

# Configure EUS with OID

## Configure Oracle 11gR2 for Enterprise User Security with Oracle Internet Directory

In Oracle 11gR2, connecting the database to an LDAP server, Oracle Internet Directory in particular, is more easy than in previous versions. It is even possible to run the LDAP connection without SSL / Advanced Security.

The basic steps are:

1. create OID
2. run netca to generate ldap.ora und sqlnet.ora
3. run dbca to register the database in the directory
4. create user schema mappings or Enterprise Roles with Enterprise Manager

## Configure TNS for LDAP server

Run netca and provide details for your OID server.

Afterwards, in \$TNS\_ADMIN, ldap.ora should look like this:

```
cat $TNS_ADMIN/ldap.ora

1. ldap.ora Network Configuration File: /u01/app/11.2.0/grid/network/admin/ldap.ora
2. Generated by Oracle configuration tools.
   DIRECTORY_SERVERS= (linux4:3060:3131)
   DEFAULT_ADMIN_CONTEXT = "dc=loopback,dc=org"
   DIRECTORY_SERVER_TYPE = OID
```

## Run DBCA to register the database

Run Database Creation Assistant, configure Database Options and register the database with OID. DBCA will create a wallet automatically.

## Configure EUS schema mappings

### Group / Shared authentication

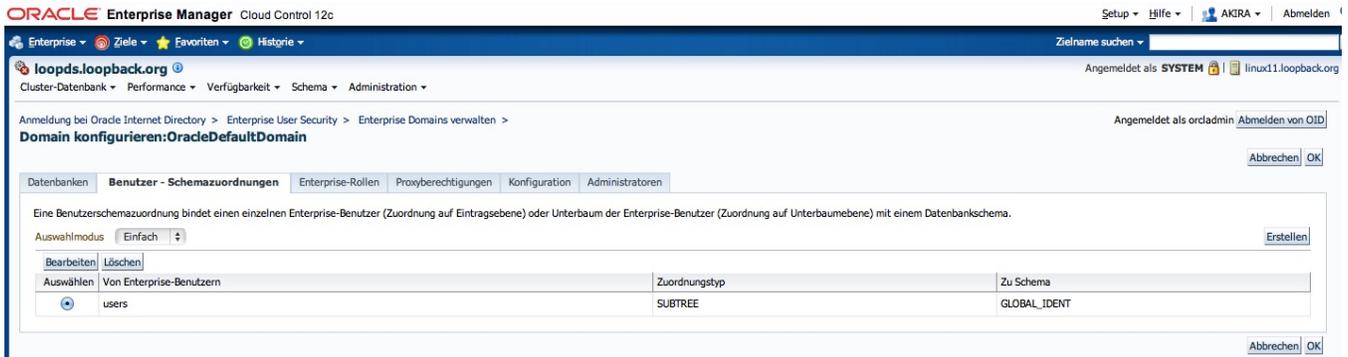
You will need at least a User/Schema mapping to access the database as a local user. You may also configure Enterprise Roles later.

Create a local User, which is identified externally:

```
SYS@loopds1> create user global_ident identified globally;
User created.
SYS@loopds1> grant connect to global_ident;
Grant succeeded.
```

Then, create a mapping in Enterprise Manager.

1. Navigate to Administration/Security/Enterprise User Security.
2. Connect to your OID as orcladmin
3. Navigate to "Enterprise Domains"
4. Configure the OracleDefaultDomain
5. Create a mapping for a selected group of users from your LDAP subtree to the GLOBAL\_IDENT schema you just created.



Alternative, you can create EUS mappings via command line. Please note that mappings can be defined at database level or at domain level:

```
[oracle@oraldap1]$ eusm listMappings realm_dn="dc=loopback,dc=org" ldap_port=3060 ldap_host=oraldap1
ldap_user_dn="cn=orcladmin" ldap_user_password=XXX database_name=pkilab
```

LIST OF DATABASE SCHEMA MAPPINGS::

```
-----
Mapping Name: MAPPING0
Mapping Type: SUBTREE
Mapping DN: cn=Users,dc=loopback,dc=org
Mapping schema: PUBLIC_DATASET
Mapping Level :DATABASE
Mapping Name: MAPPING1
Mapping Type: ENTRY
Mapping DN: cn=test,cn=Users,dc=loopback,dc=org
```

```
[oracle@linux11 ~]$ eusm listMappings domain_name="OracleDefaultDomain" realm_dn="dc=loopback,dc=org"
ldap_port=3060 ldap_host=linux4 ldap_user_dn="cn=orcladmin" ldap_user_password="XXX"
```

LIST OF DATABASE SCHEMA MAPPINGS::

```
-----
Mapping Name: MAPPING0
Mapping Type: SUBTREE
Mapping DN: cn=users, dc=loopback,dc=org
Mapping schema: GLOBAL_IDENT
Mapping Level :DOMAIN
```

## Confirm wallet location is in sqlnet.ora

In some cases, dbca does not enter the location of the wallet it created to sqlnet.ora. The wallet is necessary even if SSL is not used.

In this cases, you will encounter thsi error:

```
ORA-28030: Server encountered problems accessing LDAP directory service
```

Verify this is present in your \$TNS\_ADMIN/sqlnet.ora:

```
WALLET_LOCATION=
(SOURCE=
(METHOD=file)
(METHOD_DATA=
(DIRECTORY=/u01/app/oracle/admin/loopds/wallet)))
```

## Test the connection

```
oracle@linux10 ~]$ sqlplus test/
SQL*Plus: Release 11.2.0.3.0 Production on Sun Oct 14 11:53:38 2012
Copyright (c) 1982, 2011, Oracle. All rights reserved.
Enter password:
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
GLOBAL_IDENT@loopds1> show user
USER is "GLOBAL_IDENT"
```

## Single user authentication

Alternative, you can define any LDAP user to have his own database schema:

```
SQL> alter user AKIRA identified globally as 'uid=akira,cn=Users,dc=loopback,dc=org';
```

User altered.

```
[oracle@linux11 ~]$ sqlplus AKIRA@LOOPDS
```

```
SQL> show user;  
USER is "AKIRA"
```

This takes precedence over a group mapping.

---

See [Oracle® Database Enterprise User Security Administrator's Guide

11g Release 2 (11.2)|[http://docs.oracle.com/cd/E18283\\_01/network.112/e10744/getstrtd.htm#CBHBHADG](http://docs.oracle.com/cd/E18283_01/network.112/e10744/getstrtd.htm#CBHBHADG)]