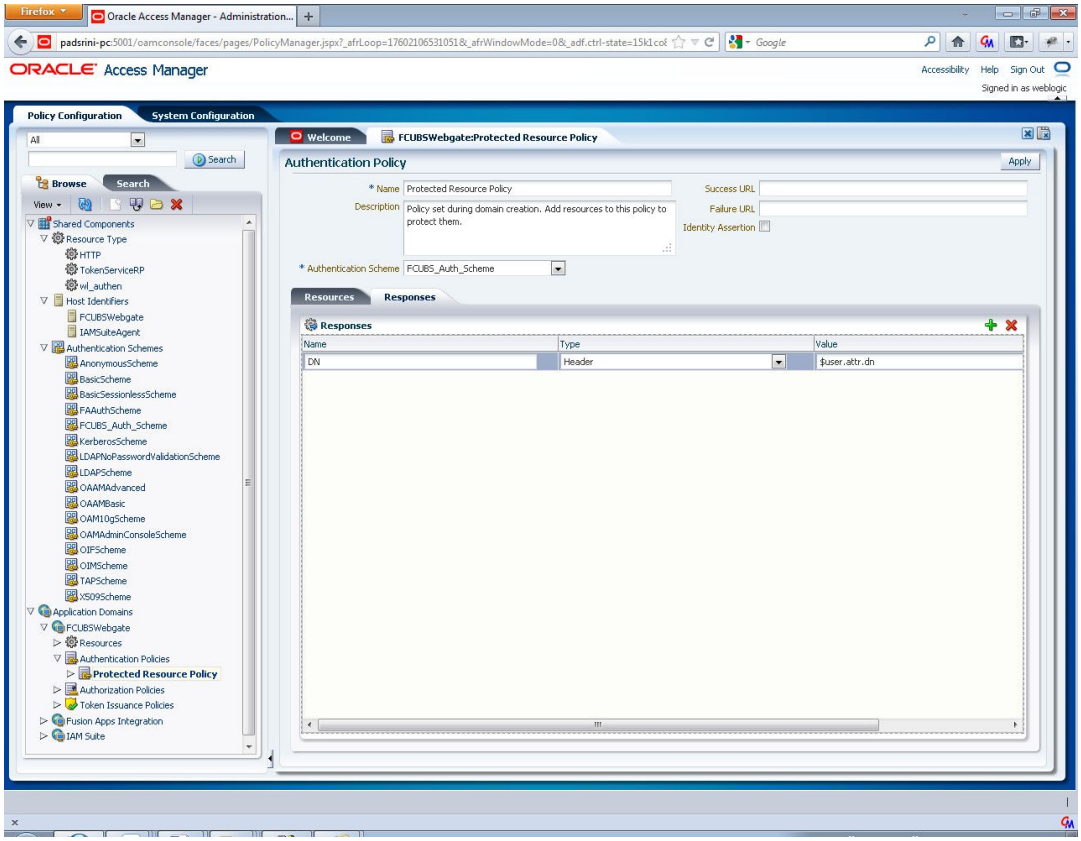
Field	Description
Name	Specify any name to identify the Authentication Policy (For example: OBCLWebPolicy)
Authentication Scheme	Select the authentication scheme from the drop-down.

19. In the **Resources** section, 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.

20. Click **Responses** tab and specify the **Name** as **DN** and the **Value** as **$user.attr.dn**.

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

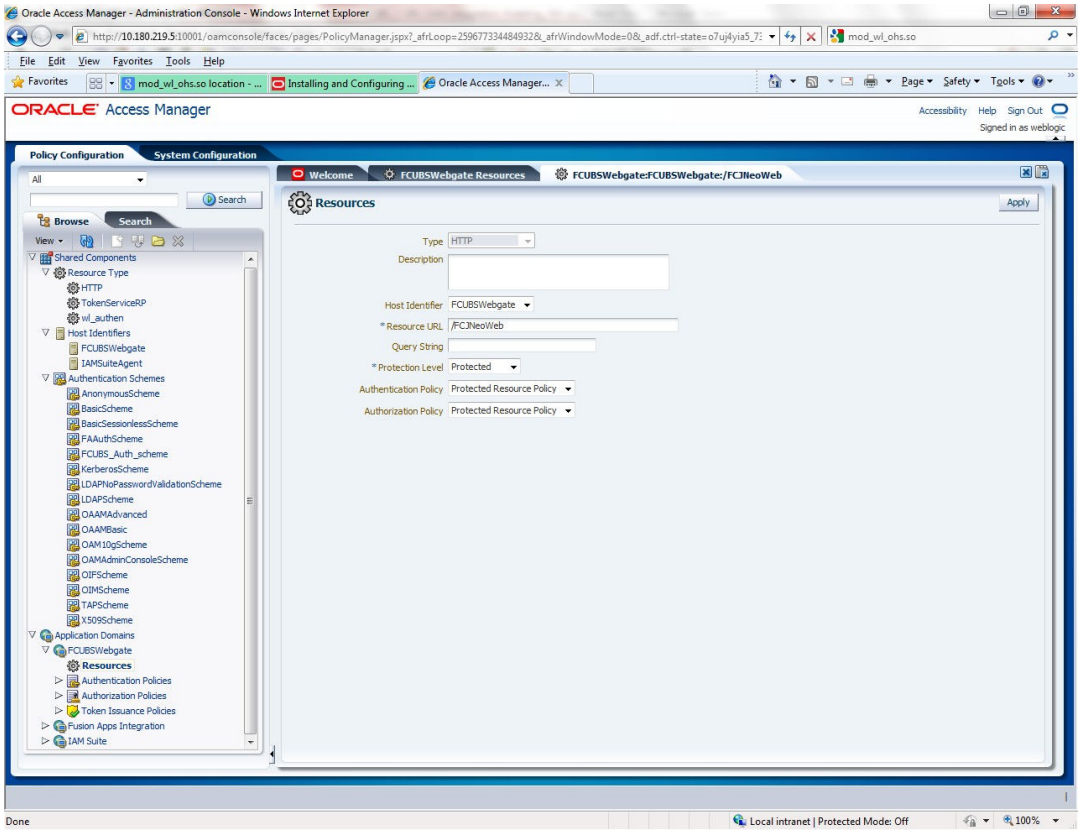
Figure 2-9 Authentication Policy - Response tab



21. To add new resources, navigate to **Policy Configuration**, click **Application Domains**, and click **OBCLWebgate**, and then click **Resources**.

    The **Resources** screen displays.

Figure 2-10 Resources



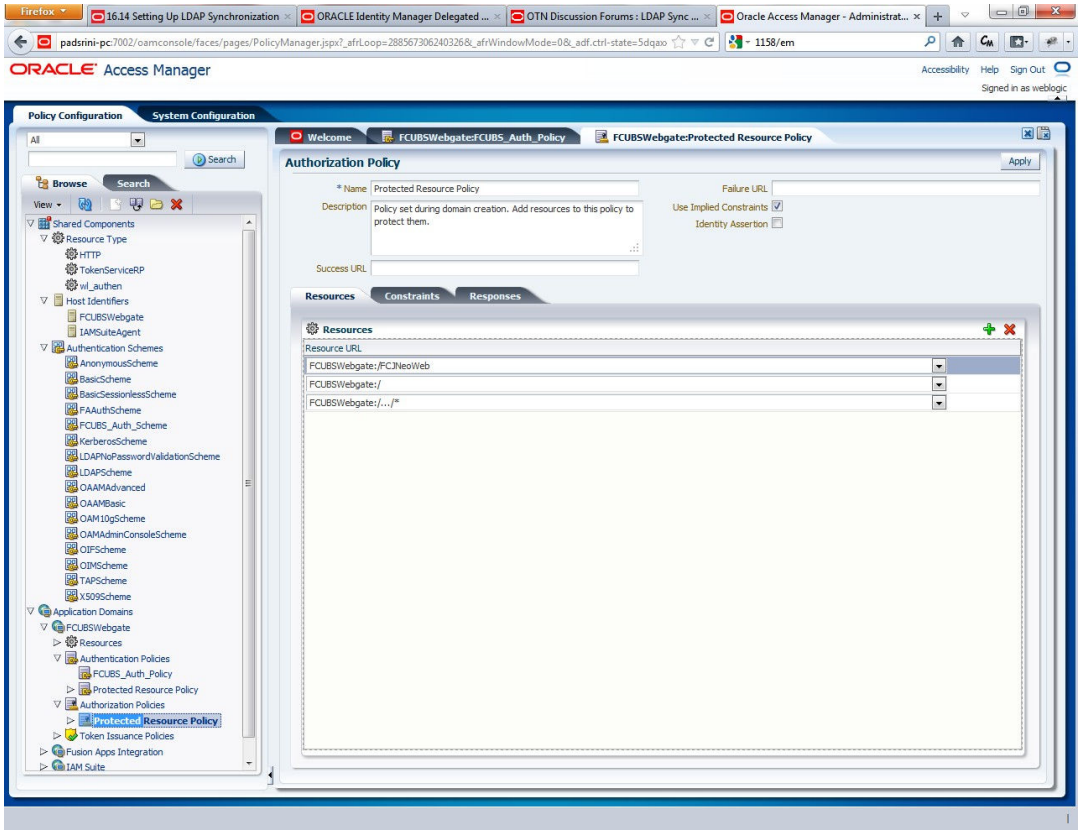
22. Click the **Create New Resource** button and specify the following details.

Table 2-4 Resources

Field	Description
Type	Select the type as **HTTP**.
Host Identifier	Select the Host Identifier as **OBCLWebgate**.
Resource URL	Specify the resource URL as **/FCJNeoWeb**.
Protection Level	Select the protection level as **Protected** from the drop-down.
Authentication Policy	Select **Protected Resource Policy** from the drop-down.
Authorization Policy	Select **Protected Resource Policy** from the drop-down.

23. Click the **Apply** button to update the resource added.
24. Check whether the resources available in the authentication policies are available in Authorization Policy. During web gate creation these values are defaulted.

Figure 2-11 Application Policy - Resources



25. Click **Responses** tab and specify the **Name** as **DN** and the **Value** as **$user.attr.dn**.

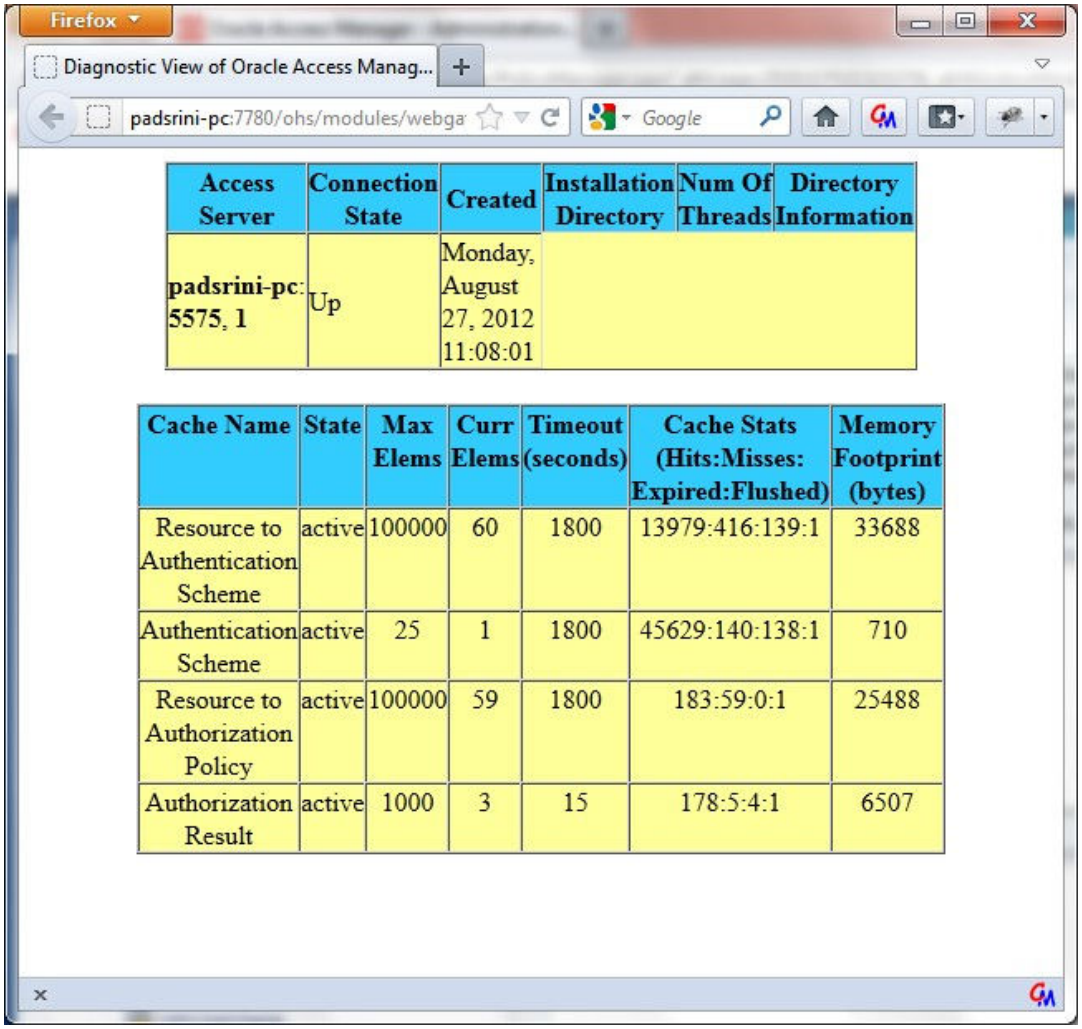
    The responses maintained in the tab will be added in the response header during the authorization.

26. 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>
    ```

27. 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.

Figure 2-12 Diagnostic View of Oracle Access Manager



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

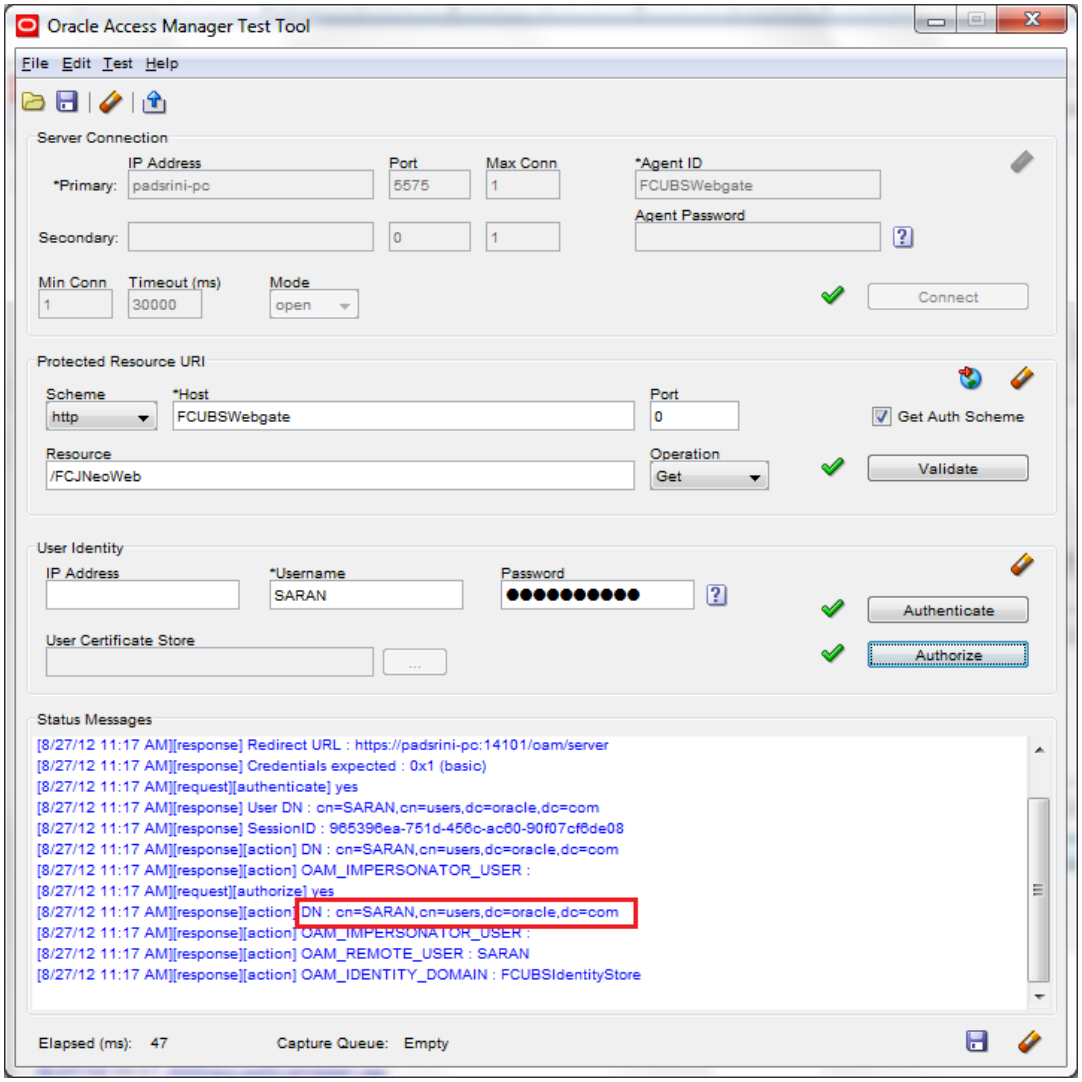
Cache Name	State	Max Elems	Curr Elems	Timeout (seconds)	Cache Stats (Hits:Misses: Expired:Flushed)	Memory Footprint (bytes)
Resource to Authentication Scheme	active	100000	60	1800	13979:416:139:1	33688
Authentication Scheme	active	25	1	1800	45629:140:138:1	710
Resource to Authorization Policy	active	100000	59	1800	183:59:0:1	25488
Authorization Result	active	1000	3	15	178:5:4:1	6507

28. Use 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 example *D:\weblogic\Middleware\Oracle_IDM1\oam\server\tester*

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

Figure 2-13 Oracle Access Manager Test Tool



2.4 Launch Oracle Banking Corporate Lending after Installation

This topic describes information on first launch of Oracle Banking Corporate Lending after installation.

1. After installing Oracle Banking Corporate Lending, launch it for first time.
   The OBCL login screen displays.
2. Specify **User ID** and **Password**.
3. Click **Login**.
   This screen is displayed because the **SSO installed** parameter is set to **N** during installation.

This topic contains the following sub-topics:

- Enable SSO
  This topic provides the systematic instructions to enable SSO details.
- Update SSO Parameters
  This topic provides the systematic instructions to update SSO parameters.

- Maintain Branch Level DN Template
  This topic provides the systematic instructions to maintain the Branch Level DN Template.
- Maintain LDAP DN for Oracle Banking Corporate Lending Users
  This topic provides the systematic instructions to maintain the LDAP DN for Oracle Banking Corporate Lending Users.
- Launch Oracle Banking Corporate Lending
  This topic provides the systematic instructions to launch Oracle Banking Corporate Lending Installer.
- Signoff in a SSO Situation
  This provides the information about Signoff from the Oracle Banking Corporate Lending session using SSO.

2.4.1 Enable SSO

This topic provides the systematic instructions to enable SSO details.

To maintain the parameters required for SSO, perform the below procedure:

1. Login into the application.
2. Navigate to **Bank Parameters Maintenance** screen and click **General Preferences** tab.

   The **Bank Maintenance - General Preferences** screen displays.
3. Select the **SSO Enabled** check box and click **OK**.

2.4.2 Update SSO Parameters

This topic provides the systematic instructions to update SSO parameters.

To maintain the parameters required for SSO, perform the below procedure:

1. Go to **Security Maintenance**, click **Sys. Administration**, and click **SSO Maintenance**.

   The **Single Sign-on Maintenance** screen displays.
2. Specify the following details:
   - **LDAP Host Name**
   - **LDAP Port number**
   - **LDAP Admin ID**
   - **LDAP Password**
   - **LDAP Base**
   - **Login Time Out Duration (in Sec)**
3. Click **Finish** to update the SSO details.

2.4.3 Maintain Branch Level DN Template

This topic provides the systematic instructions to maintain the Branch Level DN Template.

To maintain the LDAP DN template for each branch, the corresponding LDAP userid is automatically populated, which is used in the user maintenance form.

1. Navigate to the **Branch Maintenance** and click **Branch Level Parameter**.

   The **Branch Level Parameter** screen displays.

2. Click the **Preferences** tab and update LDAP DN Template.

   For example: `LDAP DN Template: cn=<FCJUSR>,cn=Users,dc=i-flex,dc=com`

   In the above template, **cn=<FCJUSR>** should not be modified and rest of the DN name can change based on the configuration.

2.4.4 Maintain LDAP DN for Oracle Banking Corporate Lending Users

This topic provides the systematic instructions to maintain the LDAP DN for Oracle Banking Corporate Lending Users.

For each user ID in Oracle Banking Corporate Lending, should be created in the LDAP. When you create the user in LDAP, make sure that the DN value is same as the LDAP DN value that will be updated in User Maintenance form.

1. Once the user is created in LDAP, navigate to the User Maintenance form in OBCL.

   If the OBCL user already exists, then unlock the user details and update the LDAP DN value which was set when creating the user in LDAP.

2. Click the **Validate** button to check whether any other user is having the same LDAP DN value.

2.4.5 Launch Oracle Banking Corporate Lending

This topic provides the systematic instructions to launch Oracle Banking Corporate Lending Installer.

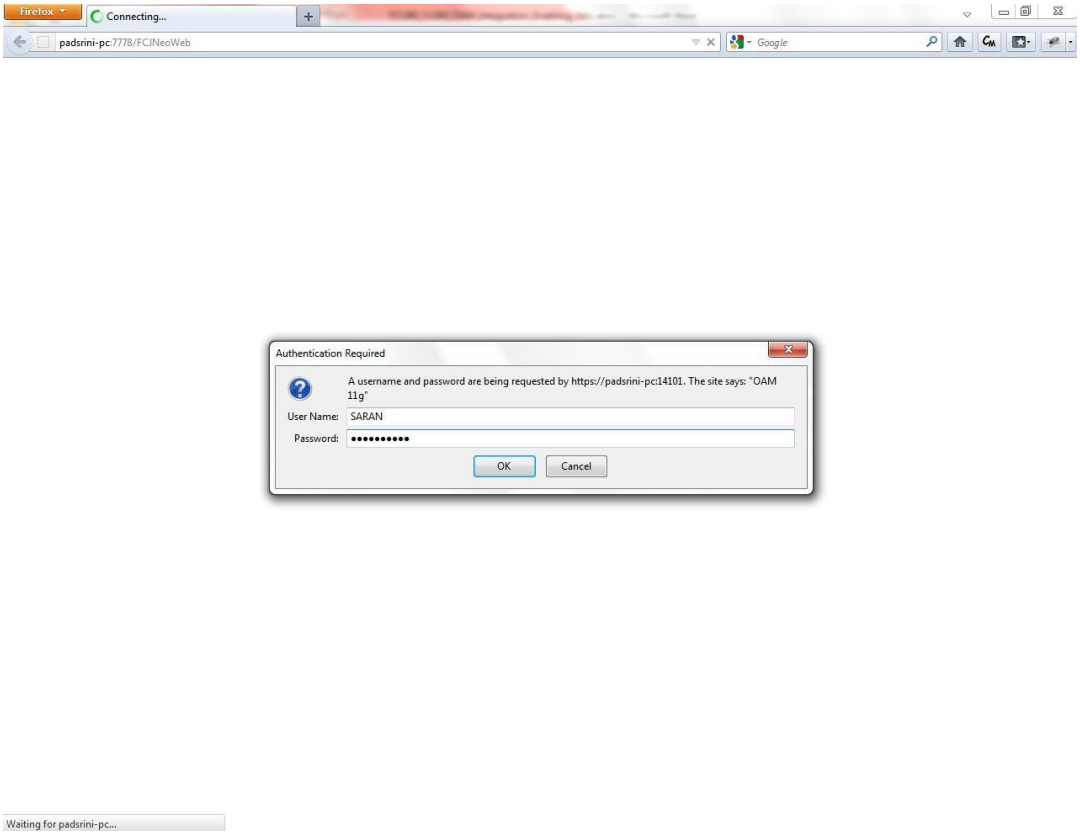
After setting up Oracle Banking Corporate Lending to work on Single Sign on mode, perform the below procedure:

1. Navigate to the interim servlet URL from your browser.

   For example: http://<hostname>:[port]/FCJNeoWeb

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

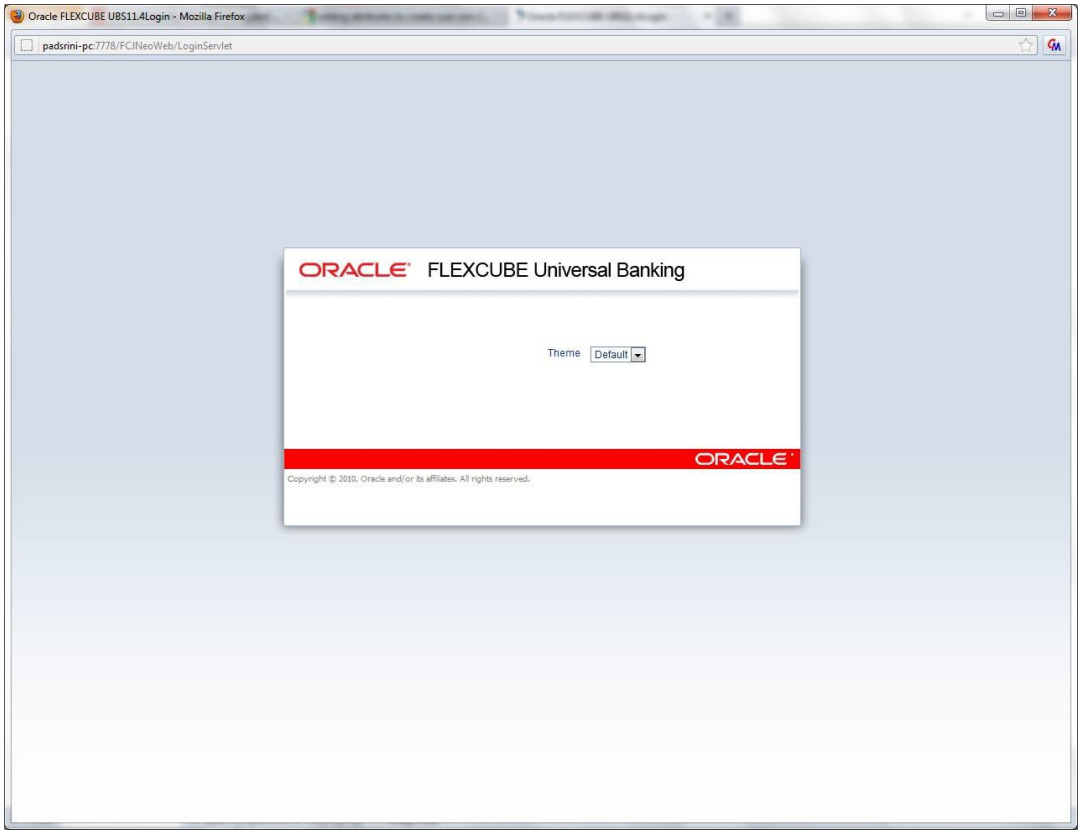
Figure 2-14 Authentication Required



2. Once the user is authenticated and authorized to access the resource, the servlet gets redirected to normal Oracle Banking Corporate Lending application server URL and now the new signon form will appear as below.

   The application will automatically redirect Oracle Banking Corporate Lending home page.

Figure 2-15 Login page



2.4.6 Signoff in a SSO Situation

This provides the information about Signoff from the Oracle Banking Corporate Lending session using SSO.

Oracle Banking Corporate Lending does not currently support single sign-off, that means when a user sign off, the session established with Oracle Access Manager does not affected in any manner.

In a SSO situation, the **Exit** and **Logoff** actions will function as **Exit**, that means on clicking these, the user will exit from the Oracle Banking Corporate Lending session. If you want to re-launch Oracle Banking Corporate Lending, use the Oracle Banking Corporate Lending launch URL.