

Oracle Access Manager Integration  
Oracle FLEXCUBE Universal Banking  
Release 14.4.0.4.0  
May 2021



# Table of Contents

<b>1. PREFACE .....</b>	<b>1-3</b>
1.1 INTRODUCTION.....	1-3
1.2 AUDIENCE .....	1-3
1.3 ABBREVIATIONS .....	1-3
1.4 DOCUMENTATION ACCESSIBILITY .....	1-3
1.5 ORGANIZATION .....	1-3
1.6 GLOSSARY OF ICONS .....	1-4
1.6.1 <i>Related Documents</i> .....	1-4
<b>2. ENABLING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER.....</b>	<b>2-1</b>
2.1 INTRODUCTION.....	2-1
2.2 BACKGROUND AND PREREQUISITES .....	2-1
2.2.1 <i>Software Requirements</i> .....	2-1
2.3 BACKGROUND OF SSO RELATED COMPONENTS.....	2-2
2.3.1 <i>Oracle Access Manager (OAM)</i> .....	2-2
2.3.2 <i>LDAP Directory Server</i> .....	2-2
2.3.3 <i>WebGate/AccessGate</i> .....	2-2
2.3.4 <i>Oracle Adaptive Access Manager</i> .....	2-3
2.4 ASSUMPTIONS .....	2-3
2.5 INSTALL AND CONFIGURE ORACLE ACCESS MANAGER .....	2-3
2.5.1 <i>Installation of Infrastructure and OAM</i> .....	2-3
2.5.2 <i>Run the Repository Creation Utility</i> .....	2-3
2.5.3 <i>Configure the Oracle Access Management 12c Domain</i> .....	2-4
2.5.4 <i>Start the Servers</i> .....	2-6
2.6 INSTALL AND CONFIGURE ORACLE UNIFIED DIRECTORY .....	2-6
2.6.1 <i>Install Oracle Unified Directory</i> .....	2-6
2.6.2 <i>Configure Oracle Unified Directory</i> .....	2-7
2.6.3 <i>Configure OUD as the Identity Store in OAM</i> .....	2-8
2.7 INSTALL AND CONFIGURE ORACLE HTTP SERVER 12C .....	2-10
2.7.1 <i>Install Oracle HTTP Server</i> .....	2-10
2.7.2 <i>Configure HTTP Server</i> .....	2-11
2.7.3 <i>Start the Servers</i> .....	2-12
2.8 CREATING OAM 12C WEBGATE.....	2-12
2.8.1 <i>Post OAM Webgate 12c Creation</i> .....	2-17

---

# 1. Preface

## 1.1 Introduction

This manual discusses the integration of Oracle FLEXCUBE Universal Banking and the Oracle Access Manager system. The configurations required for 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.
Implementation team	Implementation of Oracle FLEXCUBE Universal Banking

## 1.3 Abbreviations

Abbreviation	Description
System	Unless specified, it shall always refer to Oracle FLEXCUBE
OAM	Oracle Access Manager
OHS	Oracle HTTP Server
ODU	Oracle Unified Directory
UBS	Universal Banking Solutions
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:

<b>Chapter 1</b>	<i>Preface</i> gives information on the intended audience. It also lists the various chapters covered in this User Manual.
<b>Chapter 2</b>	<i>Enabling Single Sign-on (SSO) with Oracle Access Manager</i> discusses the method to integrate Oracle FLEXCUBE 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
	Exit
	Add row
	Delete row
	Option List

### 1.6.1 Related Documents

You may refer the following manual for more information

- Oracle Access Manager User Manual (not included with Oracle FLEXCUBE User Manuals)

---

## 2. Enabling Single Sign-on with Oracle Access Manager

### 2.1 Introduction

For the purpose of single sign-on FLEXCUBE is qualified with Oracle Identity Management 12.2.1.3.0 (Fusion Middleware 12cR2) – specifically using the Access Manager component of Oracle Identity Management. This feature is available in FLEXCUBE since the release FC UBS V.UM 7.3.0.0.0.0 .

This document provides an understanding as to how single sign-on can be enabled for a FLEXCUBE deployment using Oracle Fusion Middleware 12cR2.

In addition to providing a background to the various components of the deployment, this document also talks about Configuration to be done in FLEXCUBE and Oracle Access Manager to enable single sign-on using Oracle Internet Directory as a LDAP server.

### 2.2 Background and Prerequisites

#### 2.2.1 Software Requirements

##### **Oracle Identity and Access Management 12c R2 - 12.2.1.3.0**

- JDK 1.8 for Linux x64
- Oracle Middleware (WLS) (12.2.1.3.0) software
- Oracle Access Manager – 12.2.1.3.0
- Oracle Unified Directory - 12.2.1.3.0
- Oracle Fusion Middleware Web Tier Utilities 12c - 12.2.1.3.0
  - Oracle HTTP Server
- Optional: Oracle Adaptive Access Manager – 12.2.1.3.0 (Strong Authentication purpose only )

##### **LDAP Directory Server**

Please make sure that the LDAP server to be used for FLEXCUBE 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. Though we have only use OUD for our testing purposes):

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

For the purpose of achieving single sign on for FLEXCUBE in FMW 12cR2, it is necessary for the weblogic instance to have an explicit **Oracle HTTP server (OHS)**.

## **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**

To integrate Flexcube with OAM to achieve Single Sign-on feature, Flexcube's password policy management, like password syntax and password expiry parameters will no longer be handled by Flexcube. 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 Flexcube application users' 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 Oracle Adaptive Access Manager

Oracle Adaptive Access Manager provides an innovative, comprehensive feature set to help organizations prevent fraud and misuse. Strengthening standard authentication mechanisms, innovative risk-based challenge methods, intuitive policy administration and integration across the Identity and Access Management Suite and with third party products make Oracle Adaptive Access Manager uniquely flexible and effective. Oracle Adaptive Access Manager provides real-time and batch risk analytics to combat fraud and misuse across multiple channels of access. Real-time evaluation of multiple data types helps stop fraud as it occurs. Oracle Adaptive Access Manager makes exposing sensitive data, transactions and business processes to consumers, remote employees or partners via your intranet and extranet safer.

Oracle Adaptive Access Manager provides an extensive set of capabilities including device fingerprinting, real-time behavioral profiling and risk analytics that can be harnessed across both Web and mobile channels. It also provides risk-based authentication methods including knowledge-based authentication (KBA) challenge infrastructure with Answer Logic and OTP Anywhere server-generated one-time passwords, delivered out of band via Short Message Service (SMS), e-mail or Instant Messaging (IM) delivery channels. Oracle Adaptive Access Manager also provides standard integration with Oracle Identity Management, the industry leading identity management and Web Single Sign-On products, which are integrated with leading enterprise applications.

## 2.4 Assumptions

- The steps provided below assume that FLEXCUBE has already been deployed and is working (without single sign-on)
- For simplicity, the Steps followed in the document used non-ssl configuration. For production environment it is recommended to use SSL configuration.

## 2.5 Install and Configure Oracle Access Manager

### 2.5.1 Installation of Infrastructure and OAM

1. Run the following command to install WebLogic Server and complete all the steps:

```
cd /stage  
unzip fmw_12.2.1.3.0_infrastructure_Disk1_1of1.zip  
java -jar /stage/fmw_12.2.1.3.0_infrastructure.jar
```

2. After the above installation, install OAM binary in the above installed directory.

```
java -jar /stage/fmw_12.2.1.3.0_idm.jar
```

### 2.5.2 Run the Repository Creation Utility

1. Launch a terminal window and enter the following command

```
cd /u01/app/oracle/product/middleware/oracle_common/bin  
./rcu
```

2. Follow the table below to guide you through the installation screens:

Step	Window Description	Choices or Values
1.	Welcome1	Click <b>Next</b>

2.	Create Repository	<b>System Load and Product Load</b>
3.	Database Connection Details	<b>Database Type:</b> Oracle Database <b>Host Name:</b> oam.example.com <b>Port:</b> 1521 <b>Service Name:</b> orcl.example.com <b>Username:</b> sys <b>Password:</b> Welcome1 <b>Role:</b> SYSDBA  Click <b>OK</b> in Checking Prerequisites window
4.	Checking Prerequisites	Click <b>OK</b>
5.	Select Components	<b>Create a new prefix:</b> DEV Select schema: Oracle Access Manager  Click <b>OK</b> in Checking Prerequisites window
6.	Schema Passwords	<b>Use same passwords for all schemas</b> <b>Password:</b> Welcome1 <b>Confirm Password:</b> Welcome1
7.	Map Tablespaces	Click <b>Next</b> Click <b>OK</b> in Confirmation and Creating Tablespaces window
8.	Summary	Click <b>Create</b>
9.	Completion Summary	Click <b>Close</b>

### 2.5.3 Configure the Oracle Access Management 12c Domain

1. Launch a terminal window and enter the following command if RCU database is in RAC else follow step 2.  
cd /u01/app/oracle/product/middleware/oracle\_common/common/bin  
./config.sh
2. If RCU database is not RAC then follow this step. Edit config\_internal.sh in /u01/app/oracle/product/middleware/oracle\_common/common/ and add - Doracle.jdbc.fanEnabled=false in JVM\_ARGS and save the file.

Example:

```
JVM_ARGS="-Dpython.cachedir=/tmp/cachedir -Doracle.jdbc.fanEnabled=false
${JVM_D64} ${JVM_D64} ${UTILS_MEM_ARGS} ${SECURITY_JVM_ARGS}
${CONFIG_JVM_ARGS}"
```



Launch ./config.sh

3. Follow the table below to guide you through the configuration screens:

Step	Window Description	Choices or Values
1.	Create Domain	Select <b>Create a new domain Domain</b> <b>Location:</b> /u01/app/oracle/admin/domains/oam_domain
2.	Templates	<b>Create Domain Using Product Templates</b> Select: <b>Oracle Access Management Suite</b>
3.	Application Location	<b>Application</b> <b>Location:</b> /u01/app/oracle/admin/applications/oam_domain
4.	Administrator Account	<b>Name:</b> weblogic <b>Password:</b> Welcome1 <b>Confirm:</b> Welcome1
5.	Domain Mode and JDK	<b>Domain Mode: Production</b> <b>JDK: Oracle Hotspot</b>
6.	Database Configuration Type	<b>Host Name:</b> oam.example.com <b>DMS/Service:</b> orcl.example.com <b>Port:</b> 1521 <b>Schema Owner:</b> DEV_STB <b>Schema Password:</b> Welcome1  Click <b>Get RCU Configuration</b> If successful click <b>Next</b>
7.	Component Datasources	Click <b>Next</b>
8.	JDBC Component Schema Test	Click <b>Next</b>
9.	Advanced Configuration	Select <b>Node Manager</b> , and <b>Topology</b>
10.	Node Manager	<b>Node Manager Type:</b> Per Domain Default Location <b>Username:</b> weblogic <b>Password:</b> Welcome1 <b>Confirm Password:</b> Welcome1
11.	Managed Servers	Click <b>Next</b>

12.	Clusters	Click <b>Next</b>
13.	Server Templates	Click <b>Next</b>
14.	Coherence Clusters	Click <b>Next</b>
15.	Machines	Click <b>Add</b> <b>Name:</b> oam_machine
16.	Assign Servers to Machines	Select <b>Admin Server, oam_server1</b> and <b>oam_policy_mgr1</b> . Select <b>oam_machine</b> and click the right arrow to move the servers under oam_machine
17.	Virtual Targets	Click <b>Next</b>
18.	Partitions	Click <b>Next</b>
19.	Configuration Summary	Click <b>Create</b>
20.	Configuration Progress	Click <b>Next</b>
21.	End of Configuration	Click <b>Finish</b>

## 2.5.4 Start the Servers

1. Launch a terminal window as `oracle` and enter the following commands to star the Oracle Access Management 12c AdminServer  
`cd /u01/app/oracle/admin/domains/oam_domain/`  
`./startWebLogic.sh`
2. In another terminal window start Node Manager by running the following command:  
`nohup ./startNodeManager.sh`
3. Test the installation

Start a browser and access the Oracle Access Management Console at <http://oam.example.com:7001/oamconsole>. Login as `weblogic/Welcome1`.

Access <http://oam.example.com:14150/access> and login with `weblogic/Welcome1`.

## 2.6 Install and Configure Oracle Unified Directory

### 2.6.1 Install Oracle Unified Directory

1. Launch a terminal window and enter the following command:  
`java -jar fmw_12.2.1.3.0_oud_generic.jar`

- Follow the table below to guide you through the installation screens. For internal testing purpose we have used Standalone Installation and uploaded some sample user data.

Step	Window Description	Choices or Values
1.	Welcome	Click <b>Next</b>
2.	Auto Updates	<b>Skip Auto Updates</b>
3.	Installation Location	<b>Oracle Home:</b> /u01/app/oracle/product/middleware/oud
4.	Installation Type	<b>Standalone Oracle Unified Directory Server (Managed independently of WebLogic Server)</b>
5.	Prerequisite Checks	Click <b>Next</b>
6.	Installation Summary	Click <b>Install</b>
7.	Installation Progress	Click <b>Next</b>
8.	Installation Complete	Click <b>Finish</b>

## 2.6.2 Configure Oracle Unified Directory

- Launch a terminal window as `oracle` and enter the following command:

```
2. cd /u01/app/oracle/product/middleware/oud/oud
```

```
./oud-setup
```

- Follow the table below to guide you through the configuration screens:

Step	Window Description	Choices or Values
1.	Welcome	Click <b>Next</b>

2.	Server Administration Settings	<b>Instance Path:</b> /u01/app/oracle/product/middleware/oud/asinst_1/OU <b>Host Name:</b> oam.example.com <b>Password:</b> Welcome1 <b>Confirm Password:</b> Welcome1
3.	Ports	Select Checkbox: <b>LDAPS: Enable on Port</b>
4.	Topology Options	Select: <b>This will be a standalone server</b>
5.	Directory Data	Select: <b>Leave Database Empty</b>
6.	Oracle Components Integration	Click <b>Next</b>
7.	Server Tuning	Click <b>Next</b>
8.	Review	Click <b>Finish</b>
9.	Finished	Click <b>Close</b>

4. Import sample identity data(empl.ldif) including some users and groups. Run the following command to populate the oud1 directory server with sample data:

```
cd /u01/app/oracle/product/middleware/oud/asinst_1/OU/bin
./ldapmodify -p 1389 -D "cn=Directory Manager" -w Welcome1 -a -c -f /stage/example.ldif
```

### 2.6.3 Configure OUD as the Identity Store in OAM

1. Launch a browser and login to the OAM Console (<http://oam.example.com:7001/oamconsole>) as weblogic/Welcome1.
2. Click the Configuration tab (top right), then click User Identity Stores. Click Create in the OAM ID Stores section.
3. Specify the values as shown:
  - o **Store Name:** OUD Store
  - o **Store Type:** OUD: Oracle Unified Directory
  - o **Location:** oam.example.com:1389
  - o **Bind DN:** cn=Directory Manager

- **Password:** Welcome1
  - **Login ID Attribute:** uid
  - **User Password Attribute :** userPassword
  - **User Search Base:** ou=People,dc=example,dc=com
  - **Group Name Attribute:** cn
  - **Group Search Base:** ou=Groups, dc=example, dc=com
4. Click **Test Connection**. Assuming the connection works, click **OK** in the Connection Status window.
  5. Click **Apply** to save the definition.
  6. Access the **User Identity Stores** tab, and set **Default Store** to OUD\_Store, and then Click **Apply**.
  7. Click **Application Security**, and then **Authentication Modules** under the **Plug-ins** tile.
  8. Click **Create > Create LDAP Authentication Module**. Enter the following values and click **Apply**:
    - **Name:** LDAPOverOUD
    - **User Identity Store:** OUD\_store
  9. Click the **Launch Pad** tab, and click the **Authentication Schemes** link in the Access Manger tile. In the **Search Authentication Schemes** page, click **Search**. Select the **LDAPScheme** row in the search result and click **Edit**.  
In the **LDAPScheme**, click **Duplicate**. It creates a new scheme with the name '**Copy of LDAP Scheme**'. Change this scheme as follows, and then click **Apply**.

### **Basic Style Authentication Scheme**

Enter the below details and click 'Apply':

- Name : Name of the Authentication Scheme
- Authentication Level : 1
- Challenge Method : BASIC
- Challenge Redirect URL : /oam/server
- Authentication Module : LDAPOverOUD
- Refer the section 'Creating Authentication Module 2.6.2' of this document.
- Challenge Parameters : ssoCookie=http  
contextType=default  
contextValue=/oam  
challenge\_url=/CredCollectServlet/BASIC

### **Form Style Authentication Scheme**

Enter the below details and click 'Apply':

- Name : Name of the Authentication Scheme
- Authentication Level : 2
- Challenge Method : FORM
- Challenge Redirect URL : /oam/server
- Authentication Module : LDAPOverOUD

- Challenge URL : /pages/login.jsp
- Context Type : default
- Context Value : /oam
- Challenge Parameters : ssoCookie=http

## 2.7 Install and Configure Oracle HTTP Server 12c

### 2.7.1 Install Oracle HTTP Server

1. Launch a terminal window and enter the following command to install OHS:  

```
cd /stage
chmod +x fmw_12.2.1.3.0_ohs_linux64.bin
./fmw_12.2.1.3.0_ohs_linux64.bin
```
2. Follow the table below to guide you through the installation screens:

Step	Window	Choices or Values
1.	Welcome	Click <b>Next</b>
2.	Auto Updates	Click <b>Next</b>
3.	Installation Location	<b>Oracle Home:</b> /u01/app/oracle/product/middleware/
4.	Installation Type	<b>Collocated HTTP Server (Managed through WebLogic Server)</b>
5.	Prerequisite Checks	Click <b>Next</b>
6.	JDK Selection	<b>JDK Home:</b> /u01/app/oracle/product/jdk
7.	Prerequisite Checks	Click <b>Next</b>
8.	Installation Summary	Click <b>Install</b> . The installation screen will appear*
9.	Installation Complete	Click <b>Finish</b>

## 2.7.2 Configure HTTP Server

1. Launch a terminal window as `oracle` and enter the following command to stop the WebLogic Admin Server:  

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
./stopWebLogic.sh
```
2. Run the following command to launch the Configuration Wizard:  

```
cd /u01/app/oracle/product/middleware/oracle_common/common/bin
./config.sh
```
3. Follow the table below to guide you through the configuration screens:

Step	Window	Choices or Values
1.	Create Domain	Select <b>Update an existing domain</b> <b>Domain Location:</b> /u01/app/oracle/admin/domains/oam_domain
2.	Templates	<b>Oracle HTTP Server (Collocated)</b>
3.	Database Configuration Type	<b>Get RCU Configuration</b> Click <b>Next</b>
4.	Component Datasources	Click <b>Next</b>
5.	JDBC Component Schema Test	Click <b>Next</b>
6.	Advanced Configuration	<b>System Components</b>
7.	System Components	Click <b>Add</b> <b>System Component:</b> ohs1
8.	OHS Server	Click <b>Next</b>
9.	Machine	Click <b>Next</b>
10.	Assign System Components to Machines	Select <b>ohs1</b> and <b>oam_machine</b> and click the arrow to move ohs1 under oam_machine
11.	Configuration Summary	Click <b>Update</b>
12.	Configuration Progress	Click <b>Next</b>
13.	End of Configuration	Click <b>Finish</b>

### 2.7.3 Start the Servers

1. Launch a terminal window and run the following command to start the WebLogic AdminServer. Enter `weblogic/Welcome1` as the username and password when prompted:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
./startWebLogic.sh
```

2. In another terminal window run the following command to stop and start Node Manager:

```
nohup ./startNodeManager.sh &
```

3. In the same terminal window run the following command to start Oracle HTTP Server. Enter `Welcome1` as the password when prompted:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
./startComponent.sh ohs1
```

4. Following to show after OHS successfully started-

```
Successfully Connected to Node Manager.
Starting server ohs1 ...
Successfully started server ohs1 ...
Successfully disconnected from Node Manager.
Exiting WebLogic Scripting Tool.
Done
```

5. Launch a browser and check the OHS is accessible by accessing the URL <http://oam.example.com:7777>

## 2.8 Creating OAM 12c Webgate

Follow the below steps to create a Webgate:

1. Launch a terminal window as oracle and enter the following command:

```
cd /u01/app/oracle/product/middleware/webgate/ohs/tools/deployWebGate
./deployWebGateInstance.sh -w \
/u01/app/oracle/admin/domains/oam_domain/config/fmwconfig/components/OHS/instance/ohs1 \
-oh /u01/app/oracle/product/middleware/
```

2. Check that a webgate directory and subdirectories were created:

```
ls -lart
/u01/app/oracle/admin/domains/oam_domain/config/fmwconfig/components/OHS/instance/ohs1/web
gate/
total 16
drwxr-x--- 7 oracle oinstall 4096 Aug 16 07:12 ..
drwxr-xr-x 4 oracle oinstall 4096 Aug 16 07:12 .
drwxr-xr-x 3 oracle oinstall 4096 Aug 16 07:12 tools
```

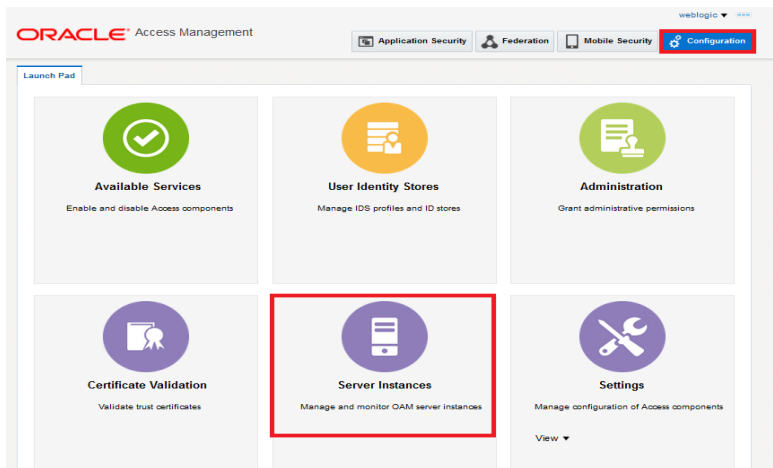


```
drwxr-xr-x 3 oracle oinstall 4096 Aug 16 07:12 config
```

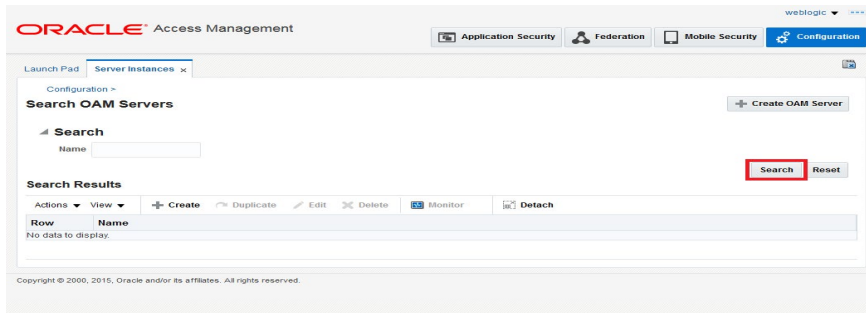
3. Run the following command:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/u01/app/oracle/product/middleware/lib
cd /u01/app/oracle/product/middleware/webgate/ohs/tools/setup/InstallTools
./EditHttpConf -w
/u01/app/oracle/admin/domains/oam_domain/config/fmwconfig/components/OHS/instance/ohs1 \
-oh /u01/app/oracle/product/middleware/
```

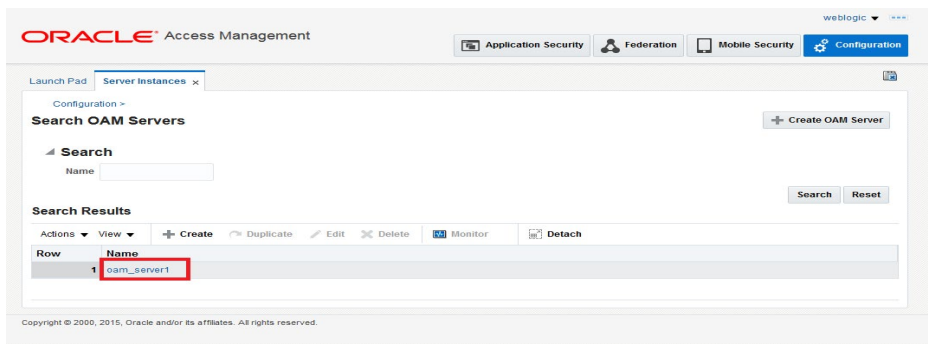
4. Register the WebGate with OAM by click on 'Server Instances' under Configuration.



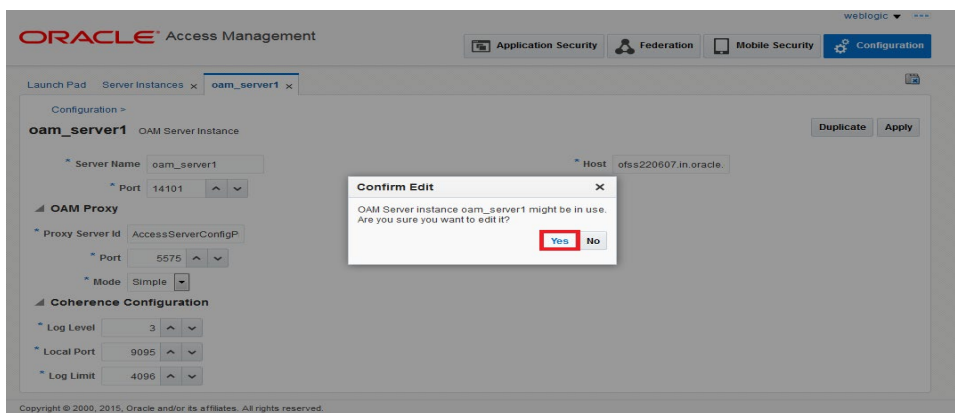
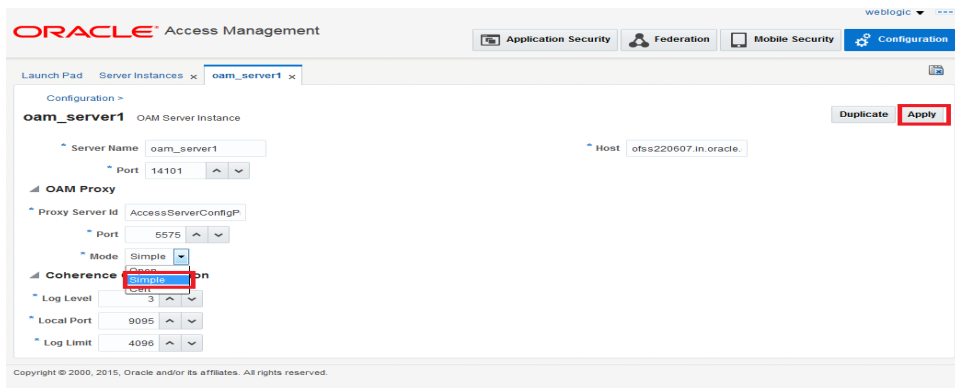
5. Click on 'Search'.

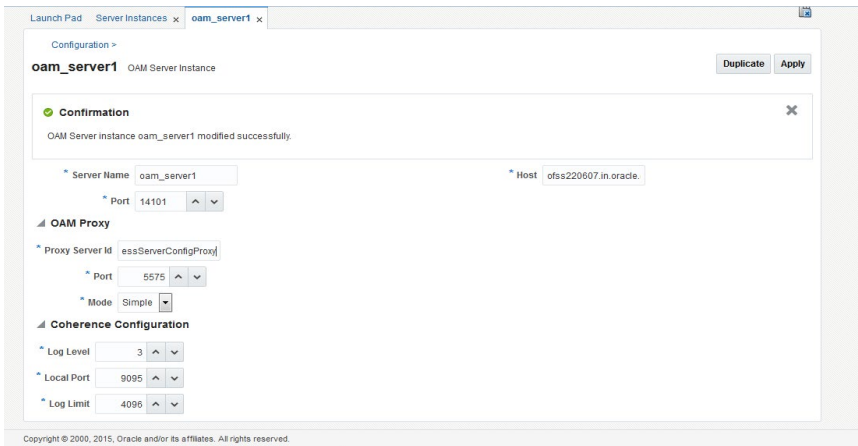


6. Edit oam\_server1.

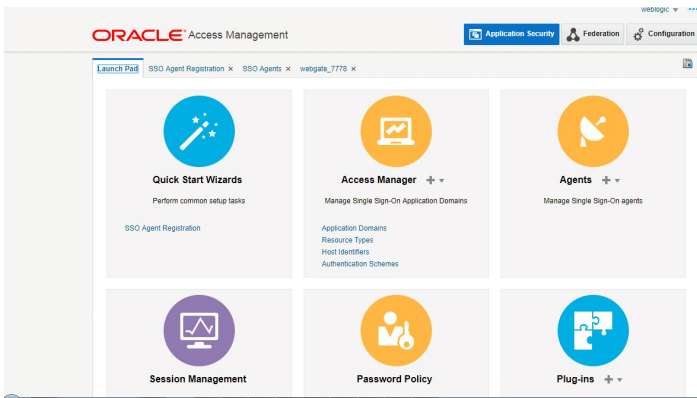


7. Modify the Mode from Open to Simple and click on 'Apply'.

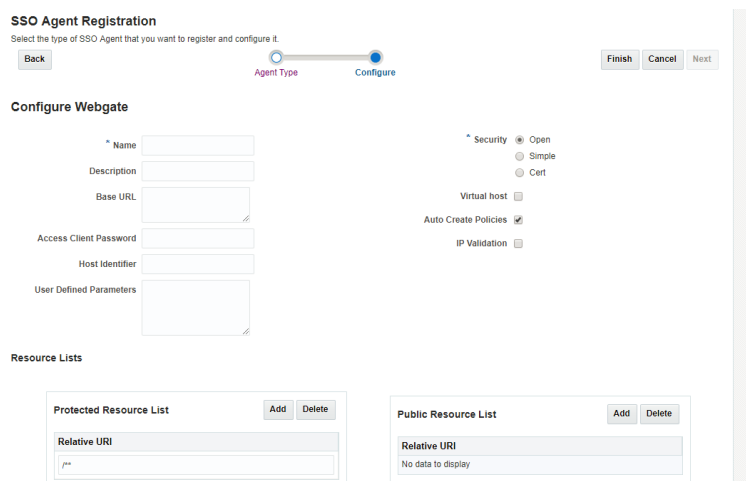




8. Click on SSO Agent Registration



9. Fill the value and click Finish—



Select **Agent Type**: Webgate and click **Next**.

On the **Configure WebGate** page enter details as follows, and then click **Finish**:

Name : Custom Webgate Name

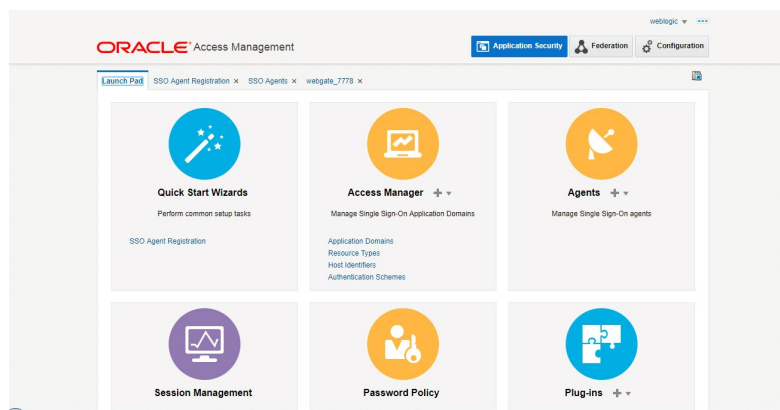
Base URL : The host and port of the computer on which the Web server for the Webgate is installed. For example, http://example\_host:port or https://example\_host:port. The port number is optional.

Security : Simple

Protected Resource List : for FCUBS : /FCJNeoWeb  
For FCIS : /FCISNeoWeb

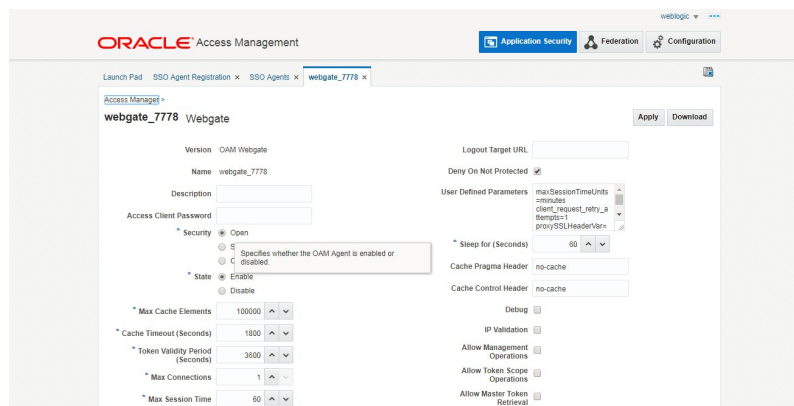
User Defined Parameters : filterOAMAuthnCookie=false

10. Click “Agent” in Application Security



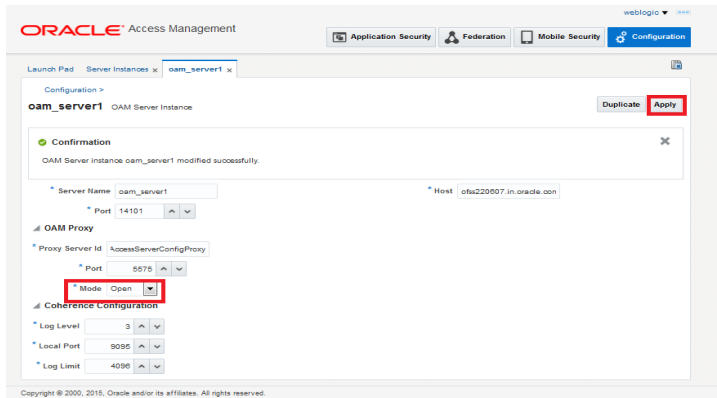
11. Click Search and open the Webgate Agent created in the above step.

Change the value in User Definer Parameters to below  
proxySSLHeaderVar=nonssl



12. Click on ‘Apply’.

13. Change the value of Mode back to Open in oam\_server1 on Server Instance and click ‘Apply’.



14. Click **Download** and save the webgate\_7777.zip to /stage.

15. Copy the WebGate zip in the below directory and unzip-

/domains/OAM\_domain/config/fmwconfig/components/OHS/ohs1/webgate/config

16. Modify the value in httpd.conf present in below location:

/domains/OAM\_domain/config/fmwconfig/components/OHS/ohs1/

Add the below text at the end of the file

include "webgate.conf"

17. Restart the Servers

Launch a terminal window as oracle and run the commands below to stop all the servers.

Enter weblogic and Welcome1 for username and password if prompted:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
```

```
./stopComponent.sh ohs1
```

```
./stopNodeManager.sh
```

```
./stopManagedWebLogic.sh oam_policy_mgr1
```

```
./stopManagedWebLogic.sh oam_server1
```

```
./stopWebLogic.sh
```

Run the following commands launching new terminal windows as oracle to start the servers:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
```

```
./startWebLogic.sh
```

```
./startManagedWebLogic.sh oam_server1
```

```
./startManagedWebLogic.sh oam_policy_mgr1
```

```
./startNodeManager.sh
```

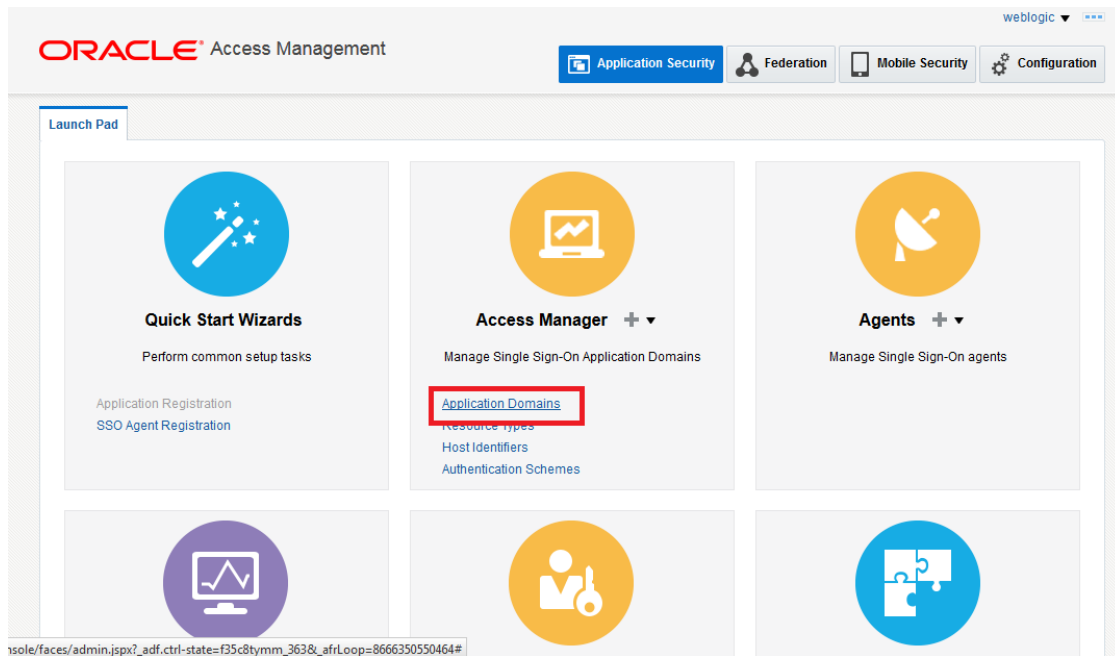
```
./startComponent.sh ohs1
```

## 2.8.1 Post OAM Webgate 12c Creation

Follow the below steps to configure the webgate created.

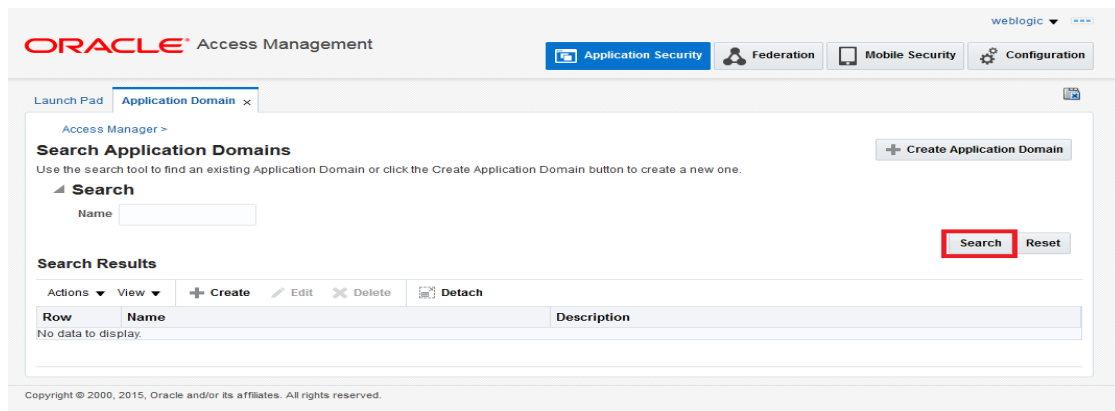
## 2.8.1.1 Application Domains Changes

18. Click on 'Application Domains' in Access Manager under Application Security

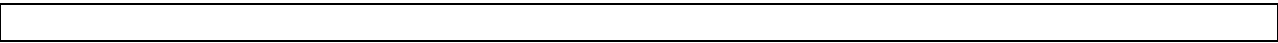


The screenshot shows the Oracle Access Management interface. At the top, there is a navigation bar with 'Application Security', 'Federation', 'Mobile Security', and 'Configuration' tabs. Below this is a 'Launch Pad' section with six tiles. The 'Access Manager' tile is highlighted, and the 'Application Domains' link within it is circled in red. The URL at the bottom of the page is: `ts/sole/faces/admin.jspx?_adf.ctrl-state=f35c8tyymm_363&_afrcLoop=8666350550464#`

19. Click on 'Search' to find the Webgate.



The screenshot shows the 'Search Application Domains' page in Oracle Access Management. The page has a search bar with a 'Search' button highlighted in red. Below the search bar, there is a 'Search Results' section with a table header: 'Row', 'Name', and 'Description'. The table is currently empty, displaying 'No data to display.' The URL at the bottom of the page is: `Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.`



ORACLE Access Management weblogic ▾

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain x

Access Manager >

### Search Application Domains

[+ Create Application Domain](#)

Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one.

**Search**

Name

[Search](#) [Reset](#)

**Search Results**

Actions ▾ View ▾ [+ Create](#) [Edit](#) [Delete](#) [Detach](#)

Row	Name	Description
1	FlexcubeWebgate	Application Domain created through Remote Registration
2	Fusion Apps Integration	Policy objects enabling integration with Oracle Fusion Applications
3	IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications

20. Click on 'Authentication Polices'.

ORACLE Access Management weblogic ▾

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain x FlexcubeWebgate x

Access Manager >

### FlexcubeWebgate Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

[Summary](#) [Resources](#) [Authentication Policies](#) [Authorization Policies](#) [Token Issuance Policies](#) [Administration](#)

[Apply](#)

\* Name

Description

\* Session Idle Timeout (minutes)

Allow OAuth Token

Allow Session Impersonation

Enable Policy Ordering

21. Click on 'Protected Resource Policy'.

ORACLE Access Management

weblogic

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain x FlexcubeWebgate x

Access Manager >

**FlexcubeWebgate** Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Summary Resources **Authentication Policies** Authorization Policies Token Issuance Policies Administration

Select an existing Authentication Policy from the list or click the Create Authentication Policy button to create a new one.

Actions View + Create Duplicate Edit Delete Detach

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	Protected Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

22. Choose the Authentication Scheme created earlier in 'Creating Authentication Scheme'.

Launch Pad Application Domain x FlexcubeWebgate x FlexcubeWebgate : Protect... x

Access Manager >

**Protected Resource Policy** Authentication Policy Duplicate Apply

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

Name Protected Resource Policy Success URL

Description Policy set during domain creation. Add resources to this policy to protect them. Failure URL

Select the challenge mechanism required to authenticate the user.

Authentication Scheme

- LDAPScheme
- AdaptiveAuthenticationScheme
- AnonymousScheme
- BasicFAScheme
- BasicScheme
- BasicSessionlessScheme
- ESSOProvAuthnScheme
- FAAdminLocalScheme
- FAAuthScheme
- FederationMTScheme
- FlexcubeBasicOAMScheme
- FlexcubeFormOAMScheme
- FlexcubeKBAOAMScheme
- WebAccessScheme
- LDAPNoPasswordValidationScheme
- LDAPScheme
- OAMAdvanced
- OAMBasic
- OAM10gScheme
- OAMAdminConsoleScheme

Resources

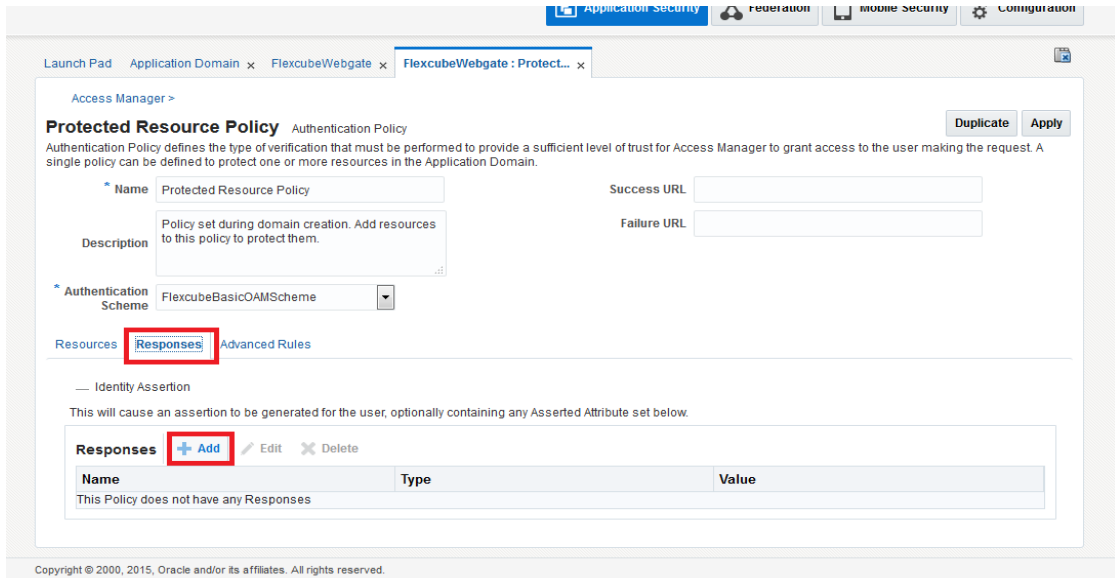
Resource Type

Query String

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

23. Click 'Responses' tab and click + Add button to Add 'DN' variable to the Response Header.





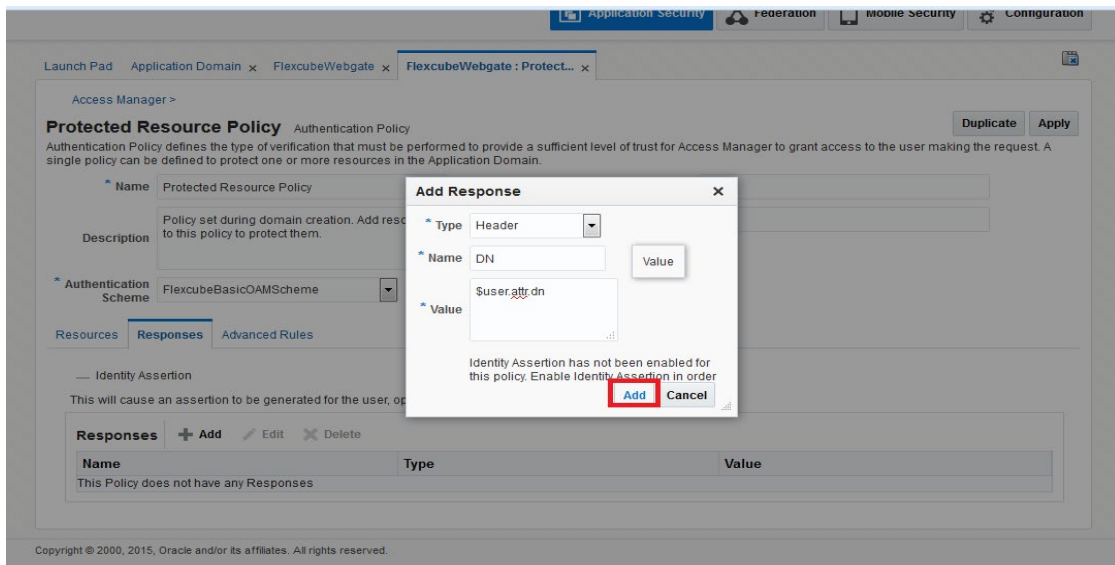
24. Enter the following values in the Add Response Window:

Type : Header

Name : DN

Value : \$user.attr.dn

Click on Add button



25. Click on Apply to Save the Changes

Launch Pad Application Domain x FlexcubeWebgate x FlexcubeWebgate : Protect... x

Access Manager >

**Protected Resource Policy** Authentication Policy Duplicate **Apply**

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

**Confirmation** ✕

Authentication Policy, Protected Resource Policy, modified successfully

\* Name Protected Resource Policy Success URL

Description Policy set during domain creation. Add resources to this policy to protect them. Failure URL

\* Authentication Scheme FlexcubeBasicOAMScheme

Resources Responses Advanced Rules

Identity Assertion

This will cause an assertion to be generated for the user, optionally containing any Asserted Attribute set below.

Responses + Add / Edit ✕ Delete

Name	Type	Value
DN	Header	Suser.attr.dn

26. Click on 'Authorization Policies' and then click on 'Protected Resource Policy'.

ORACLE Access Management weblogic

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain x FlexcubeWebgate x

Access Manager >

**FlexcubeWebgate** Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Summary Resources Authentication Policies **Authorization Policies** Token Issuance Policies Administration

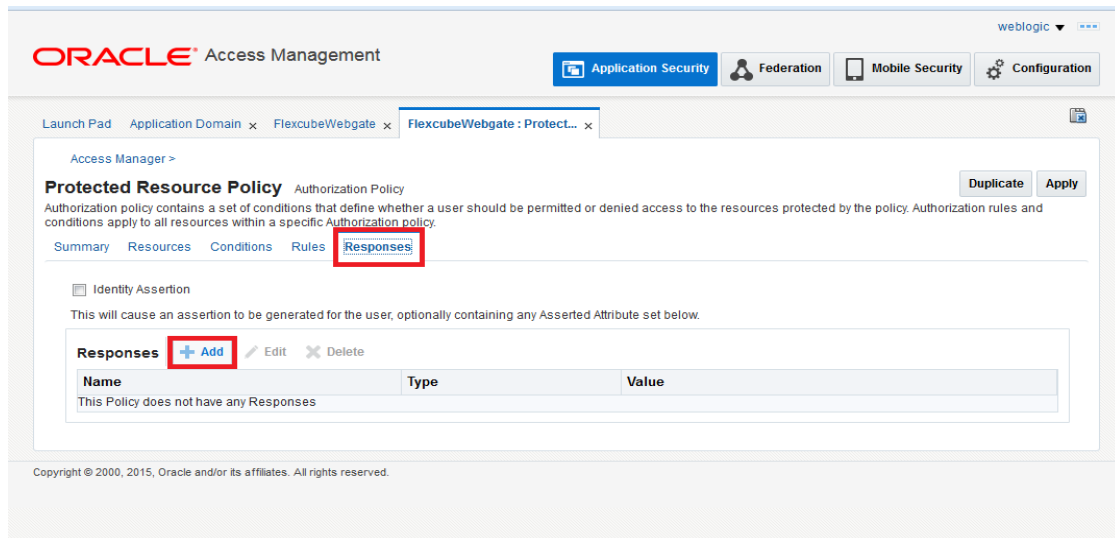
Select an existing Authorization Policy from the list or click the Create Authorization Policy button to create a new one.

Actions View + Create ✕ Duplicate / Edit ✕ Delete Detach

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	<b>Protected Resource Policy</b>	Policy set during domain creation. Add resources to this policy to protect them.

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

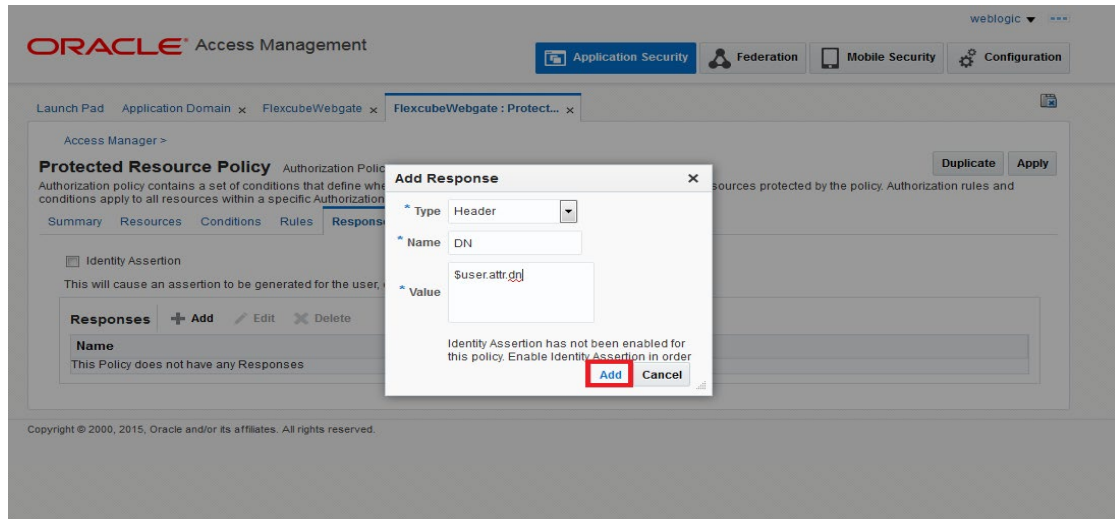
27. Click on 'Response' tab and click on + Add button to Add 'DN' variable to the Response Header.



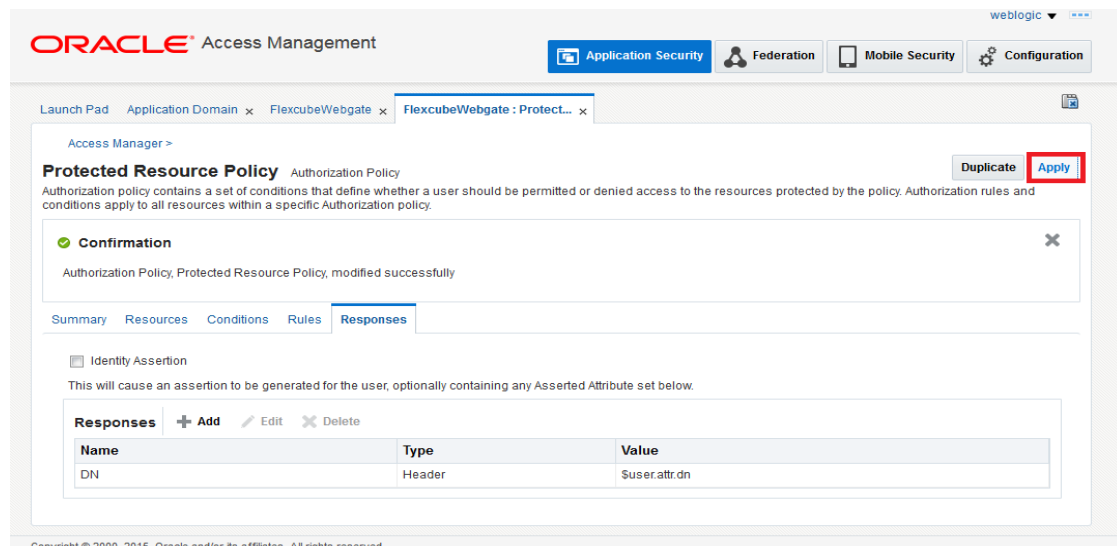
28. Enter the following values in the Add Response Window :

Type : Header  
 Name : DN  
 Value : \$user.attr.dn

Click on Add button



29. Click on 'Apply' to Save the changes.



### 2.8.1.2 Copying Generated Files and Artifacts to the Oracle HTTP Server WebGate Instance

Perform the following steps to copy the artifacts generated while creating the Oracle 12c Webgate to the Webgate installation directory:

- Navigate to <DOMAIN\_HOME>/output/\$WebgateAgentName
- Select the following files
  - ObAccessClient.xml
  - password.xml
- cwallet.sso
  - cwallet.sso.lck

Copy the files to <ORACLE\_MIDDLEWARE>/<ORACLE\_WIBTIER\_HOME> /instances/instance1/config/OHS/ohs1/webgate/config/

/Middleware/OAM\_Home/user\_projects/domains/OAM\_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config

- Select the remaining 2 files
  - aaa\_key.pem
  - aaa\_cert.pem
- Copy the files to <ORACLE\_MIDDLEWARE>/<ORACLE\_WIBTIER\_HOME> /instances/instance1/ config/OHS/ohs1/webgate/config/simple

### **2.8.1.3 Configuring mod\_wl\_ohs for Oracle HTTP server Routing**

To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server, add the directive shown below to the mod\_wl\_ohs.conf file available in <ORACLE\_MIDDLEWARE> /<ORACLE\_WEBTIER\_HOME>/instances/instance1/config/OHS/ohs1.

```
<Location /FCJNeoWeb>
```

```
    SetHandler weblogic-handler
```

```
    WebLogicHost ofss00002.in.oracle.com
```

```
    WeblogicPort 7002
```

```
    WLProxySSL OFF
```

```
    SecureProxy OFF
```

```
    WLSSLWallet
```

```
    "<ORACLE_MIDDLEWARE>/<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1/keystores/default"
```

```
</Location>
```

**Note:** In the above example, ofss00002.in.oracle.com is the server name where the Flexcube Application is deployed, 7002 is the SSL port and FCJNeoWeb is the context root of the FLEXCUBE application

### **2.8.1.4 Restart the Servers**

1. Launch a terminal window as oracle and run the commands below to stop all the servers. Enter weblogic and Welcome1 for username and password if prompted:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
```

```
./stopComponent.sh ohs1
```

```
./stopNodeManager.sh
```

```
./stopManagedWebLogic.sh oam_policy_mgr1
```

```
./stopManagedWebLogic.sh oam_server1
```

```
./stopWebLogic.sh
```

2. Run the following commands launching new terminal windows as oracle to start the servers:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
```

```
./startWebLogic.sh
```

```
./startManagedWebLogic.sh oam_server1
```

```
./startManagedWebLogic.sh oam_policy_mgr1
```

```
./startNodeManager.sh
```

```
./startComponent.sh ohs1
```

### **2.8.1.5 Testing the FCUBS Application through WebGate**

Close any open existing browsers and launch a new one. Access the OHS  
URL: <http://oam.example.com:7777/FCJNeoWeb>



Oracle Access Manager Integration  
[May] [2021]  
Version 14.4.0.4.0

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/](http://www.oracle.com/financialservices/)

Copyright © [2007], [2021], Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

**U.S. GOVERNMENT END USERS:** Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.