

Implementing Oracle Identity Management Using External Authentication Plug-In

Dinesh Gupta

Lucidity Consulting Group

dgupta@luciditycg.com

- Oracle DBA Manager
- 13 Years experience working with various Oracle Technologies
- Currently providing software and infrastructure solutions, database administration and E-Business Suite implementations.



The better way to make business decisions.



About Lucidity

- Lucidity Consulting group provides high-quality consulting services to mid-market companies in a cost effective manner.
- Lucidity is considered one of the premier providers of Oracle related consulting services including E-Business suite implementation, managed client support services, and technology integration including database administration services.
- Lucidity was named 'Partner of the Year' in 2002, 2006 and 2007 for the Mid-West region and recognized as 'Certified Advantage Partner' by Oracle.
- Lucidity was named one of the Best Companies to work for in Texas.

Objectives

- Show how to install and integrate Oracle Identity Management with a standard LDAP directory using External Authentication Plug-In.
- Configure Directory Integration Services using an LDAP directory as the source of the truth.
- Show how to integrate and setup provisioning of user information between LDAP directory, Oracle Internet Directory and E-Business Suite.
- Novell eDirectory will be used as an example but the solution can be implemented with Microsoft Active Directory or other LDAP directories.

Overview

- Implementing Single Sign-On (SSO) functionality for the E-Business Suite allows organizations to share one user definition throughout multiple parts of their enterprise.
- Typically, the common user definition is stored in a Lightweight Directory Access Protocol (LDAP) repository such as Novell eDirectory, Microsoft Active Directory or Oracle Internet Directory.
- If the passwords are stored in third-party LDAP directory such as Novell eDirectory, then Oracle Internet Directory can be configured to use an external authentication plug-in that authenticates users against the third-party directory server.

Overview

- In this configuration, the Oracle Single Sign-On server, the third-party single sign-on server, and the partner application form a chain of trust.
- The Oracle Single Sign-On server delegates authentication to the third-party single sign-on server, becoming essentially a partner application to it.
- The E-Business Suite and other Oracle products continue to work only with the Oracle Single Sign-On server, and are unaware of the third-party single sign-on server. Implicitly, however, they trust the third-party server.

Supported Architectures

- Type of Integration with E-Business Suite
 - SSO and OID
- Oracle Application Server 10g must be installed in a separate ORACLE_HOME on an existing application tier node or on a stand-alone server with access to Oracle E-Business Suite 11i database.
- Users are authenticated by:
 - External third-party LDAP directory such as Novell eDirectory.
- Master source-of-truth for user information
 - External third-party LDAP directory such as Novell eDirectory.

Supported Architectures

- Direction of synchronization of user information with external directory
 - From third-party user repository to OID
- Method for initial population of user information in OID and Release 11i
 - From third-party user repository to OID to Release 11i
 - From third-party user repository to OID, independently in Release 11i, then link on first sign-on with link-on-the-fly
- Method for ongoing updates to user information
 - From third-party user repository to OID to Release 11i

Supported Architectures

- OracleAS 10g can be installed on the same machine or each component can be installed on standalone machines.
- Each Oracle component must be installed under a separate ORACLE_HOME.
- For the purpose of this discussion following assumptions have been made:
 - Oracle E-Business Suite Release: 11.5.10.2
 - Oracle Single Sign-On Release: 10.1.4.0.1
 - Oracle Internet Directory: 10.1.4.0.1
 - Oracle SSO/OID Admin Name: orcladmin
 - Operating System: SuSE Linux 9
 - Novell eDirectory: 8.7.3.9

Overview of High Level Tasks

- Install OracleAS Identity Management Infrastructure 10g in a separate ORACLE_HOME
- Register E-Business Suite with OID and SSO
- Synchronize Novell eDirctory with OID and SSO
- Enable authentication using External Plug-In.

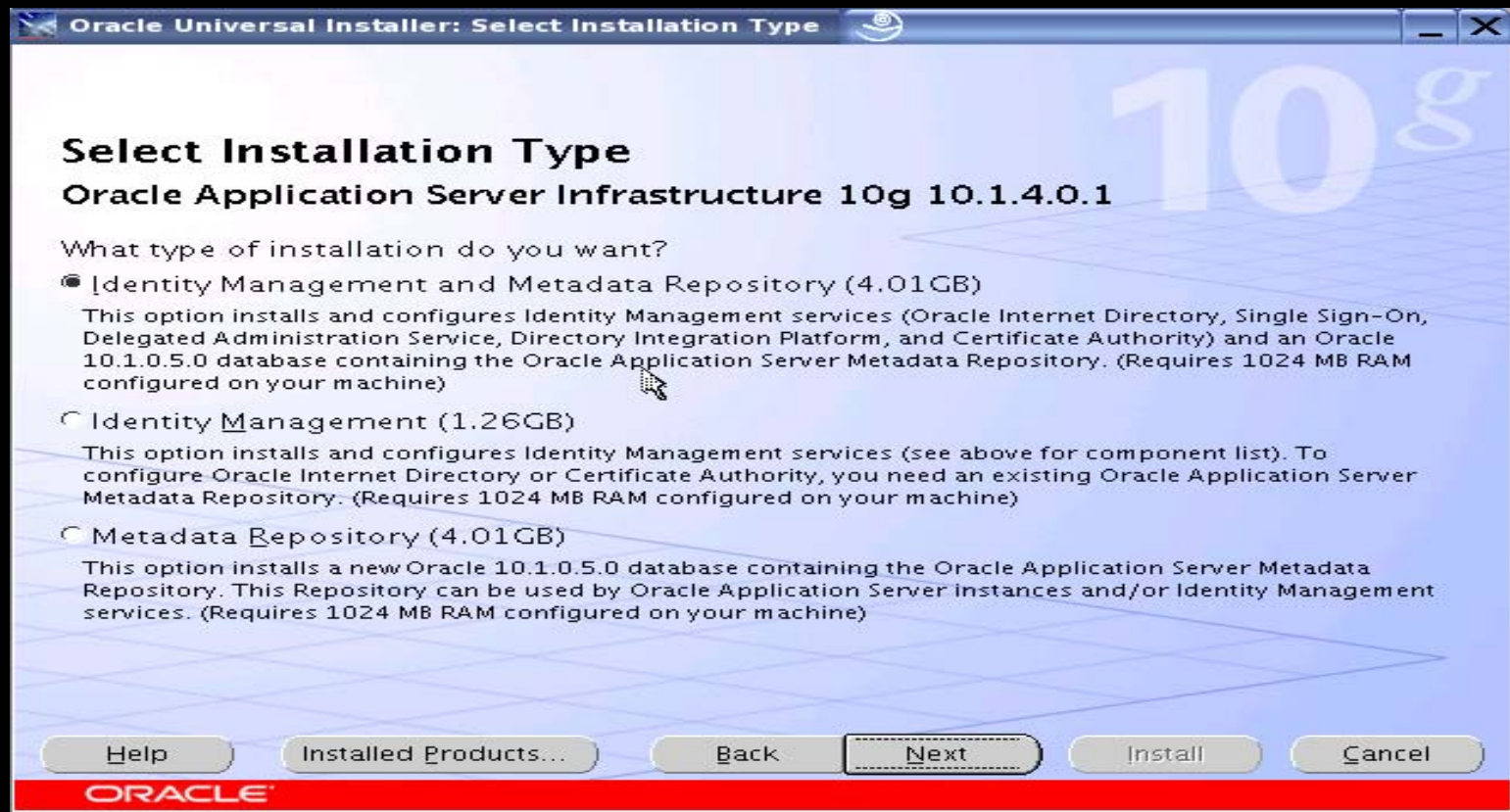
Installation Tasks

- **Install Oracle Application Server 10g (10.1.4.0.1)**
 - Install OracleAS Identity Management Infrastructure 10g in a separate ORACLE_HOME
 - On the Install screen, choose Oracle Application Server Infrastructure 10g.
 - Next choose Identity Management and Metadata Repository.
 - Next choose components - Oracle Internet Directory and Single-Sign-On.

Installation Tasks



Installation Tasks



Installation Tasks



Installation Tasks

Oracle Universal Installer: Specify Namespace in Internet Directory

Specify Namespace in Internet Directory

Specify a location, or namespace, in Oracle Internet Directory to contain users, groups, and Identity Management policies. This namespace will be the default Identity Management Realm.

☒ Suggested Namespace:

☐ Custom Namespace:

Example: dc=acme,dc=com

Help Installed Products... Back Next Install Cancel

ORACLE

Installation Tasks

Oracle Universal Installer: Specify Database Configuration Options

Specify Database Configuration Options

Database Naming
A Global Database Name, typically of the form "name.domain", uniquely identifies an Oracle database. In addition, each database is referenced by at least one Oracle System Identifier (SID). Specify the Global Database Name and SID for this database.

Global Database Name: SID:

Database Character Set
The number of language groups to be stored determine which database character set to use. See "Help" for the definition of language groups. For the Unicode database character set, select "Unicode Standard UTF-8 AL32UTF8"

Select Database Character set:

Database File Location
Use the file system for database storage. For best database organization and performance, Oracle recommends installing database files and Oracle software on separate disks.

Specify Database File Location:

ORACLE

Installation Tasks

Specify Instance Name and ias_admin Password

All Oracle Application Server Infrastructure instances installed on a host must have unique names. The hostname and domain name of the host are appended to the instance name.

Each Oracle Application Server Infrastructure instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.

The password must have a minimum of 5 alphanumeric characters, maximum 30 characters, and at least one of the characters must be a number.

Administrator Username: ias_admin

Instance Name:

ias_admin Password:

Confirm Password:

ORACLE

Installation Tasks



Configure and Register E-Business with OID and SSO

- Verify if the installation was successful by logging into the OID and SSO
 - http://<host_name>:7777/oiddas
 - http://<host_name>:7777/pls/sso
- Prepare the E-Business Suite for integration with OID:
 - ATG RUP 4 or above
 - SSO 10g integration patch
 - Other possible patches: 5502871, 5589902

Configure and Register E-Business with OID and SSO

- Choose Provisioning profile
 - One way Provisioning from OID to E-Business Suite
 - Provisioning Attributes from OID to E-Business Suite
 - Provisioning Events: Creation, Modification and Deletion
 - OID Attributes → FND_USER table in E-Business Suite
 - UID → USER_NAME
 - DESCRIPTION → DESCRIPTION
 - MAIL → EMAIL_ADDRESS
- Register E-Business Suite with SSO and OID
 - **\$FND_TOP/11.5.0/admin/template>
txkrun.pl -script=SetSSOReg
-provtmp=ProvOLDToApps.tmp**

Configure and Register E-Business with OID and SSO

- Profile Options
 - Applications w/SSO (APPS_SSO)
SSWA w/SSO
 - Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN)
Local, SSO or Both
- Login with Single Sign-On
 - http://<host_name>:port/oa_servlets/AppsLogin
- Login for Local authentication
 - http://<host_name>:port/OA_HTML/AppsLocalLogin.jsp
- Any new user created in OID will be provisioned in E-Business Suite.
- Existing user accounts will be connected via Link-on-the-Fly using GUID.

Synchronize Novell eDirectory with OID and SSO - Configuration

- Configure Synchronization from Novell eDirectory → OID
 - Oracle Internet Directory
 - Realm: cn=users, dc=pecousa, dc=com
 - Host: oracleap1dev.pecousa.com
 - Novell eDirectory
 - Tree: PECO_TEST
 - Object Context: Peco
 - Admin Name: Admin
 - Admin Context: O=Peco
 - Ldap clear text: 389
 - eDirectory Host: 192.168.10.100

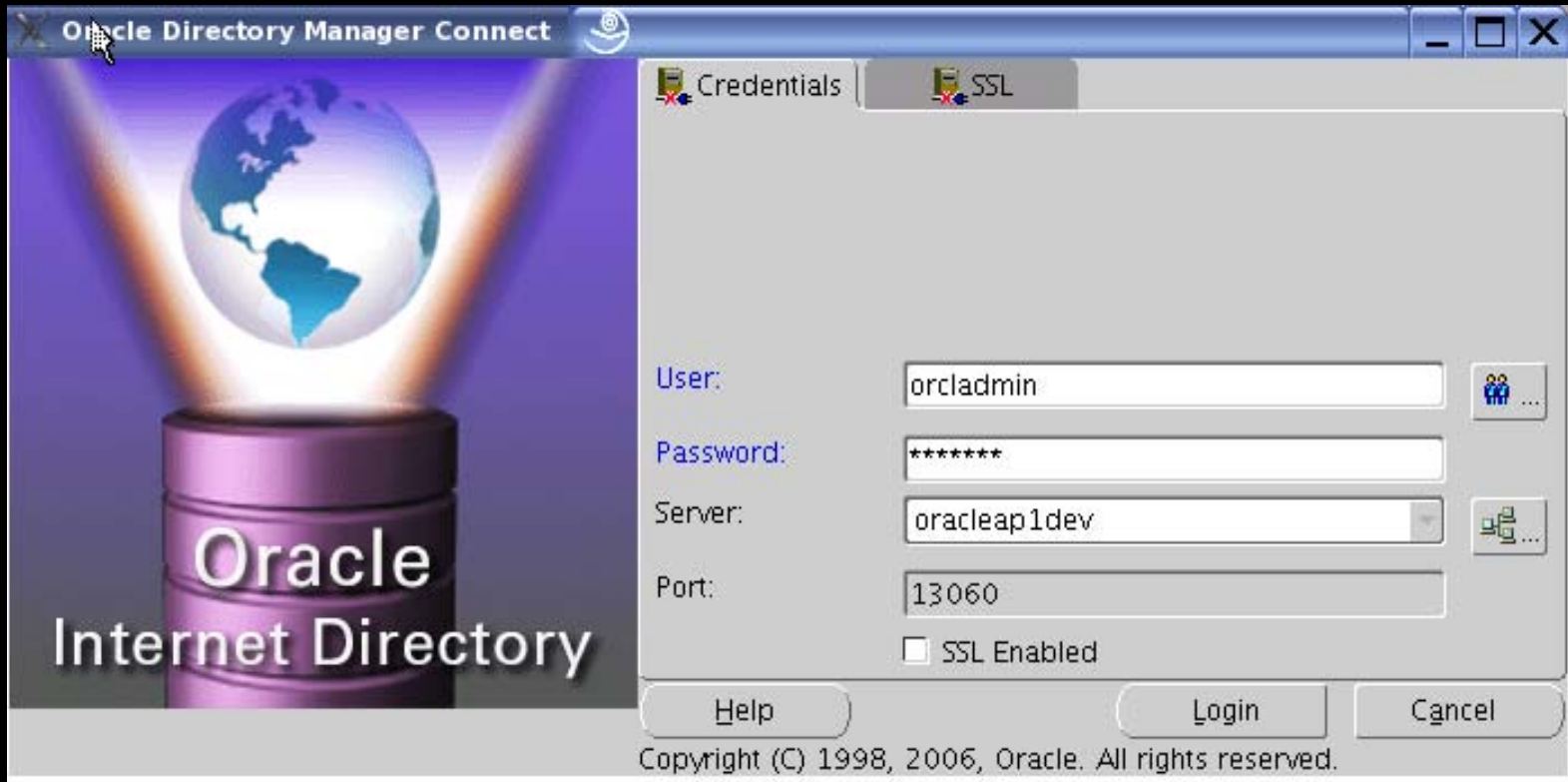
Synchronize Novell eDirectory with OID and SSO – Create Profile

- Verify connectivity
 - Connect to eDirectory
 - `ldapbind -h 192.168.10.100 -h 389 -D "cn=admin,o=peco" -p *****`
 - Connect to OID
 - `ldapbind -h oracleap1dev -p 13060 -D "cn=orcladmin" -p *****`
- Create Synchronization Profiles
 - Create a new Import profile to import users from eDirectory to OID
 - Use dipassistant and expressconfig option to create the Import profile
 - `dipassistant expressconfig -h oracleap1dev -p 13060 -3rdpartyds eDirectory -configset 1`

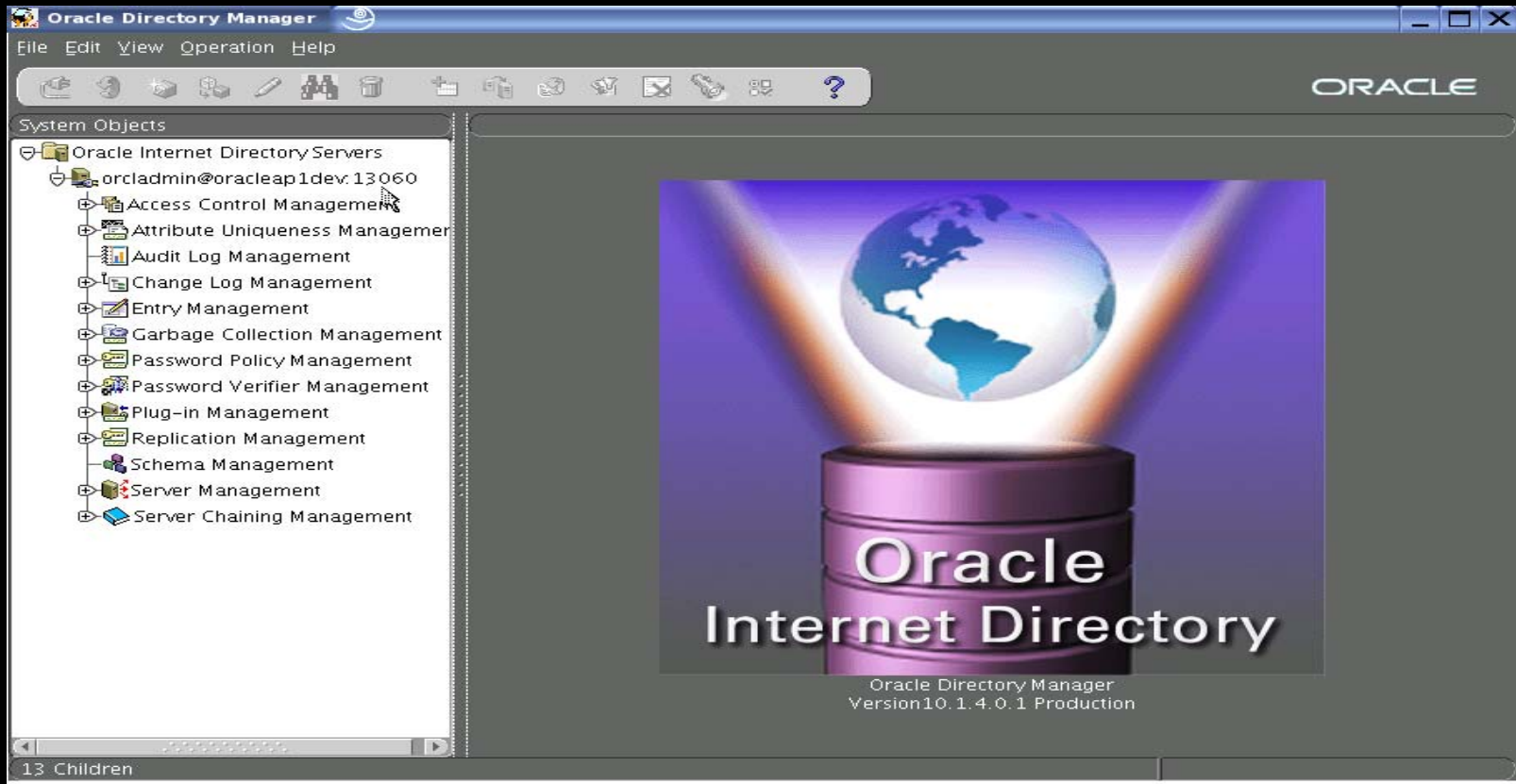
Synchronize Novell eDirectory with OID and SSO – Verify Profile

- Verify created profile:
 - Login to Oracle Directory Manager
 - Server Management → Integration Server → Configuration Set 1
 - On the right side, you should see eDirectoryImport
- Disable/Enable created profile using command line
 - `dipassistant modifyprofile -profile eDirectoryImport -host oracleap1dev -port 13060 -dn cn=orcladmin -passwd ***** odip.profile.mapfile=$ORACLE_HOME/ldap/odi/conf/eDirectoryImport.map odip.profile.status=DISABLE`
 - `dipassistant modifyprofile -profile eDirectoryImport -host oracleap1dev -port 13060 -dn cn=orcladmin -passwd ***** odip.profile.mapfile=$ORACLE_HOME/ldap/odi/conf/eDirectoryImport.map odip.profile.status=ENABLE`

Oracle Directory Manager - Login



Oracle Directory Manager - Menu



Oracle Directory Manager – Enable Import Profile

The screenshot shows the Oracle Directory Manager application window. The left pane displays the 'System Objects' tree, with 'Configuration Set1' under 'Integration Server' selected. The right pane shows the 'Integration Connectors' table, which lists various connectors and their synchronization modes and statuses. The 'eDirectoryImport' connector is highlighted, showing a status of 'ENABLE'.

Connector Name	Synchronization Mode	Connector Status
eDirectoryImport	IMPORT	ENABLE
eDirectoryExport	EXPORT	DISABLE
eDirectoryExp	EXPORT	DISABLE
TaggedExport	EXPORT	DISABLE
LdifExport	EXPORT	DISABLE
OracleHRAgent	IMPORT	DISABLE
ActiveChgImp	IMPORT	DISABLE
OpenLDAPImport	IMPORT	DISABLE
eDirectoryImp	IMPORT	DISABLE
TaggedImport	IMPORT	DISABLE
Idifimport	IMPORT	DISABLE
IplanetExport	EXPORT	DISABLE
ActiveExport	EXPORT	DISABLE
ActiveImport	IMPORT	DISABLE
OpenldapExport	EXPORT	DISABLE
IplanetImport	IMPORT	DISABLE

Buttons at the bottom right: Create, Edit, Delete, Refresh. A Help button is located at the bottom left of the main pane.

Synchronize Novell eDirectory with OID and SSO – Provision Users

- Once the Import profile has been enabled, create a new user in Novell eDirectory
- The new user will show up in OID and eventually in E-Business Suite
- For the existing users from Novell eDirectory to show up in OID and E-Business, use bootstrap option of dipassistant
 - `dipassistant bootstrap -profile I_eDirectoryImport -host oracleap1dev -port 13060 -dn cn=orcladmin -passwd *****`

Synchronize Novell eDirectory with OID and SSO – Verify User

Oracle Identity Management Provisioning Console - Users - Microsoft Internet Explorer

Address: http://oracleap1dev.pecousa.com:7777/oiddas/ui/oracle/ldap/das/pages/UserSearch

Norton 360 Fraud monitoring is on

ORACLE Identity Management Provisioning Console

Logout Realm Management Help

Home My Profile Directory Configuration

Users | Groups | Services | Applications

Logged in as orcladmin

Users

Search Go Advanced Search Provisioning Search

Search is conducted over attributes listed below.

View Edit Privileges Delete Unlock Enable Disable Create Bulk

Previous 1-25 of 268 Next 25

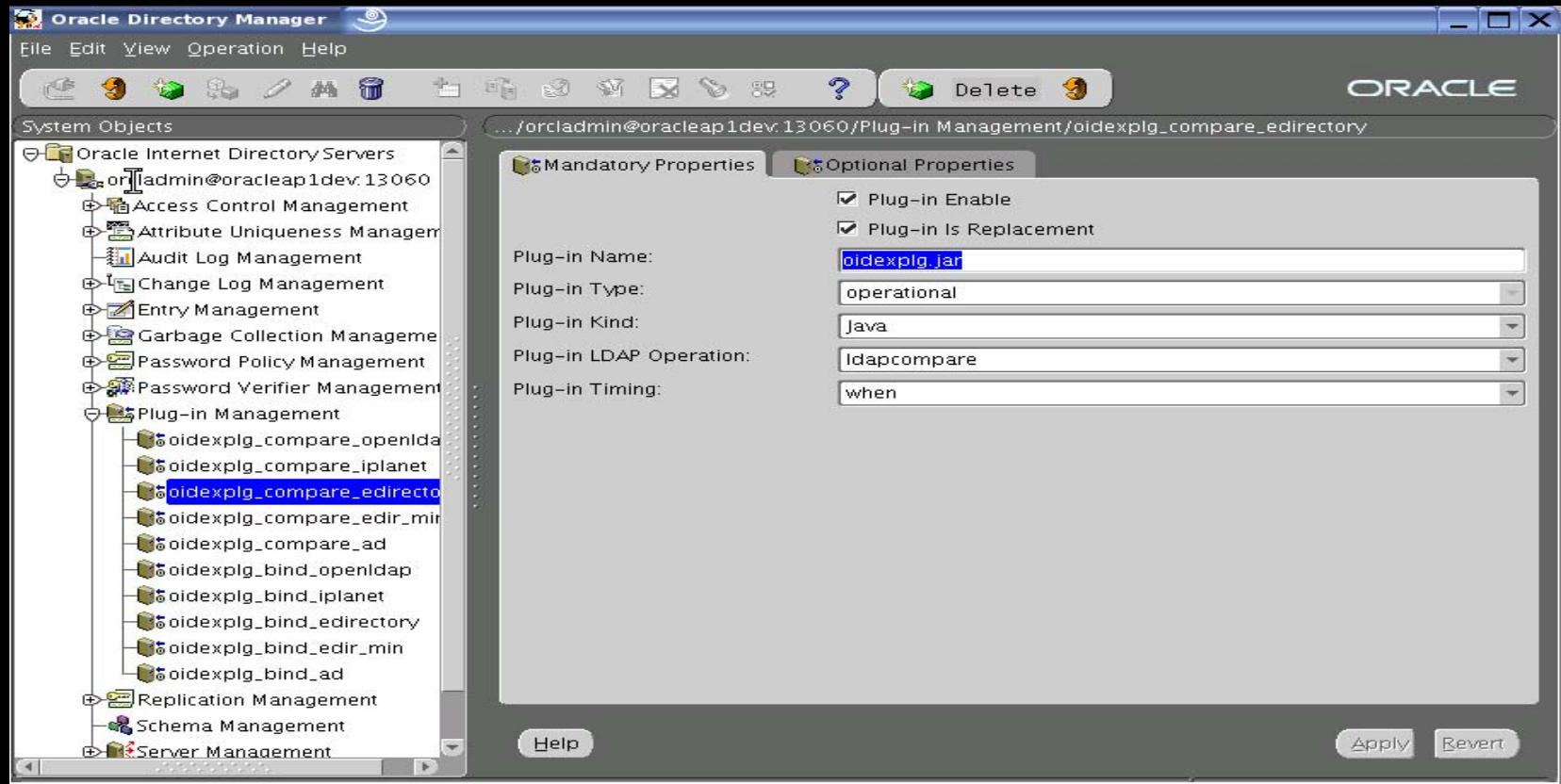
Select	User ID	Email Address	First Name	Last Name	Job Title	Work Phone	Locked	Enabled
<input checked="" type="radio"/>	aarhei			HEINE				✓
<input type="radio"/>	admin			admin				✓
<input type="radio"/>	admin_oid	orcladmin	orcladmin	orcladmin				✓
<input type="radio"/>	adrdel			DeLeon				✓
<input type="radio"/>	albtam			tamayo				✓
<input type="radio"/>	allwal			walker				✓
<input type="radio"/>	anggon			gonzales				✓
<input type="radio"/>	anhmei			mei				✓
<input type="radio"/>	annhop			hopkins				✓
<input type="radio"/>	anotherstest			Test				✓
<input type="radio"/>	ashbar			barham				✓
<input type="radio"/>	ashken			kendrick				✓
<input type="radio"/>	asuzam			zam				✓
<input type="radio"/>	berros			Ross				✓

Done Internet

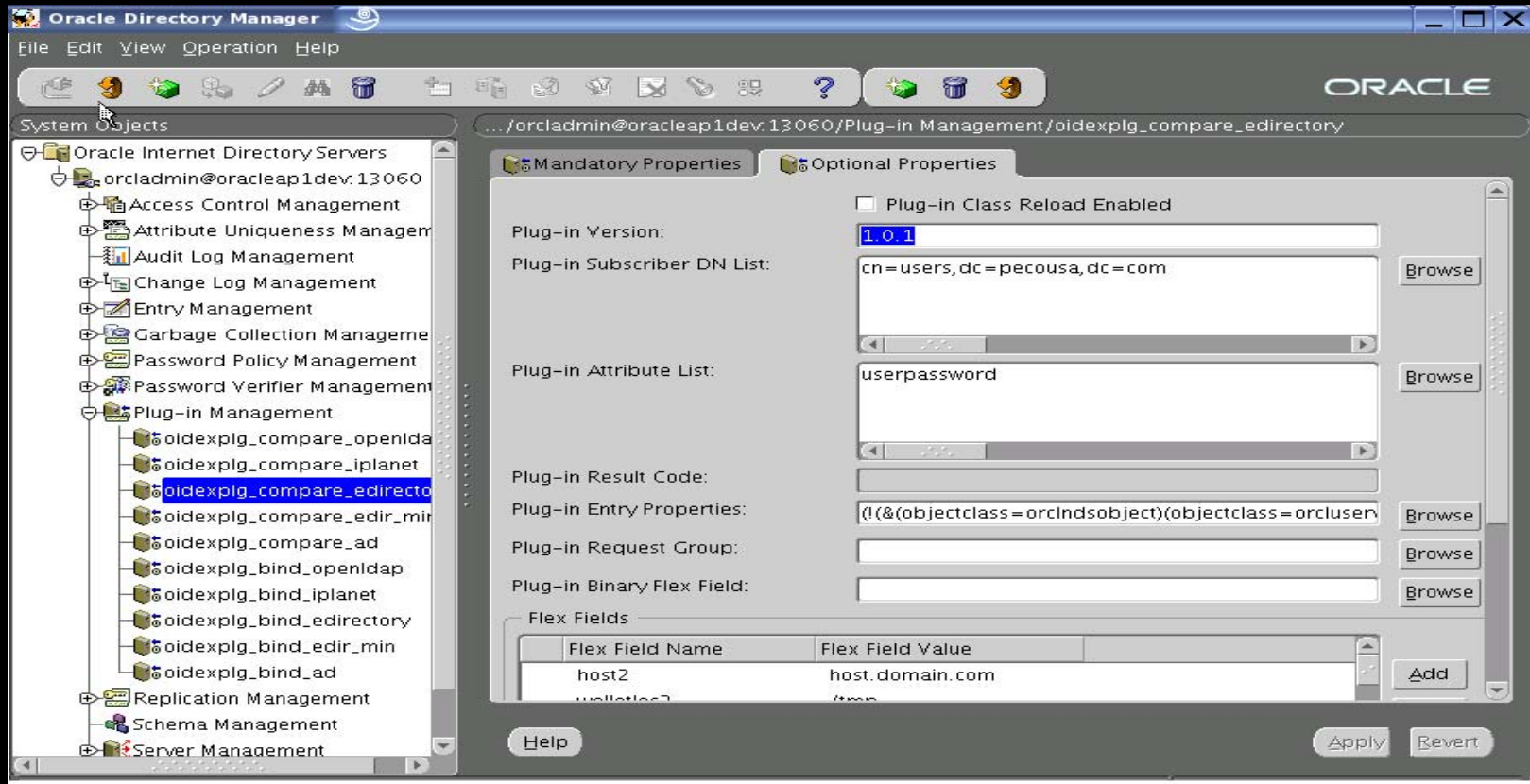
Enable Authentication using External Plug-In

- Drop and re-create External Authentication Plug-In for eDirectory
 - Create a new user testid with password as edirpass in eDirectory
 - The user will be created in OID
 - Set password manually in OID as oidpass
 - Verify with ldapbind that you can connect as the new user to OID with oidpass as password
 - set the adwhencompare and adwhenbind profiles to DISABLE –
 - delete adwhencompare and delete adwhenbind
 - \$ORACLE_HOME/ldap/admin/oidspediri.sh
 - Check that the two plug-ins are enabled.
 - Stop and start the OIDLDAPD instances
 - Retry the ldapbind as testid user with oidpass as password. It should now fail because the plug-in is enabled.
 - Retry the ldapbind, but substitute the eDirectory password for the OID password. If this works, test the user can logon to oiddas and that they can display their profile.

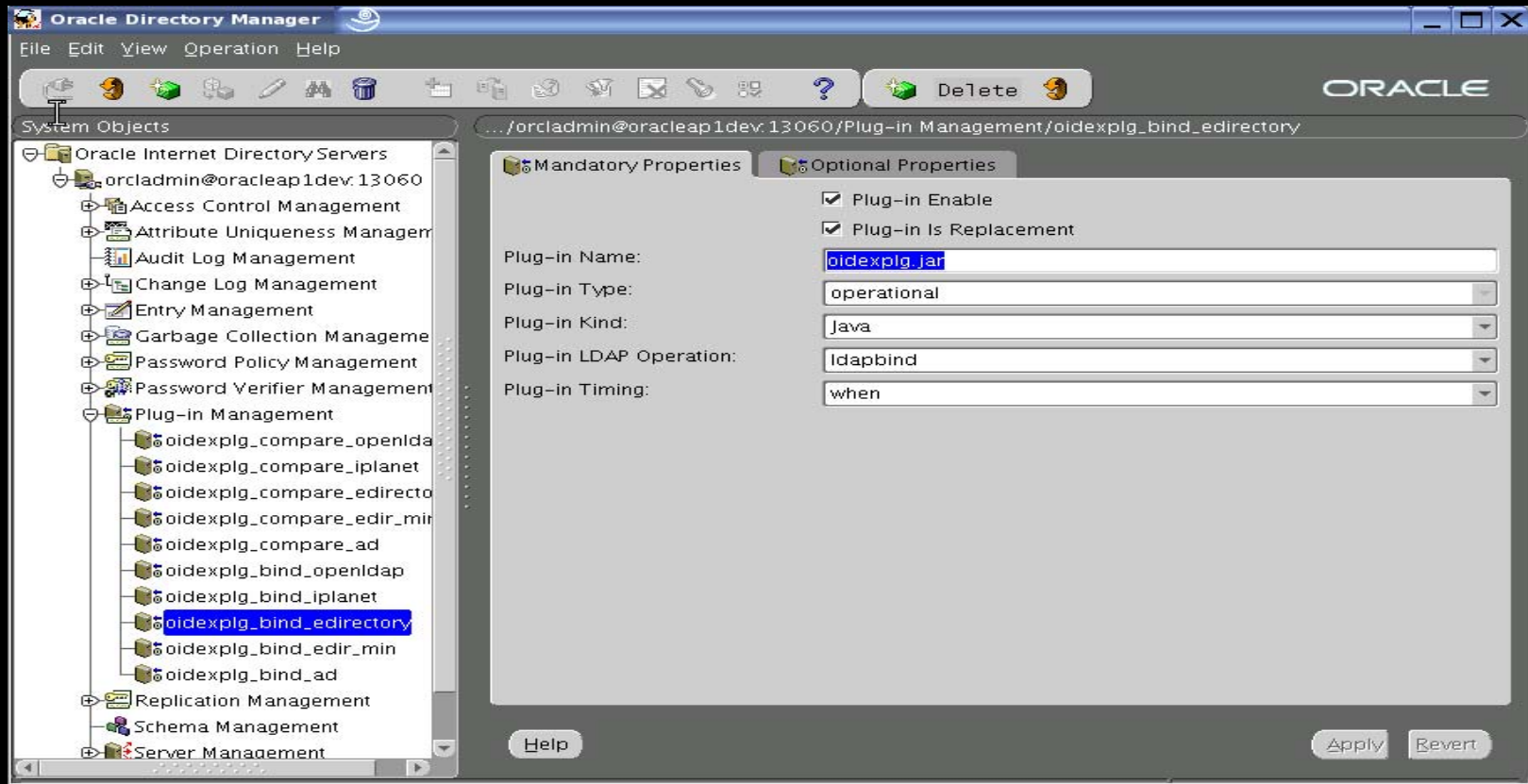
Oracle Directory Manager - External Plug-In – Compare Profile



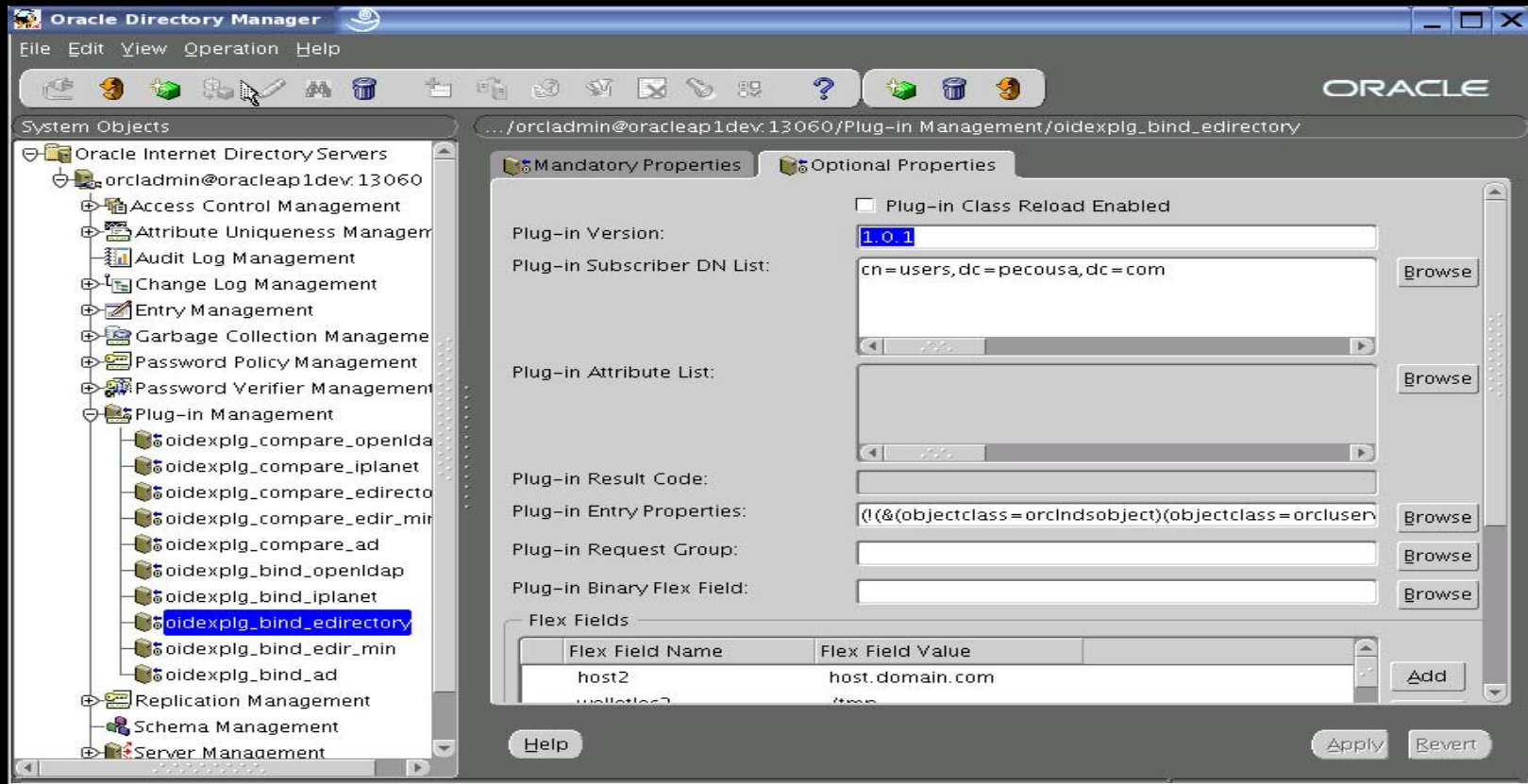
Oracle Directory Manager - External Plug-In – Compare Profile



Oracle Directory Manager - External Plug-In – Bind Profile



Oracle Directory Manager - External Plug-In – Bind Profile



Single Sign-On – Login

The screenshot shows a Microsoft Internet Explorer browser window titled "Sign In - Microsoft Internet Explorer". The address bar displays a URL from oracleap1dev.pecousa.com. A Norton 360 security bar is visible above the main content area, showing "No fraud detected". The page header includes the Oracle Identity Management logo and the text "PECO_TEST eDir - DEV L Instance". The main heading is "Sign In" with a question mark icon. Below this is a sub-heading "Sign In" and a prompt: "Enter your Single Sign-On user name and password to sign in." There are two input fields: "User Name" with the value "orcladmin" and "Password" with masked characters. There are "OK" and "Cancel" buttons at the top right and bottom right of the form area. At the bottom of the page, there is a disclaimer: "Unauthorized use of this site is prohibited and may subject you to civil and criminal prosecution. Copyright © 1999, 2006 Oracle. All rights reserved."

Sign In - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://oracleap1dev.pecousa.com:7777/sso/pages/login.jsp?site2pstoretoken=v1.4~72723BAC~B66D50700711A70942F1524D8837DC167A274C5E6699A468A9631B8ED97F290BD60422F4 Go Links SnagIt

Norton 360 No fraud detected Options

ORACLE Identity Management
PECO_TEST eDir - DEV L Instance

Sign In ?

OK Cancel

Sign In

Enter your Single Sign-On user name and password to sign in.

User Name orcladmin

Password

OK Cancel

Unauthorized use of this site is prohibited and may subject you to civil and criminal prosecution.
Copyright © 1999, 2006 Oracle. All rights reserved.

Done Internet

Summary

- ✓ Discussed installation tasks for Oracle Identity Management in to an existing 11i environment.
- ✓ Discussed how to register OID and SSO with E-Business Suite.
- ✓ Discussed how to synchronize Novell eDirectory with OID/SSO and E-Business Suite.
- ✓ Discussed how to enable authentication using external plug-in.

QUESTIONS & ANSWERS