

Active Directory to Oracle Internet Directory (OID) Integration

To integrate Oracle Application Server with Active Directory follow these steps.

Active Directory Synchronization

1. The ability to connect to Active Directory from Oracle may be verified using the following commands on appserver.oraclegiants.com:

```
cat oracle.env
```

```
export ORACLE_HOME=/d02/oracle/OID
```

```
export ORACLE_SID=orasso
```

```
export PATH=$PATH:$ORACLE_HOME/bin
```

```
cd $ORACLE_HOME/bin
```

```
./ldapbind -p 389 -h msad.appsdba.info -D "Administrator@appsdba.info" -w "Oracle123"
```

bind successful

You should see a message “**bind successful**”

2. The next step in the configuration process is to create a synchronization profile.

copy the following files from \$ORACLE_HOME/ldap/odi/conf directory to some other place:

```
copy activechg.map.master activechgimp.map <your specified dir>
```

```
copy activeexp.map.master activeexp.map <your specified dir>
```

Edit each of the map files substituting the DOMAIN RULES to match your configuration (see <Doc ID 235180.1>)

Modify DomainRules and AttributeRules as follows

```
vi /d02/oracle/OID/ldap/odi/conf/activechgimp.map
```

DomainRules

```
cn=users,dc=appsdba,dc=info:cn=users,dc=appsdba,dc=info:*,cn=users,dc=appsdba,dc=info  
###
```

AttributeRules

```
sn : : person : sn : : person  
uid : 1 : inetorgperson: cn : : person  
uid : 1 : inetorgperson: uid : : inetorgperson
```

```
DomainRules  
cn=users,dc=appsdba,dc=info:cn=users,dc=appsdba,dc=info:*,cn=users,dc=appsdba,dc=info  
###  
AttributeRules  
sn : : person : sn : : person  
uid : 1 : inetorgperson: cn : : person  
uid : 1 : inetorgperson: uid : : inetorgperson  
# attribute rule common to all objects  
objectguid: :binary: :orclobjectguid:string: :bin2b64(objectguid)  
ObjectSID: :binary: :orclObjectSID:string:orclADObject:bin2b64(ObjectSID)  
distinguishedName: : : :orclSourceObjectDN: :orclADObject  
# attribute rule for mapping windows organizationalunit  
ou: : :organizationalunit:ou: : organizationalunit:  
# attribute rule for mapping directory containers  
cn: : :container: cn: :orclContainer:  
# attribute rule for mapping director domains  
dc: : :domain: dc: :domain:
```

load the mapping file(s) into their respective profiles:

```
dipassistant mp -port 389 -dn cn=orcladmin -passwd oracle10g -profile ActiveChgImp  
odip.profile.mapfile=/d02/oracle/OID/ldap/odi/conf/activechgimp.map
```

Profile successfully modified.

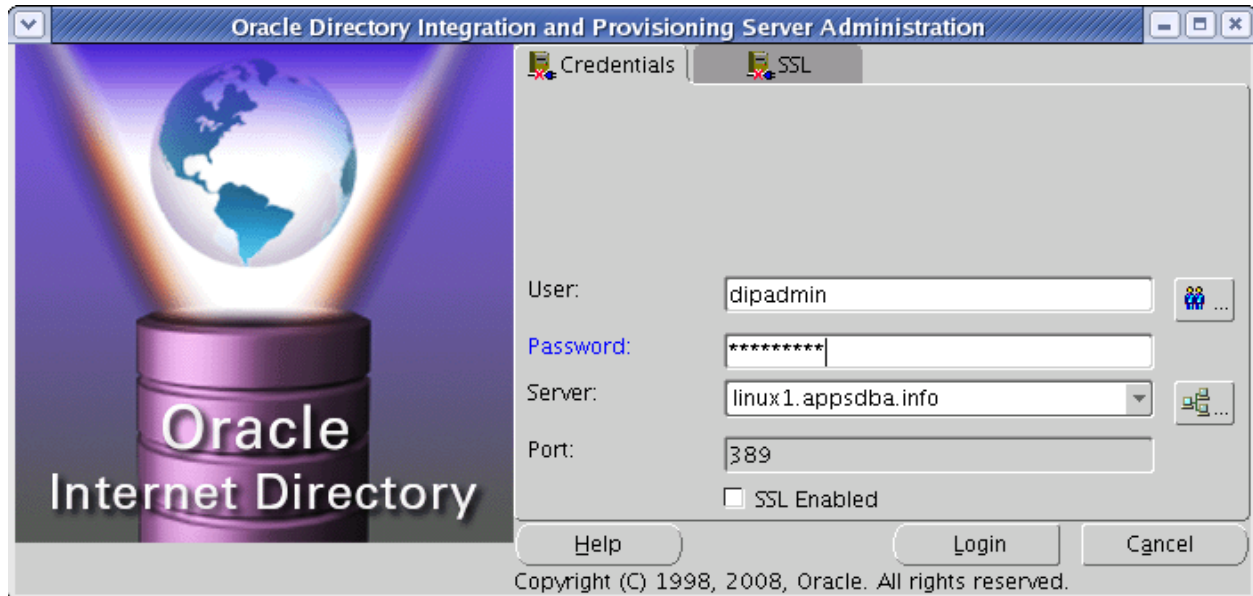
Run the following ldapsearch to obtain the last change number on OID

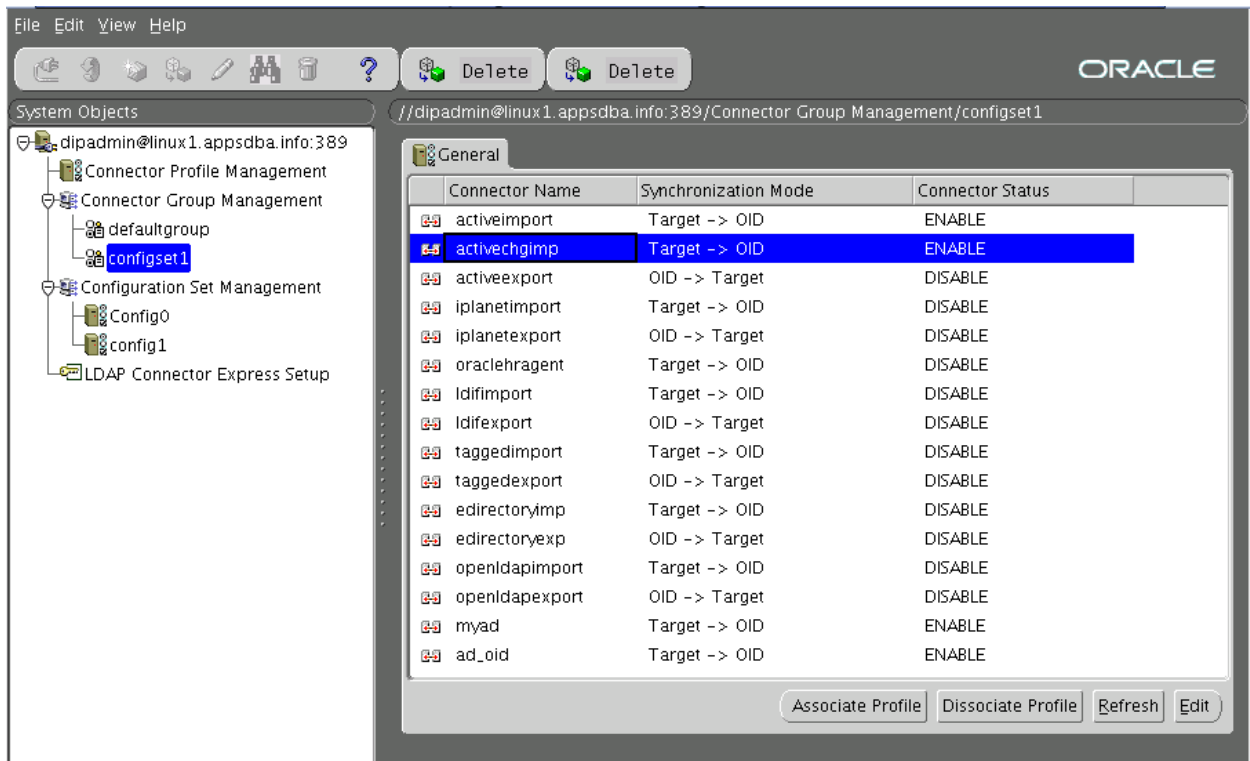
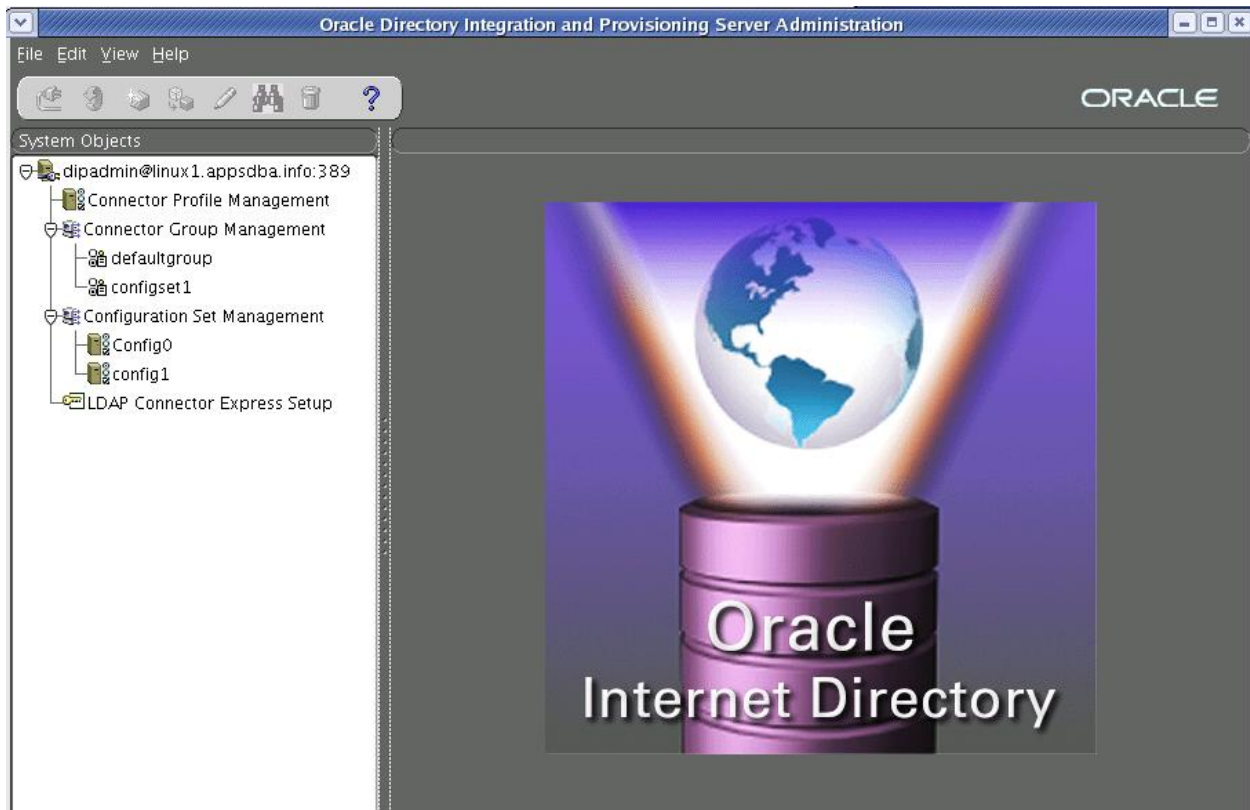
```
ldapsearch -p 389 -D "cn=orcladmin" -w "oracle10g" -b "" -s base "objectclass=*" lastchangenumber
```

lastchangenumber=2899

Verify the profile properties by launching dipassistant

dipassistant -gui





Click Edit

The screenshot shows a configuration window titled "Integration Profile: activechgimp". It has several tabs: "General", "Mapping", "Filtering", "Status", and "Others". The "General" tab is selected. The fields are as follows:

Connector Name:	activechgimp
Connected Directory Host:	msad.appsdba.info
Connected Directory Port:	389
	<input type="checkbox"/> Connected Directory SSL Enabled
Synchronization Mode:	Target -> OID
Connector Status:	Enable
Connected Directory Account:	Administrator@appsdba.info
Connected Directory Account Password:	*****
Interface Type:	LDAP
Profile Version:	2.0
Connected Directory Type:	Microsoft Active Directory

At the bottom, there are buttons for "Help", "OK", and "Cancel".

Verify that the PROFILE STATUS is set to ENABLE

For testing you may wish to set the scheduling interval to 20 seconds

Integration Profile: activechgimp

General Mapping Filtering Status Others

Domain Rules

Line No	Source Domain	Destination Domain	Do
1	cn=users,dc=appsdba,dc=info	cn=users,dc=appsdba,dc=info	*

Add Delete Edit

Attribute Rules


Line No	Source Objectclass	Source Attribute(s)
1	person	sn
2	inetorgperson	uid
3	inetorgperson	uid
4		objectguid
5		ObjectSID
6		distinguishedName

Add Delete Edit Validate Save to File

Help OK Cancel

Ready

Error

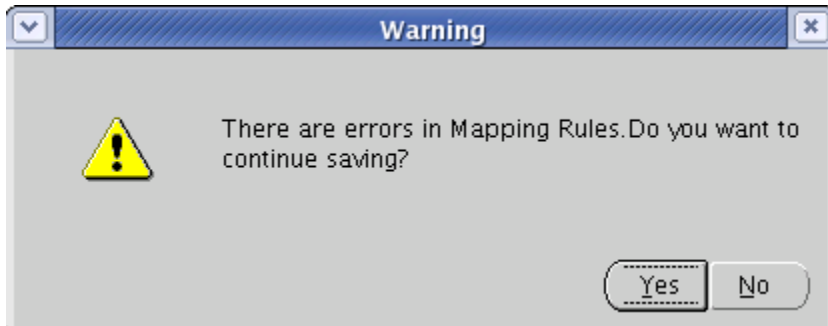
 ERRORS:

Error (line 5): source attribute 'objectsid' doesn't belong to object class 'top'
Error (line 5): destination attribute 'orclobjectsids' doesn't belong to object class 'top'
Error (line 30): destination attribute 'owner' doesn't belong to object class 'orclprivilegegroup'

WARNINGS:

Warning (line 10): Source attribute 'samaccountname' is optional for a required destination attribute 'orclsamaccountname'
Warning (line 10): Source attribute 'userprincipalname' is optional for a required destination attribute 'orclsamaccountname'
Warning (line 14): Source attribute 'samaccountname' is optional for a required destination attribute 'sn'
Warning (line 26): Source attribute 'cn' is optional for a required destination attribute 'cn'
Warning (line 31): Source attribute 'samaccountname' is optional for a required destination attribute 'orclsamaccountname'

OK Details



The above warnings can be ignored.
Refer to dipassistant -gui Tool Improperly Flagging Mapping Rules as Errors (Doc ID 1218873.1)

3> The first time you migrate data from AD to OID is known as bootstrap. To run the bootstrap execute the following

dipassistant bootstrap -port 389 -profile ActiveChgImp -dn cn=orcladmin -passwd oracle10g

```
[orasso@linux1 conf]$ dipassistant bootstrap -port 389 -profile ActiveChgImp -dn cn=orcladmin -passwd oracle10g
-----
Bootstrapping in progress.....

Bootstrapping completed.
#entries read ..... 20
#entries filtered ..... 0
#entries ignored ..... 0
#successfully processed entries ... 20
#failures ..... 0
```

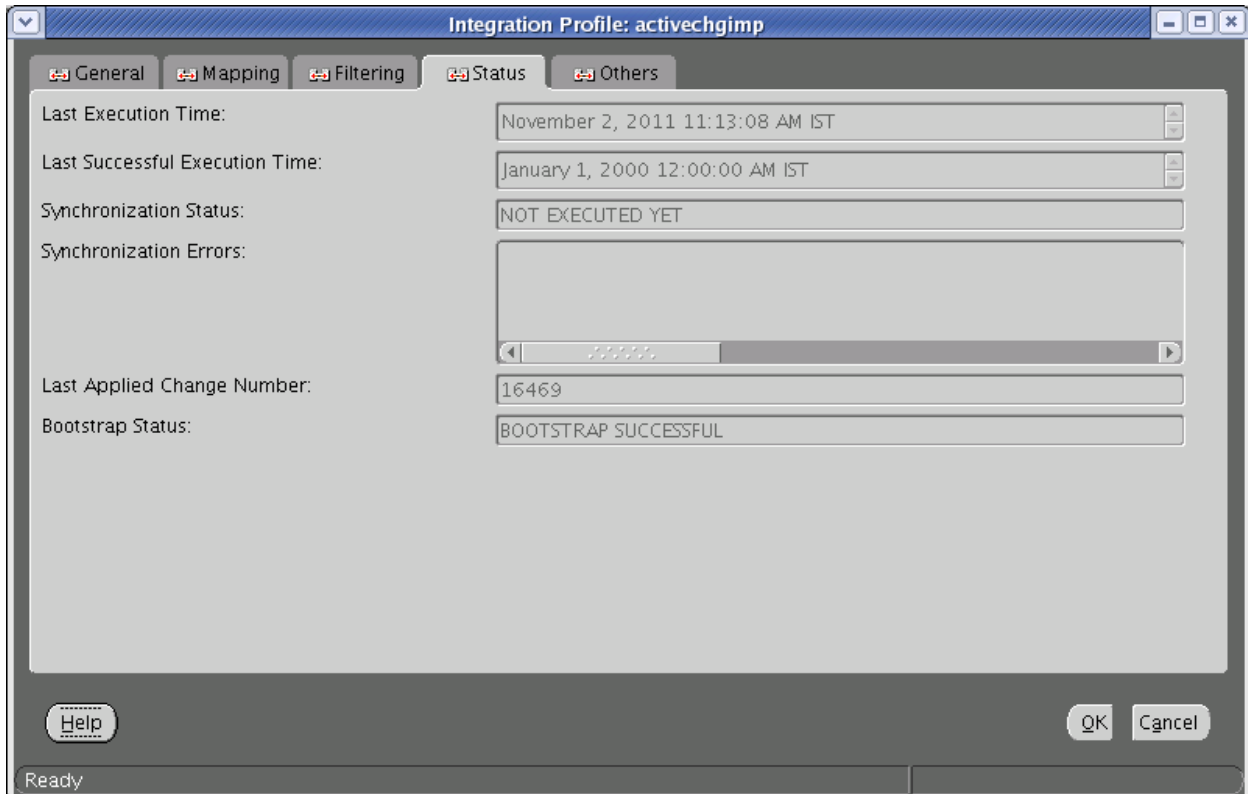
Please see the log file for more information.

Updating the profile's last change number Done.
Updated successfully

Log file information

```
cd $ORACLE_HOME/ ldap/odi/log
-rw-r----- 1 orasso dba 2382 Nov 2 11:20 bootstrap.trc
-rw-r--r-- 1 orasso dba 123395 Nov 2 11:20 bootstrap.log
-rw-r----- 1 orasso dba 424 Nov 2 11:20 ActiveChgImp.trc
```

To see the status of the bootstrap return to the Oracle DIP Console and click **Refresh**



Finally run this command to start the Directory Integration and Provisioning Server:

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

```
[orasso@linux1 ~]$ oidctl connect=orasso server=odisrv instance=2 configset=1 flags="port=389" start
NLS_LANG not set in environment
Setting NLS_LANG to AMERICAN_AMERICA.AL32UTF8
oidctl:Waiting for oidmon to start ODISRV (instance=2)
oidctl:Started ODISRV (instance=2) with PID : 24238 successfully
```

4. ,“It is possible that you may want some or all of your Oracle 10g Application Server users to authenticate using their user credentials stored in Active Directory, or that you don't want your Active Directory user passwords stored in OID at all. If this is your desired authentication model, OID has a feature called "External Password Authentication". External Password Authentication allows you to setup OID so that when a user authenticates against OID, OID will actually check the users credentials against the Active Directory server rather than OID.

Another reason you may need to setup external authentication has to do with the fact that the AD import connector we setup on the previous pages, cannot migrate hashed passwords from AD to OID. This is because Microsoft uses a proprietary hashing algorithm called Unicode password encryption that is not supported in OID. OID supports the most commonly used password encryption's such as MD5, MD4, SHA, SSHA, and Crypt to name a few. Microsoft does not support any of these. So if you want to authenticate using your Microsoft passwords you will need to setup the External Password Plug-in.” (source: oracle.com)

A prerequisite for External Password Authentication is that OID must be configured to import AD users. We accomplished this in steps #1 and 2 above.

To configure External Authentication, run the \$ORACLE_HOME/ldap/admin /oidspadi.sh script. This script will prompt for several parameters about your AD and OID systems.

Enter the AD server (fully qualified domain name) or IP address:
oraclegiantsAD.oraclegiants.com

SSL: n

Enter the port number that the AD server is running on: 389

OID database: infra

Enter the "ods" database schema user password: password

Enter the FQDN of the server that OID is running on: appserver.oraclegiants.com

Enter the port number that OID server is running on: 389

Enter the password for the orcladmin user: password

Enter the subscriber search base. This is the DN of the users container in OID that you want to authenticate to AD: cn=users,dc=oraclegiants,dc=edu

Leave the "Plug-in Request Group DN" blank. Just hit enter without a value.

An important value is the "Exception Entry Property". This value acts as a filter and determines where users will authenticate. If you leave this value null, all users will authenticate using their credentials stored in AD. The value you enter here will determine which users will authenticate against OID and which users will authenticate against AD.

Here is the "Exception entry property" currently configured:
((cn=orcladmin)(cn=portal) (cn=portal_admin) (cn=ias_admin))

This value tells OID that every user except the user "cn=orcladmin" and "cn=portal" will authenticate using credentials stored in AD.

Currently oraclegiants is not setup for the backup Active Directory failover.

OID is now populated with users and groups via bootstrap migration from Active Directory. The Oracle Directory Integration and Provisioning tool has been setup so that it will utilize the Active Directory Connector to keep this account information synchronized. Oracle has been instructed to authenticate user migrated from AD using the Active Directory External Authentication Plug-in.

Long story short: It's now possible to login to Portal via SSO using one of the migrated AD users with its corresponding AD password.

As an example the AD user carrb@oraclegiants.com is able to authenticate using his AD password of "password". Also the OID user "portal" is able to authenticate using the OID password of "carrb1".

Note: the username format must be user@oraclegiants.com

5. Configure Zero Sign-on (Windows Native Authentication)

The Oracle SSO server has a feature which enables Microsoft Internet Explorer users to automatically authenticate to their web applications using their desktop credentials. This is known as Windows Native Authentication (a.k.a. Auto Sign-on or Zero Sign-on). To accomplish this we need to configure "Active Directory External Authentication Plug-in" in order to validate user-supplied passwords "behind the scenes" during a user login. This will be covered in a later post

To search for a user

`./ldapsearch uid=kishore@appsdba.info`

```
[orasso@linux1 bin]$ ./ldapsearch uid=kishore@appsdba.info
cn=kishore a,cn=users,dc=appsdba,dc=info
orcldsourceobjectdn=CN=Kishore A,CN=Users,DC=appsdba,DC=info
krbprincipalname=Kishore@APPSDBA.INFO
orclsamaccountname=APPSDBA.INFO$Kishore
sn=Kishore
sn=A
displayname=Kishore
mail=Kishore@appsdba.info
uid=Kishore@appsdba.info
orclobjectguid=+UvtHFen6kWiMcXl1DcEWg==
orclobjectsids=AQUAAAAAAAAUVAAAAdt4yiW8YIbLTh4BUgQAAA==
cn=Kishore A
orcluserprincipalname=Kishore@appsdba.info
objectclass=inetorgperson
objectclass=person
objectclass=orcluserV2
objectclass=orcladuser
objectclass=orcladobject
objectclass=organizationalPerson
objectclass=top
```

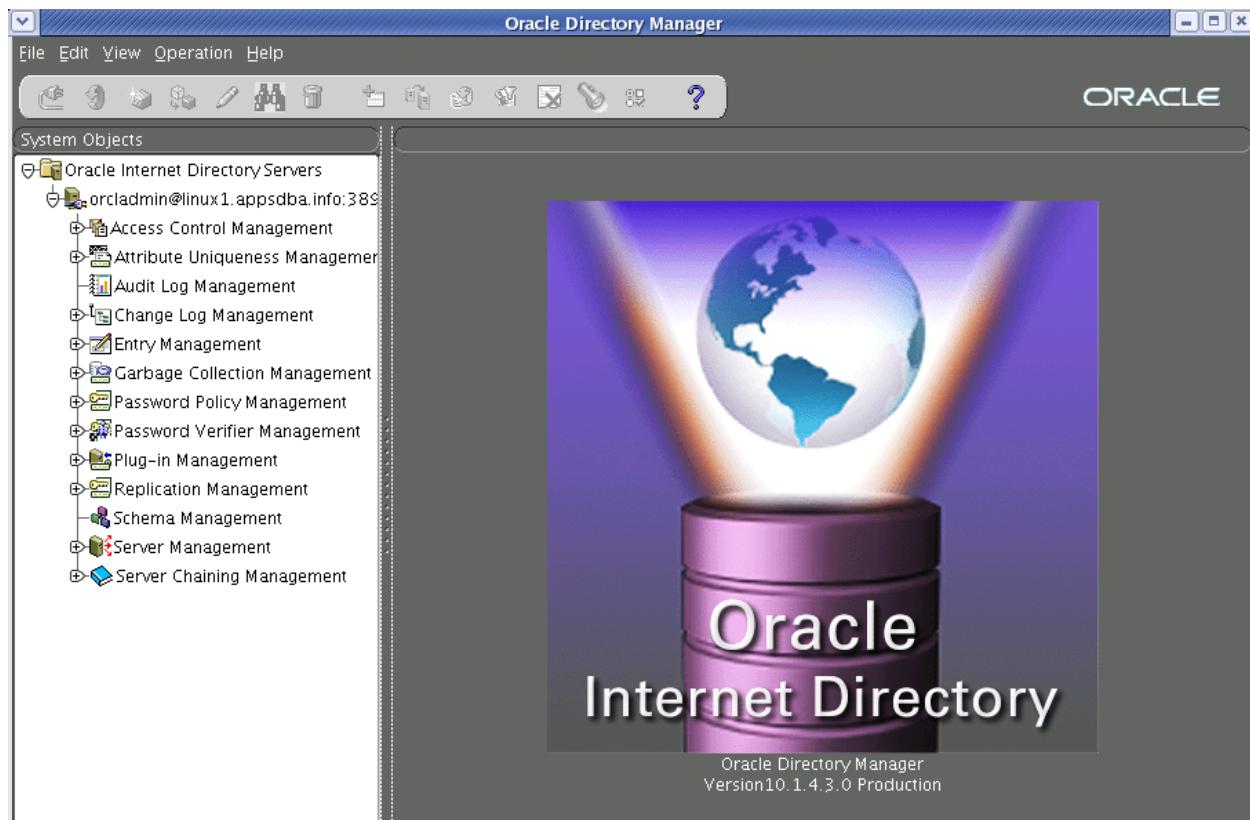
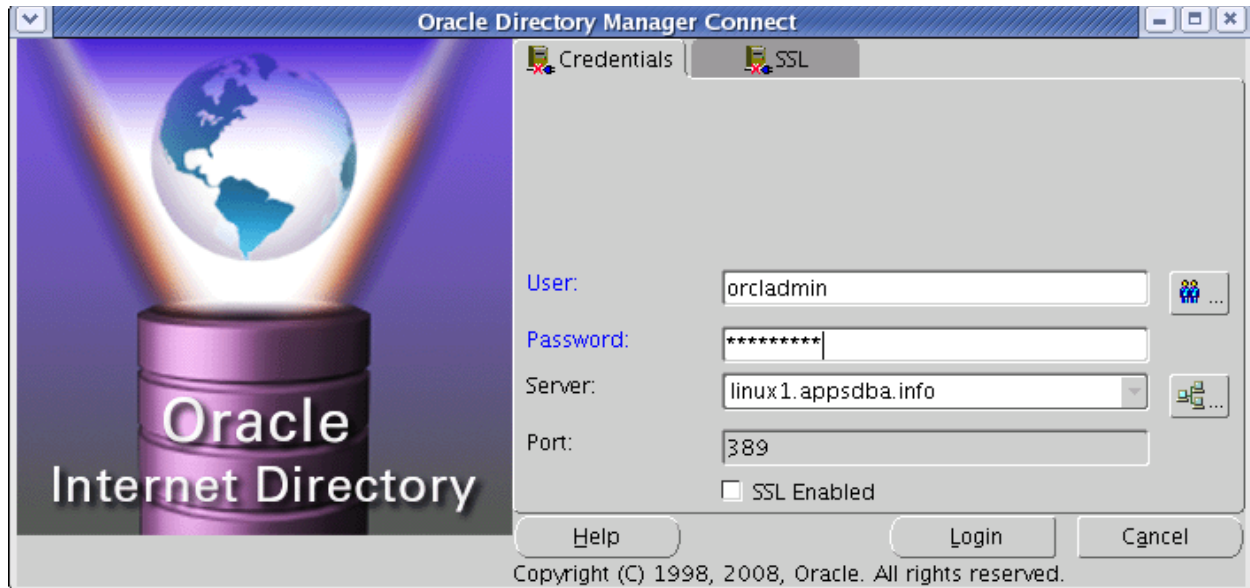
Start and Stop scripts

```
start.sh
echo "Starting DB ..."
sqlplus / as sysdba << END
startup
END
echo "Starting Listener ..."
lsnrctl start
sleep 5
echo "Starting Middle Tier ..."
$ORACLE_HOME/opmn/bin/opmnctl startall
sleep 5
echo "Starting DB Sync Process ..."
oidctl conn=orasso server=odisrv instance=1 configset=0 flags="host=linux1.appsdba.info port=389
grpcid=default" start
sleep 20
echo "Starting AD Sync Process ..."
oidctl conn=orasso server=odisrv instance=2 configset=1 flags="host=linux1.appsdba.info port=389
grpcid=defaultgroup debug=63" start
sleep 5
echo "Starting EM Console"
emctl start iasconsole
#exit 0
```

```
cat stop.sh
echo "Stop DB Sync Process ...."
oidctl conn=orasso serv=odisrv inst=1 conf=0 flags="host=linux1.appsdba.info port=389" stop
sleep 20
echo "Stop AD Sync Process ...."
oidctl conn=orasso serv=odisrv inst=2 conf=1 flags="host=linux1.appsdba.info port=389" stop
sleep 20
echo "Stop EM services ...."
emctl stop iasconsole
echo "Stop Middle tier Services ...."
$ORACLE_HOME/opmn/bin/opmnctl stopall
sleep 10
echo "Stop DB ...."
lsnrctl stop
sqlplus / as sysdba << END
shutdown immediate
END
#exit 0
```

To invoke Directory manager

oidadmin



<http://www.oraclegiants.com/Active-Directory-OID-Integration.htm>

<http://www.iselfschooling.com/Free Oracle Training/04 Advanced/03 Articles 3/lesson06.htm>
↓

<http://www.freeoraclehelp.com/2011/09/oid-integration-with-ms-active.html>

DIP Synchronization with Microsoft Active Directory Quick Start Guide (Doc ID 267153.1)
DIP Synch/Prov Changes Required After Applying 10.1.4.2 or 10.1.4.3 IDM Patchset (Doc ID 462523.1)