Design Specifications
Oracle FLEXCUBE Investor Servicing
Release 12.0.3.0.0
[April] [2014]

Table of Contents

ORACLE

1. Introduction

1.1 Scope of the Document

For the purpose of single sign-on Oracle FLEXCUBE is qualified with Oracle Identity Management 10.1.4.0.1 – specifically using the Access Manager component of Oracle Identity Management. This feature is available in the releases FCIS 8.4.0.0.0.0.0 and onwards of Oracle FLEXCUBE Investor Servicing.

This document is expected to provide an understanding as to how single sign-on can be enabled for a Oracle FLEXCUBE host deployment.

In addition to providing a background to the various components of the deployment, this document:

- provides detailed steps as to how to install the various Oracle FLEXCUBE components required for the purpose of single sign-on
- Configuration in Oracle FLEXCUBE and Oracle Access Manager to enable single sign-on.

1.2 Abbreviations and Terms

Abbreviation	Description
FS	Functional Specification Document
FCIS	Oracle FLEXCUBE Investor Servicing
UT	Unit Trust
BPEL	Business Process Execution Language
Oracle IPM	Oracle Imaging and Process Manager

2. Background and Pre-requisites

2.1 Software Requirement

Oracle Access Manager (10.1.4.0.1) – OAM

- Identity server
- Web Pass
- Policy Manager
- Access Server
- Web Gate

LDAP Directory Server

Please make sure that the LDAP which is been used for Flexcube 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

OC4J App Server (Conditional requirement)

For the purpose of achieving single signon for FCJ if OC4J is used for deployment then it is necessary for this OC4J instance to have an explicit **Oracle HTTP server.** Therefore a standalone OC4J instance will not do.

Microsoft .net Framework

2.2 Background of SSO related components

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 FLEXCUBE with OAM to achieve Single Sign-on feature, Oracle FLEXCUBE'S password policy management, like password syntax and password expiry parameters can no longer be handled by Oracle 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 Oracle FLEXCUBE application users' passwords.

2.2.3 Webgate

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.

Note

This document will not discuss the configuring and setting up of OAM and LDAP directory server. This will be provided by the corresponding Software provider.

3. Installation

3.1 Pre-requisites

The installation steps provided below assume that OracleFLEXCUBE IS has already been deployed and is working (without single sign-on).

The installation 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.

Keep a back up of the httpd.conf when the OID and OAM installation and set up is complete. After the deployment of the servlet is finished and webgate is installed ensure that the block of lines between the following lines is present in httpd.conf.

##***** BEGIN Oracle NetPoint WebPass Specific ****

##***** END Oracle NetPoint Specific ****

#*** BEGIN Oracle Policy Manager Specific ****

#*** END Oracle Policy Manager Specific ****

#*** BEGIN WebGate Specific ****

#*** END WebGate Specific ****

For an example please refer to the Appendix of this document.

4. Configuration

4.1 Configuring Oracle FLEXCUBE for Single-Sign On

4.1.1 Choosing a Webgate

Separate Web server specific installation packages are provided for WebGate components. Be sure to choose the appropriate installation package for your Web server and platform.

In Case of Windows Platform (For oc4j server) - Oracle_Access_Manager10_1_4_0_1_Win32_OHS_WebGate.exe

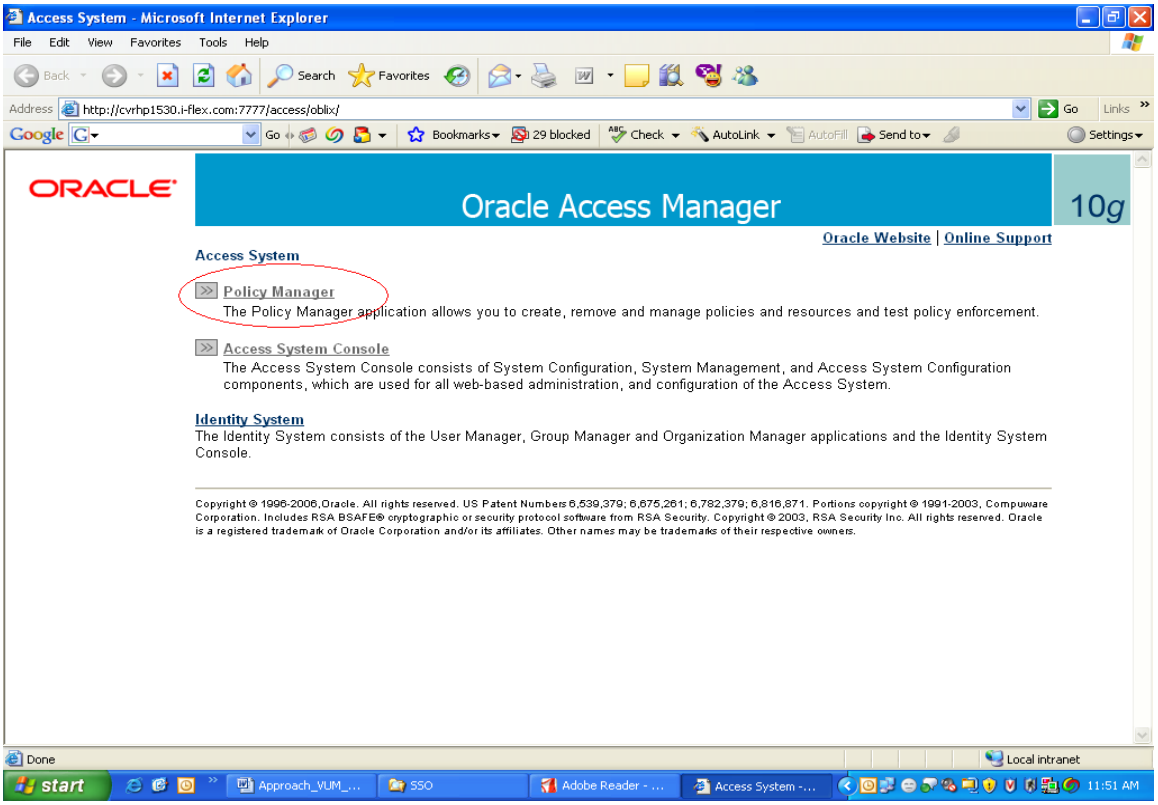
In Case of Linux Platform - Oracle_Access_Manager10_1_4_0_1_ linux_OHS_WebGate.exe

4.1.2 Steps to setup the policy domain and protecting the URL

Launch the Access System Console from your browser by specifying the URL that connects to the Policy Manager. For instance, http://*hostname*:*port*/access/oblix

Where, *hostname* refers to machine that hosts the Web server; *port* refers to the HTTP port number; /access/oblix connect to the Access System Console.

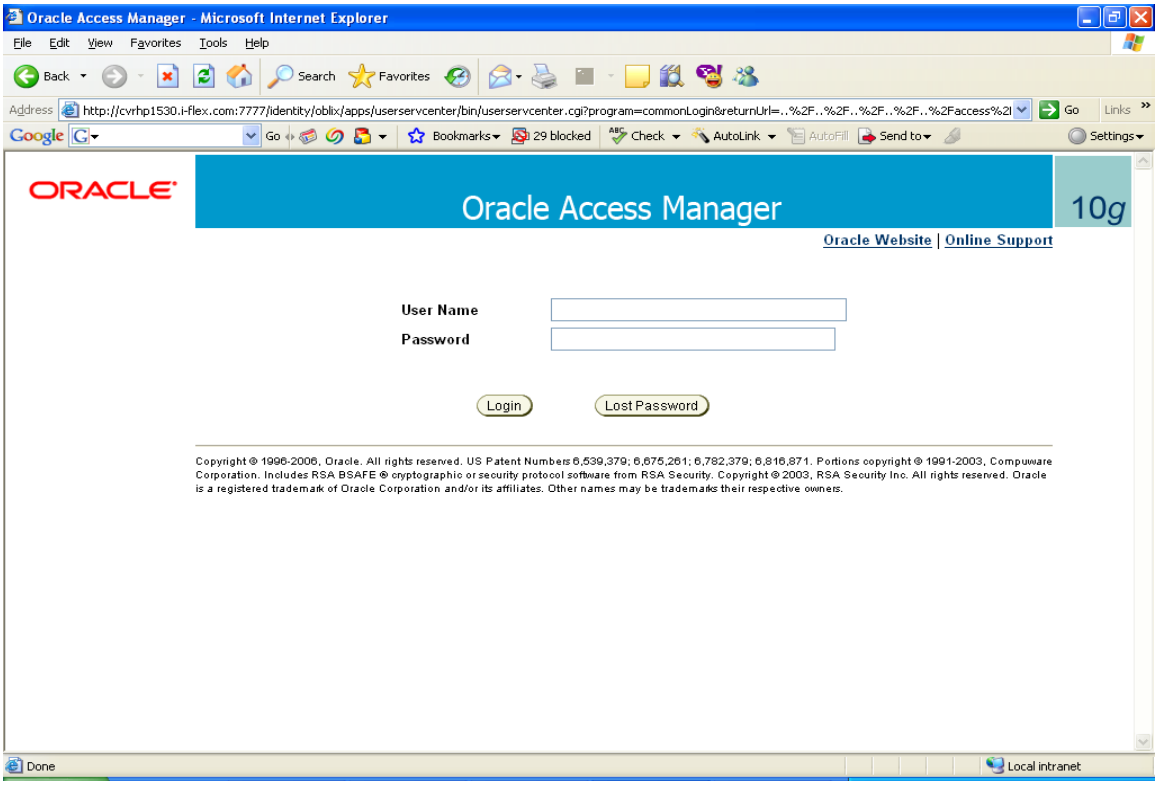
You will see the main Access System page. Figure 1



After that click on the Policy Manager Link in the page. (Marked in RED).You will get the below login page.

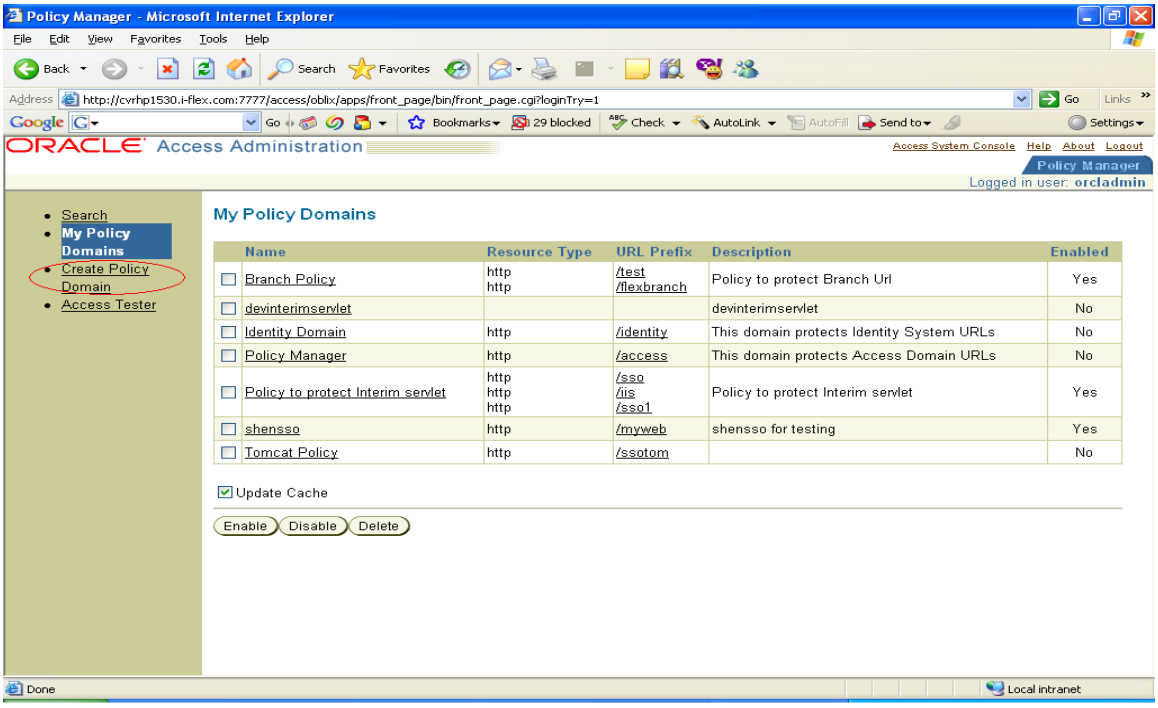
After getting the Login Page, provide admin user name and password to login.

By default admin user id for OID is **orcladmin.** (Use the Password for the admin which is given while installing).

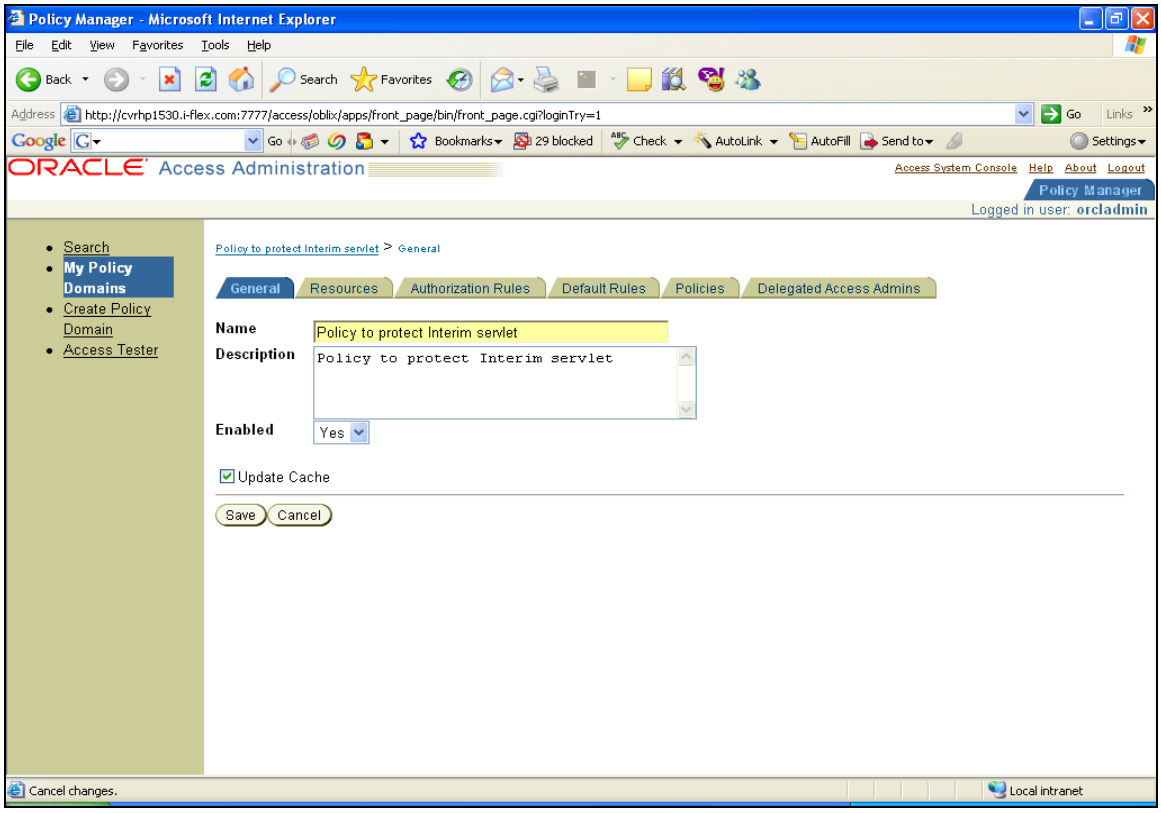


Once admin user has logged in you will get the policy domain page which is shown below. By default you can see two policies (unless other policies have been created for the purpose of other applications in the enterprise).

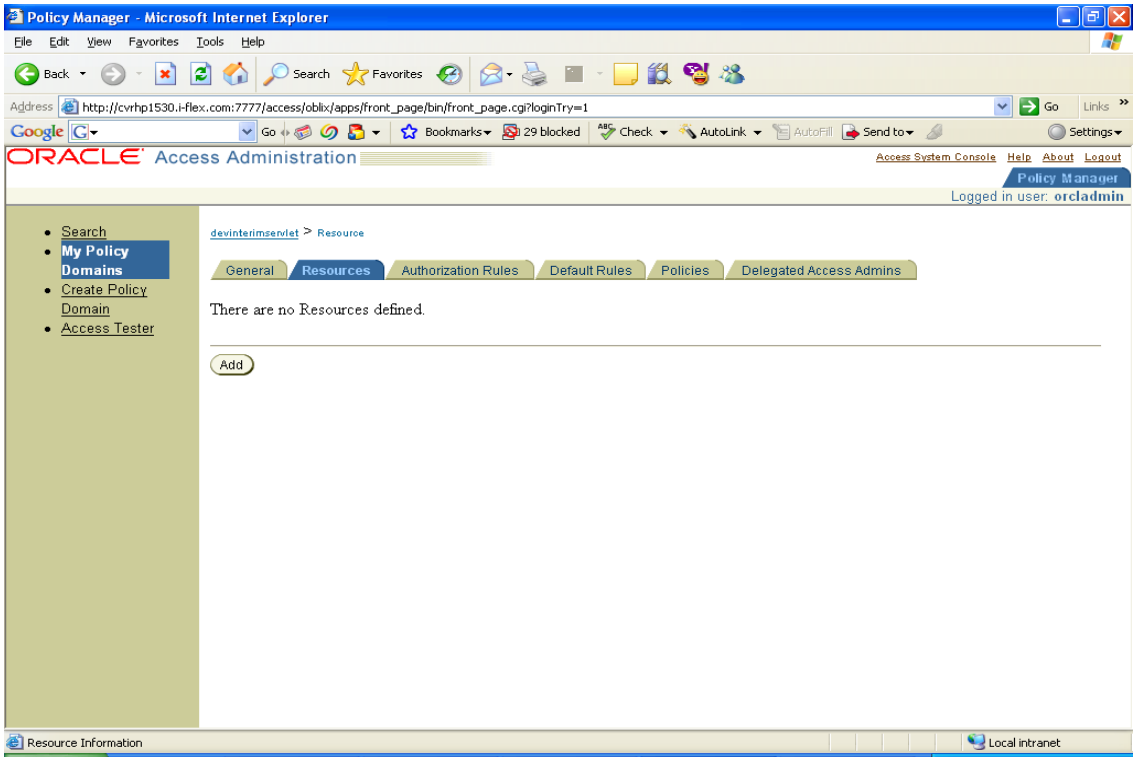
- Identity Domain
- Policy Manager

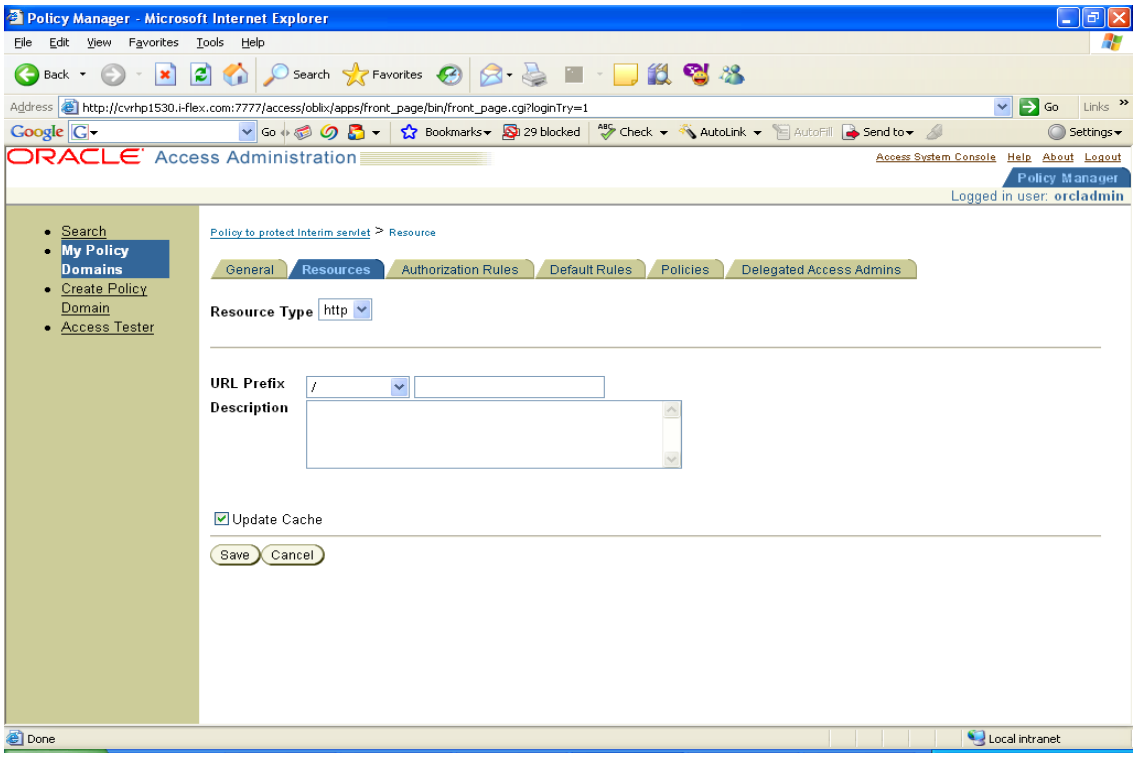


For protecting the resources for SSO a new policy domain has to be created. For creating new policy domain use **Create Policy Domain** option in LSM. (Marked in above Figure). After Selecting Create Policy Domain you will get the below screen (Figure below).

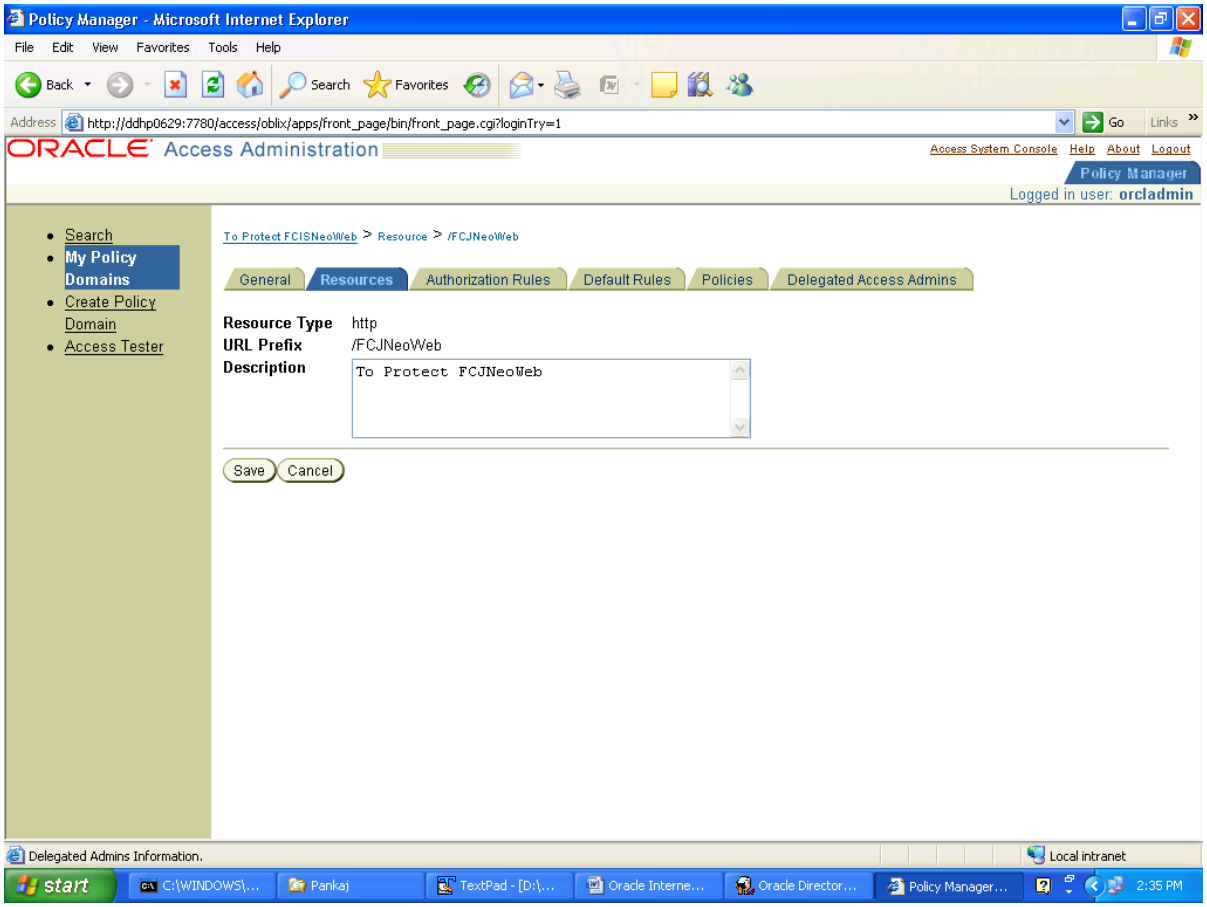


In **general** tab provide the name and description for your Policy and Select the Enabled status to YES and give Save. Then Select the **Resources** tab you will get the below page. While creating new policy no resources will be defined in default, we have to add the resources which need to be protected for SSO. (Figure below).

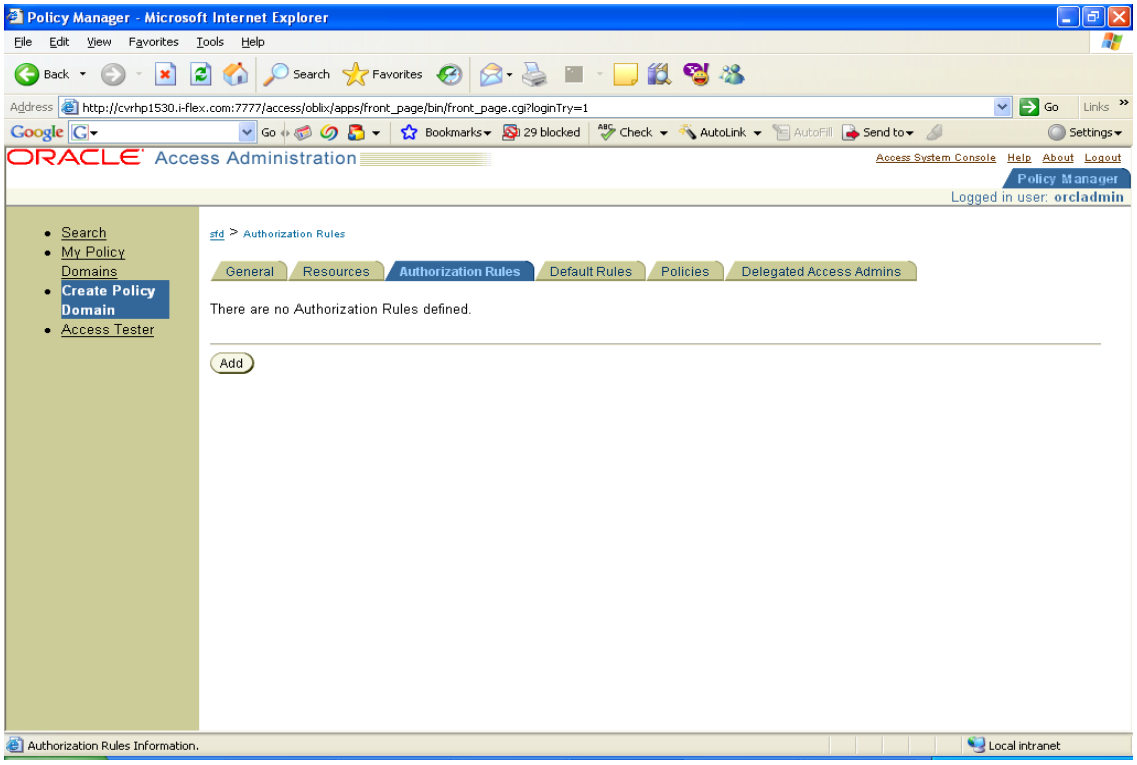

Policy Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://cvrhp1530.i-flex.com:7777/access/oblix/apps/front_page/bin/front_page.cgi?loginTry=1
Go Links
Google Go Bookmarks 29 blocked Check AutoLink AutoFill Send to Settings
ORACLE Access Administration
Access System Console Help About Logout
Policy Manager
Logged in user: orcladmin
Search
My Policy Domains
Create Policy Domain
Access Tester
devinterimservlet > Resource
General Resources Authorization Rules Default Rules Policies Delegated Access Admins
There are no Resources defined.
Add
Resource Information
Local intranet


Policy Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://cvrhp1530.i-flex.com:7777/access/oblix/apps/front_page/bin/front_page.cgi?loginTry=1
Go Links
Google Go Bookmarks 29 blocked Check AutoLink AutoFill Send to Settings
ORACLE Access Administration
Access System Console Help About Logout
Policy Manager
Logged in user: orcladmin
Search
My Policy Domains
Create Policy Domain
Access Tester
Policy to protect Interim servlet > Resource
General Resources Authorization Rules Default Rules Policies Delegated Access Admins
Resource Type http
URL Prefix /
Description
Update Cache
Save Cancel
Done
Local intranet

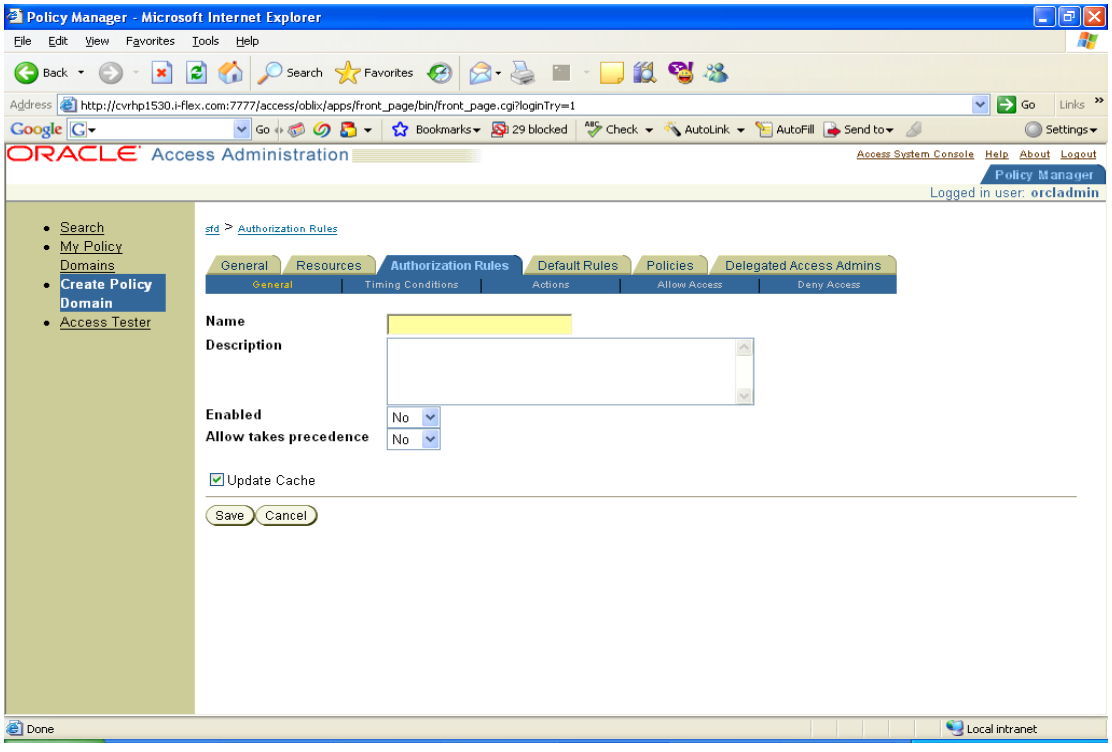
Click on the Add button you will get the above page for creating URL prefix (Figure below). Give **FCJNeoWeb** in URL prefix text box and provide the description. After providing the details the screen will look like below.



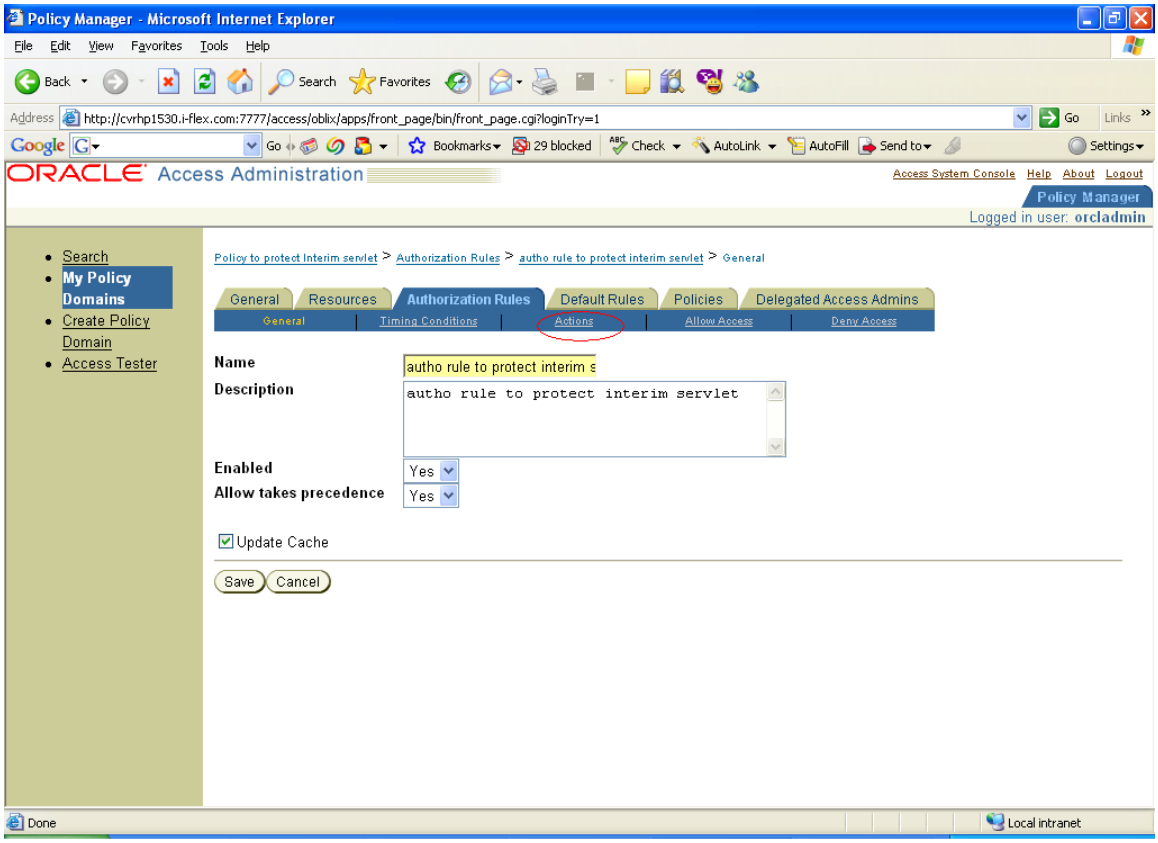
Now press Save. Your URL prefix is created and next move to **Authorization Rules** Tab. You will get the below screen (Figure 8).



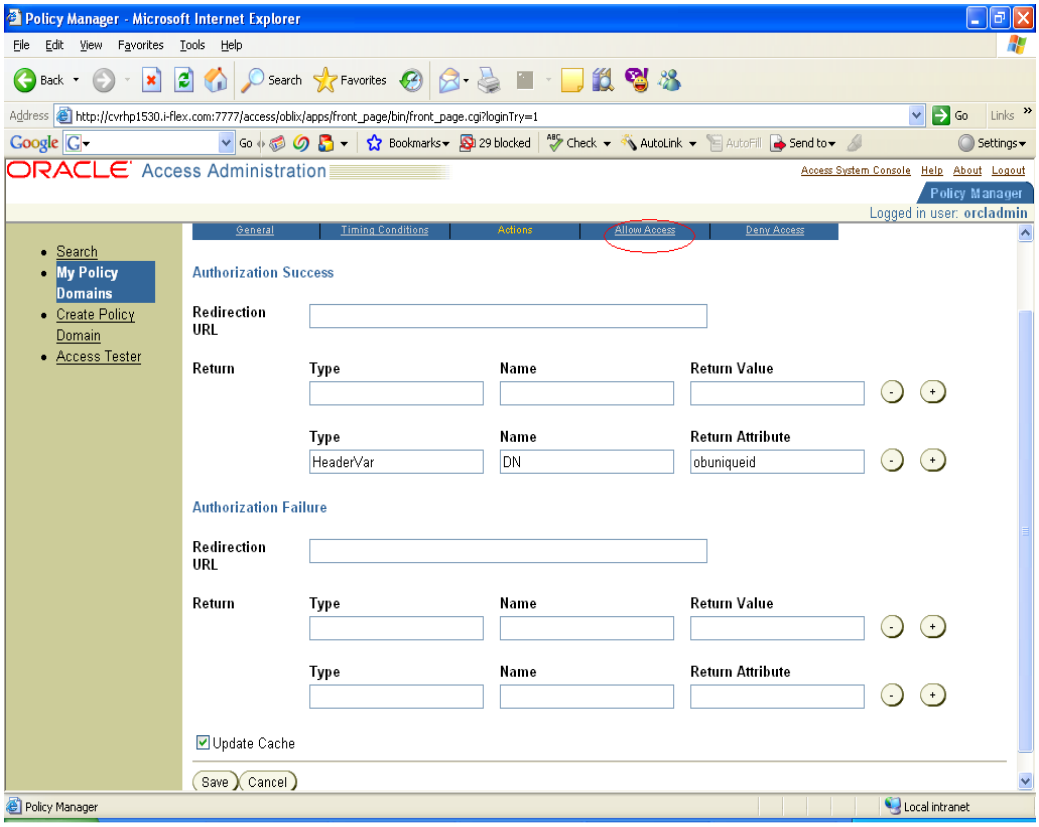
By default no rules is defined. Click on Add button to create new rule.



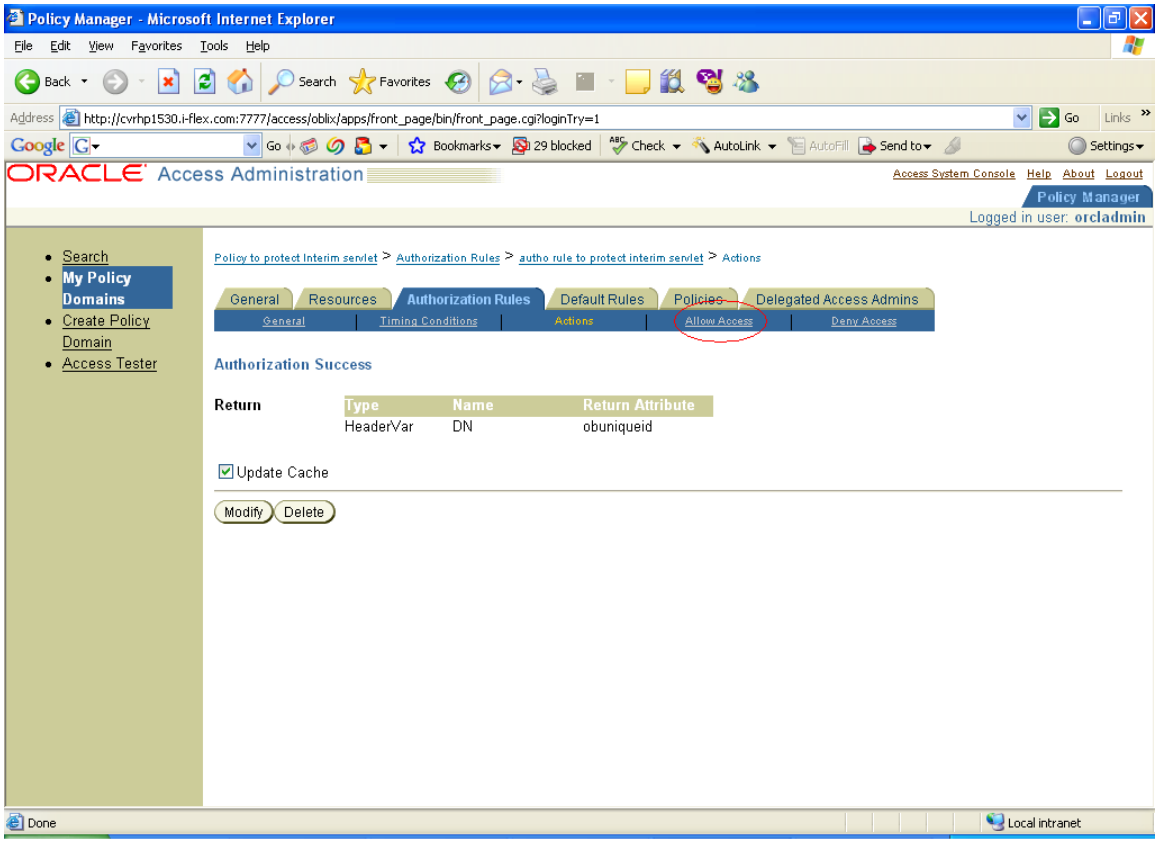
Give name and description for your rule and Select **Yes** for Enabled and Allow precedence drop down box. Then proceed with Clicking on save button.



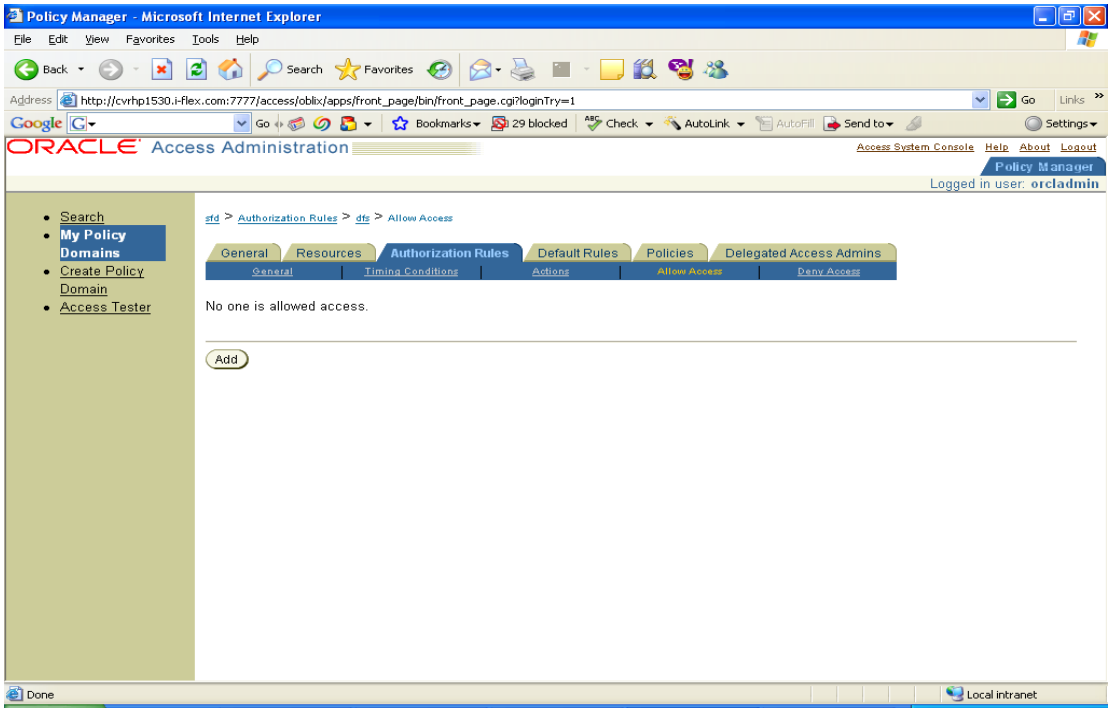
After Save, Next select the **Actions** Sub menu (Marked in above figure). Now you will get the below page for providing details for the action like redirection URL and what need to be returned for success and failure authorization will be there. For SSO we need to give detail for return value in case of authorization Success.



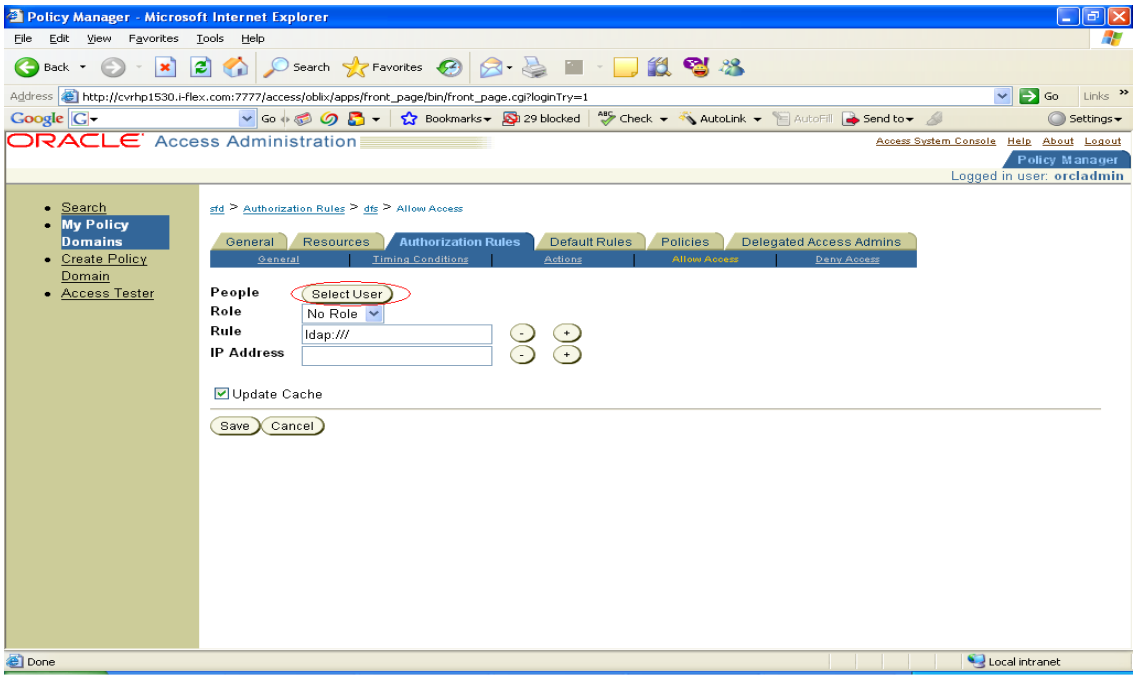
Mention the Type as **HeaderVar** and in Name give as **DN** and return attribute as **obuniqueid.** All the above values are default keywords for getting DN name. Then give save. Now you can see the below page. (Figure 12).



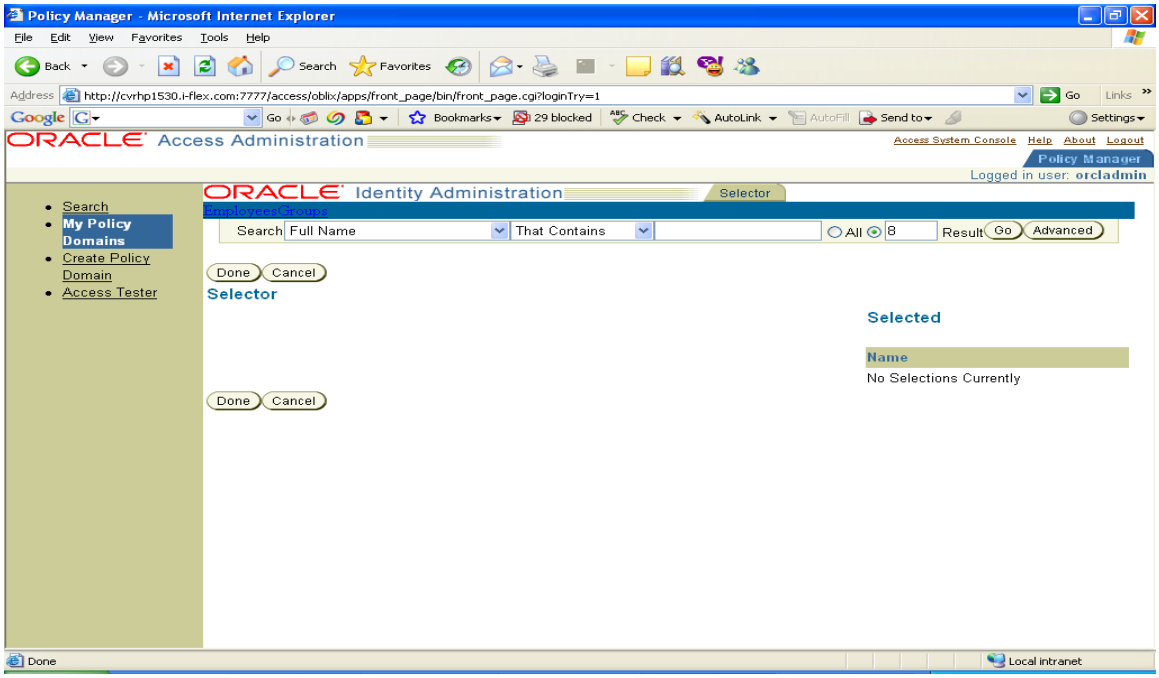
Now we need to specify the users who need access the protected resources. So click on **Allow Access** sub menu (Marked in above Figure). Here we can select the users (already created in OID) for giving access by selecting from the list. By default no users will have access.



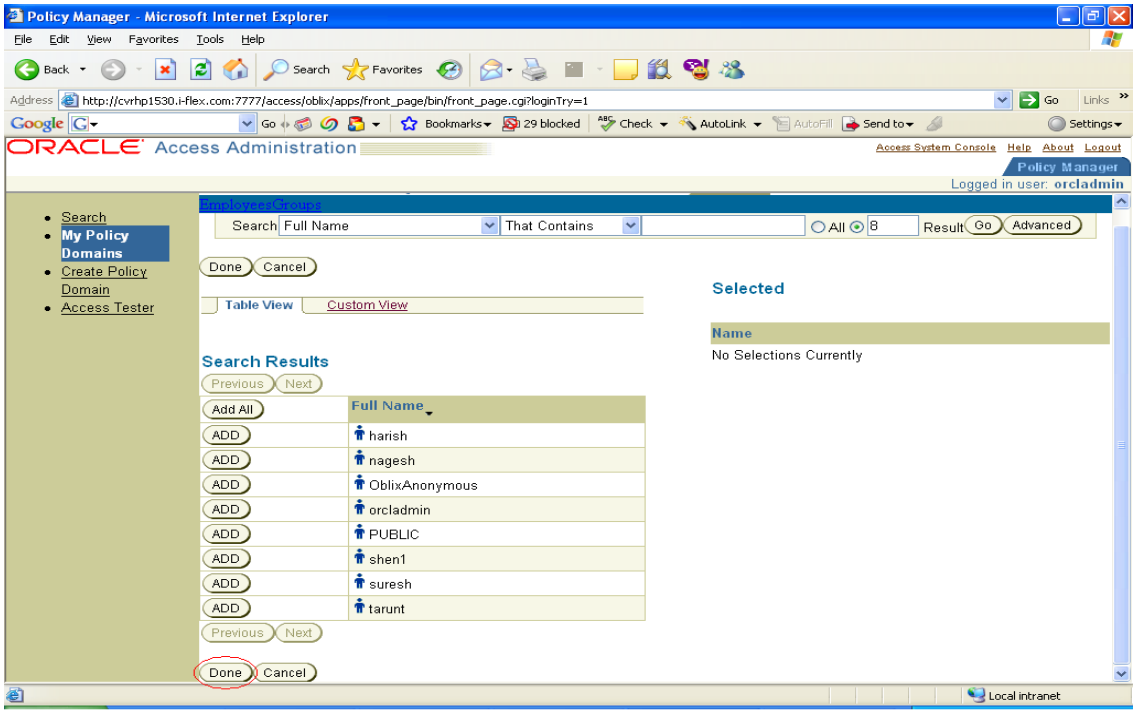
Now press Add button to give access to get the below screen and click Select User button in the page shown below.



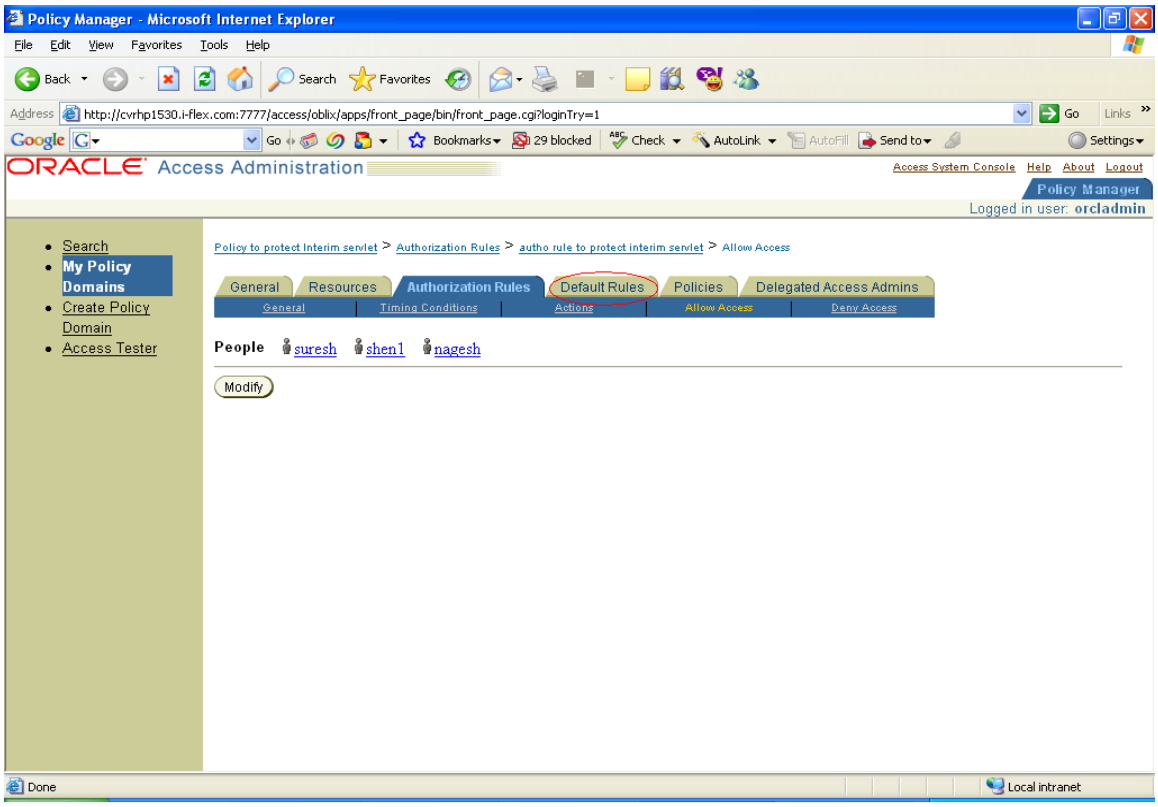
Now you will get a search page for searching the users..



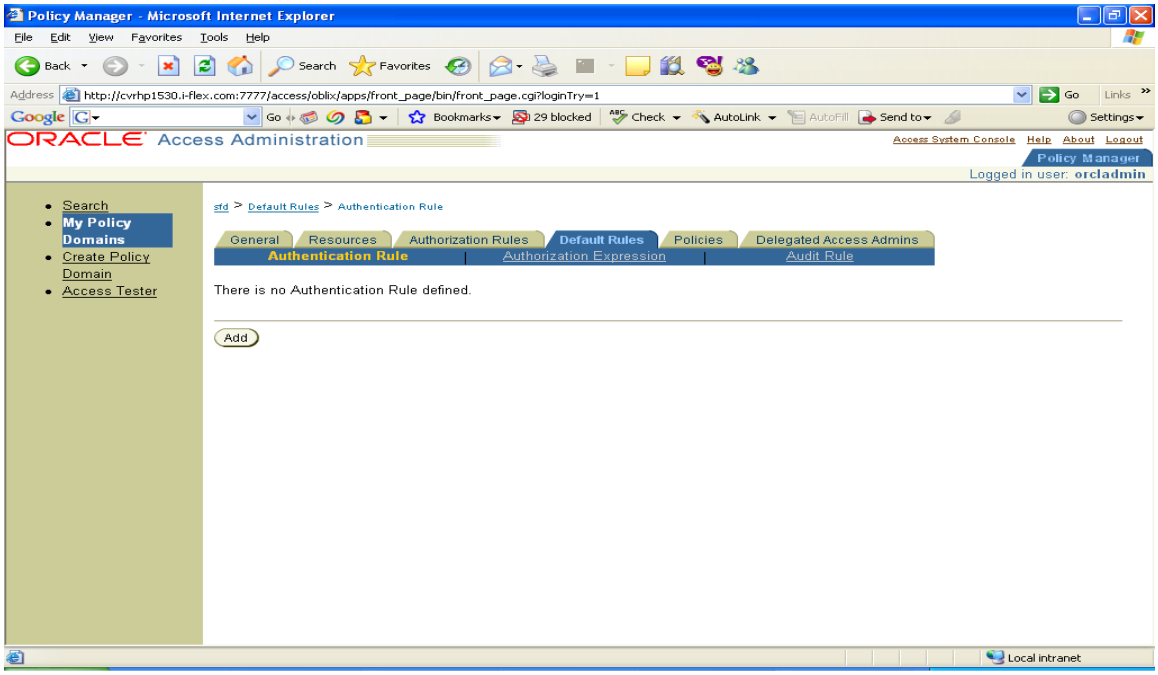
You can search with some key values if you know the users in OID or simply press **Go** button so that all the users in OID will be listed as shown below.



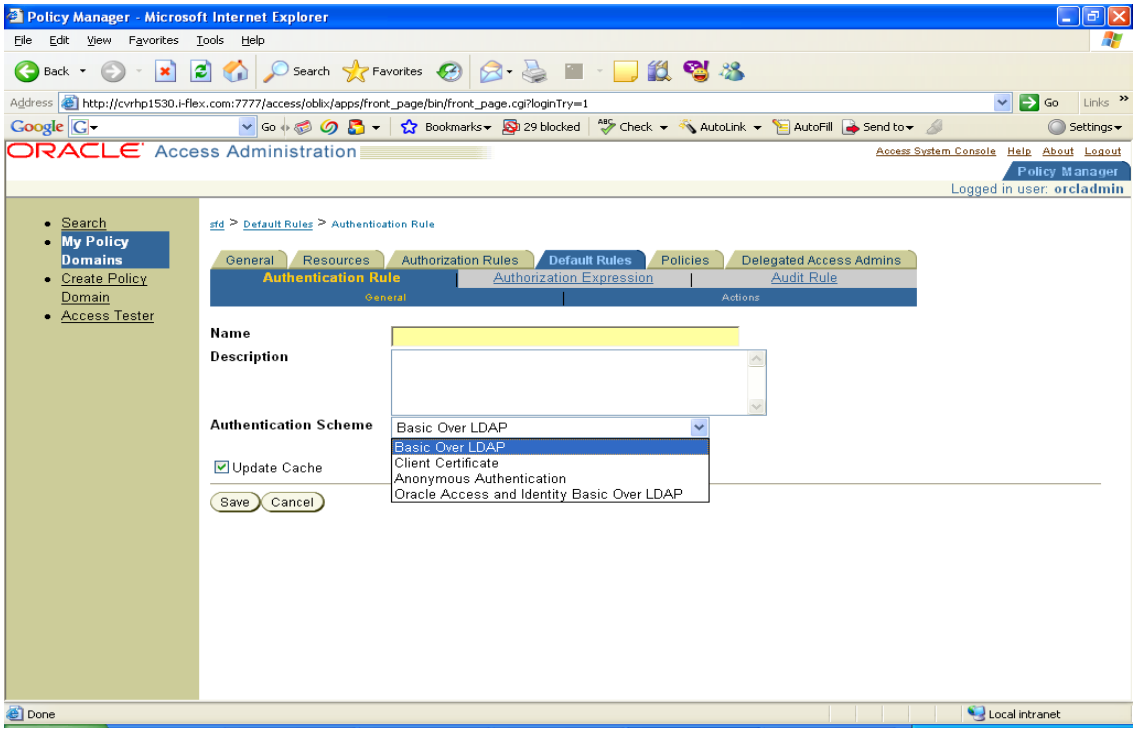
After giving Go, you will get the above screen with the list of users. Now **ADD** the users who need access, then the selected users will appear in the RSS (Right Side Screen) under **Selected** list. After adding the users, give **Done** and will take you to save then press **Save** button to complete the allow access process. At Last you will get the below screen.



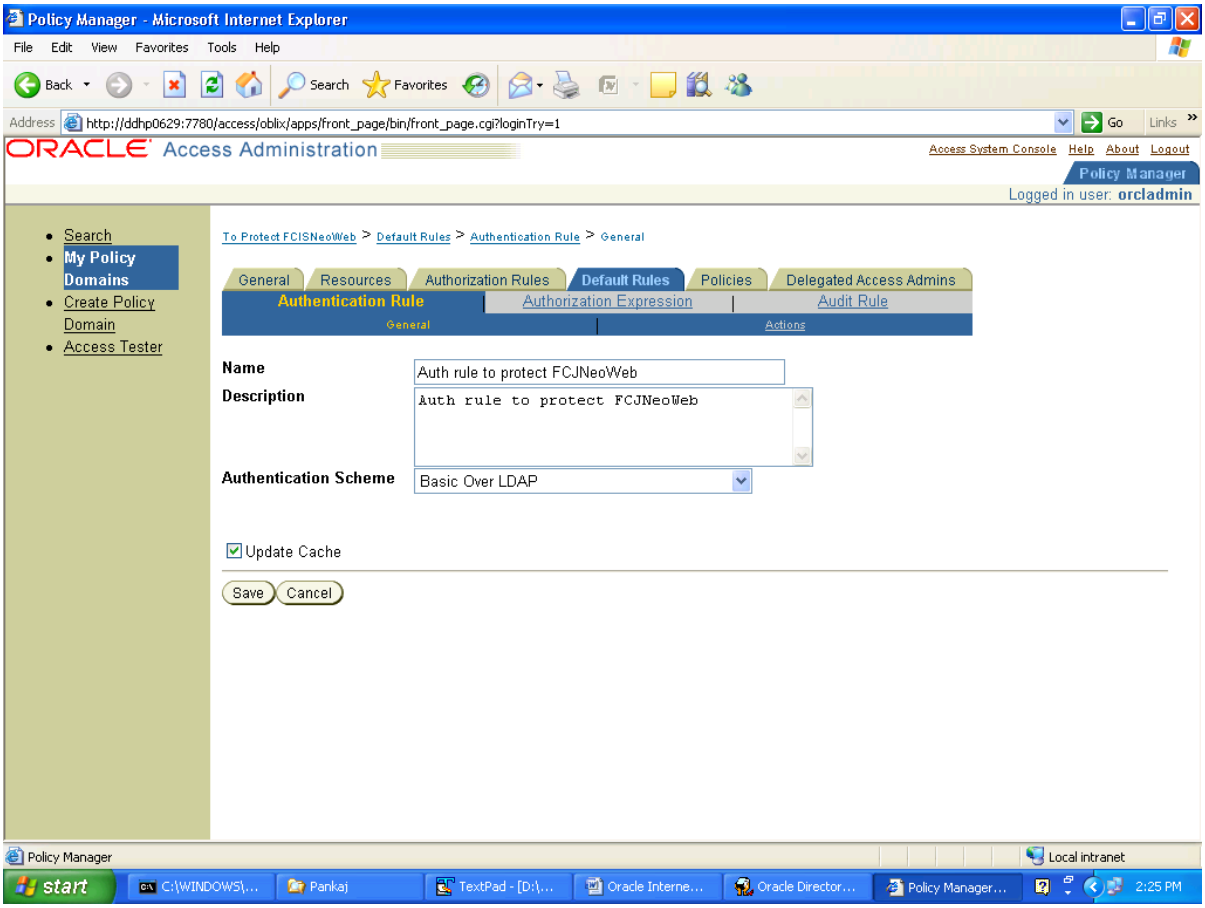
Next Select the **Default Rules** tab option to give authentication rule details. By default no authentication rules is defined.



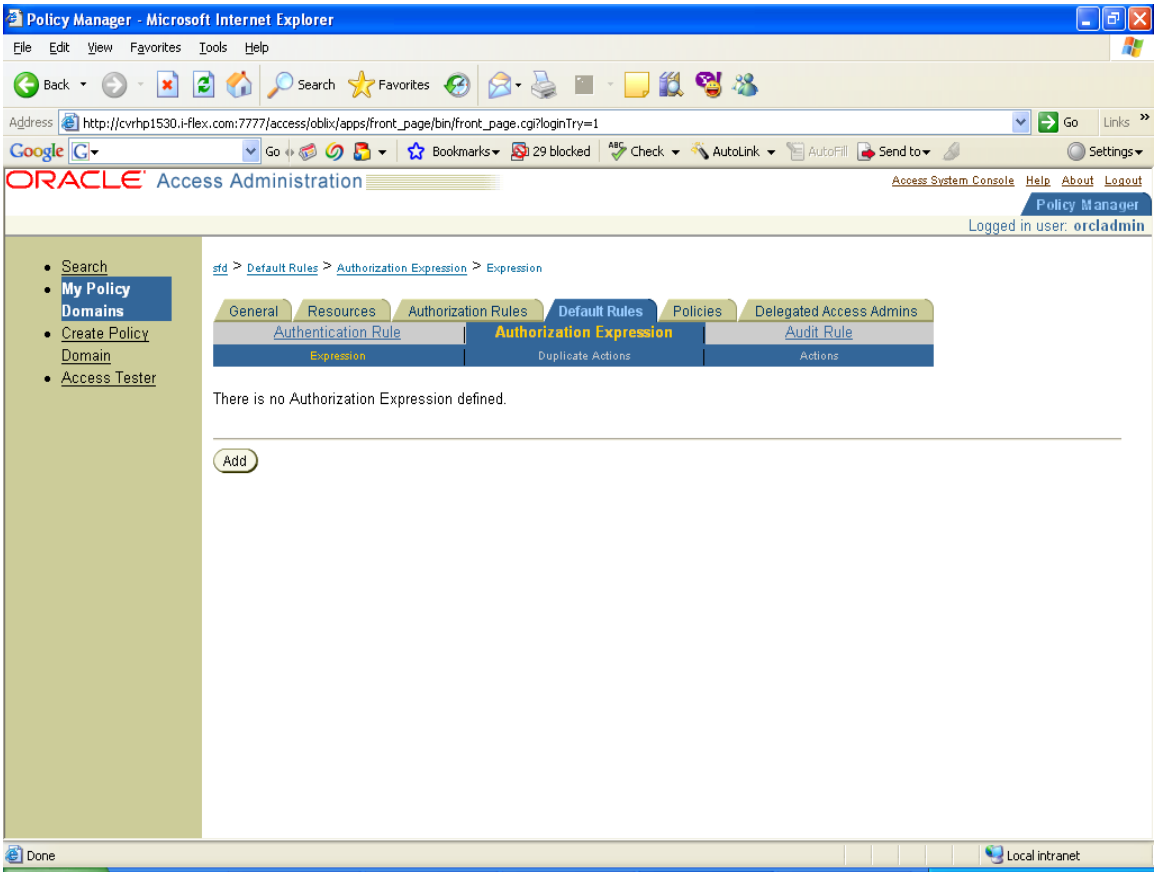
Press the Add button to attach the authentication rule for the policy.



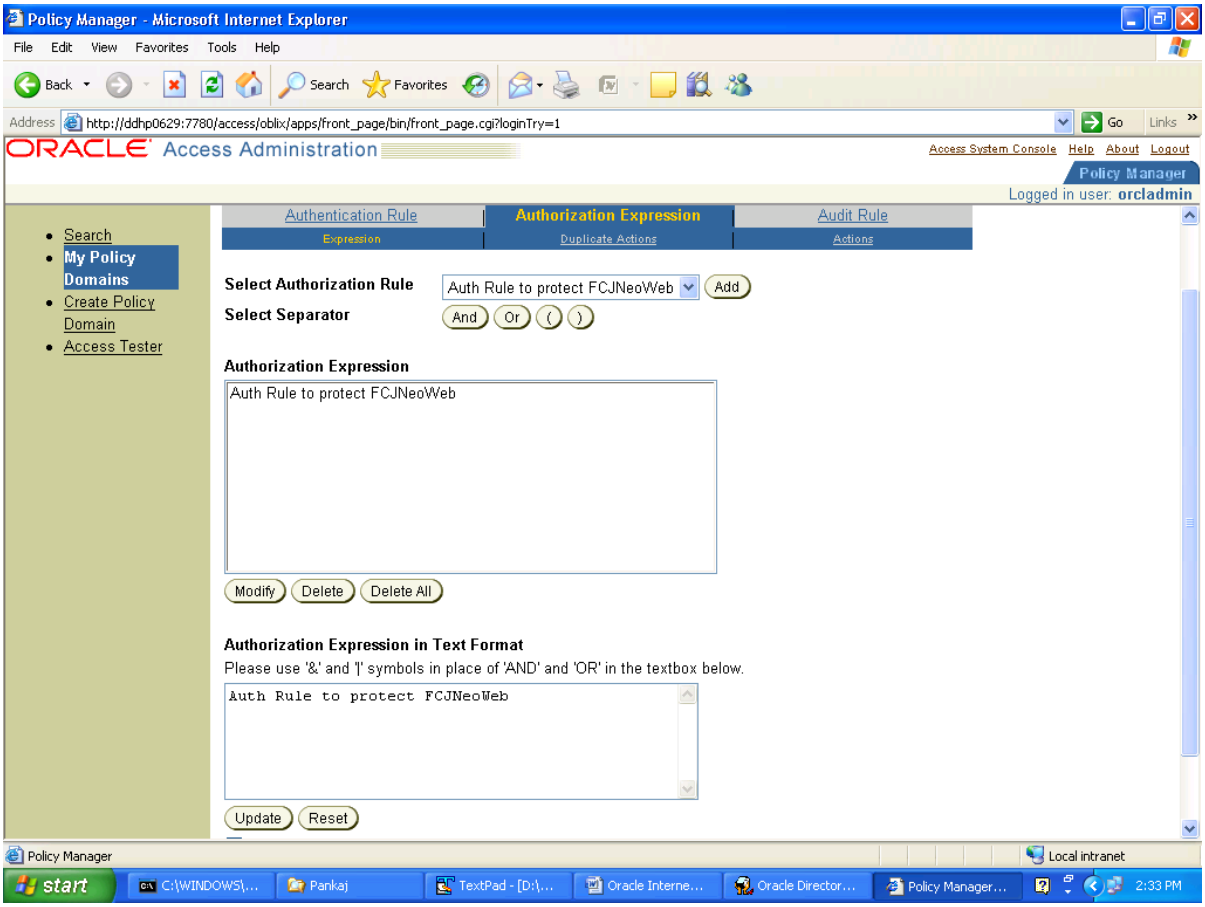
Give name and description for your authentication rule. For authentication Scheme you can find various options in Dropdown list. Select **Basic Over LDAP** option. Then give Save to proceed.



Next Select the Authorization Expression in sub menu (Marked in above figure) to attach the created authentication rule for the policy. In default no authorization expression is defined. Select Add to create new expression.

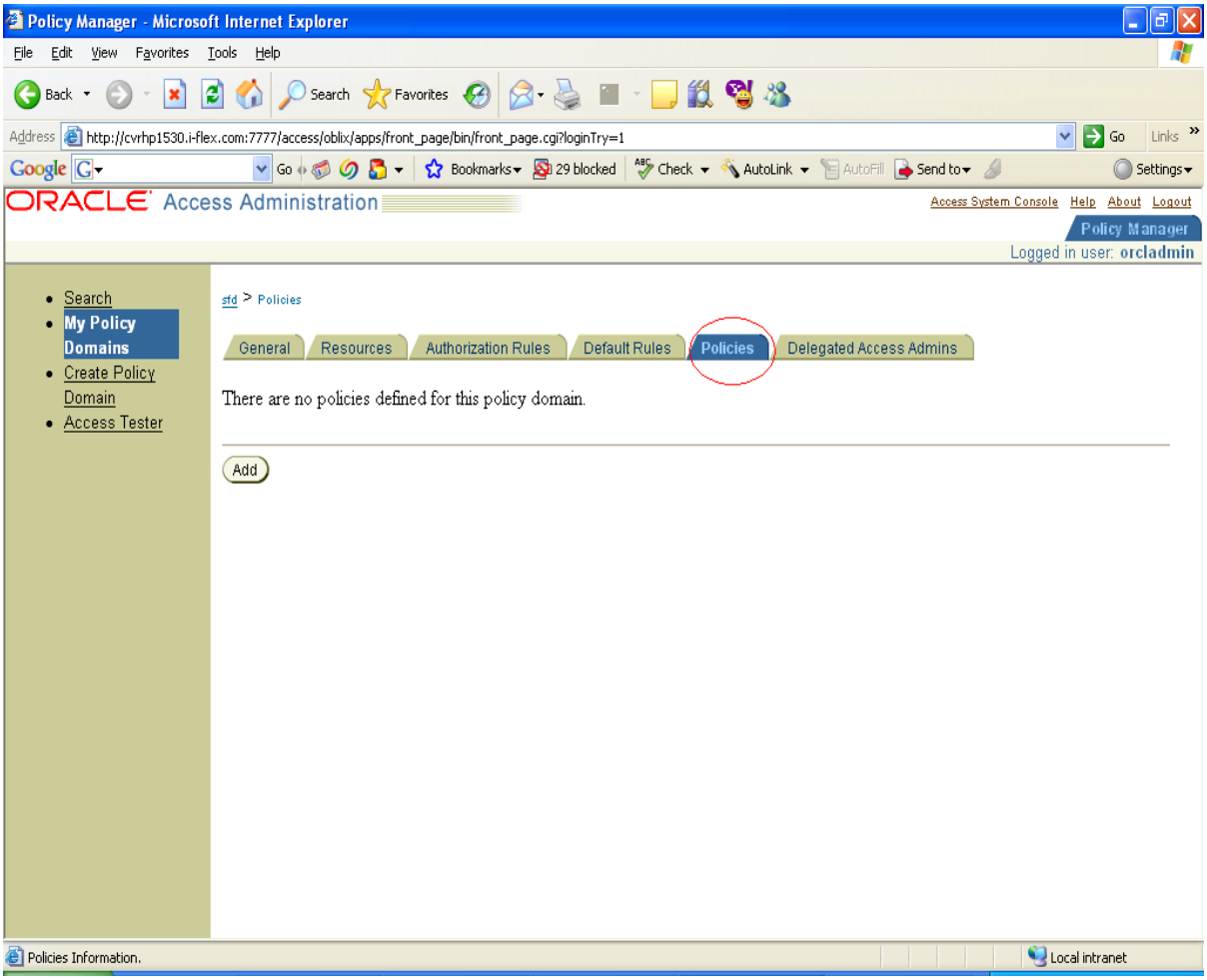


You will get the below page, when clicking Add button. You can find the authorization rule created earlier will be available in Select authorization rule drop down. Now press add button so that the selected rule will be available in Authorization Expression Text area and Authorization Expression in Text Format text area. (If you have more than one rule maintained you can still attach both the rule, various selector are available to attach more than one rule).

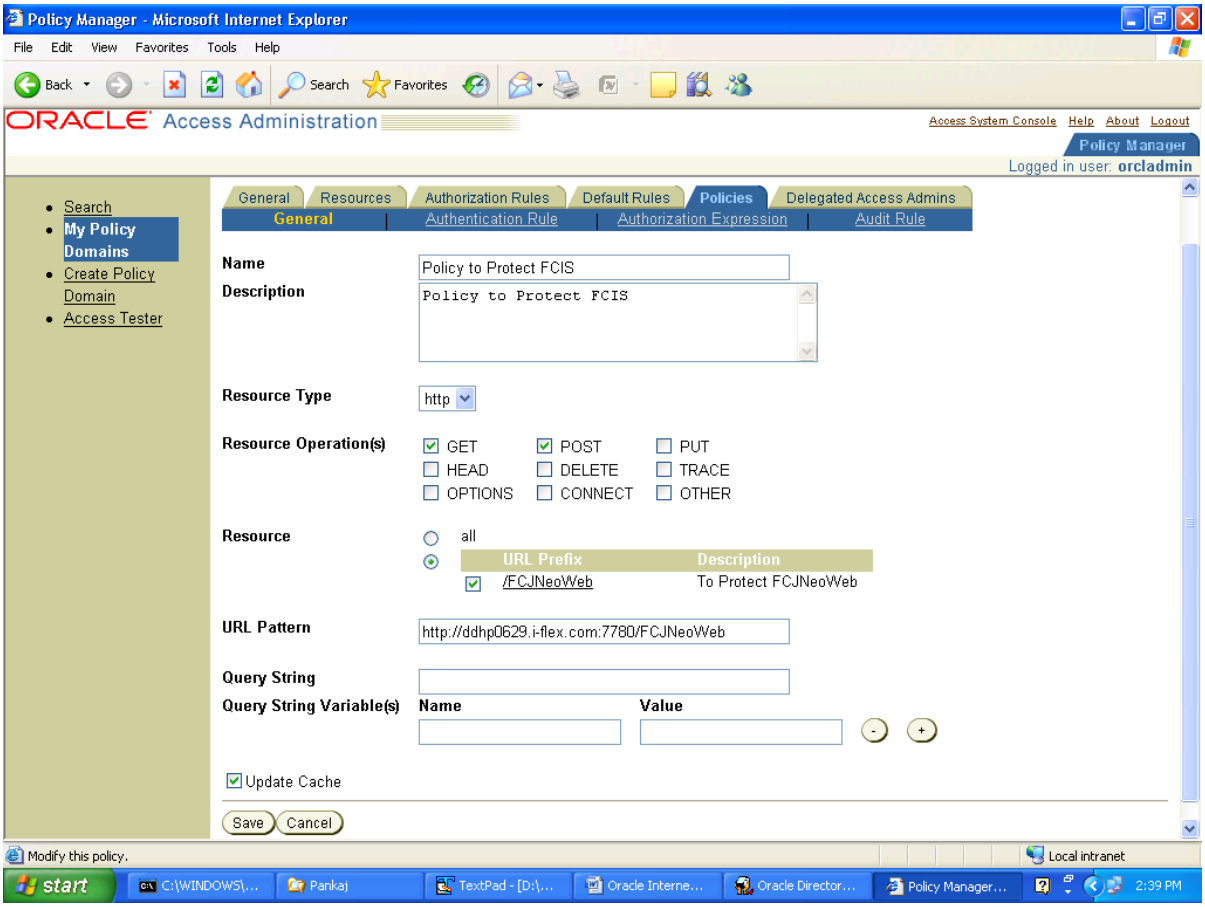


Then save the changes and next select the Action in the sub menu (Marked in above figure) and do the same as followed for the previous action.

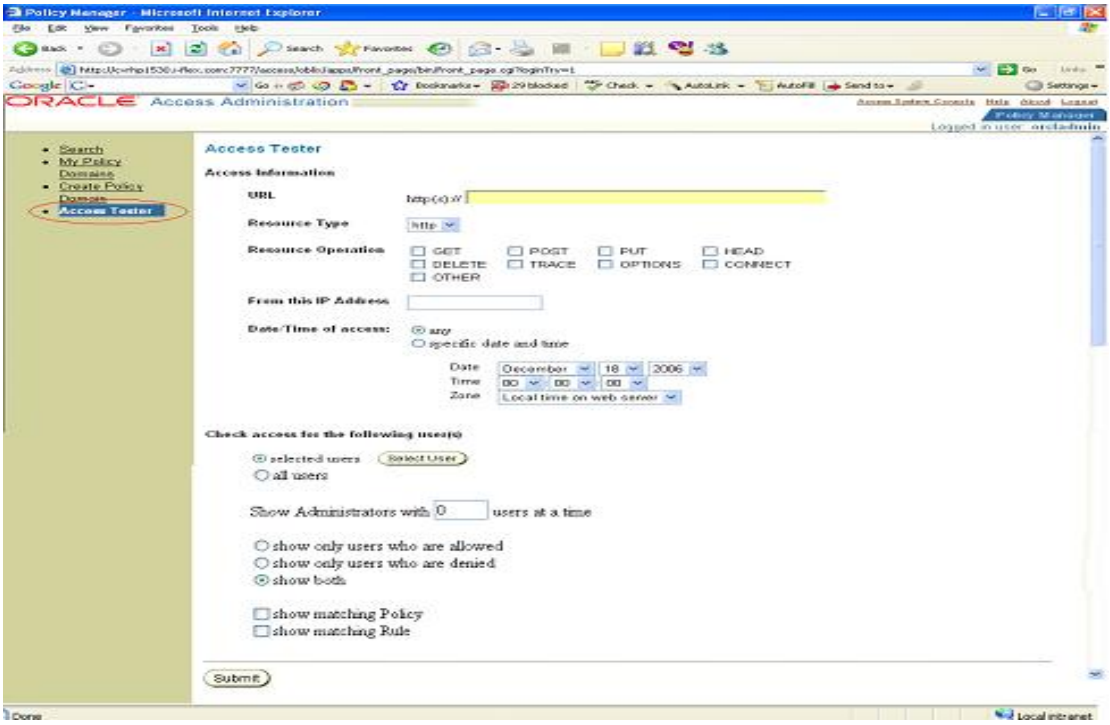
After finishing the default Rule process you will get the screen as below. Now select Policies option from the tab option. This is the place where we mention the URL which needs to be protected for SSO. (Marked in below screen). By default no policies is defined. Press Add to attach the policy.



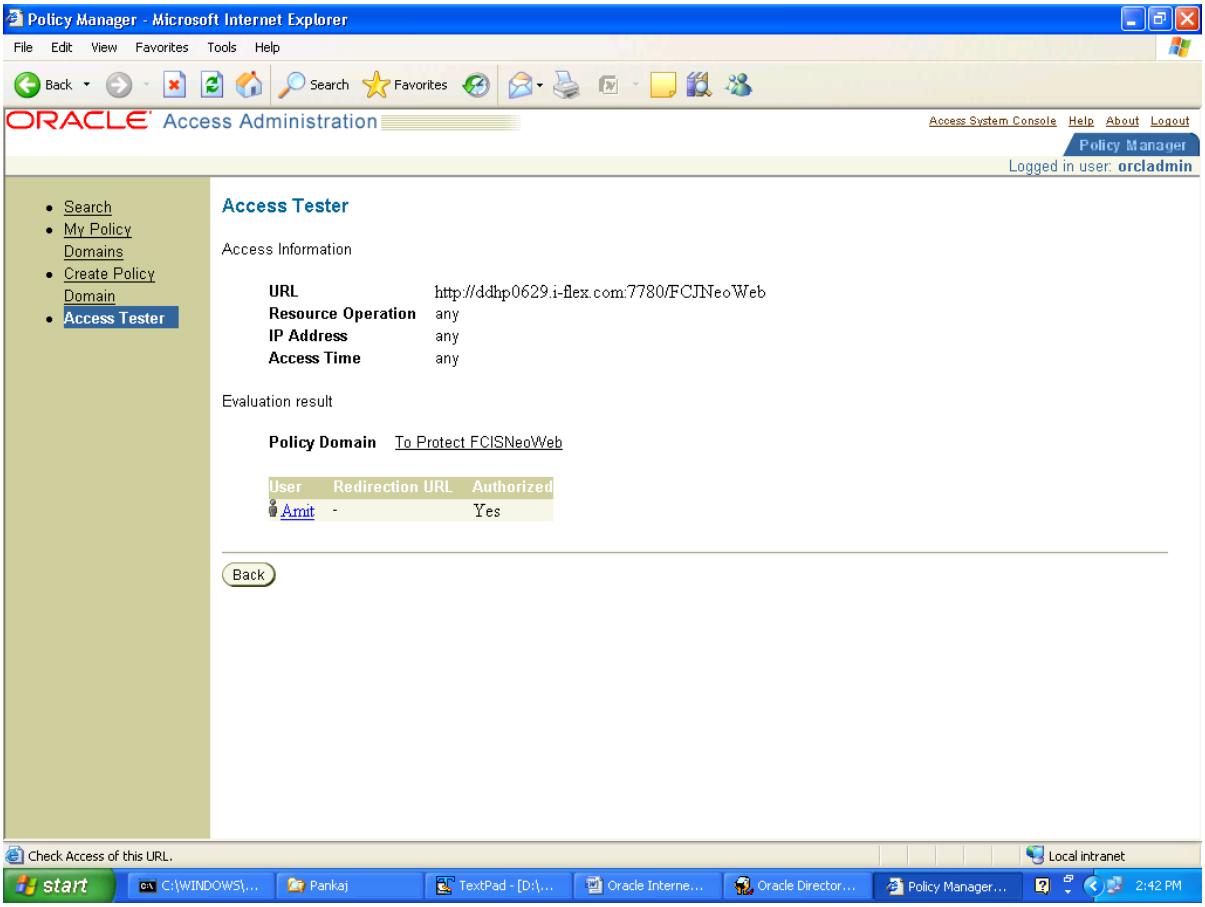
Now provide the name and description of the policy. Check the GET and POST checkbox for Resource Operations. You can find the URL prefix which added earlier is available. Check the URL prefix created (**/FCJNeoWeb**) and in URL pattern give the full URL which needs to be protected. For instance, http://ddhp0629:7780/FCJNeoWeb



Then save the changes made for the policies. This is how to create the policy domain and protect the resource. After creating policy domain we can test whether users has the access to it. Select **Access tester** link in LSM shown below.



Now provide the url which is protected in URL text box, then Select any one user you have access Using Select User button as did early. Next Press the submit button in the above page. If the validation is success then you will get the below screen


Policy Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
ORACLE Access Administration
Access System Console Help About Logout
Policy Manager
Logged in user: orcladmin
Search
My Policy Domains
Create Policy Domain
Access Tester
Access Tester
Access Information
URL http://ddhp0629.i-flex.com:7780/FCJNeoWeb
Resource Operation any
IP Address any
Access Time any
Evaluation result
Policy Domain To Protect FCISNeoWeb
User Redirection URL Authorized
Amit - Yes
Back
Check Access of this URL.
Local intranet
start
C:\WINDOWS\...
Pankaj
TextPad - [D:\...
Oracle Interne...
Oracle Director...
Policy Manager...
2:42 PM

5. First launch of Oracle FLEXCUBE after Installation

5.1 Introduction

After installing Oracle FLEXCUBE and while launching it for first time, the normal FCJ login screen with user ID and password will appear, this is because when installing the 'sso installed' parameter will set to 'N'.

5.2 Bank Parameter Maintenance

To enable SSO for Oracle FLEXCUBE IS, Run the below query for the default bank created during installation in SMS module.

Update sttm_bank
Set SSO_Installed='Y';

5.3 Maintaining Branch Level DN Template (Branch Maintenance)

For home branch (000) LDAP DN template should be maintained, which is used in Oracle FLEXCUBE IS user maintenance Form to populate corresponding LDAP userid automatically from this template. Go to branch level parameter screen and Click on Preferences Icon.

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

Here in this above template **cn=<FCJUSR>** part preferably must be there and it should not be altered, but the rest of the DN name can change based on the configuration.

Run the below queries to enable Single Sign on.

Update sttm_branch
Set Ldap_Template='cn=<FCCUSR>,cn=Users,dc=i-flex,dc=com'
Where Branch_Code='000';

Update CSTM_BRANCH_LOC_PARAMS

Set Param_Value='Y'

Where Param_Name='SSO_INSTALLED';

Update FBTB_PARAMS
Set Param_Value='Y'
Where Param_Name='SSO_INSTALLED';

5.4 Maintaining fcis.properties file

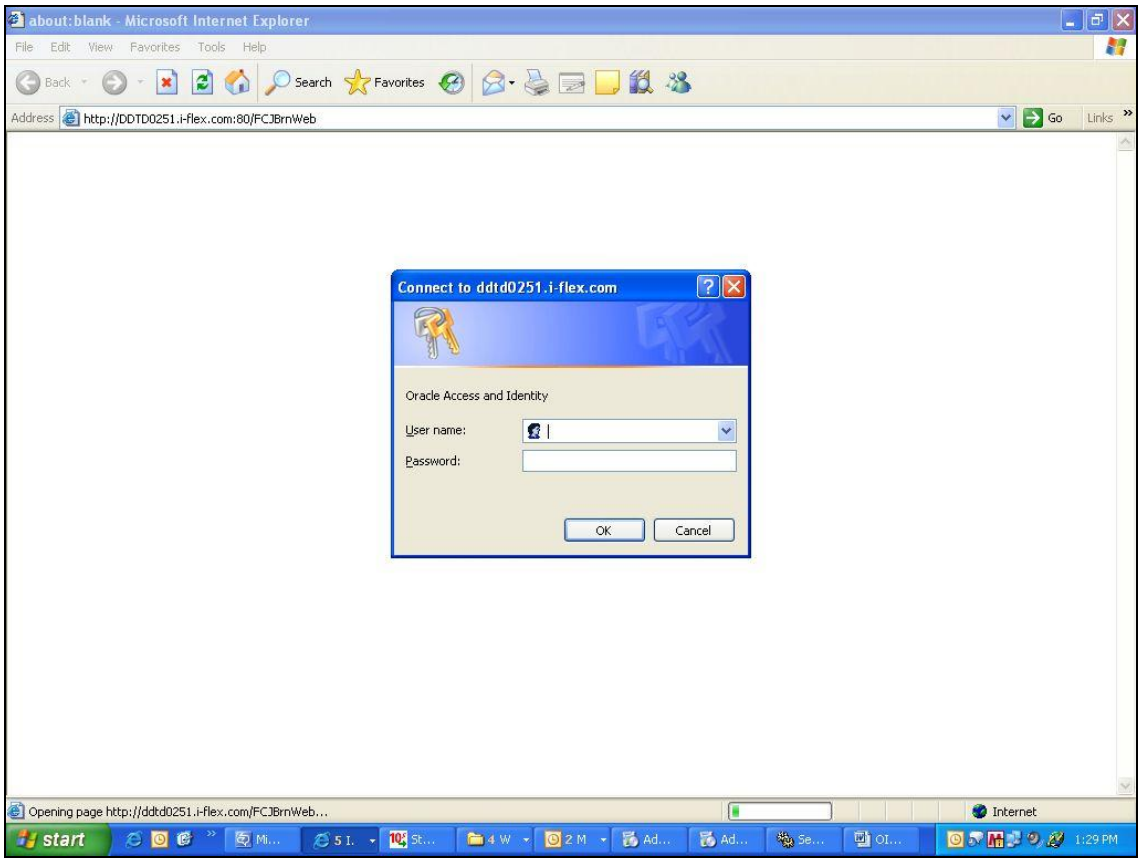
Go to **fcubs.property** file maintained in the application server and update the SSO_REQ flag to 'Y'.

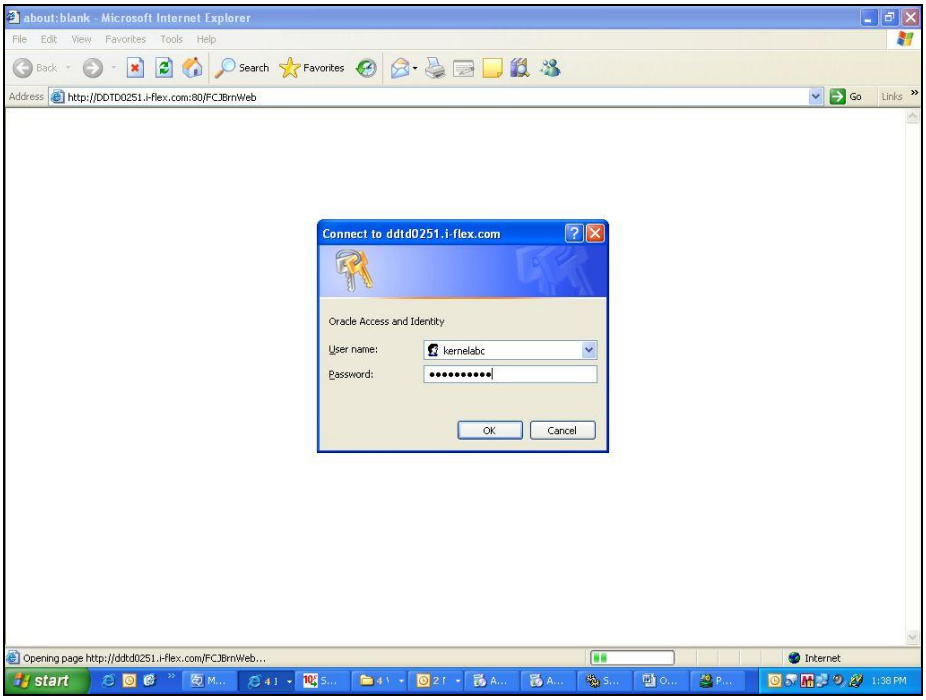
5.5 Launching FLEXCUBE

After setting up FLEXCUBE to work on Single Sign on mode, navigate to the interim servlet URL from your browser.

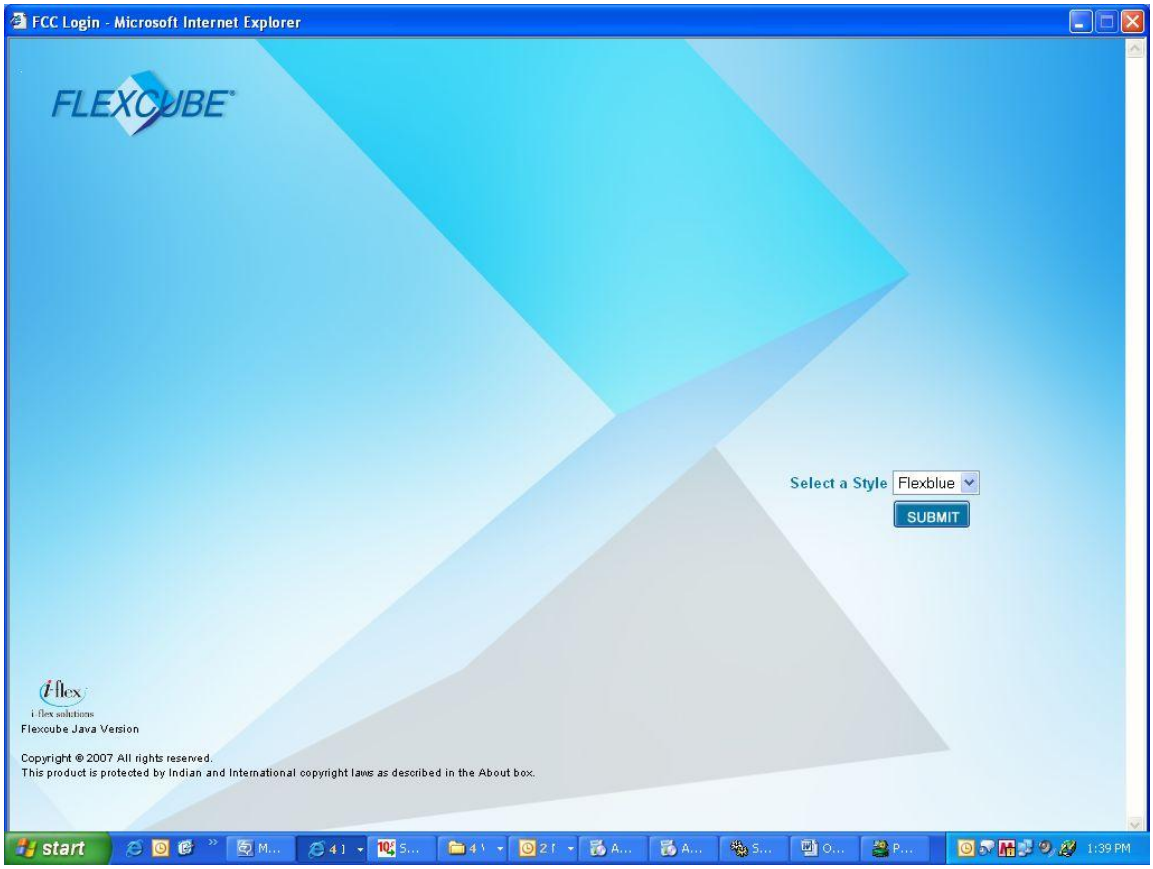
For e.g.: http://<hostname>:[port]/FCISNeoWeb

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 FLEXCUBE application server URL and now the new signon form will appear.



When clicking on OK button, the user is taken to application browser window directly without asking for FLEXCUBE IS user-id and password.

5.6 Signoff in a Single Signon Situation

Oracle FLEXCUBE does not provide for single signoff currently, i.e., when a user signs off in Oracle FLEXCUBE, the session established with Oracle Access Manager by the user will not be modified in any manner.

In a single signon situation the “Exit” and “Logoff” actions in Oracle FLEXCUBE IS will both function as “Exit”, i.e., on clicking these, the user will “exit” FLEXCUBE IS and will need to relaunch FLEXCUBE IS using the Oracle FLEXCUBE IS launch URL (refer section 5.4).

6. APPENDIX - HTTPD.CONF

httpd.conf

```
.
.
.
.
.
.
.
.
# Note: Copy the lines below only if they do not already exist in your httpd.conf
##**** BEGIN Oracle NetPoint WebPass Specific ****


  include "D:\Program Files\NetPoint\WebComponent\identity/oblix/.apacheconfig"

   AddHandler cgi-script .cgi


   LoadModule OBWebPass_Module "D:\Program
Files\NetPoint\WebComponent\identity/oblix/apps/webpass/bin/webpass_ohs.dll"



    obwebpassinstalldir "D:\Program Files\NetPoint\WebComponent\identity"

    Alias /identity/oblix  "D:\Program Files\NetPoint\WebComponent\identity/oblix/"


    <Directory "D:\Program Files\NetPoint\WebComponent\identity/oblix/">

        DirectoryIndex index.htm index.html

    </Directory>


    <Location /identity/oblix/apps/asynch/bin/asynch.cgi>

        SetHandler asynch

    </Location>


    <Location /identity/oblix/apps/common/bin/common.cgi>

        SetHandler common

    </Location>
```

```
<Location /identity/oblix/apps/corpdir/bin/corpdir.cgi>
    SetHandler corpdir
</Location>

<Location /identity/oblix/apps/admin/bin/corpdir_admin.cgi>
    SetHandler corpdiradmin
</Location>

<Location /identity/oblix/apps/admin/bin/front_page_admin.cgi>
    SetHandler front_pageadmin
</Location>

<Location /identity/oblix/apps/admin/bin/genconfig.cgi>
    SetHandler genconfig
</Location>

<Location /identity/oblix/apps/groupservcenter/bin/groupservcenter.cgi>
    SetHandler groupservcenter
</Location>

<Location /identity/oblix/apps/admin/bin/groupservcenter_admin.cgi>
    SetHandler groupservcenteradmin
</Location>

<Location /identity/oblix/apps/help/bin/help.cgi>
    SetHandler help
</Location>

<Location /identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi>
```

```
    SetHandler lost_pwd_mgmt
</Location>

<Location /identity/oblix/apps/npw/bin/npw.cgi>
    SetHandler npw
</Location>

<Location /identity/oblix/apps/objservcenter/bin/objservcenter.cgi>
    SetHandler objservcenter
</Location>

<Location /identity/oblix/apps/admin/bin/objservcenter_admin.cgi>
    SetHandler objservcenteradmin
</Location>

<Location /identity/oblix/apps/querybuilder/bin/querybuilder.cgi>
    SetHandler querybuilder
</Location>

<Location /identity/oblix/apps/selector/bin/selector.cgi>
    SetHandler selector
</Location>

<Location /identity/oblix/apps/admin/bin/servcenter_admin.cgi>
    SetHandler servcenteradmin
</Location>

<Location /identity/oblix/apps/admin/bin/setup_admin.cgi>
    SetHandler setupadmin
</Location>
```

```
   <Location /identity/oblix/apps/admin/bin/sysmgmt.cgi>

      SetHandler sysmgmt

   </Location>


   <Location /identity/oblix/apps/userservcenter/bin/userservcenter.cgi>

      SetHandler userservcenter

   </Location>


   <Location /identity/oblix/apps/admin/bin/wrsc_admin.cgi>

      SetHandler wrscadmin

   </Location>


##**** END Oracle NetPoint Specific ****

#*** BEGIN Oracle Policy Manager Specific ****
include "D:\program files\NetPoint\WebComponent\access/oblix/.apacheconfig"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/libobnspr4.dll"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/libobplc4.dll"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/libobplds4.dll"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/obsoftokn3.dll"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/obnss3.dll"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/obssl3.dll"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/obnsldap32v50.dll"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/obnsldappr32v50.dll"
LoadFile "D:\program files\NetPoint\WebComponent\access/oblix/lib/obnsldapssl32v50.dll"
Alias /access/oblix "D:\program files\NetPoint\WebComponent\access/oblix/"
LoadModule OBAccessManager "D:\program
files\NetPoint\WebComponent\access/oblix/lib/webpluginsssl.dll"
obinstalldir "D:\program files\NetPoint\WebComponent\access"

<Location /access/oblix/apps/front_page/bin/front_page.cgi>
   SetHandler obfrontpage
</Location>

<Location /access/oblix/apps/common/bin/common.cgi>
   SetHandler obcommon
</Location>

<Location /access/oblix/apps/admin/bin/genconfig.cgi>
   SetHandler obgenconfig
</Location>
```

```
<Location /access/oblix/apps/admin/bin/sysmgmt.cgi>
   SetHandler obsysmgmt
</Location>

<Location /access/oblix/apps/admin/bin/setup_admin.cgi>
   SetHandler obsetupadmin
</Location>

<Location /access/oblix/apps/admin/bin/front_page_admin.cgi>
   SetHandler obfrontpageadmin
</Location>

<Location /access/oblix/apps/admin/bin/wrsc_admin.cgi>
   SetHandler obwrscadmin
</Location>

<Location /access/oblix/apps/help/bin/help.cgi>
   SetHandler obhelp
</Location>

<Location /access/oblix/apps/policyservcenter/bin/policyservcenter.cgi>
   SetHandler obpolicyservcenter
</Location>

#*** END Oracle Policy Manager Specific ****

#*** BEGIN WebGate Specific ****

LoadModule obWebgateModule "D:\Program
Files\NetPoint\WebComponent\access/oblix/apps/webgate/bin/webgate.dll"
WebGateInstalldir "D:\Program Files\NetPoint\WebComponent\access"
WebGateMode PEER

<Location /access/oblix/apps/webgate/bin/webgate.cgi>
SetHandler obwebgateerr
</Location>

<Location "/oberr.cgi">
SetHandler obwebgateerr
</Location>

<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>

#*** END WebGate Specific ****
```

Design Specififcation
[April] [2014]
Version 12.0.3.0.0

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/