

Oracle Access Manager 11gR1

Hyperion

Single Sign-On Configuration

Revision History

Date	Version	Description	Author
12/05/10	V1	Oracle Access Manager 11gR1 Hyperion Single Sign-On Configuration	Jeff Nester (Oracle)

Table of Contents

1. Configure Hyperion WebGate to Redirect Traffic	2
2. Configure the OAM Policy	2
3. Configure the WORLD group in OID	3
4. Configure Hyperion	5

1. Configure Hyperion WebGate to Redirect Traffic

The Hyperion WebGate redirection configuration is different than PeopleSoft and OBIEE. Hyperion is not running in WebLogic and therefore requires a different proxy technique. We will configure the OHS instance supporting the Hyperion integration as a reverse proxy.

Assumptions: The OHS that will reverse proxy to Hyperion is installed on webhost.oracle.com and the name of the OHS instance is **hype**. The Hyperion application is available at hyperion.oracle.com port **9000**. Oracle Access Manage is installed on oamserver.oracle.com. These instructions also assume that the WebGate is already and configured in the hype OHS instance and registered with OAM as **hypeOHSOAM11G**.

Configure OHS as a reverse proxy by doing the following steps:

First modify the **httpd.conf** file located at **D:\Oracle\Middleware\Oracle_WT1\instances\instance1\config\OHS\hype** on webhost.oracle.com and append the following lines to the file:

```
ProxyPass / http://hyperion.oracle.com:9000/  
ProxyPassReverse / http://hyperion.oracle.com:9000/
```

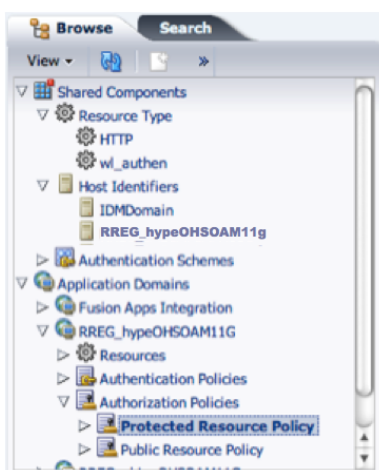
Restart the OHS server by doing the following in a command window:

```
d:  
cd \oracle\Middleware\Oracle_WT1\instances\instance1\bin  
opmnctl.bat restart-proc ias-component=hype
```

2. Configure the OAM Policy

Login to the oamconsole at <http://oamserver.oracle.com:7001/oamconsole> as weblogic

Double Click on Application Domains → RREG_hypeOHSOAM11G → Authorization Policies → Protected Resource Policy:



Click on the Responses tab and specify the Response as shown below:

The screenshot shows the 'Authorization Policy' configuration window with the 'Responses' tab selected. The policy name is 'Protected Resource Policy'. The description is 'Policy set during domain creation. Add resources to this policy to protect them.' The 'Use Implied Constraints' checkbox is checked. The 'Responses' table contains one entry:

Name	Type	Value
HYPLOGN	Header	\$user.attr.uid

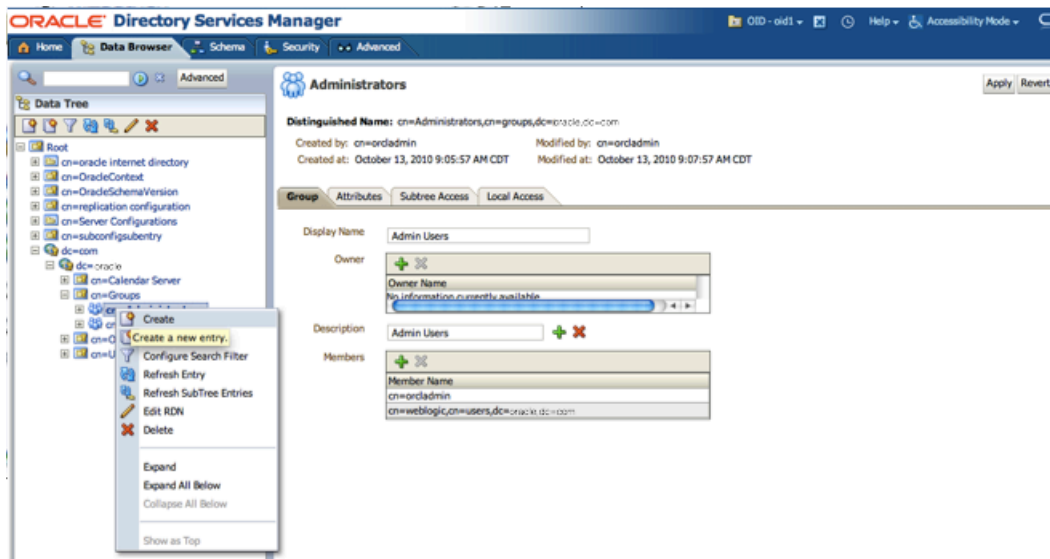
Name: HYPLOGN, Type: Header, Value is \$user.attr.uid

3. Configure the WORLD group in OID

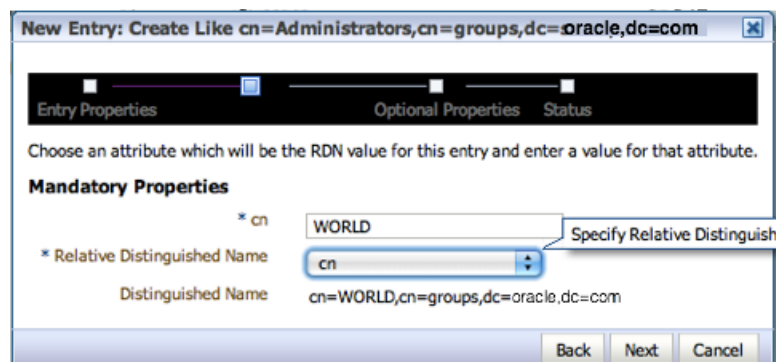
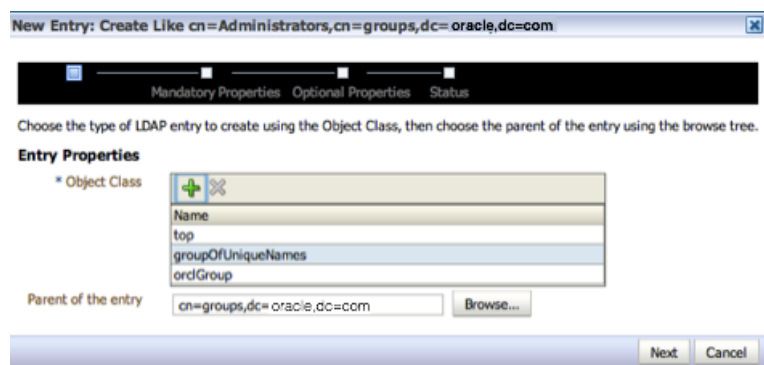
Using a browser go to <http://oamserver.oracle.com:7005/odsm> and connect to the OID using cn=orcladmin.

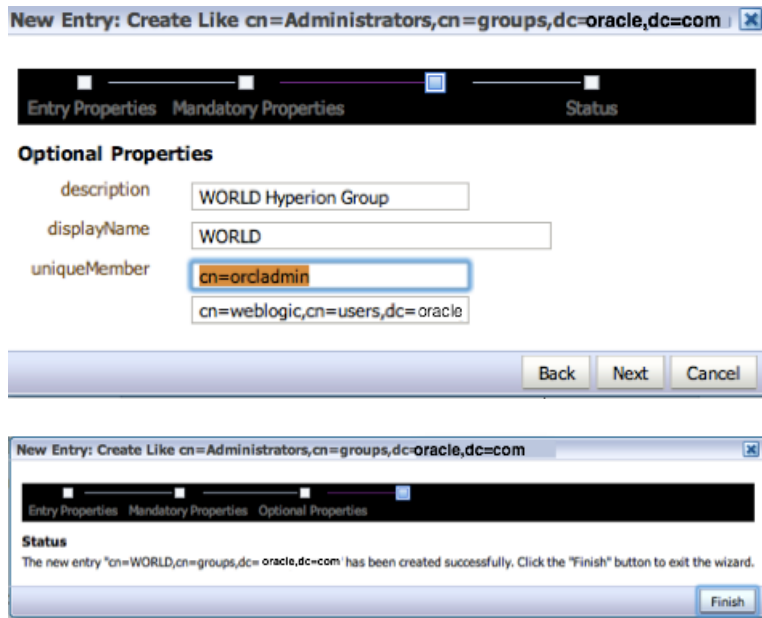
The screenshot shows the 'Connect' dialog box for 'OID - oid1'. The 'User Name' field contains 'cn=orcladmin', the 'Password' field is masked with asterisks, and the 'Start Page' dropdown is set to 'Home'. The dialog includes a 'Remove' button, a 'Connect' button, and a 'Cancel' button. Copyright information for Oracle is displayed at the bottom.

Go to the **Data Browser** tab and locate the **Administration** group and right click on it and select **Create Like**:



Enter the data as shown below:

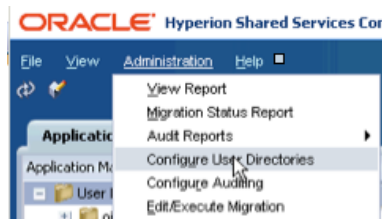




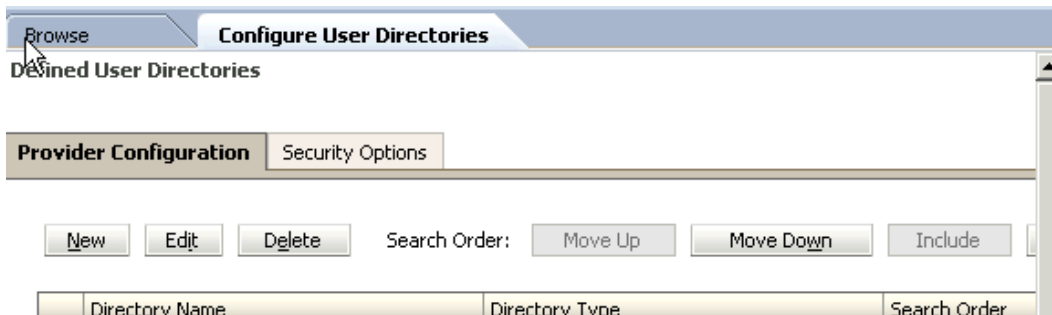
Add all Hyperion users that are in OID to this new Group.

4. Configure Hyperion

Login to Hyperion by going to <http://hyperion.oracle.com:9000/workspace> as the user Admin. Under Administration select **Configure User Directories**:



Click on the New Button:



Select **LDAP** and click **Next**:

The screenshot shows the 'Configure User Directories' wizard. The 'Directory Type' section is titled 'Choose the Directory Type'. There are four radio button options: 'Lightweight Directory Access Protocol(LDAP)' (selected), 'Microsoft Active Directory(MSAD)', 'SAP', and 'Relational Database(Oracle, DB2, SQL Server)'. At the bottom, there are 'Help', 'Next', and 'Cancel' buttons.

Enter the appropriate data for OID and click **Next**:

The screenshot shows the 'Configure User Directories' wizard at Step 1: LDAP Connection Information. The 'Server Information' section contains the following fields and values:

- Directory Server: Oracle Internet Directory (dropdown)
- * Name: oid
- * Host Name: oamserver.oracle,dc=com
- * Port: 3060
- SSL Enabled:
- * Base DN: dc=satdc,dc=com (with a 'Fetch DNs' button)
- ID Attribute: orclguid
- Maximum Size: 0
- Trusted:
- Anonymous Bind:
- * User DN: cn=orcladmin (with an 'Append Base DN' checkbox)
- * Password: [masked]

At the bottom, there is a 'Show Advanced Options' checkbox and 'Help', 'Back', 'Next', 'Save', and 'Cancel' buttons.

Enter **cn=orcladmin** and click the **Auto Configure** button:

Configure User Directories

1. LDAP Connection Information > **2. LDAP User Configuration** > 3. LDAP Group Configuration >

User Configuration

Enter the unique identifier of a user in the directory and click Auto Configure to detect user configuration

cn=orcladmin

User RDN:

Login Attribute:

First Name Attribute:

Last Name Attribute:

Email Attribute:

Object Class:

Show Advanced Options

After the screen automatically fills in click the **Next** button:

Configure User Directories

1. LDAP Connection Information > **2. LDAP User Configuration** > 3. LDAP Group Configuration >

User Configuration

Enter the unique identifier of a user in the directory and click Auto Configure to detect user configuration

cn=orcladmin

User RDN: cn=Users

Login Attribute: cn

First Name Attribute: givenName

Last Name Attribute: sn

Email Attribute: mail

Object Class:

person

Show Advanced Options

Now check the support Groups checkbox and then enter **cn=World** and click **Auto Configure**:

Browse **Configure User Directories**

1. LDAP Connection Information > 2. LDAP User Configuration > 3. LDAP Group Configuration >

Support Groups

Group Configuration

Enter the unique identifier of a group in the directory and click Auto Configure to detect group configuration

Group RDN:

Name Attribute:

Object Class:

Show Advanced Options

Help

Once the Screen has automatically filled in click **Save**:

LDAP Connection Information LDAP User Configuration **LDAP Group Configuration**

Support Groups

Group Configuration

Enter the unique identifier of a group in the directory and click Auto Configure to detect group configuration

Group RDN:

Name Attribute:

Object Class:

Show Advanced Options

Help

Next we enable Single Sign-On click on the Security Options tab and check the **Show Advanced Options**. Now Check the **Enable SSO** checkbox and select **Oracle Access Manager** as the provider and click **Save**:

Browse **Configure User Directories**

Defined User Directories

Provider Configuration **Security Options**

Basic Configuration

Token Timeout: 480 mins

Enable HTTP Access to Security Configuration:

SAP Keystore Timeout: secs

Show Advanced Options

Delegated User Management

Enable Delegated User Management Mode:

Single Sign-On Configuration

Enable SSO:

SSO Provider or Agent: Oracle Access Manager

SSO Mechanism: Custom HTTP Header HYPLOGIN

Custom Module

Authentication Module:

Help Save Cancel

At this point the entire configuration is completed and Hyperion must be restarted.

NOTE: We have found that if you reboot Hyperion the database connections are not released on the database server. If you do not restart the database Hyperion will fail to restart.