Using Secure Enterprise Search with Microsoft's Active Directory

An Oracle White Paper
May 2006

Table of Contents:

Introduction

So you've just installed Secure Enterprise Search. You know you need to use Oracle Internet Directory (OID) for secure searching, but your company uses Active Directory as its directory standard. What do you do?

This paper runs you through the steps necessary to install OID, and set up External Authentication against Active Directory.

Much of this information is available elsewhere, but figuring out exactly which steps are required simply to use Secure Enterprise Search can be something of a minefield.

Assumptions

1. Secure Enterprise Search has been installed on a Linux machine with no other Oracle products present, using the default name 'SES' and default port 7777.
2. The name of this linux machine is **seshost.us.example.com**
3. Active Directory is installed on a Windows 2003 server called **adhost.us.example.com.** The domain is called **ADDOM**. AD uses the default LDAP ports of 389 and 636.
4. OID and Oracle Application Server are to be installed onto the same machine as Secure Enterprise Search (seshost.us.example.com)

Installing OID

First we must install various components of Oracle Application Server (AS) to get our OID infrastructure. We need Oracle Application Server 10g Release 2 (not Release 3 – this does not include OID). At the time of writing the current release is 10.1.2.0.2, available for download from
http://www.oracle.com/technology/software/products/ias/htdocs/101202.html

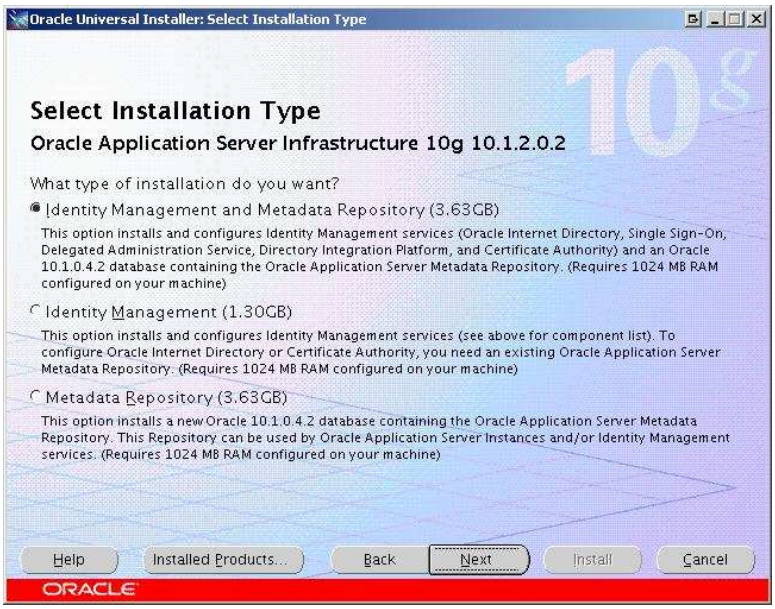
For Linux there are four CDs of data to download (we will assume from here on that you are installing OID onto a Linux system – there may be variations in commands on other operating systems).

Download all four files, and unzip each one into a directory called Disk1 through to Disk4 respectively. Change directory to Disk1, and run the Oracle Universal Installer via the command ./runInstaller

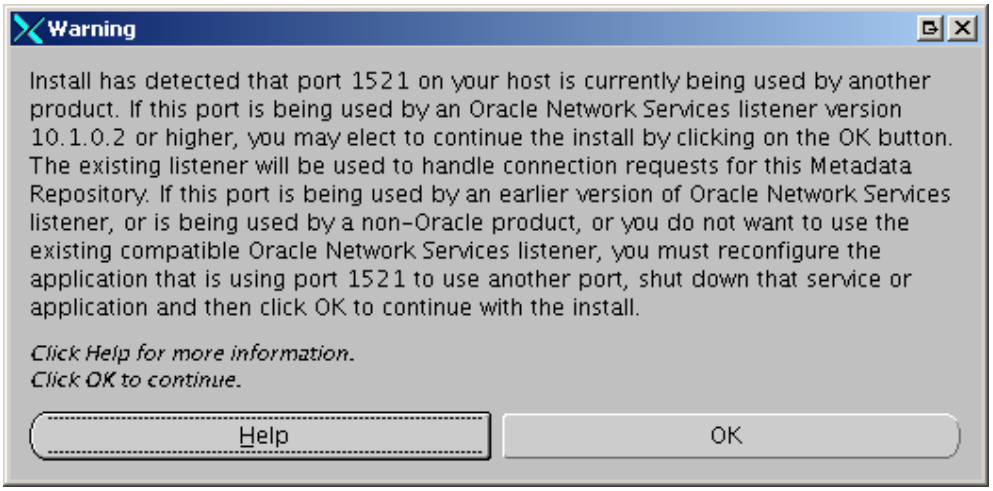
On the first screen you will be prompted for file locations. Select a location for your install directory (we will refer to this as $ORACLE_HOME from here on).

In the second screen you will be prompted to "Select a Product to Install". Choose the second option – Oracle Application Server Infrastructure".

Next you will be asked to "Select Installation Type". Choose the first option, Identity Management and Metadata Repository".

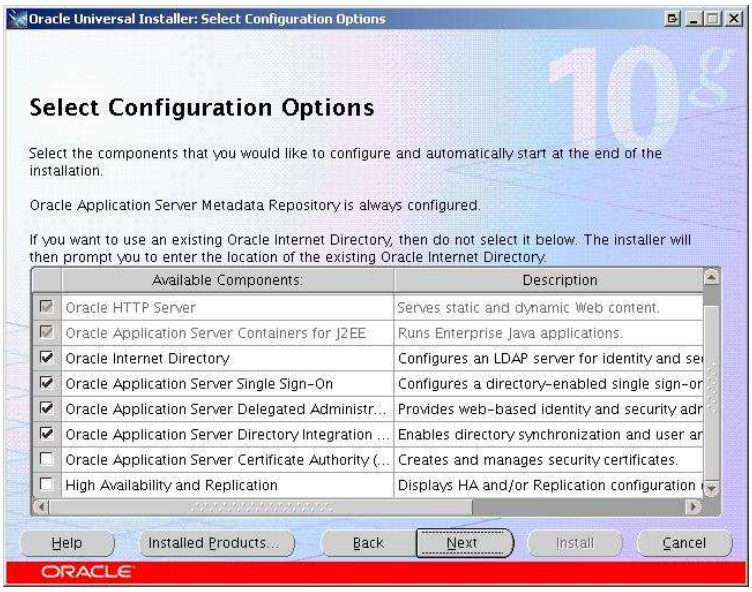


If you have already installed SES, you will get the warning box below. You can click OK – the two products can share a Network Services (TNS) listener.

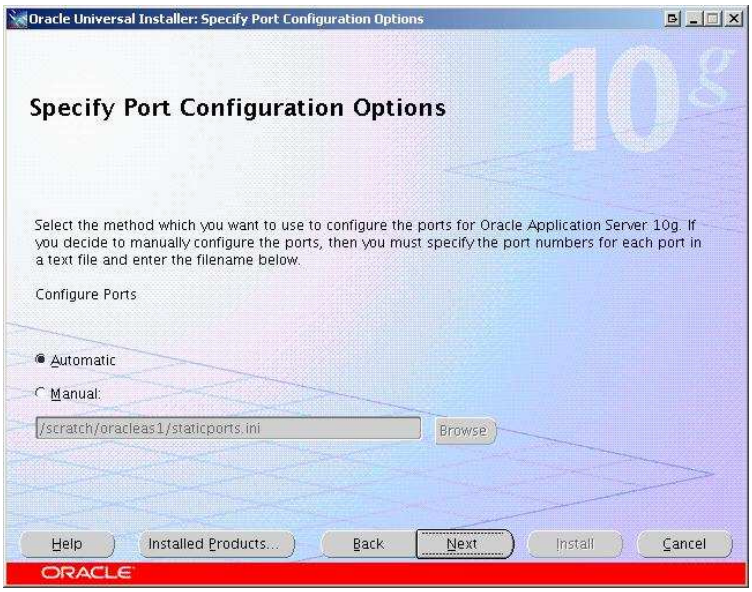


After the various checks have run, you will have to “Select Configuration Options”. Ensure the following boxes are all checked:

- Oracle Internet Directory
- Oracle Application Server Single Sign-On
- Oracle Application Server Delegated Administration
- Oracle Application Server Directory Integration

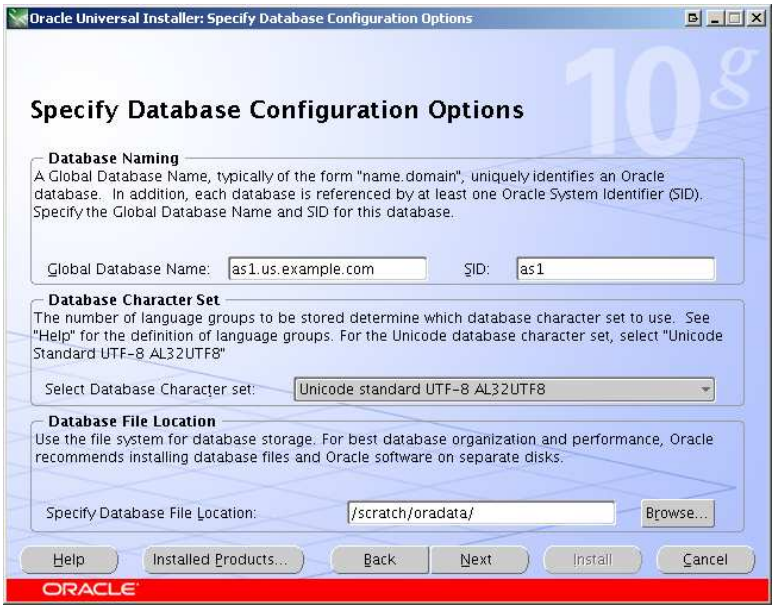


You will next be prompted for the Port Configuration. If this is an installation onto a fresh machine with only SES installed, you can accept the “Automatic” defaults. If you need to choose particular ports, you should edit the file Disk1/stage/Response/staticports.ini to set the required port numbers, save that somewhere and specify the file name in the installer screen.

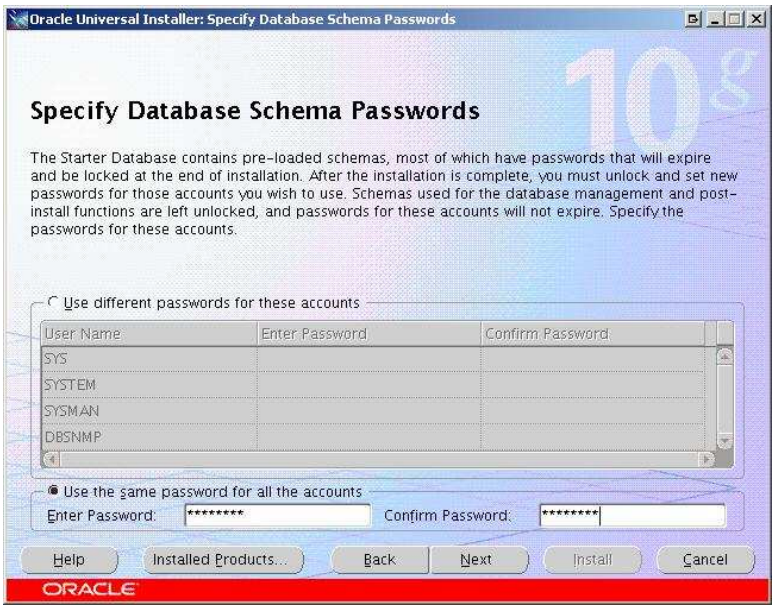


Next comes the Namespace setting. The suggested namespace will normally be derived from your machine’s domain, and you can accept that. Beware – if the suggested namespace is dc=localhost,dc=localdomain your network settings are probably not correct, and you are unlikely to be able to successfully build OID with Single Sign-On. Check you /etc/hosts file for a full name entry for the local machine, and if necessary run the “domainname” command as root to set your domain name correctly.

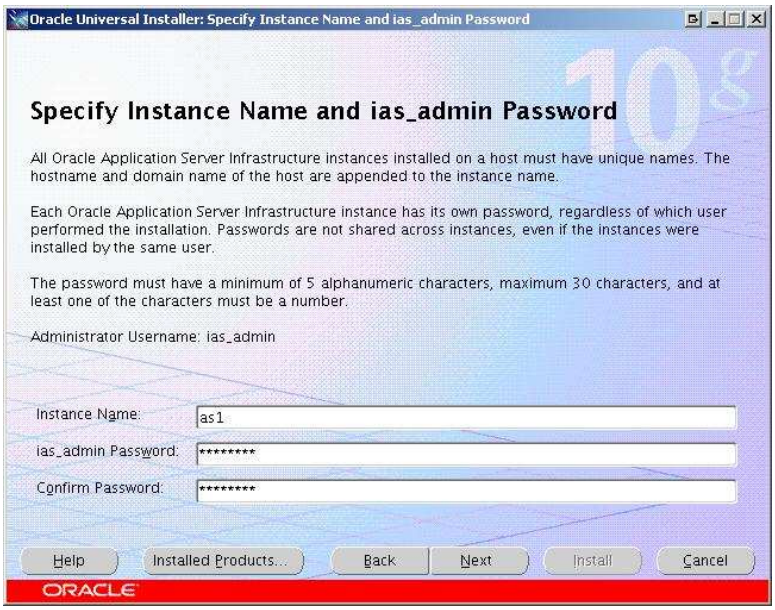
Now you will be asked for Global Database Name and SID. You can choose your own name here up to 8 characters – the GDN will be the SID with your domain as a suffix. The DB character set should be UTF-8 AL32UTF8.



Next you specify the passwords for various accounts. For simplicity of setup I would strongly suggest using the same passwords for all accounts – you can change them later if required.



In the final screen you specify an instance name (a name of your choice) and the password for ias_admin. The ias_admin password will be the password for orcladmin and other OracleAS related accounts. It is recommended to use the same password as in the last screen.



Oracle Application Server and OID will then proceed to install. This should take between 15 and 30 minutes on a typical machine.

Creating a Directory

After installation, set the environment variable ORACLE_HOME to your installation directory, and ensure that $ORACLE_HOME/bin is in your PATH. Make sure that your DISPLAY variable is set correctly to start X programs (I use "xterm" to test).

Then type "oidadmin&". This will fire up the OID Directory Manager gui. The first prompt will be:

Click on OK and you will be presented with an empty list of server names. Click on "Add" and add the name of the machine you have just installed onto. If you used a non-standard port you will need to specify that as well (from here on I'm going to assume you used standard ports).

Select the server you just added and click on "OK". You then get to a connect screen. Enter "cn=orcladmin" (or just "orcladmin") as the User, and the ias_admin installation password. Choose the server you just added on the drop-down list if not already shown.

You will now be in the main Directory Manager screen. We will need to come back to this later. You can either leave it open or close it and start it again with "oidadmin&" when you need it.

Next we'll check that the Active Directory server is visible from this machine. My AD server is ukp16509.uk.oracle.com and the domain name is "ADDOM":

```
ldapbind -h ukp16509.uk.oracle.com -p 389 -D Administrator@addom -w
'Passw0rd'
```

Where –h specifies the Active Directory host, -p the port number, -D the AD administrator name, and –w the administrator's password.

If successful you should receive a message:

```
bind successful
```

Express Configuration

Assuming our Active Directory meats certain assumptions, we can use Express Configuration to define the mapping between Active Directory and OID. The assumptions are listed at
http://download-west.oracle.com/docs/cd/B14099_19/idmanage.1012/b14085/odip_actdir003.htm#sthref794

If your AD installation *does not* fit these assumptions, you will need to follow the detailed steps in that manual for creating a mapping configuration.

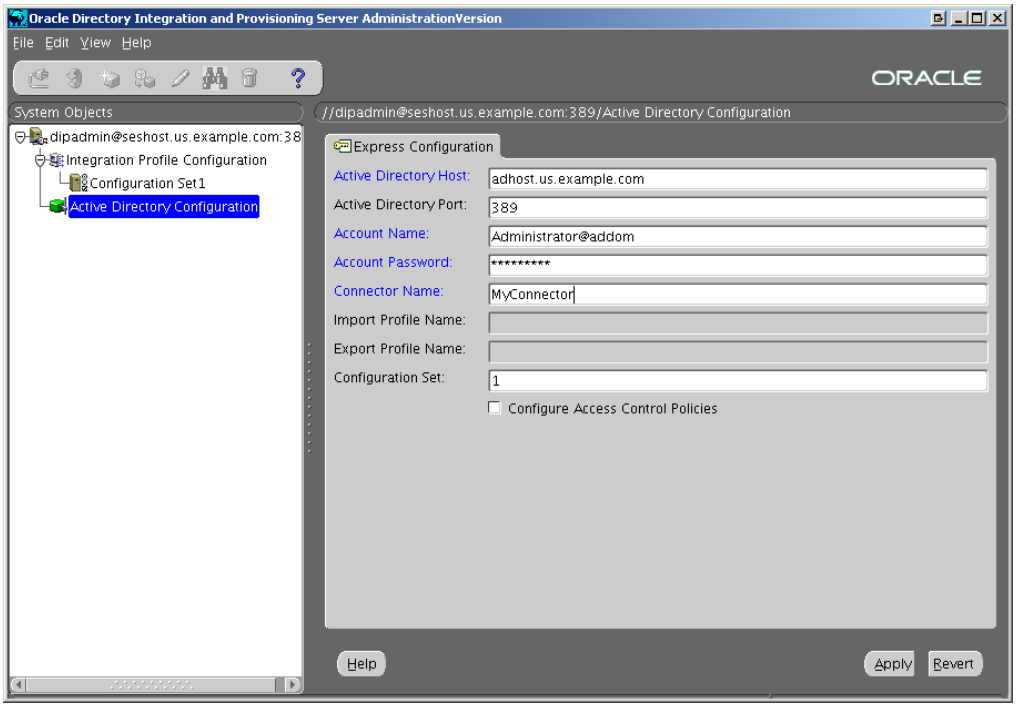
If your AD installation *does* fit these assumptions, proceed as follows:

Run the Directory Integration and Provisioning assistant:

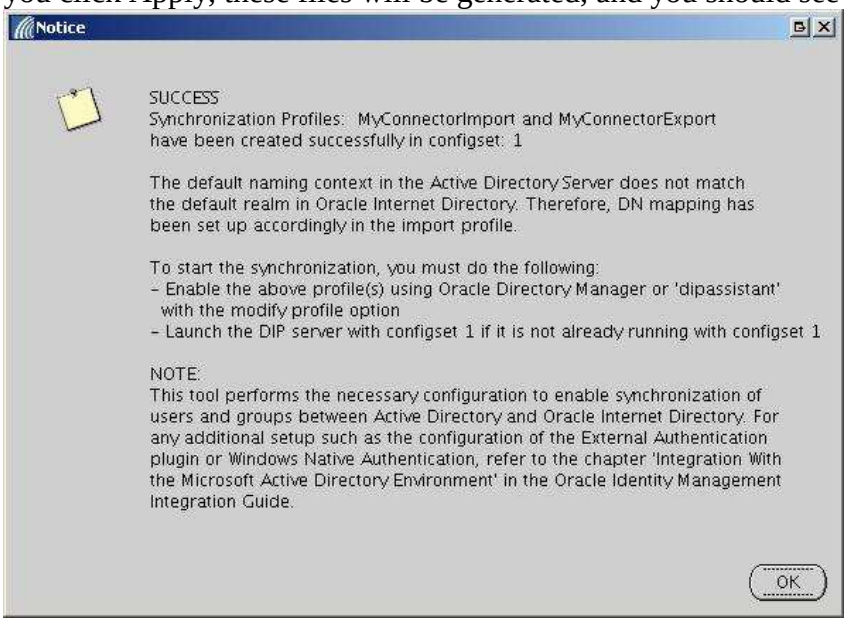
```
cd $ORACLE_HOME/ldap/odi/conf
dipassistant –gui
```

When prompted, leave the user set to “dipadmin” and enter the ias_admin password given during installation

This will start up a GUI tool as below:



Choose Active Directory Configuration and enter the required details. The account name should be Administrator@ADdomain. The Connector Name is a name you can specify – we will use MyConnector in this example. Configuration Set should be left at "1". This will generate two files, MyConnectorImport.map and MyConnectorExport.map. When you click Apply, these files will be generated, and you should see a message such as:



Now exit dipassistant.

The next step is the "bootstrap" process which actually performs the copy of current users from AD to OID. We do this from the command line:

```
Prompt$ cd $ORACLE_HOME/ldap/odi/conf
Prompt$ $ORACLE_HOME/bin/dipassistant bs -profile MyConnectorImport -
host seshost.us.example.com -port 389 -dn cn=orcladmin -passwd
password1 -log ../log/bs01.log -logseverity 15 -trace ../log/bs01.trc -
tracelevel 63
```

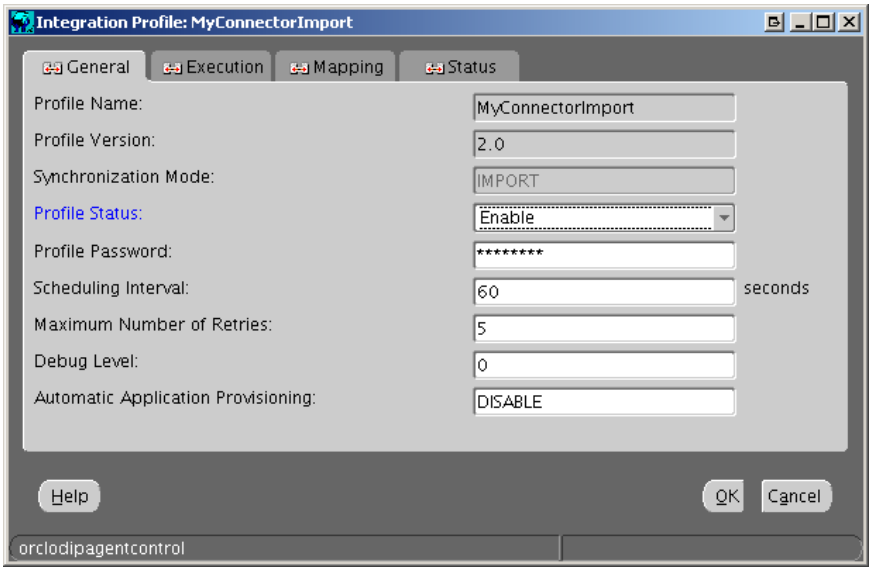
The output of this command on my system was:

```
-----------------------------------------------
Bootstrapping in progress.....

Bootstrapping completed.
 #entries read ..................... 22
 #entries filtered ................. 0
 #entries ignored .................. 0
 #successfully processed entries ... 22
 #failures ......................... 0

Please see the log file for more information.
-----------------------------------------------
```

After the bootstrap we need to enable the MyConnectorImport profile. Start up dipassistant again (see details above), go to Configuration Set1 under Integation Profile Configuration, double-click on MyConnectorImport and set Profile Status to “Enable”.



Now we need to start the Directory Integration Server “odisrv” demon which monitors AD and performs the actual synchronization. We do this using the oidctl command:

```
oidctl server=odisrv instance=2 configset=1 connect=as1
flags="port=389" start
```

The string used for “connect” here is the SID of our database.

Now we need to configure the Oracle Internet Directory external authentication “plugin” which enables Single Sign-On to check the user’s password with ActiveDirectory. We do this using a script provided with the OID installation:

```
sh $ORACLE_HOME/ldap/admin/oidspadi.sh
```

The dialog is presented below: Responses are in blue.[No Answer] indicates that no response was given to a particular question.

```
-----------------------------------------
  OID Active Directory Plug-in Configuration
-----------------------------------------

Please make sure Database and OID are up and running.

Please enter Active Directory host name: adhost.us.example.com
Do you want to use SSL to connect to Active Directory? (y/n) n
Please enter Active Directory port number [389]: 389
```

Please enter DB connect string: as1
Please enter ODS password: password1
Please enter confirmed ODS password: password1

Please enter OID host name: seshost.us.oracle.com
Please enter OID port number [389]: 389
Please enter orcladmin password: password1
Please enter confirmed orcladmin password: password1

Please enter the subscriber common user search base [orclcommonusersearchbase]: cn=Users,dc=us,dc=example,dc=com
Please enter the Plug-in Request Group DN: [No Answer]
Please enter the exception entry property [(!(objectclass=orcladuser))]: [No Answer]

Do you want to setup the backup Active Directory for failover? (y/n) n

Installing Plug-in Packages ...
…

Done.

Next, we need to enable the profiles which will copy over any changes and additions. Go to the OID Admin Screen (if still open, otherwise restart it with “oidadmin”).

Go to Plug-in Management, find the adwhencompare and adwhenbind entries, and set Plug-in Enable to “Enable” for both of them (if not already set).

Further information how to troubleshoot the external authentication plugin can be found in How to Configure OID External Authentication Plug-In

Checking External Authentication

Now check that external authentication is working correctly for LDAP. In my case, I have a user testuser01 in my AD. The AD name for this user is testuser01@addom.oracle.com, the OID full name is cn=testuser01,cn=users,dc=uk,dc=oracle,dc=com.

```
Prompt$ ldapbind -h adhost.us.example.com -D
"testuser01@addom.oracle.com" -w 'password'
bind successful
Prompt$ ldapbind -D "cn=testuser01,cn=users,dc=us,dc=example,dc=com" -w
'password'
bind successful
```

The first of these commands is checking directly against the AD , the second is checking against the local OID. Both have succeeded as evidenced by the “bind successful” output.

Optional: Turn off external authentication: Go into oidadmin, choose Plug-in Management, adwhencompare, and set Plug-in Enable to Disable. Try again

```
Prompt$ ldapbind -D "cn=testuser01,cn=users,dc=us,dc=example,dc=com" -w
'password'
Authentication fails insufficient privileges
```

Remember to enable the plugin after this test!

If these tests work, you could try changing the user’s password in AD and make sure you can still bind. If so, this proves that external authentication is working correctly.

Next try creating a new user in AD, and ensure you can access that new user using the ldapbind command. It will take (by default) a minimum of one minute for new users to appear in OID.

If new users are NOT appearing, try restarting the odi server:

```
Prompt$ oidctl server=odisrv instance=2 connect=as1 stop
Prompt$ sleep 30
Prompt$ oidctl server=odisrv instance=2 configset=1 connect=as1
flags="port=389" start
```

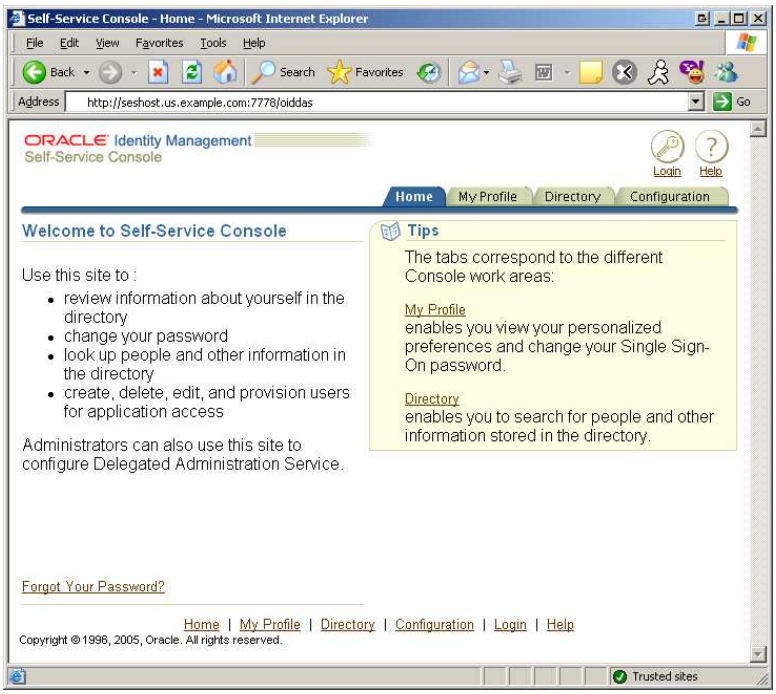
Further information how to configure and test the synchronization and external authentication can be found in Oracle Identity Management Integration Guide

Checking SSO

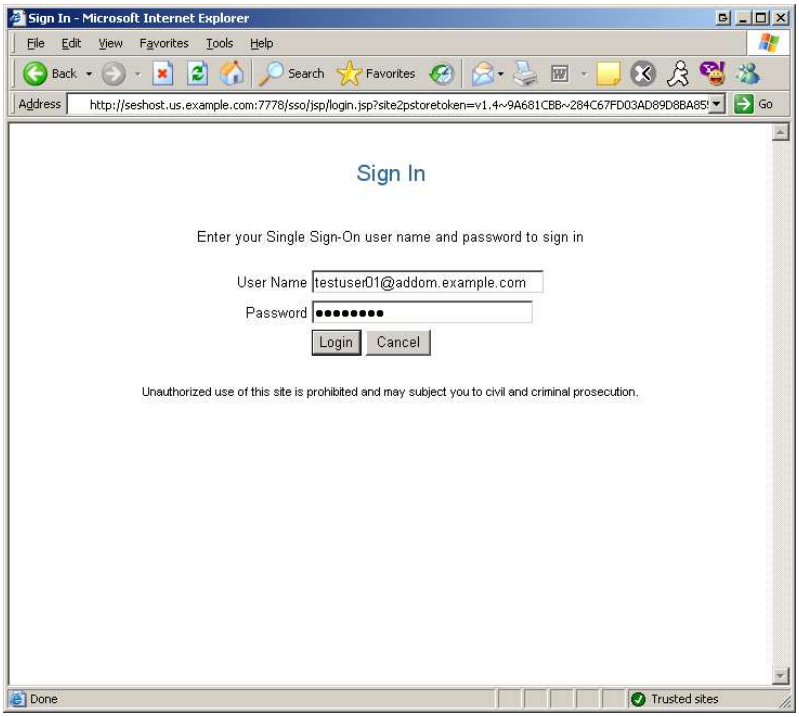
To ensure SSO is working correctly, go to a browser and open a URL like:
http://seshost.us.example.com:7778/oiddas -
where

seshost.us.example.com is the full name of the OID machine, and

7778 is the port for Oracle Application Server. Note that if you already installed Secure Enterprise Search was installed on a NON-default port (ie. Anything other than 7777), OracleAS will probably use port 7777.



This should bring you to the Self-Service Console. Click on the login button on the top right. Enter the AD name, eg. username@addomain.com and the AD password.



If all is well you should now be logged in – proving that SSO is working with external authentication from AD.

Linking Secure Enterprise Search with OID and SSO

This area is covered by the Secure Enterprise Search Administrator's Guide:
http://download-west.oracle.com/docs/cd/B28527_01/doc/search.1016/b19002/toc.htm
- but we'll summarize it here.

1. Install Secure Enterprise Search, if you have not already done so.
2. In the SES Administration screens, go to Global Settings, Directory Setup.
3. Enter the details for the OID server (Realm Distinguished Name would be dc=us,dc=example,dc=com for our example, and Administrator User Name is normally cn=orcladmin)
4. Set ORACLE_HOME and ORACLE_SID environment variables appropriately for your Secure Enterprise Search installation (ORACLE_HOME is the installation directory, ORACLE_SID is the "Search Server Name" – default "ses" – provided at install. Ensure $ORACLE_HOME/bin is in your path.
5. Edit $ORACLE_HOME/oc4j/j2ee/OC4J_SEARCH/config/http-web-site.xml and add the words `protocol="ajp13"` immediately after `<web site` So it now reads:
   ```
   <web-site port="7314" protocol="ajp13" display-name="Oracle
   Secure Search SSL Web Site">
   ```
6. Start SQL*Plus
   `sqlplus eqsys/installpassword`
   And run one of the following commands:
   For all content to be protected by SSO:
   exec eq_adm.set_secure_mode(3)
   For only secure content to be protected by SSO
   exec eq_adm.set_secure_mode(2)
   Then quit from SQL*Plus.
7. Restart the SES mid-tier using
   searchctl restart
   Note that SES will be unavailable at this point until the rest of the changes have been made.
8. Set ORACLE_HOME to installation directory for Oracle Application Server.
9. Edit $ORACLE_HOME/Apache/Apache/conf/mod_osso.conf Add the following within IfModule:
   ```
   <Location /search/query/ssoLogin.jsp>
      require valid-user
     AuthType Basic
   </Location>
   ```
   (For all content secured - mode 3 - remove /ssoLoin.jsp from the above)
10. Edit $ORACLE_HOME/Apache/Apache/conf/mod_oc4j.conf and add the following within IfModule:
    `Oc4jMount /search/* ajp13://server:ses_port`
    where server is the full name of your server, and ses_port is the original port number that was being used by SES (default 7777)
11. Restart the Application Server using the command
    `$ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server`

Now, if all goes well you should be able to access Secure Enterprise Search via the AS port, eg:
http://seshost.us.example.com:7778/search/admin and
http://seshost.us.example.com:7778/search/query

Go to the Query page URL, and click on the login button on the top right (If you haven't closed your browser since logging into OID you may find you're already logged in – so log out first). Log in using the syntax username@fulldomainname.

Logging in using ShortName

By default the SSO server uses OID attribute "uid"as login name. Currently we have to login using the full user@domain syntax. To change that so that we can log in using the AD login name "user", we need to make a change to OID.

There are two options to do this:

1st Option: Change the mapping rule Directory Integration server uses to map AD users to OID users. To do so

```
cd $ORACLE_HOME/ldap/admin/odi/conf
```

Edit MyConnectorImport.map

uid is set in the mapping file to be mapped to userprincipalname which is testuser01@addom.oracle.com

```
# Map the userprincipalname to the nickname attr by default
userPrincipalName: : :user:uid: :inetorgperson:userPrincipalName
```

You can disable this mapping rule (via #) and enable

```
# If this rule is enabled, userprincipalname rule needs to be disabled
#sAMAccountName: : :user:uid: :inetorgperson
```

After making these changes, run a command like:

```
$ORACLE_HOME/bin/dipassistant modifyprofile -profile MyConnectorImport
-host seshost.us.example.com -port 389 -dn cn=orcladmin -passwd
password1 odip.profile.mapfile=MyConnectorImport.map
```

This process is described in more detail in the Integration Guide Customizing Mapping Rules.

2nd Option: change the settings in Delegated Administration Services preferences from uid to eg. Cn as described in

Oracle Identity Management Guide to Delegated Administration

Eg.:

From a browser, enter the oiddas URL as used before, such as http://seshost.us.example.com:7778/oiddas

Login as orcladmin (with the ias_admin installation password), and click on the "Configuration" tab on the top right. Where it says "Attribute for Login Name", change the value from "uid" to "sn", and click on "Submit"

You will need to restart all AS processes, using:

```
$ORACLE_HOME/opmn/bin/opmnctl stopall
$ORACLE_HOME/opmn/bin/opmnctl startall
```

- but then after that you will be able to log in to SSO using the user's ShortName.

Process Complete!

You should now be able to use Active Directory users anywhere within Secure Enterprise Search that you could normally use OID users. In particular, you can create ACLs to protect datasources or documents by specifying AD users or groups.

Further References

Oracle Identity Management Integration Guide
Oracle Internet Administrator Guide
Oracle Application Server Single Sign-On Administrator Guide
Note:199222.1 How to Protect a MidTier Path with Single Sign-On (SSO) mod_osso
How to Configure OID External Authentication Plug-In

Roger Ford 10-May-2006
roger.ford@oracle.com

Using Secure Enterprise Search with Microsoft's Active Directory
March 2006
Author: Roger Ford
Contributing Author: Olaf Stullich

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com