

# Oracle Adaptive Access Manager Basic Oracle Access Manager Integration

## Revision History

Date	Version	Description	Author
11/28/2010	V1	Oracle Adaptive Access Manager Basic Oracle Access Manager Integration	Jeff Nester (Oracle)

### Table of Contents:

1. Introduction.....	2
2. Install WebLogic.....	2
3. Run RCU.....	3
4. Configure OAAM.....	3
5. Create Policies to Protect.....	11
6. Create OAAMADMIN user.....	13
7. Modify oam-config.xml.....	16
8. Start OAAM_ADMIN.....	16
9. Load Necessary Policies and Questions into OAAM.....	16
10. Shutdown OAAM_ADMIN Server.....	19
11. Start OAAM_SERVER.....	19
12. Modify JDBC resource in WebLogic.....	20
13. Shutdown OAAM_SERVER Server.....	20
14. Start OAM_SERVER.....	20
15. Test the configuration.....	20
16. Appendix: OID Work Around.....	21

## 1. Introduction

This document was created to show how to integrate Oracle Access Manager (OAM) 11gR1 and Oracle Adaptive Access Manager (OAAM) 11gR1 using the OAAM Basic method. There are two integration methods available BASIC and Advanced. This document will not discuss Advanced integration. The primary difference between the Basic and Advanced is that Basic does not require OAAM to be running. All of the necessary code has been added to OAM. There are limitations to the OAAM Basic integration. The Basic integration only provides Knowledge Based Authentication (KBA.) All of the other features of OAAM are not available using this method.

**NOTE:** It has been determined that there is a significant issue with the OAM/OAAM integration on windows. This problem has not been replicated on Oracle Enterprise Linux. These instructions are for Windows. Due to the problem that was uncovered this integration assumes that OAM users are in the native WebLogic user store. At the end of this document there is an Appendix that discusses a non-tested work around to store users in Oracle Internet Directory.

These instructions step through installing and configuring OAM and OAAM on a windows 2003 server that has 4GB of memory.

Configuration data for this installation is:

Database:	oim.homeunix.net on host: orcldb-homeunix.net
OAAM Server:	oaam11g.homeunix.net

**NOTE: It has been determined that Firefox should be used to perform all the browser based steps in this document.**

## 2. Install WebLogic

Begin the process by installing but not configuring WebLogic. The default location should be **d:\Oracle\Middleware**

### 3. Run RCU

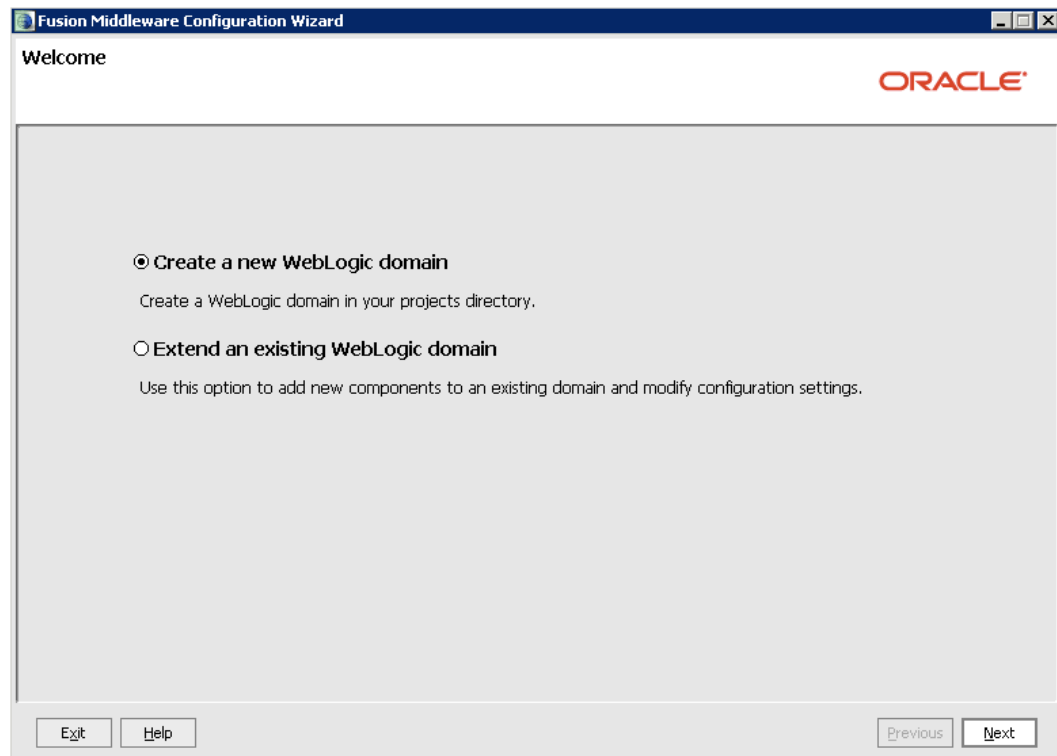
Run RCU and create the schemas for OAM and OAAM. These instructions do not configure Oracle Identity Manager (OIM) Execute the RCU utility, **rcu.bat**, that is located in the following directory under the unzipped RCU files:

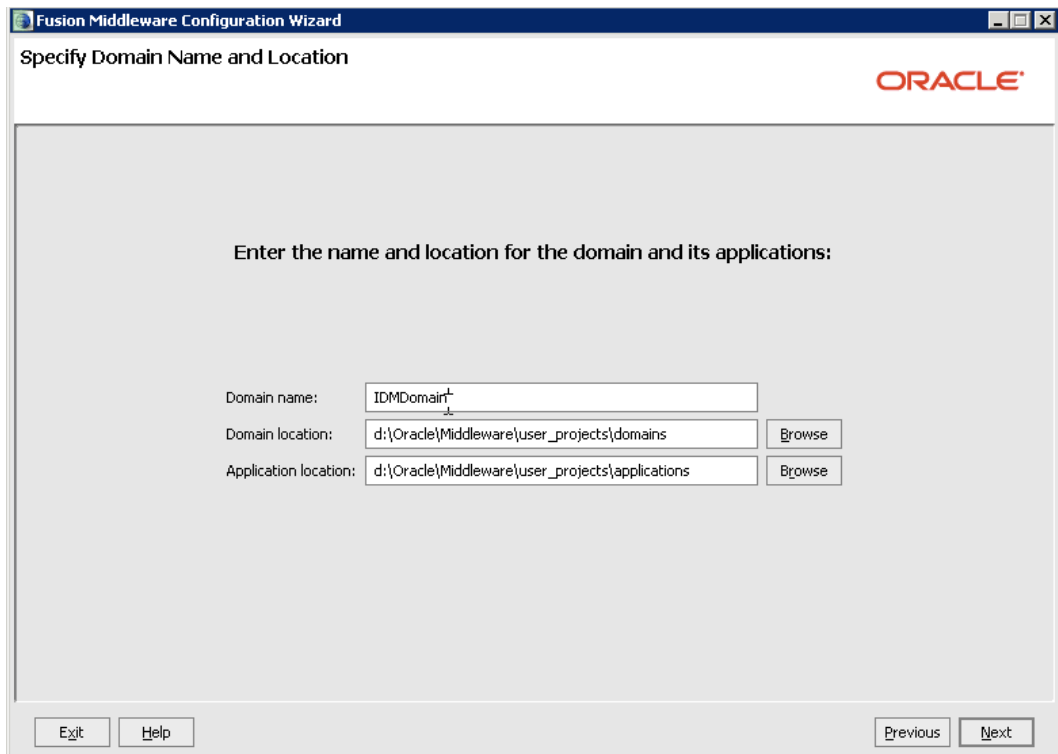
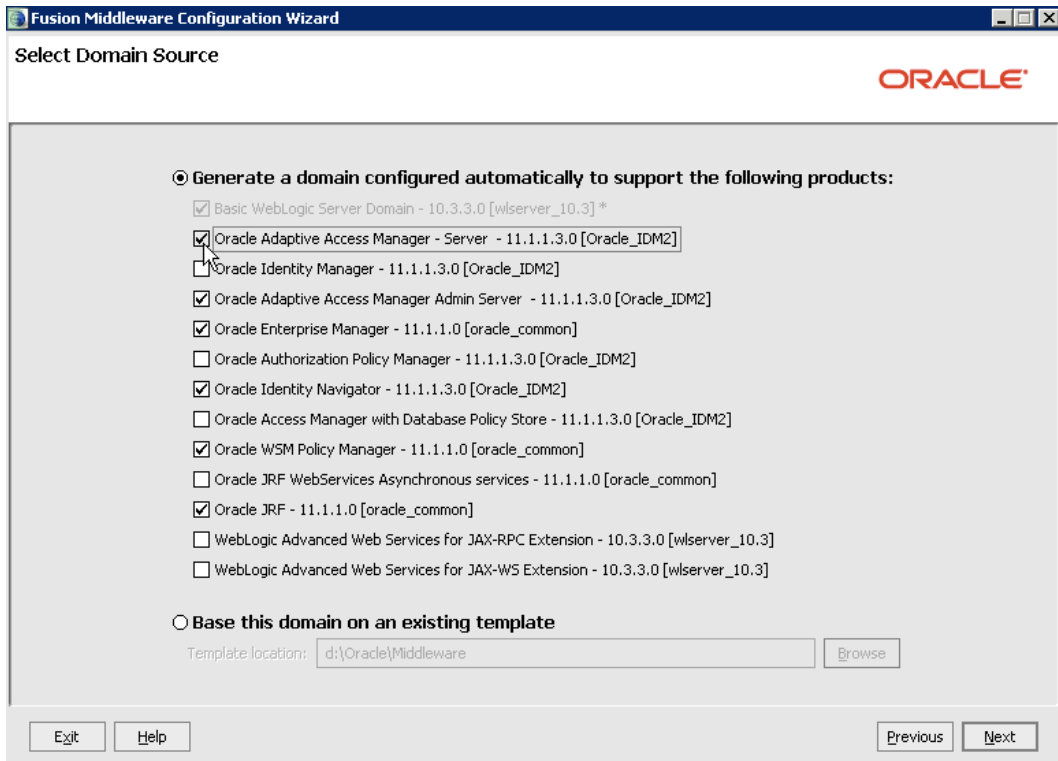
d:\kits\ofm\_rcu\_win32\_11.1.1.3\_disk1of1\rcuHome\BIN

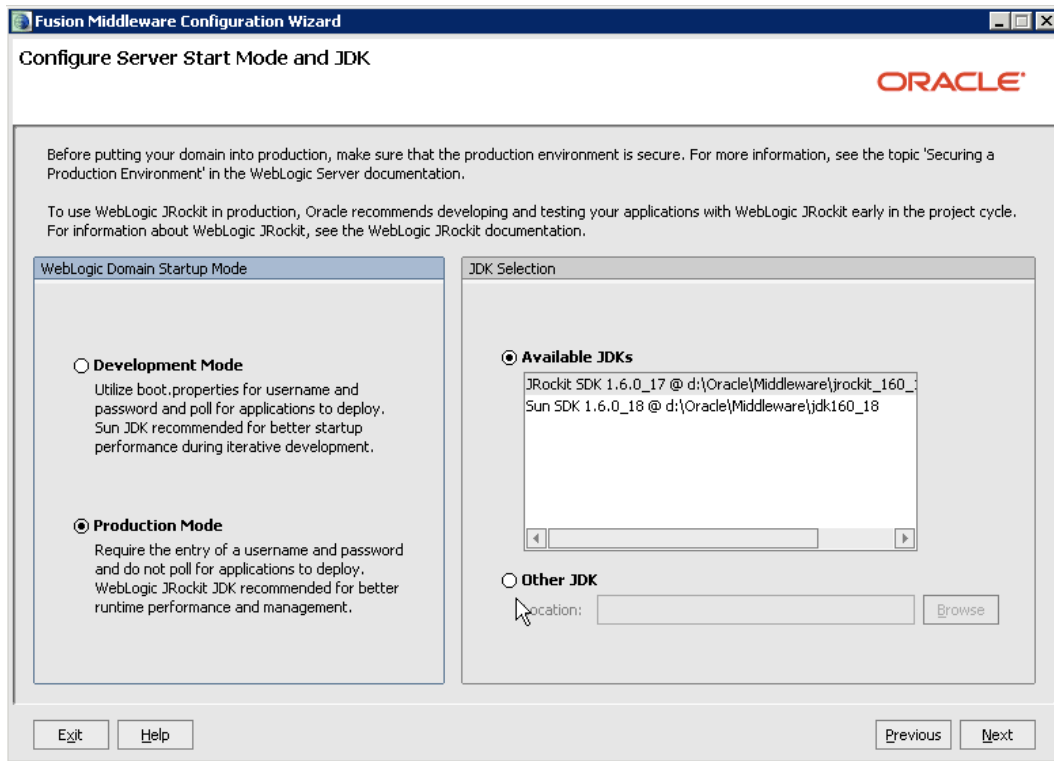
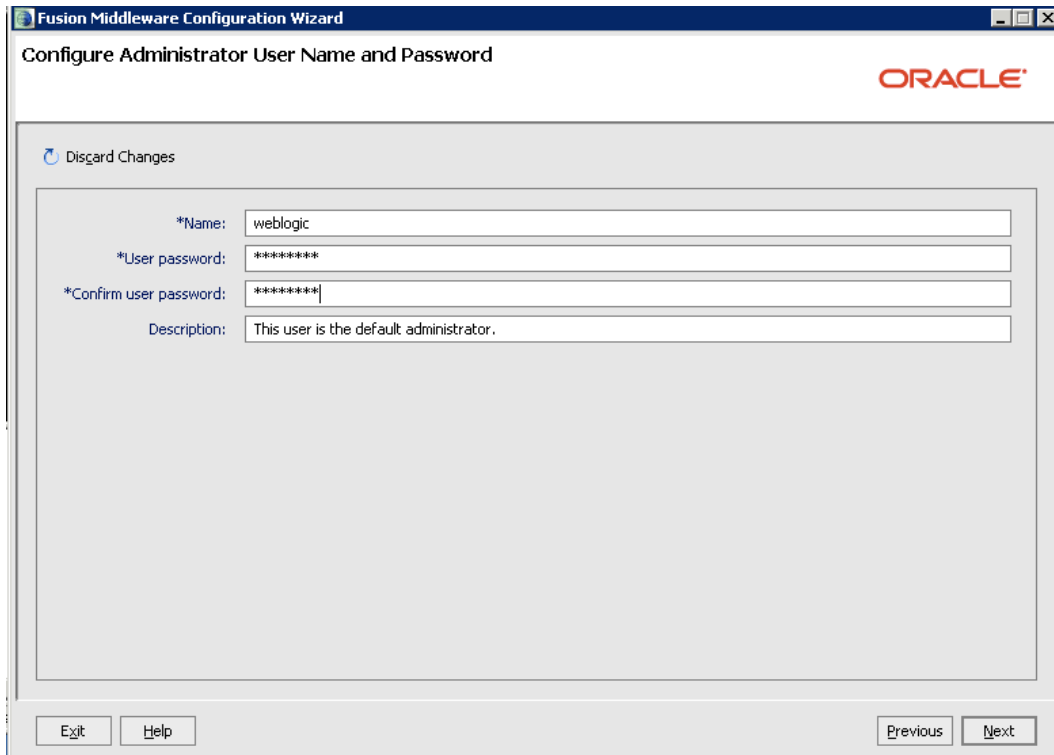


### 4. Configure OAAM

Execute the **config.cmd** file located at d:\Oracle\Middleware\Oracle\_IDM2\common\bin:







**Fusion Middleware Configuration Wizard**

### Configure JDBC Component Schema

**ORACLE**

**Note:** Change only the input fields below that you wish to modify and values will be applied to all selected rows.

Vendor:  DBMS/Service:

Driver:  Host Name:

Schema Owner:  Port:

Schema Password:

Configure selected component schemas as RAC multi data source schemas in the next panel.

	Component Schema	DBMS/Service	Host Name	Port	Schema Owner	Schema Password
<input checked="" type="checkbox"/>	OAAM Admin Schema	oim.homeunix.net	oaam11g.homeunix.	1521	DEV_OAAM	*****
<input checked="" type="checkbox"/>	OAAM Server Schema	oim.homeunix.net	oaam11g.homeunix.	1521	DEV_OAAM	*****
<input checked="" type="checkbox"/>	OAAM Admin MDS Schema	oim.homeunix.net	oaam11g.homeunix.	1521	DEV_MDS	*****
<input checked="" type="checkbox"/>	OWSM MDS Schema	oim.homeunix.net	oaam11g.homeunix.	1521	DEV_MDS	*****

**Fusion Middleware Configuration Wizard**

### Test Component Schema

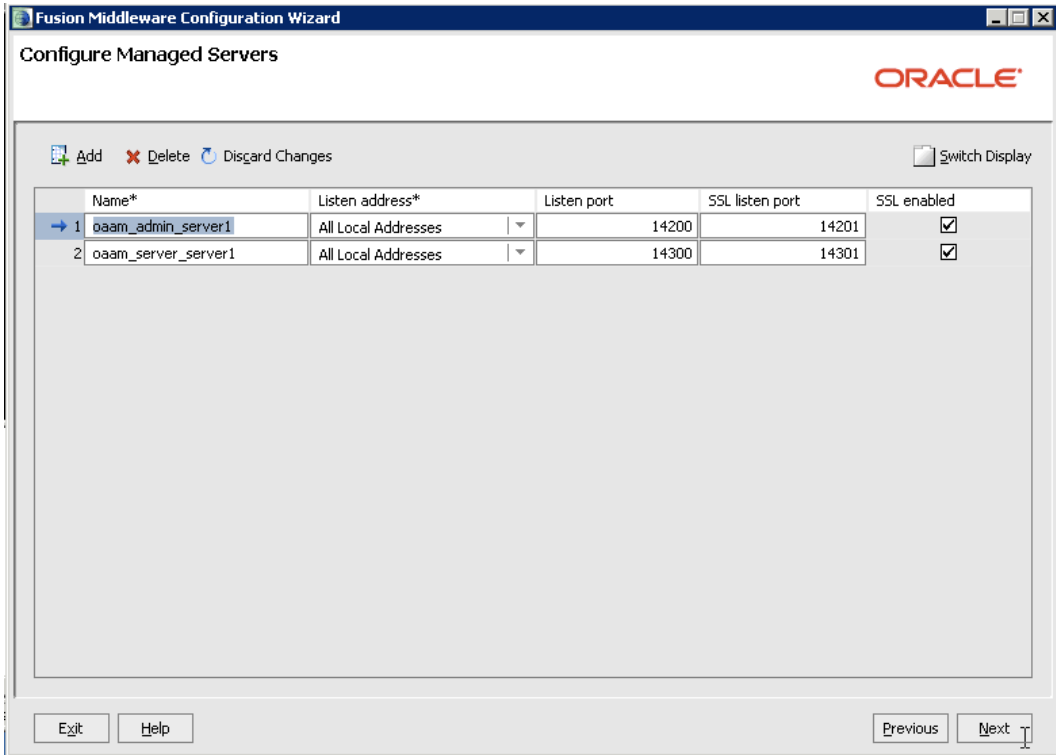
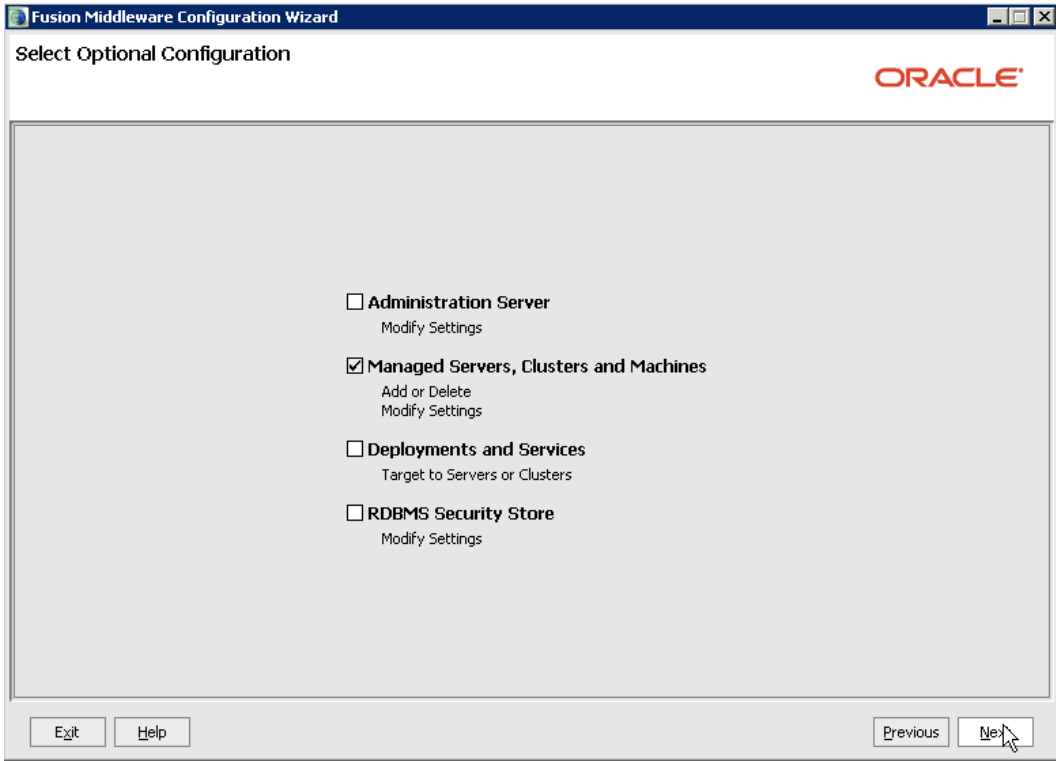
**ORACLE**

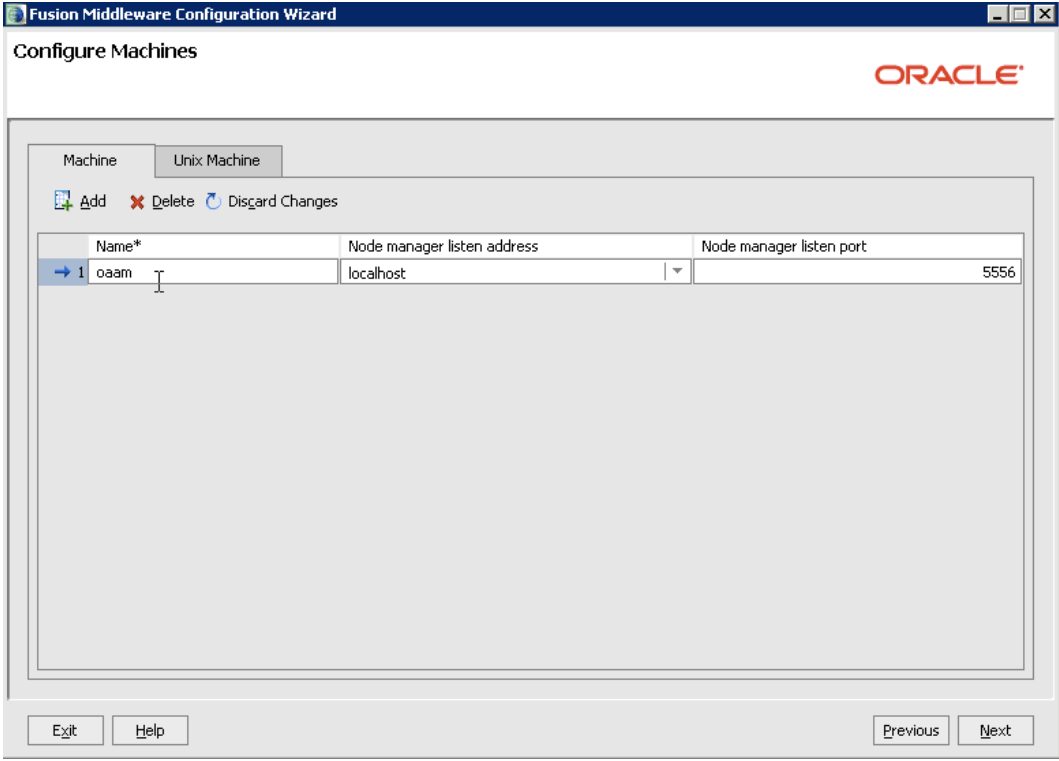
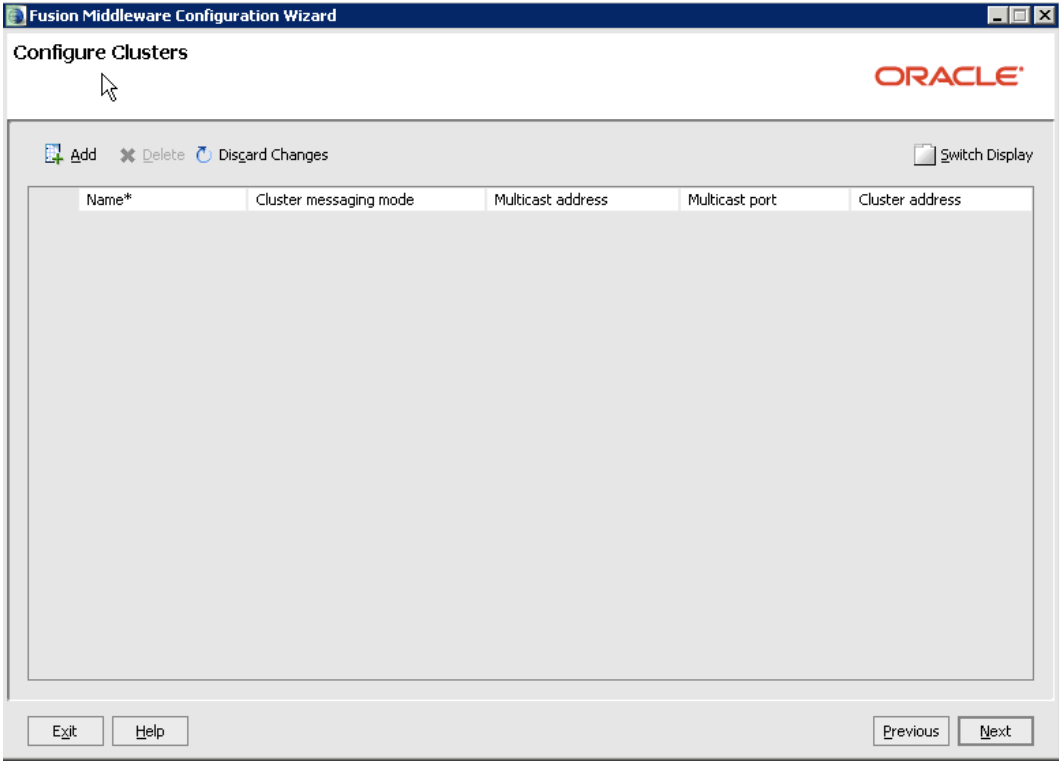
	Status	Component Schema	JDBC Connection URL
<input checked="" type="checkbox"/>	✓	OAAM Admin Schema	jdbc:oracle:thin:@orcl-db.homeunix.net:1521/oim.homeunix.net
<input checked="" type="checkbox"/>	✓	OAAM Server Schema	jdbc:oracle:thin:@orcl-db.homeunix.net:1521/oim.homeunix.net
<input checked="" type="checkbox"/>	✓	OAAM Admin MDS Schema	jdbc:oracle:thin:@orcl-db.homeunix.net:1521/oim.homeunix.net
<input checked="" type="checkbox"/>	✓	OWSM MDS Schema	jdbc:oracle:thin:@orcl-db.homeunix.net:1521/oim.homeunix.net

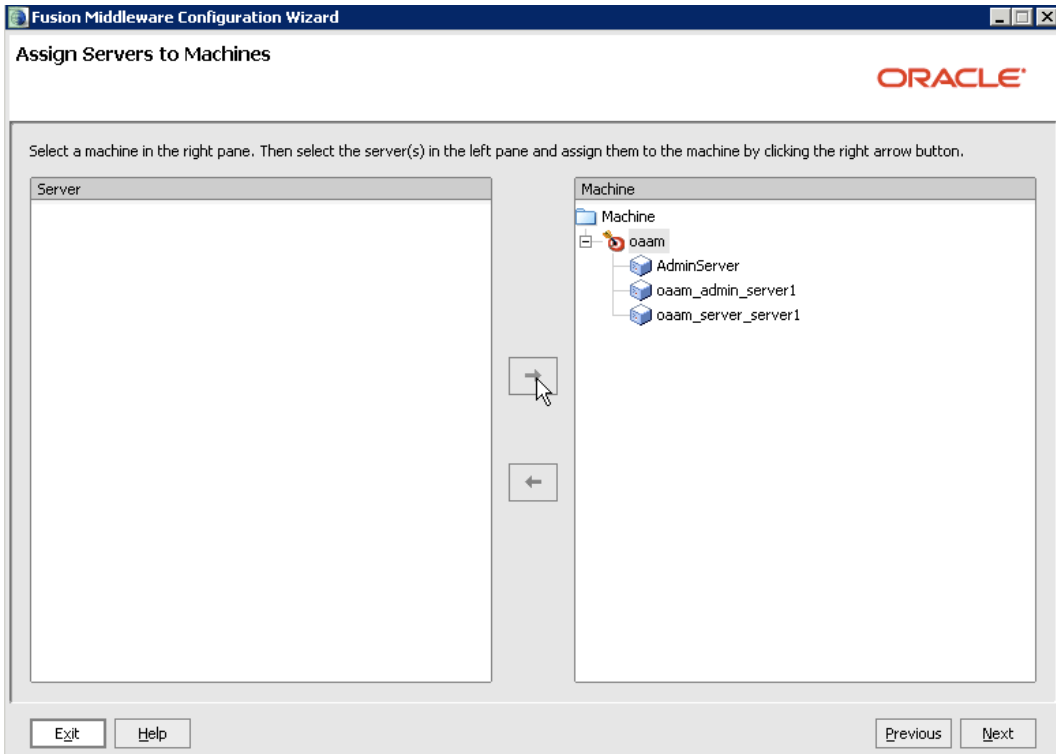
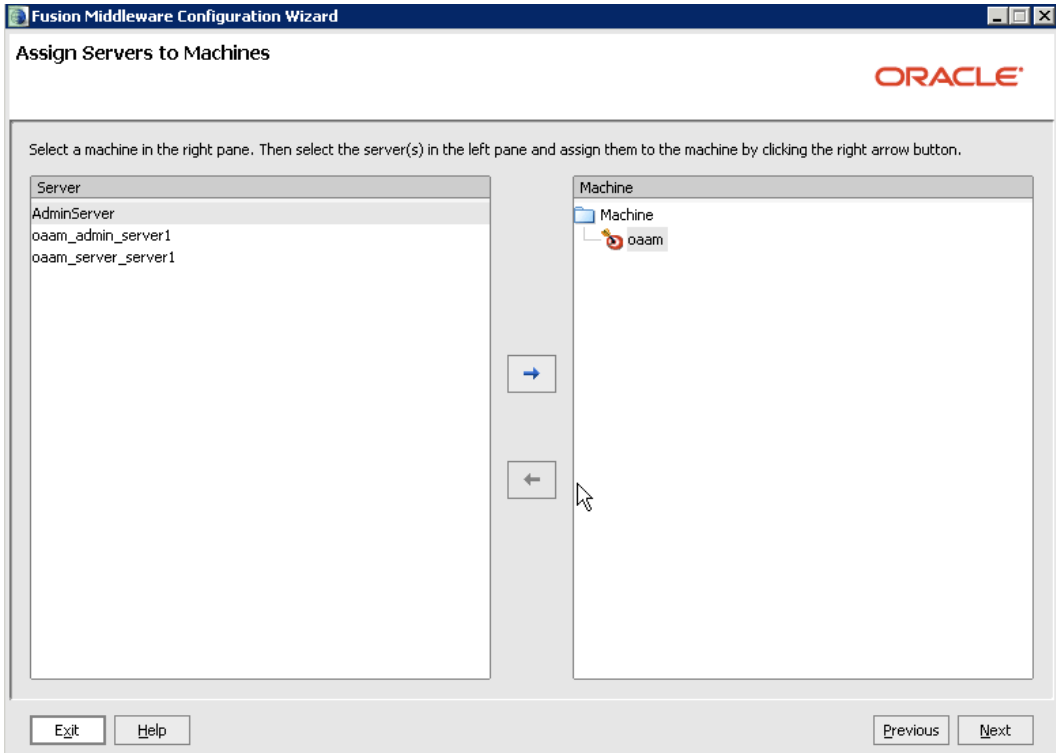
**Connection Result Log**

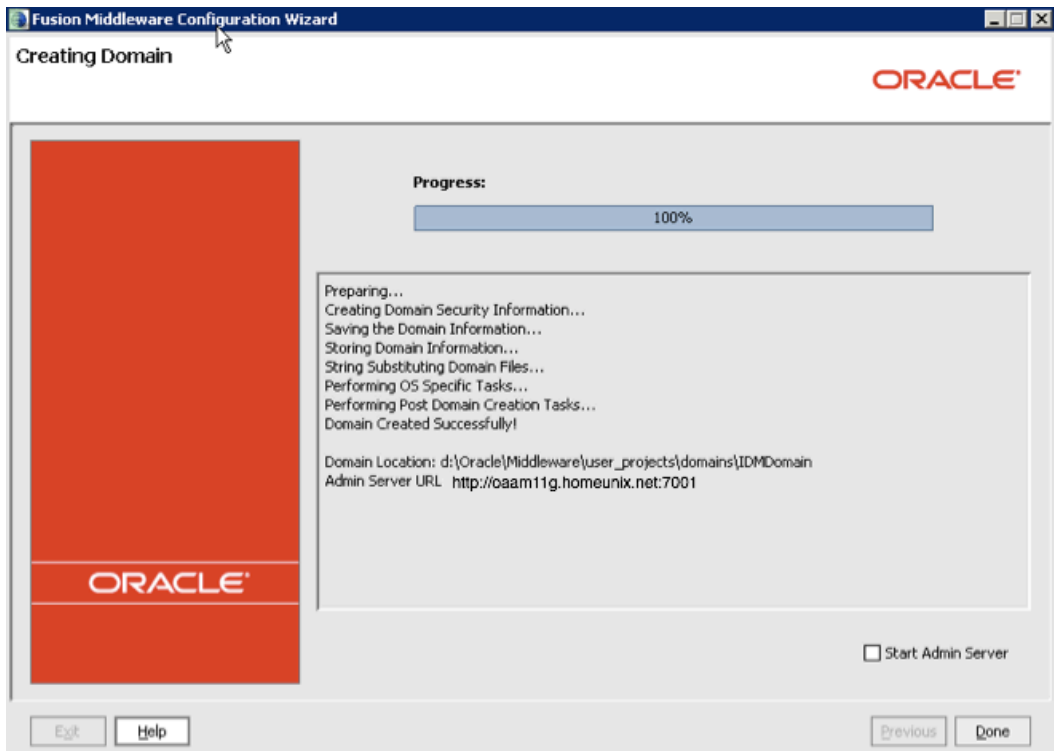
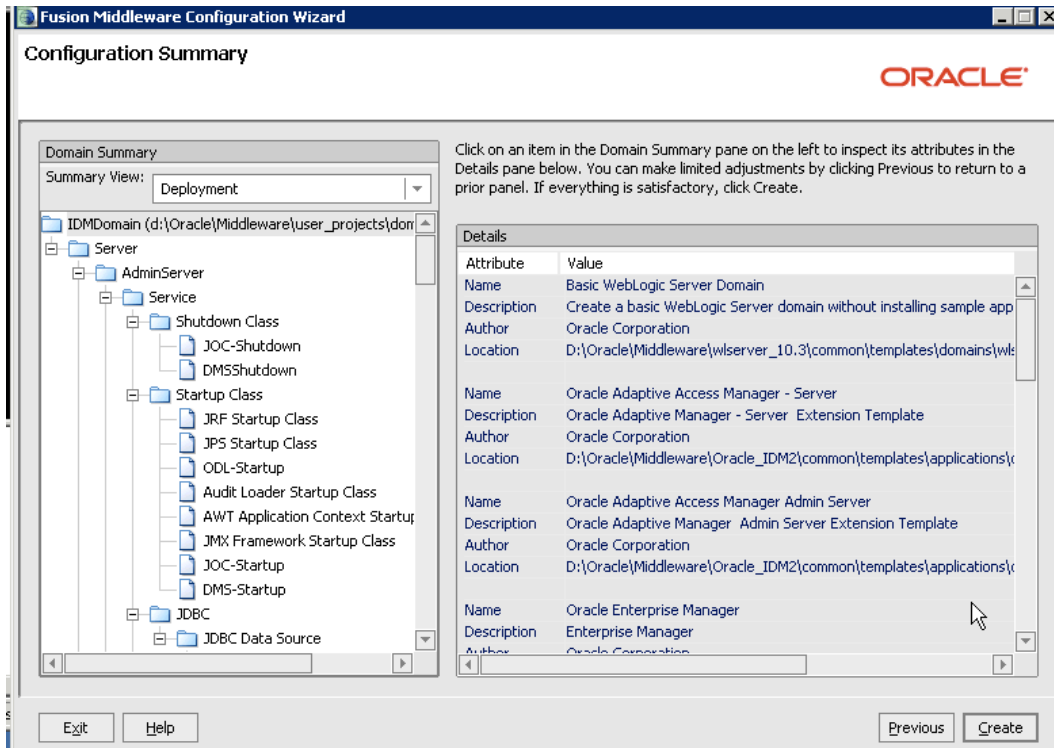
```
User=DEV_MDS
Password=*****
SQL Test=select 1 from schema_version_registry where
owner=(select user from dual) and mr_type='MDS' and
version='11.1.1.2.0'

CFGFWK-20850: Test Successful!
```

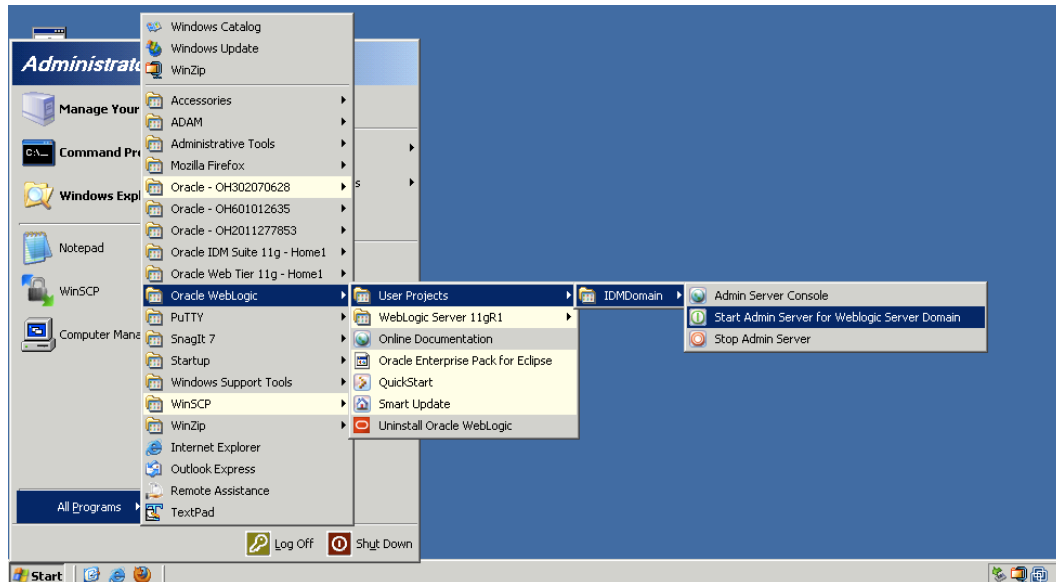








Start the Admin server as shown below:

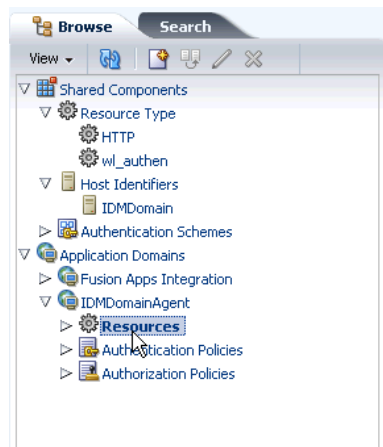


## 5. Create Policies to Protect

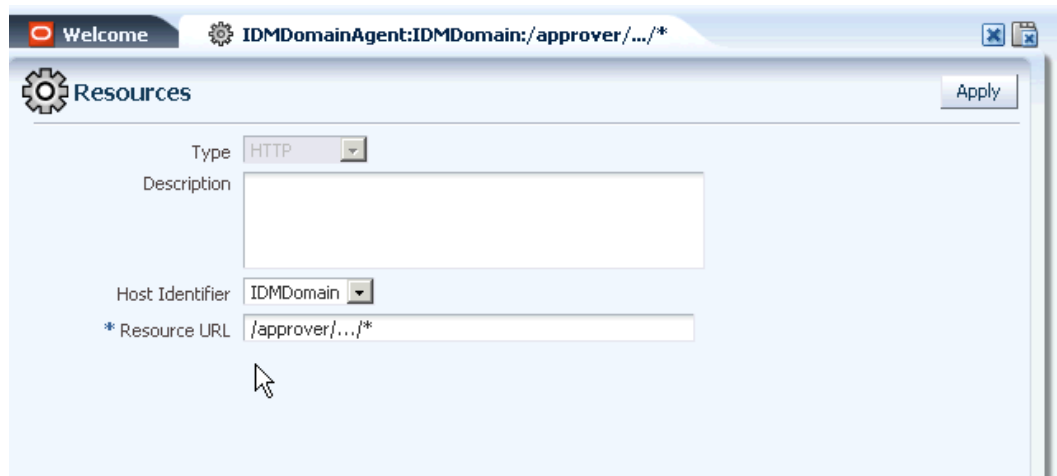
For an example we will create a policy to protect an application called approver. The approver application is a J2EE application that has been modified to allow it to be protected by IDMDomainAgent. Go to the oamconsole at

<http://oaam11g.homeunix.net:7001/oamconsole>

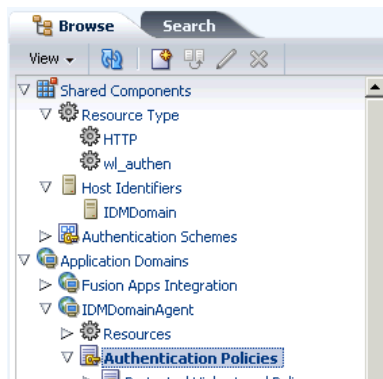
Select Resources under IDMDomainAgent.



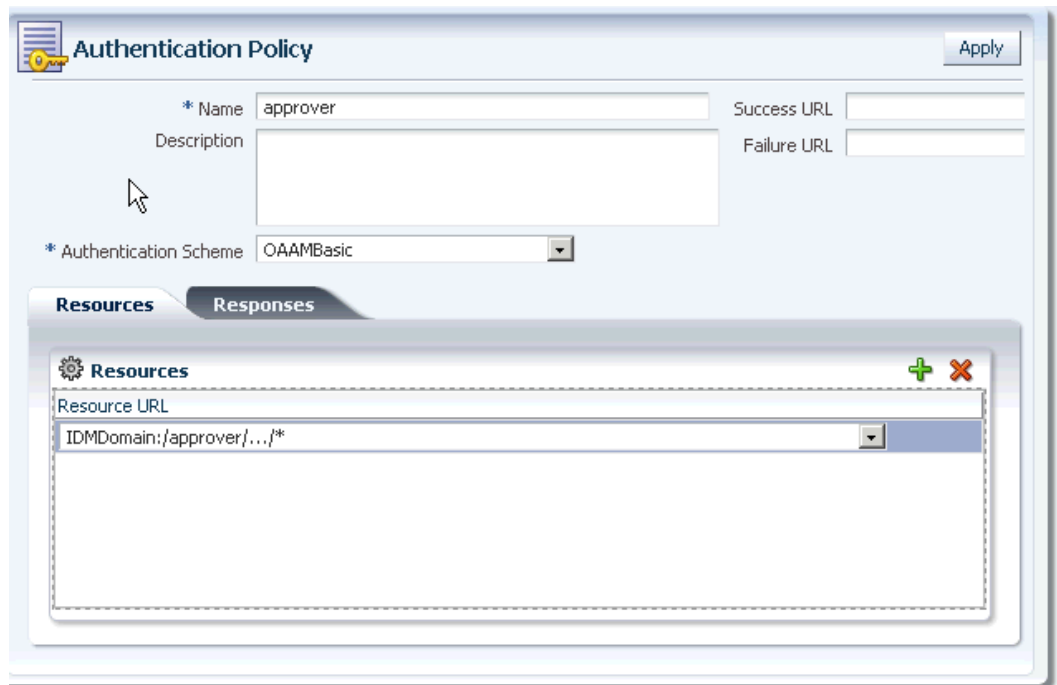
Add the following resource:



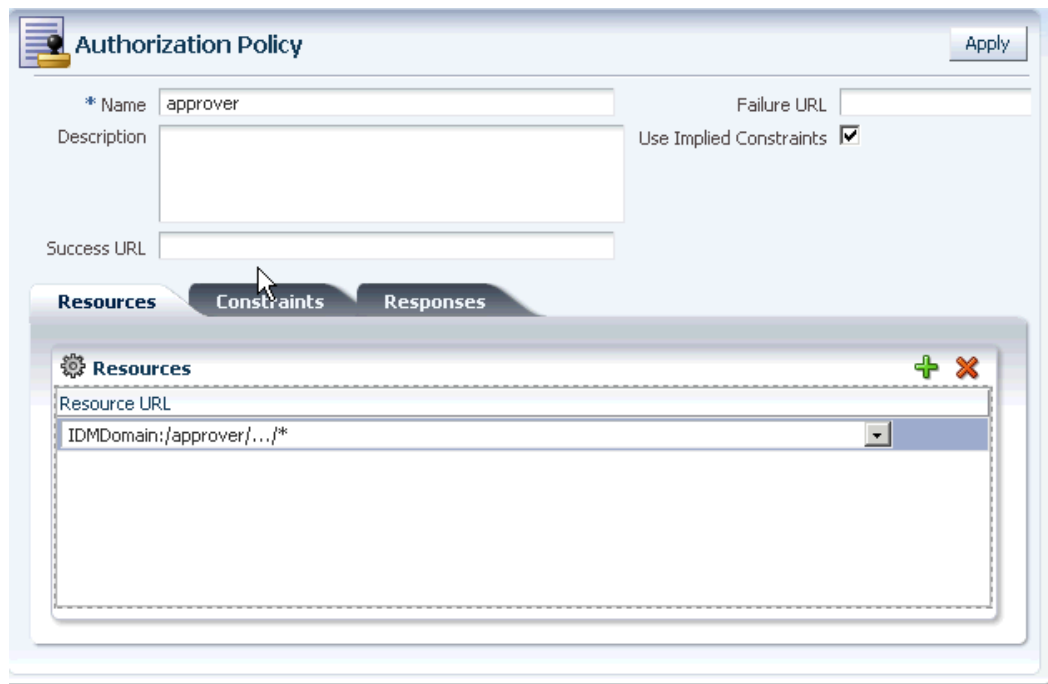
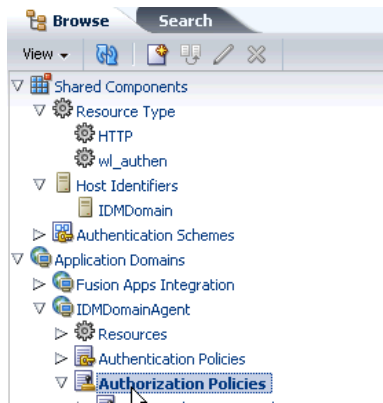
Next create a new Authentication Policy under IDMDomainAgent.



Create a New Authentication Policy called approver and make sure to set the Authentication Scheme to OAAMBasic:

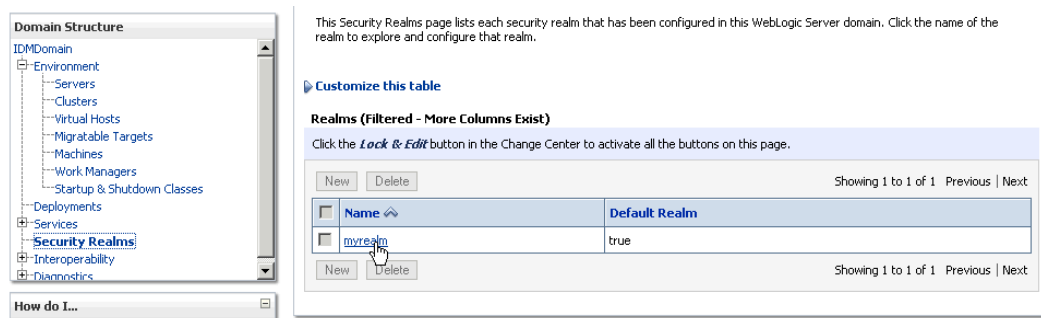


Now create a new Authorization Policy:



## 6. Create OAAMADMIN user

By default there is not a user that has the correct privileges to log into the OAAM administration console. The next steps show you how to create and grant the necessary groups to the **oaamadmin** user. Using a browser log into the WebLogic Administration Server ( <http://oaam1lg.homeunix.net:7001/console> ) and click on the **Security Realms** hyperlink on the left side of the page. Then select the **myrealm** hyperlink on the right hand side of the page.



Next click on the **Users and Groups** tab then click the **New** button:

Settings for myrealm

Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

Users Groups

This page displays information about each user that has been configured in this security realm.

[Customize this table](#)

**Users**

New Delete Showing 1 to 2 of 2 Previous | Next

<input type="checkbox"/>	Name ↕	Description	Provider
<input type="checkbox"/>	OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
<input type="checkbox"/>	weblogic	This user is the default administrator.	DefaultAuthenticator

New Delete Showing 1 to 2 of 2 Previous | Next

Enter the new user information in the **Create a New User** screen:

Create a New User

OK Cancel

**User Properties**

The following properties will be used to identify your new User.

\* Indicates required fields

What would you like to name your new User?

\* **Name:** oamadmin

How would you like to describe the new User?

**Description:** OAAM Admin User

Please choose a provider for the user.

**Provider:** DefaultAuthenticator

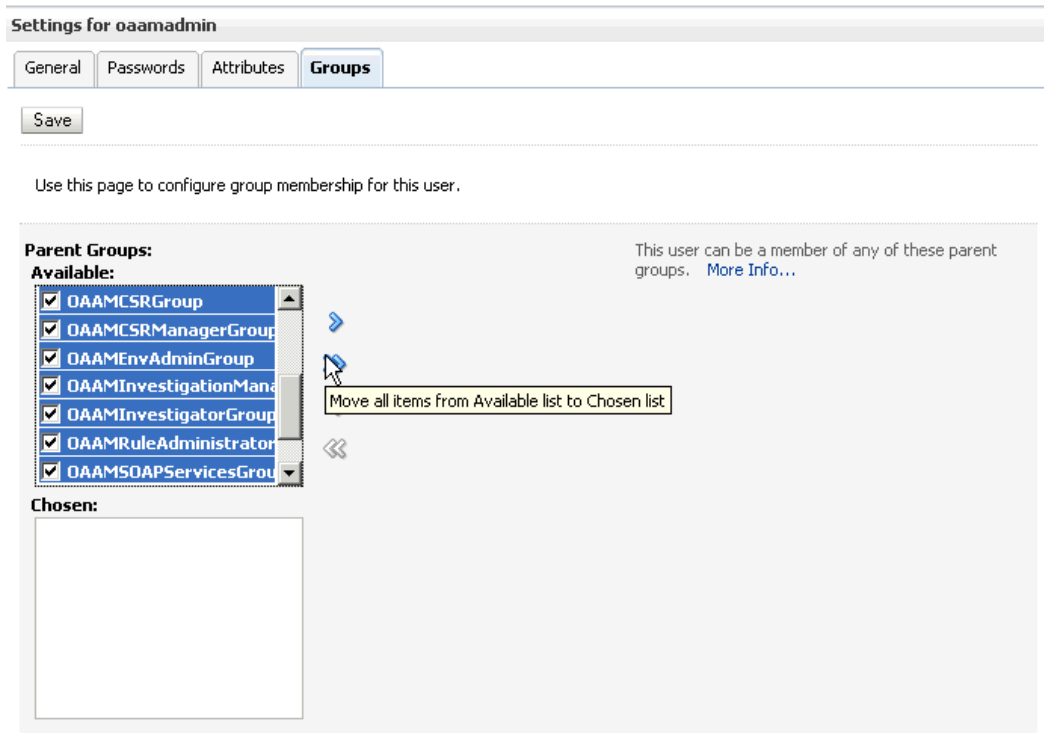
The password is associated with the login name for the new User.

\* **Password:** ●●●●●●●●

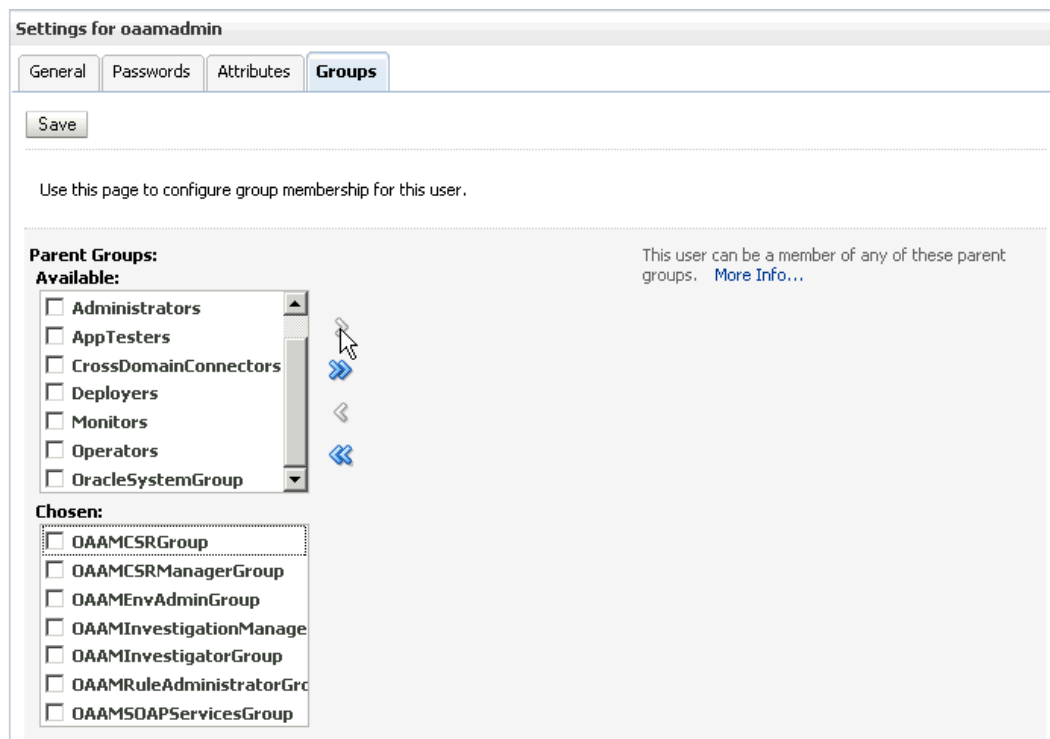
\* **Confirm Password:** ●●●●●●●●

Press OK when completed then reselect the new user **oaadmin**.

Once select check all of the OAAM Groups and then click on the **arrow** to move them to the user.



Press **Save** when complete.



At this point you can use a browser to test the new user go to [http://oaam1lg.homeunix.net:14200/oaam\\_admin](http://oaam1lg.homeunix.net:14200/oaam_admin)

## 7. Modify oam-config.xml

Using WordPad modify the oam-config.xml file that is located at:

D:\Oracle\Middleware\user\_projects\domains\IDM\_domain\config\fmwconfig

In the file locate the line:

```
<Setting Name="OAMEnabled" Type="xsd:boolean">false</Setting>
```

change false to true.

## 8. Start OAAM\_ADMIN

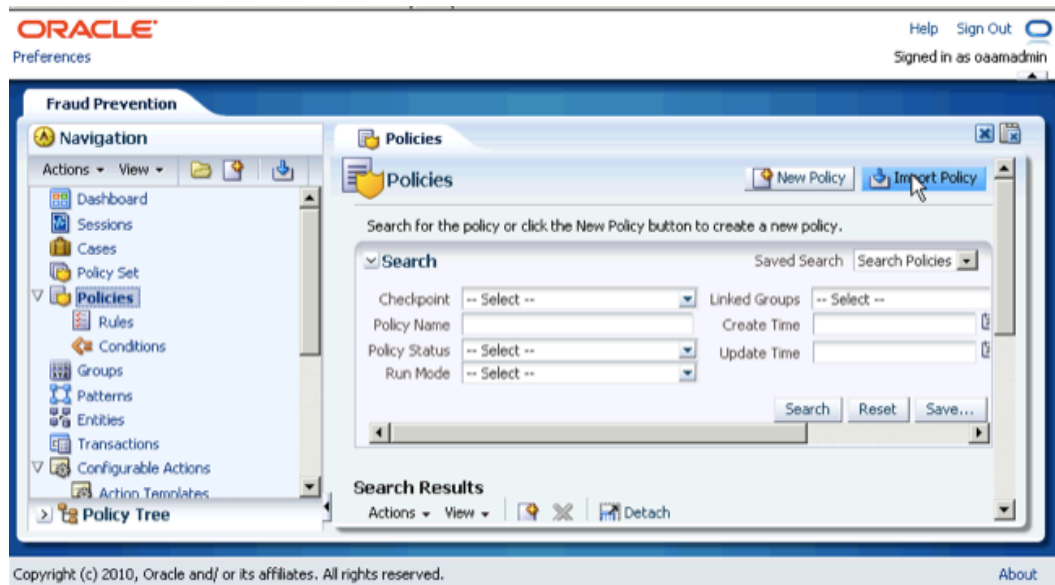
In a DOS Command window do the following to start the oaam\_admin\_server1:

```
d:  
cd: \oracle\Middleware\user_projects\domains\IDM_domain\bin  
startManagedWeblogic.cmd oaam_admin_server1
```

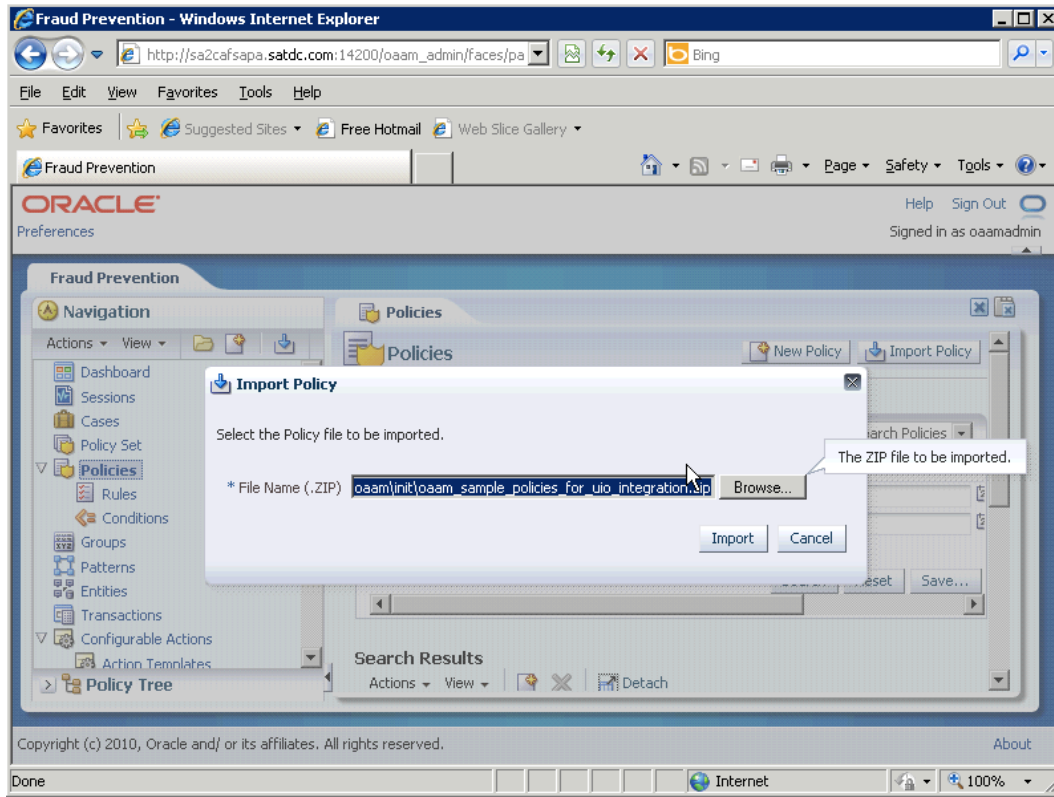
Enter the username: weblogic and password. Wait for the server to report that it has reached the **RUNNING** state before continuing.

## 9. Load Necessary Policies and Questions into OAAM

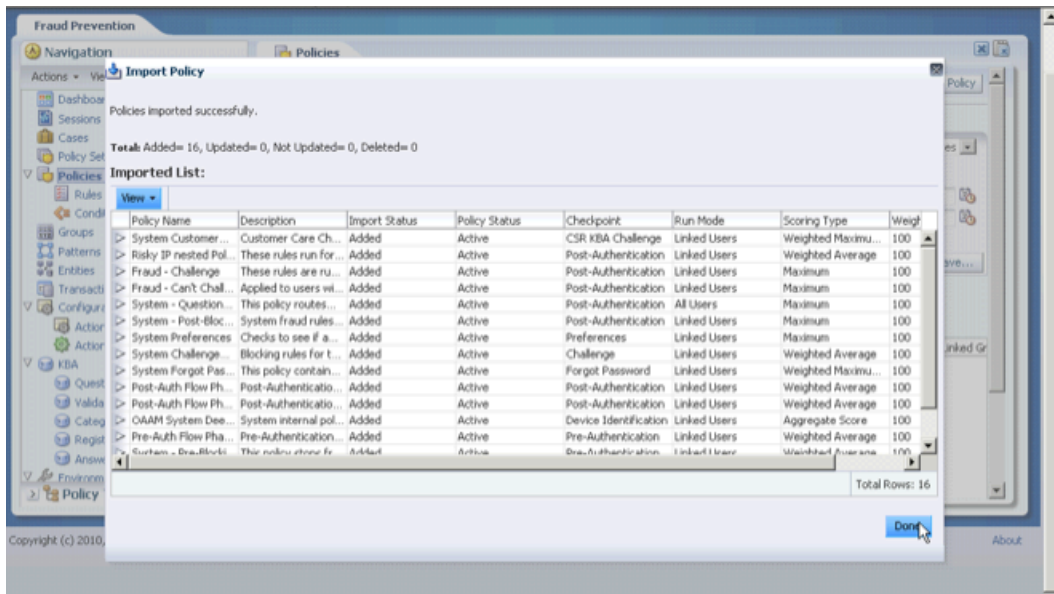
Log into the OAAM admin console at [http://oaam1lg.homeunix.net:14200/oaam\\_admin](http://oaam1lg.homeunix.net:14200/oaam_admin) as oaamadmin. Double click on the **Policies** hyperlink in the left pane and then click on the **Import Policy** button:



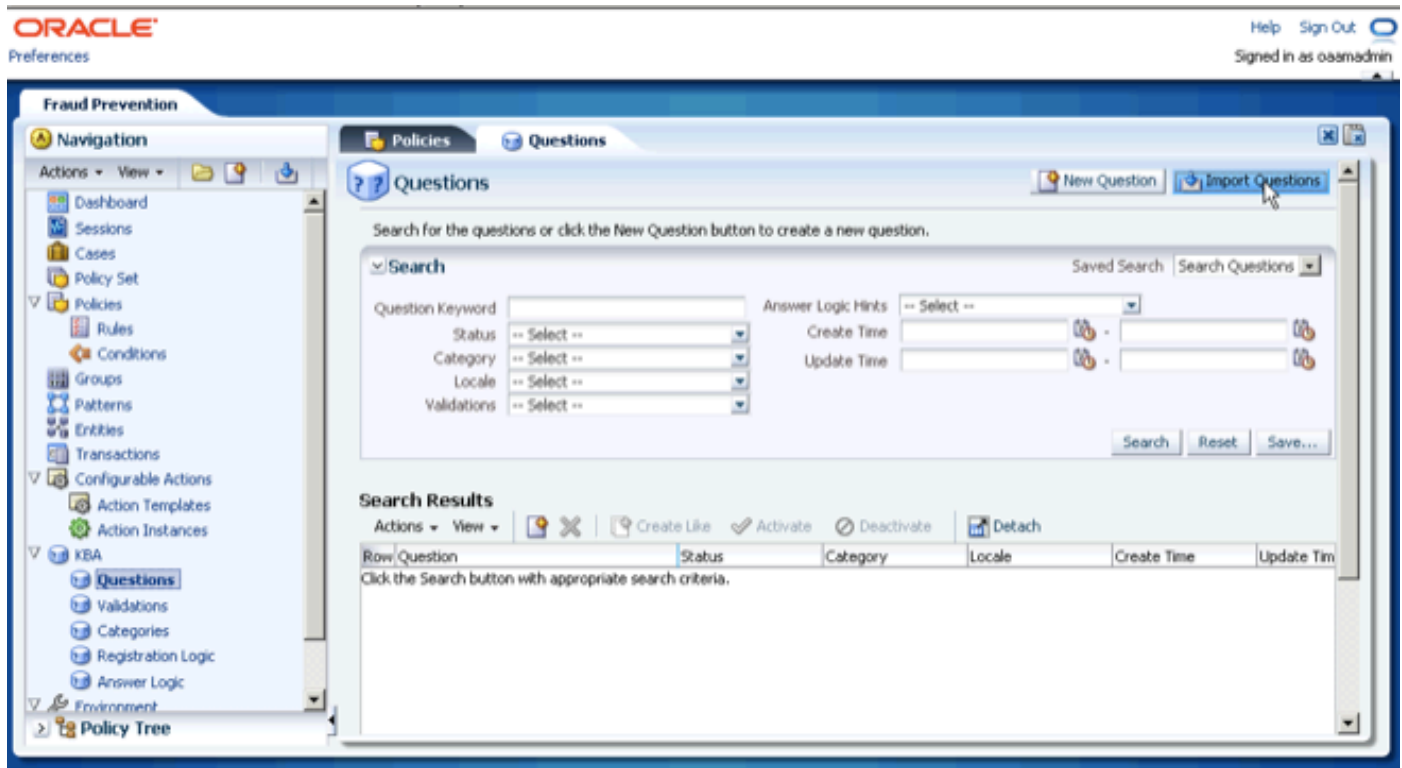
Select **d:\oracle\Middleware\Oracle\_IDM2\oam\init\oam\_sample\_policies\_for\_uio\_integration.zip** and click the **Import** button:



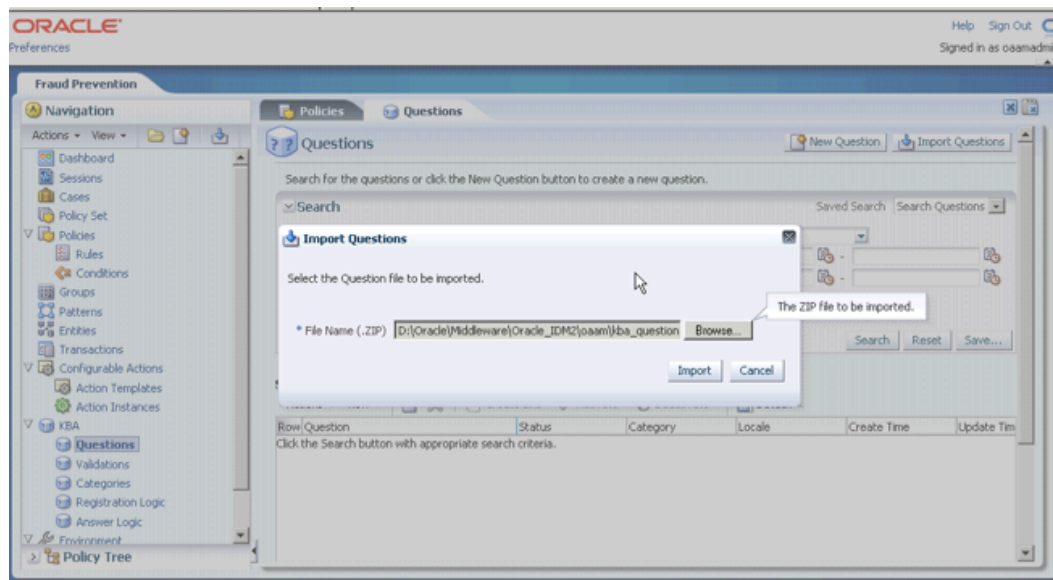
Once the Policies have been imported click **Done**:



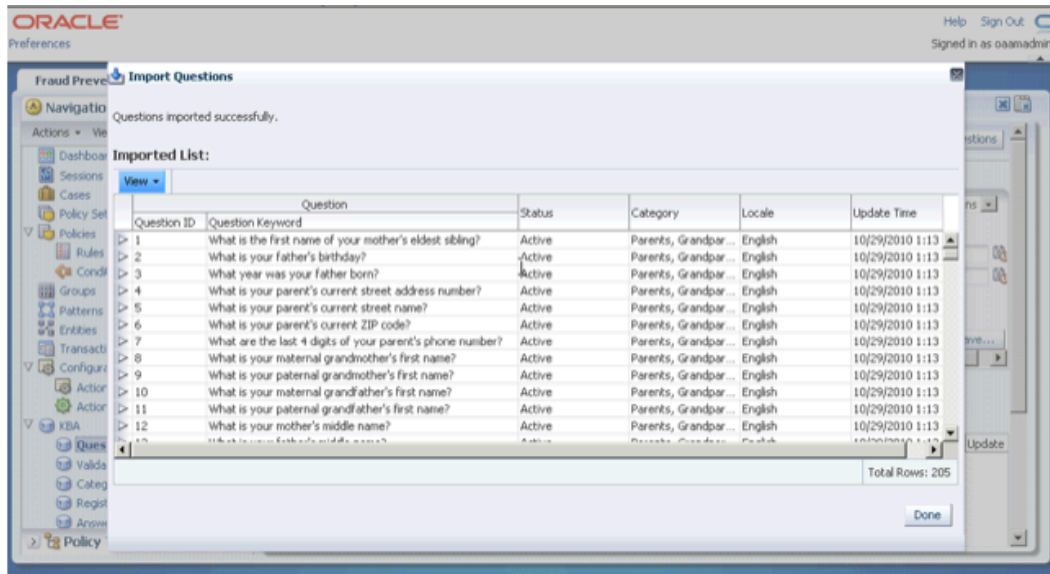
Next import the Knowledge based questions by clicking on the **Questions** Hyperlink then the **Import Questions** button:



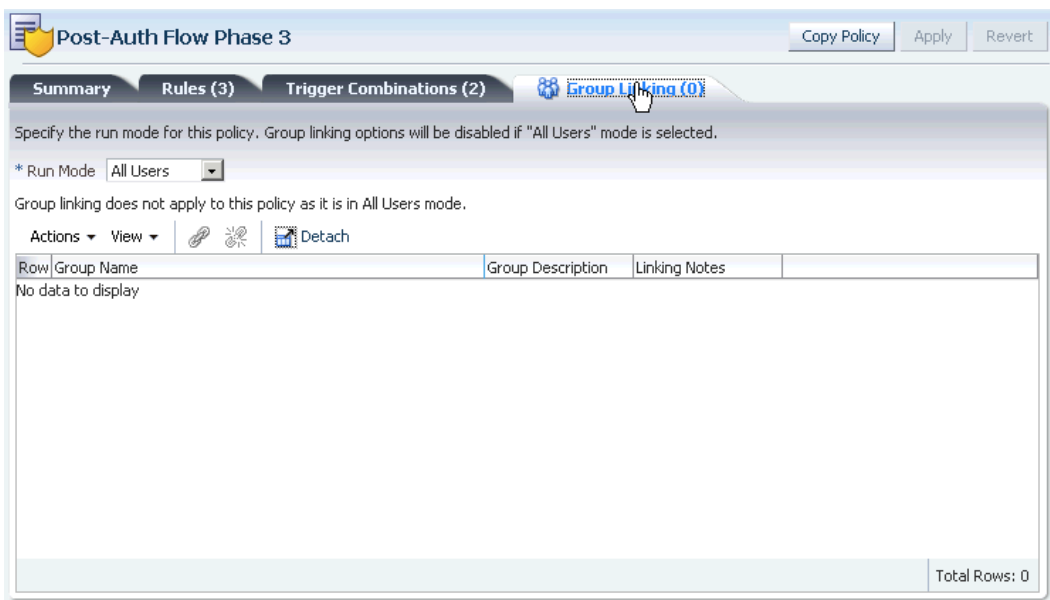
Import the English Questions from `d:\oracle\Middleware\Oracle_IDM2\oaam\init\kba_questions` and then click the **Import** Button:



Once imported click on **Done**:



Next the Post Authentication Policy 3 must be modified. Click on the Hyperlink for the policy and on the Group tab changed linked users to **All Users**. Save the changes.



## 10. Shutdown OAM\_ADMIN Server

There is not sufficient memory to keep all of the WebLogic servers running. The oam\_admin\_server1 is only needed for the above configuration. The production environment only requires the oam\_server1 that will be started later.

Shutdown the process by doing a Control C in the command window that has oam\_admin\_server1 running in it.

## 11. Start OAM\_SERVER

In a DOS Command window do the following to start the oam\_server\_server1:

```
d:  
cd: \oracle\Middleware\user_projects\domains\IDM_domain\bin  
startManagedWeblogic.cmd oam_server_server1
```

Enter the username: weblogic and password. Wait for the server to report that it has reached the **RUNNING** state before continuing.

## 12. Modify JDBC resource in WebLogic

When oam\_server\_server1 started it create a JDBC resource. This resource must be assigned to the oam\_server1 WebLogic server. Using a browser go to the WebLogic Administration server at: <http://oam11g.homeunix.net:7001/console>.

Click on Services then Database Resources. Locate the OAAM\_SERVER\_DS resource. Lock the environment by clicking on the Lock button in the upper left corner of the admin console. Now open the OAAM\_SERVER\_DS resource and click on the **Target** tab. Once there you are present a list of WebLogic servers that are available. Check the box beside oam\_server1. (Leave the existing check beside oam\_server\_server1) Save your changes. Before these changes take affect they must be activated. Click on the Activate button in the upper left corner of the Admin console. (This button replaced the Lock button that was previously used)

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled "Settings for OAAM\_SERVER\_DS" and has several tabs: Configuration, **Targets**, Monitoring, Control, Security, and Notes. The "Targets" tab is active, displaying a list of servers with checkboxes. The servers listed are AdminServer, oam\_admin\_server1, oam\_server\_server1, and oam\_server1. The checkboxes for oam\_server\_server1 and oam\_server1 are checked, while AdminServer and oam\_admin\_server1 are unchecked. There are "Save" buttons above and below the list. The left sidebar shows the "Domain Structure" tree with "JDBC" expanded to "Data Sources".

## 13. Shutdown OAAM\_SERVER Server

There is not sufficient memory to keep all of the WebLogic servers running. The oam\_server\_server1 is only started to create the JDBC resource. The production environment only requires the oam\_server1 that will be started later.

Shutdown the process by doing a Control C in the command window that has oam\_server\_server1 running in it.

## 14. Start OAM\_SERVER

In a DOS Command window do the following to start the oam\_server1:

```
d:  
cd: \oracle\Middleware\user_projects\domains\IDM_domain\bin  
startManagedWeblogic.cmd oam_server1
```

Enter the username: weblogic and password. Wait for the server to go to the RUNNING state before continuing.

## 15. Test the configuration

At this point all the configuration of OAAM is completed. To test the configuration using a browser go to:

<http://oam11g.homeunix.net:7001/approver>

You should be prompted to enter a username. Then on a separate screen you will be prompted for your password. Once the username and password is validated you will be asked to answer 3 personal questions. Once complete you should be taken to the approver application.

## 16. Appendix: OID Work Around

The bug that was uncovered with OAAM/OAM integration is that any configuration changes that are made to OAM disables OAAMBasic. So when the OID User Store is added to OAM the end result is that the

```
<Setting Name="OAAMEnabled" Type="xsd:boolean">true</Setting>
```

is reset to **false**. It has not been tested but I believe after the configuration change is made and oam\_server1 is shutdown the value can be set back to **true** and the oam\_server1 restarted.