Implementing Oracle Identity Management Using External Authentication Plug-In

Dinesh Gupta

Lucidity Consulting Group

Corporate Information:

Lucidity Consulting Group LP was formed by a group of senior managers, primarily from Arthur Andersen and Ernst and Young, who saw an opportunity in the marketplace to shed the overhead associated with their respective "Big 4" firms and deliver high quality consulting services to mid- market companies at a much more aggressive price point. Lucidity has grown at a measured but controlled pace (currently employing over 75 consultants) and is now considered one of the premier providers of Oracle related consulting services in the central US.

Lucidity is a full-service consulting firm with expertise in enterprise resource planning, customer relationship management, business process redesign, human capital management, supply chain management and advanced technology. Lucidity provides clients a full-service consulting approach that combines a unique blend of practical industry knowledge with strong project management skills and a thorough understanding of business processes and technology.

Oracle Relationship

Lucidity works exclusively with Oracle products and has achieved Oracle's highest partner status. Lucidity was named Oracle's **"Partner of the Year"** in 2002, 2006 and 2007. We specialize in the entire Oracle Applications Suite, JD Edwards Hyperion and Demantra and provide deep business process and Oracle applications implementation experience in a cost-effective manner. Lucidity has earned recognition from Oracle Corporation as being among the select few to attain the "**Certified Advantage Partner**" status. Oracle only awards this recognition to firms with proven track records or successful implementations and highly satisfied clients.

Introduction:

This white paper contains information for implementing Oracle's Identity management using external authentication plug-in. The topics covered will show how to install and integrate Oracle Identity Management with a standard LDAP directory using External Authentication Plug-In. Also, we will show how to configure directory integration services using LDAP directory as the source of the truth, and 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.

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:

The Oracle Identity Management can be implemented in several different ways. The following supported architecture was utilized for the purpose of this discussion.

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 11i database.

Supported Architecture	
Type of Integration with E-Business Suite	SSO and OID
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
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

Exhibit 1

The following assumptions have been made:

Component Name	Version
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

Exhibit 2

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 eDircetory 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.

Exhibit 3

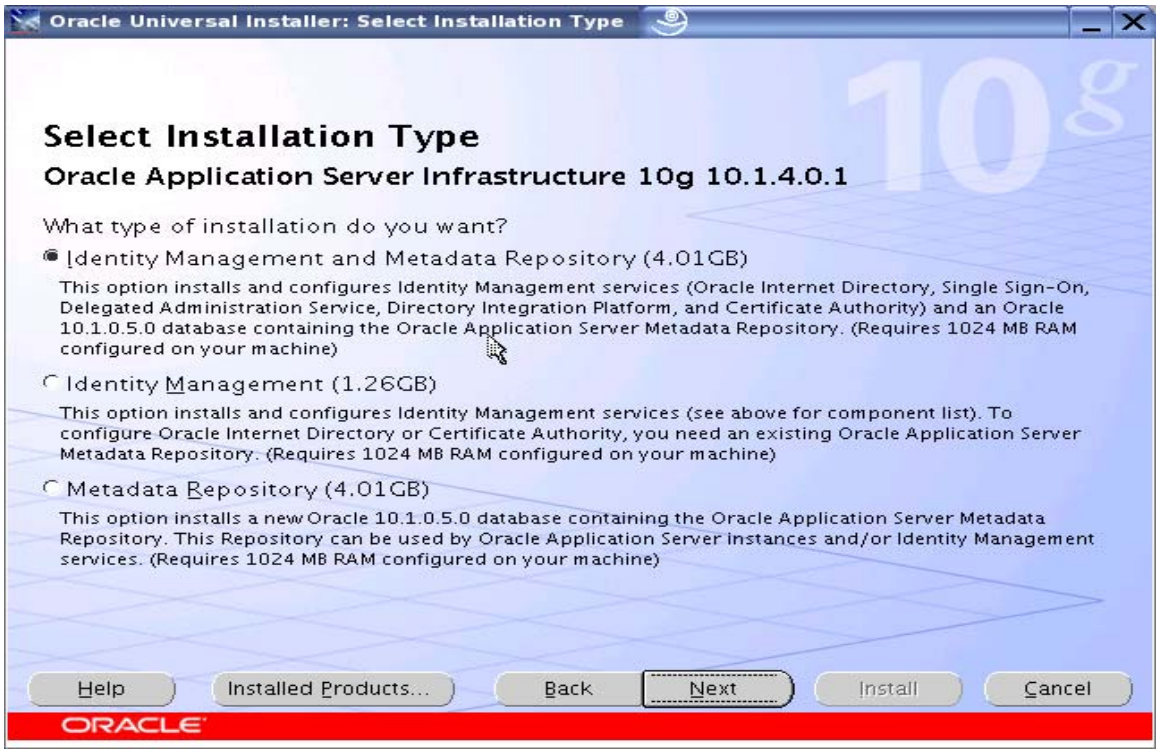

Exhibit 4

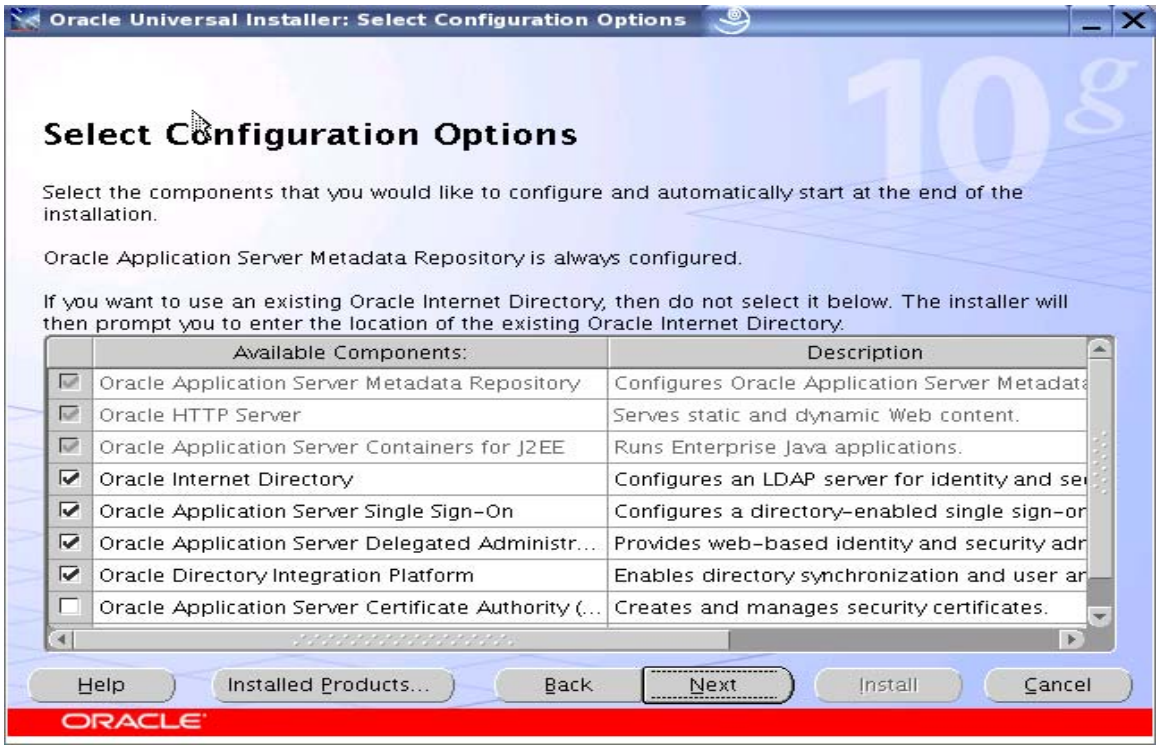

Exhibit 5

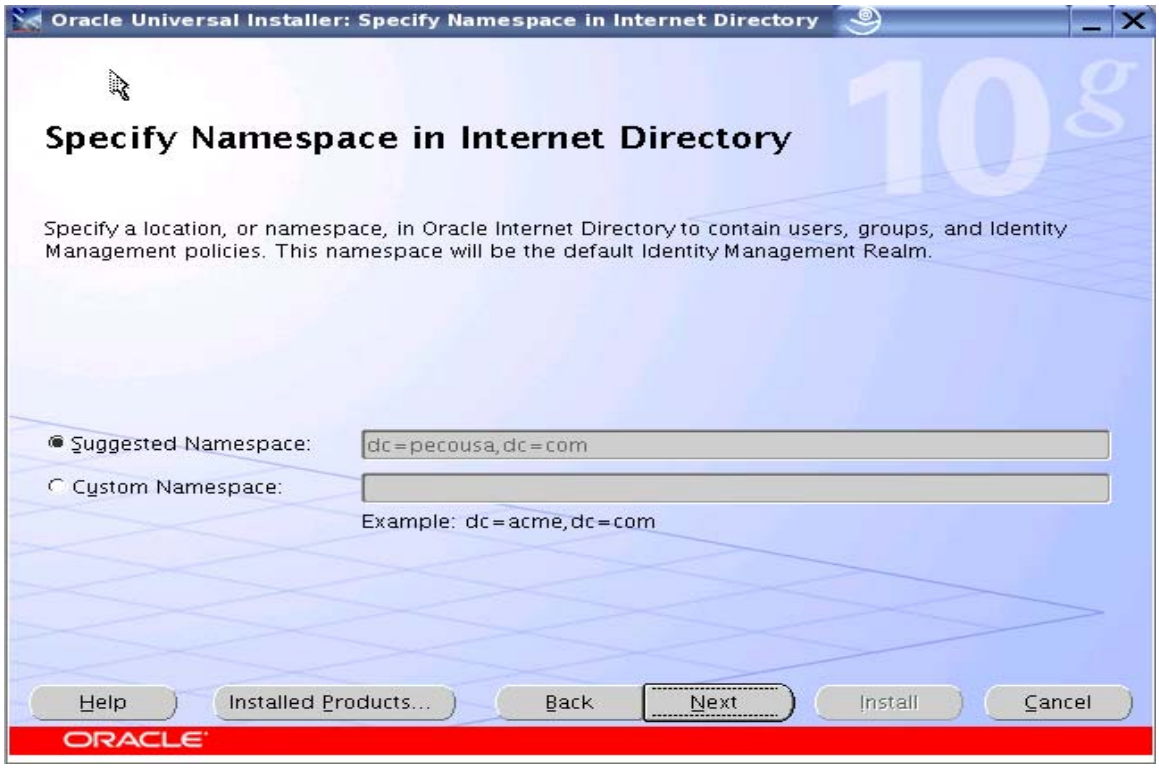

Exhibit 6

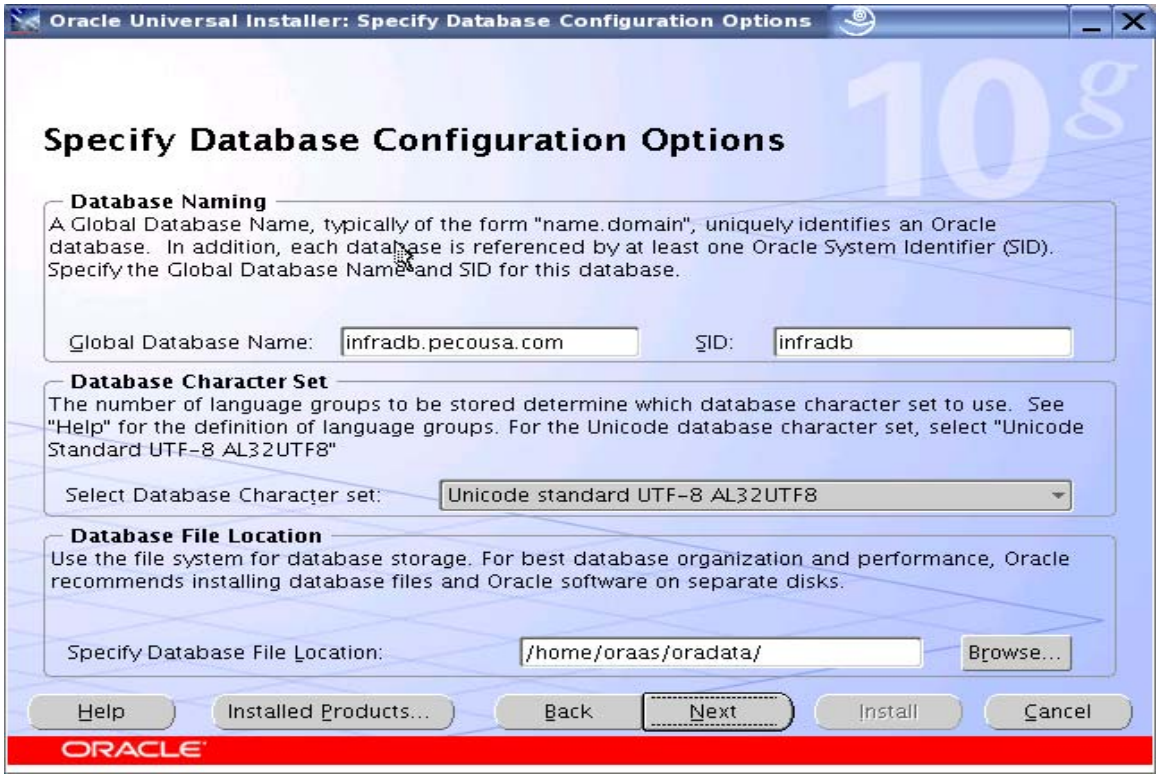

Exhibit 7

Exhibit 8

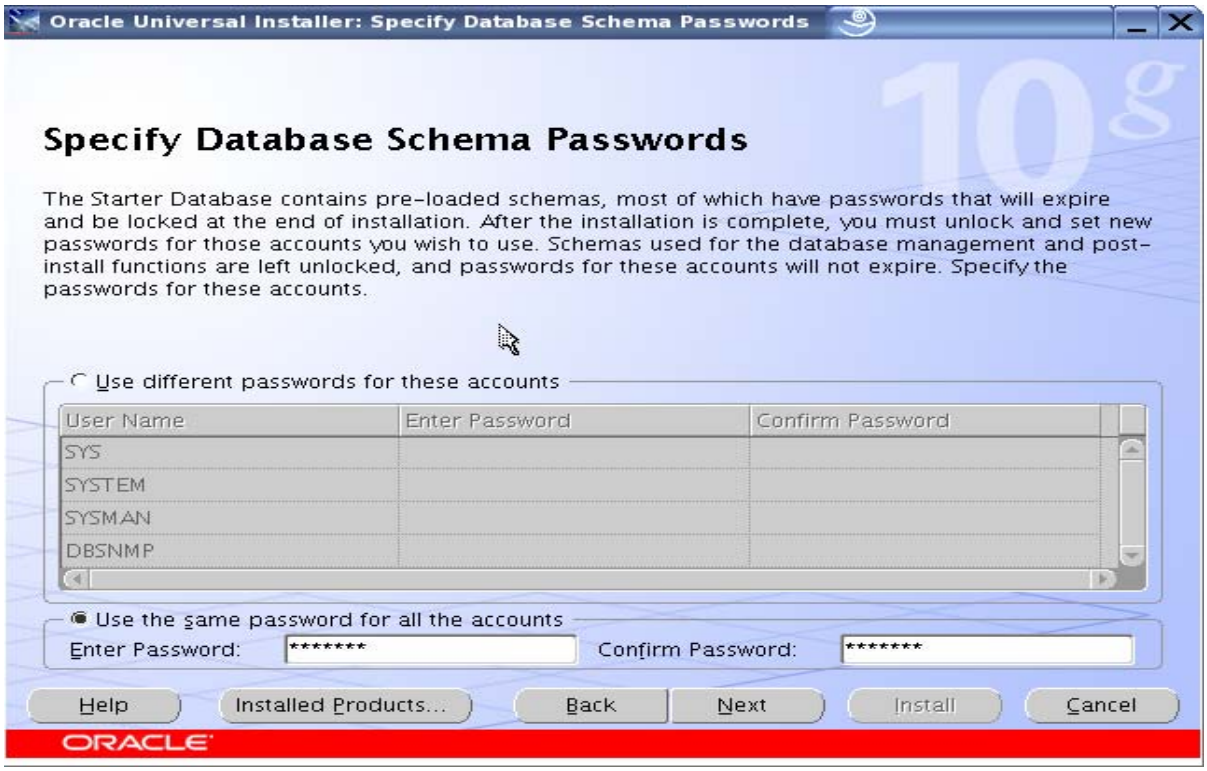

Exhibit 9

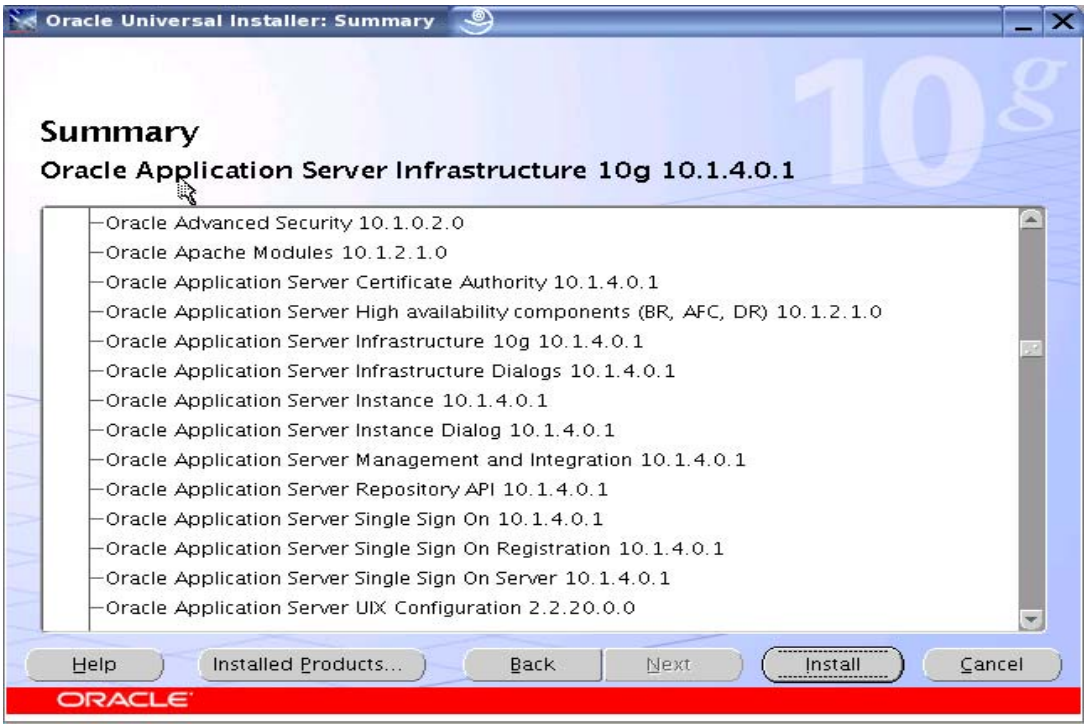

Exhibit 10

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
- 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=ProvOIDToApps.tmp
- 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
- 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
- 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

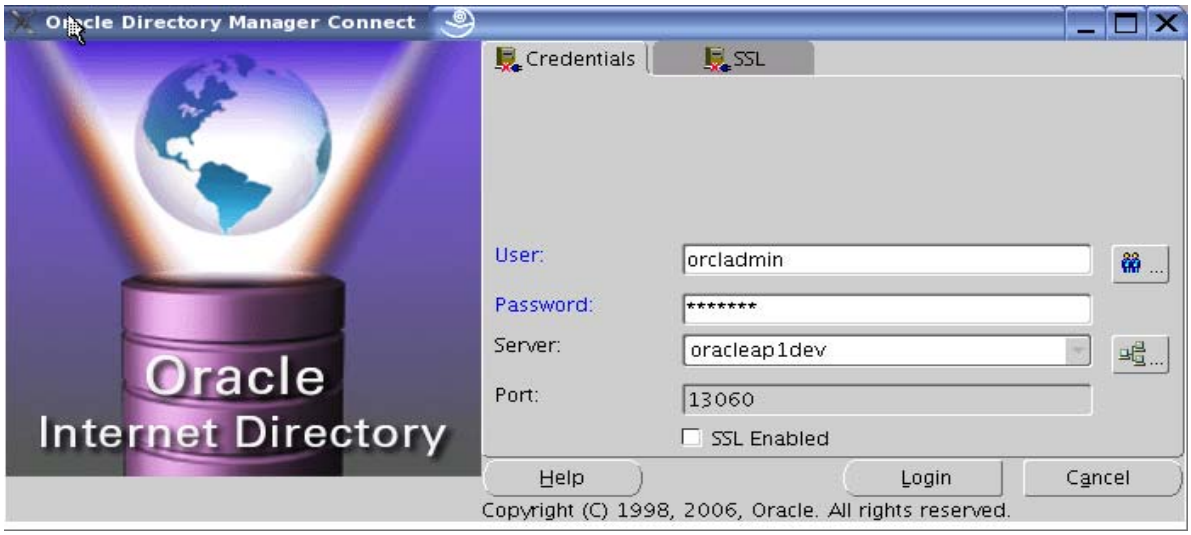

Exhibit 11

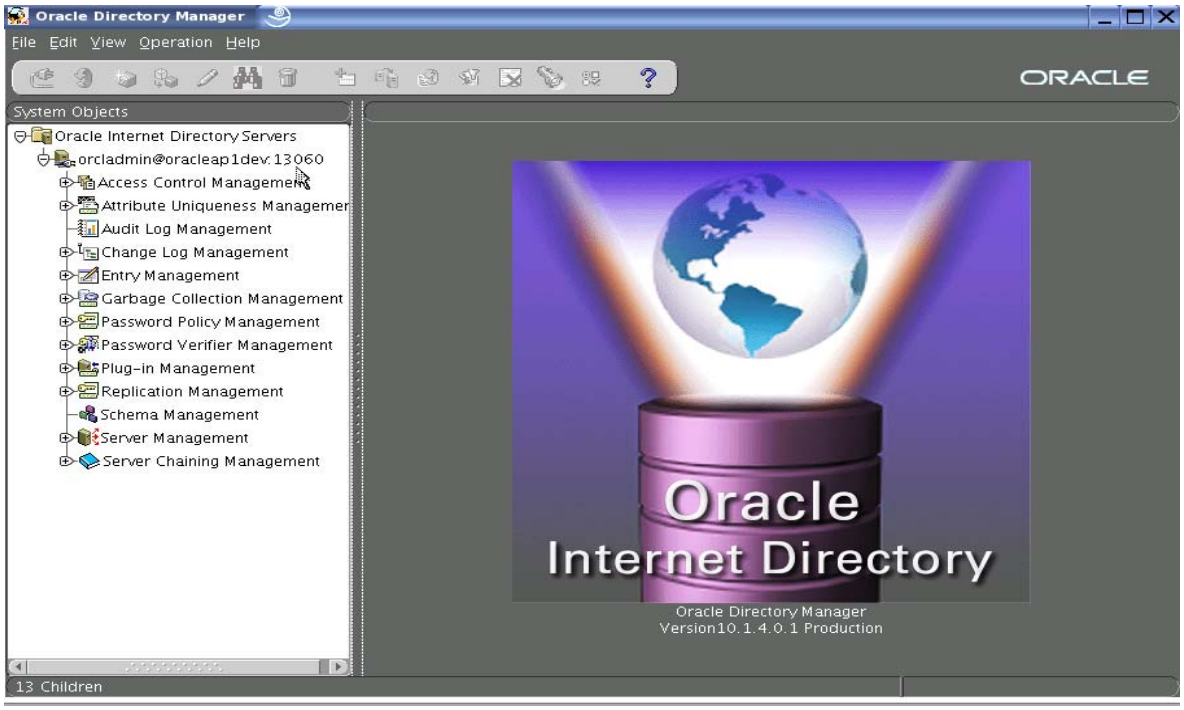

Exhibit 12

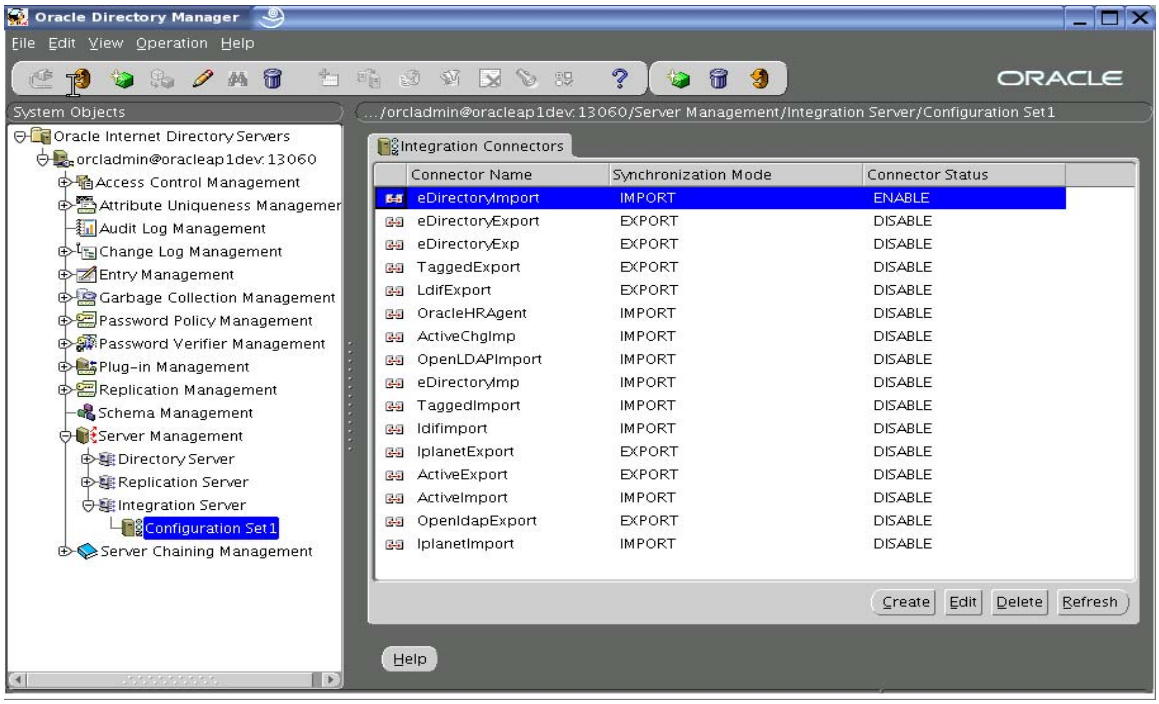

Exhibit13

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 l_eDirectoryImport -host oracleap1dev -port 13060 -dn cn=orcladmin -passwd *****

Synchronize Novell eDirectory with OID and SSO – Verify User:

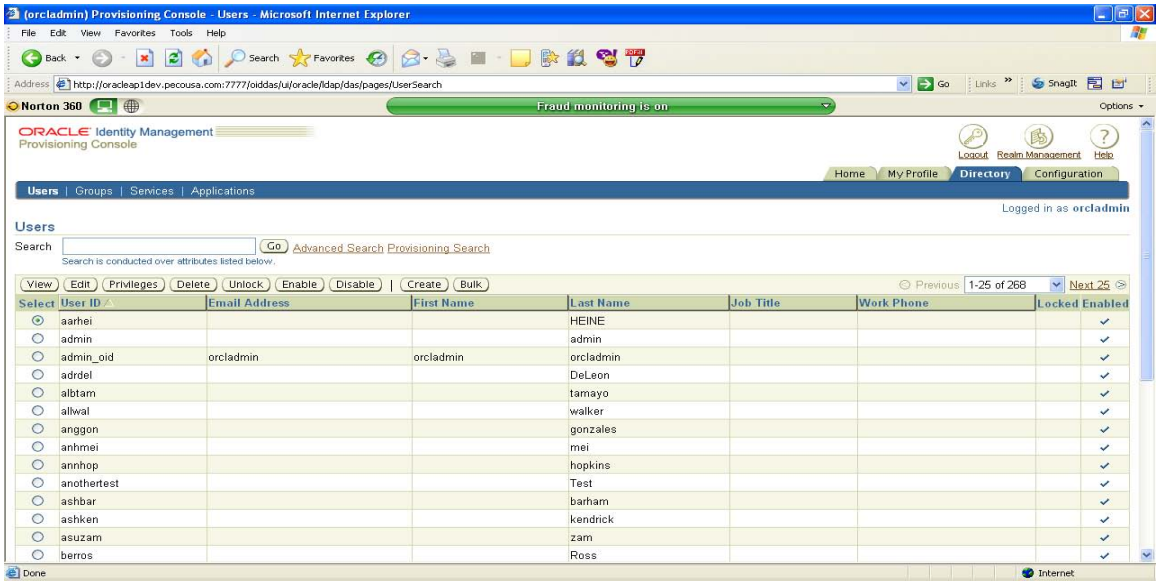

Exhibit 14

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.

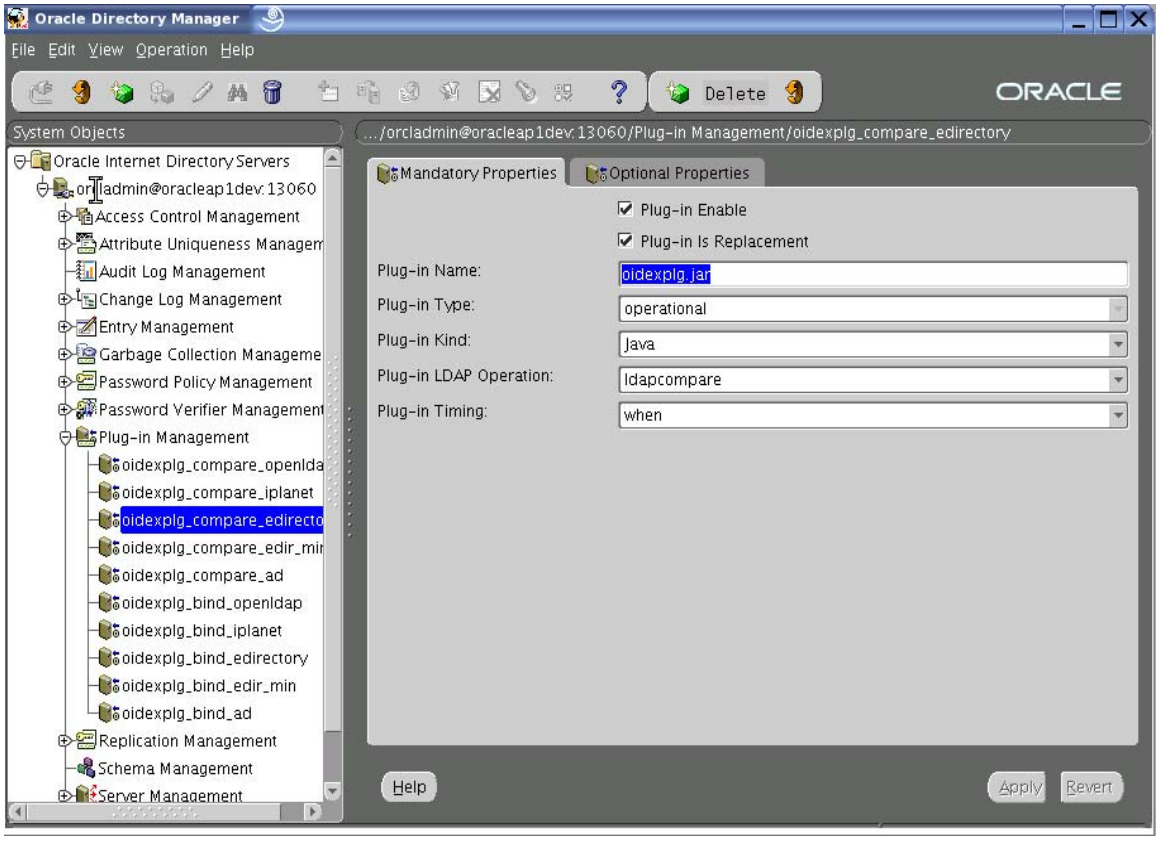

Exhibit 15

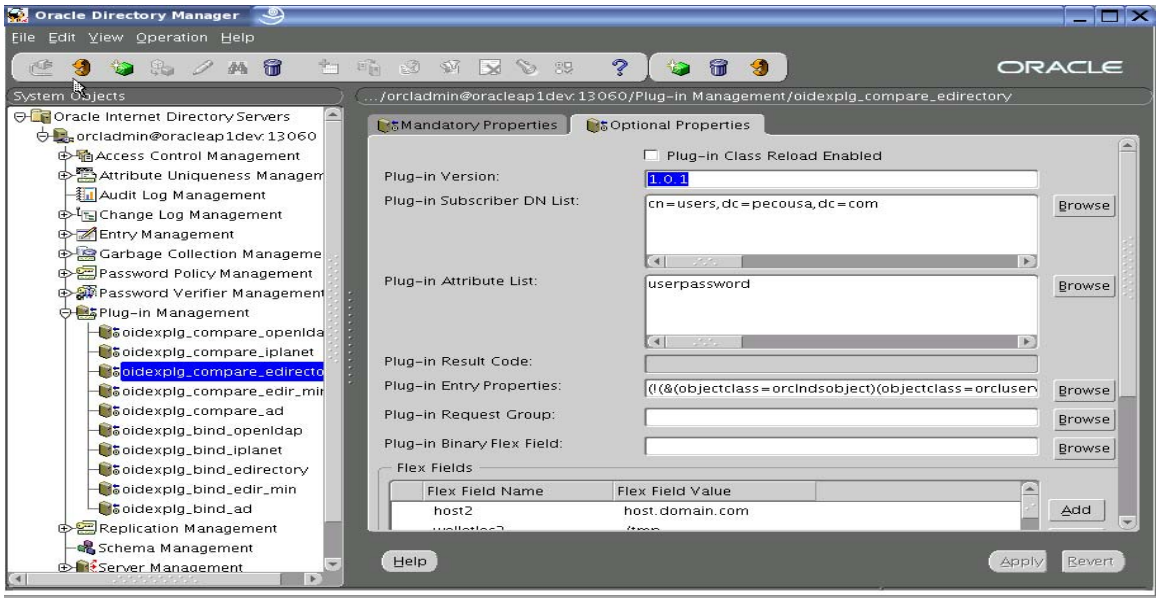

Exhibit 16

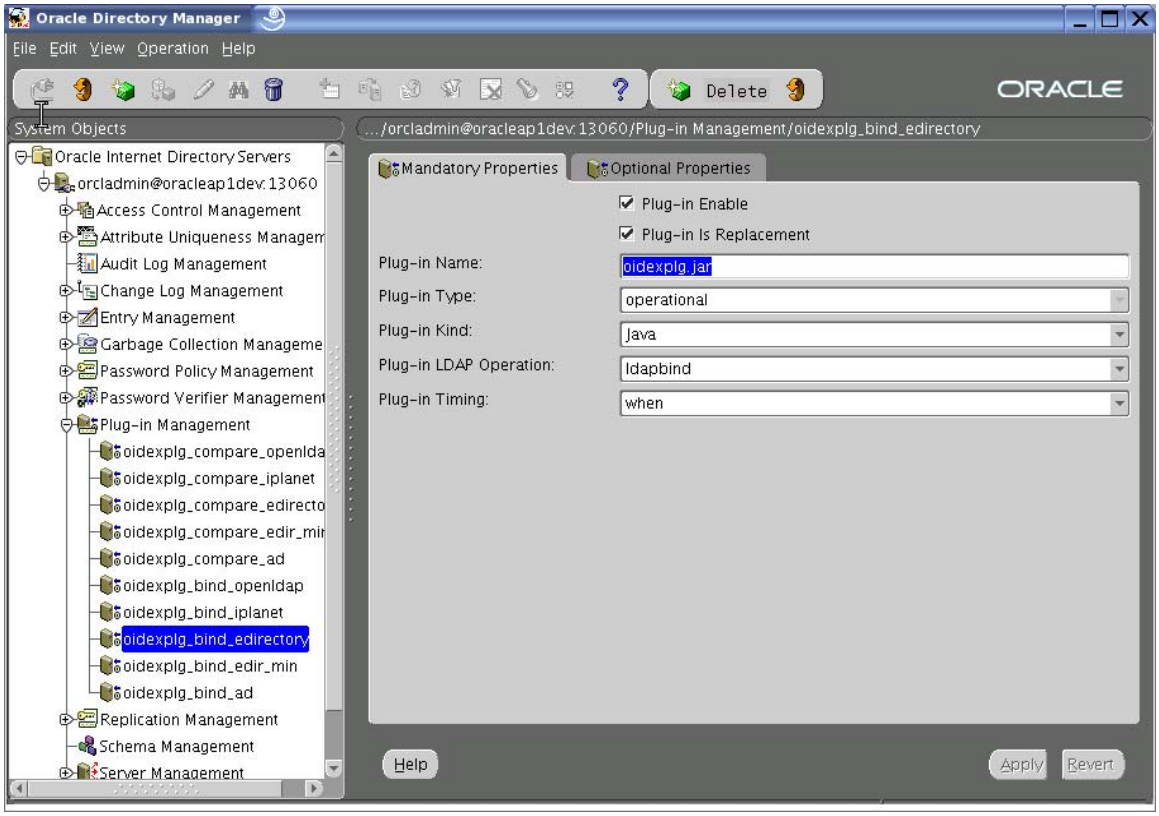

Exhibit 17

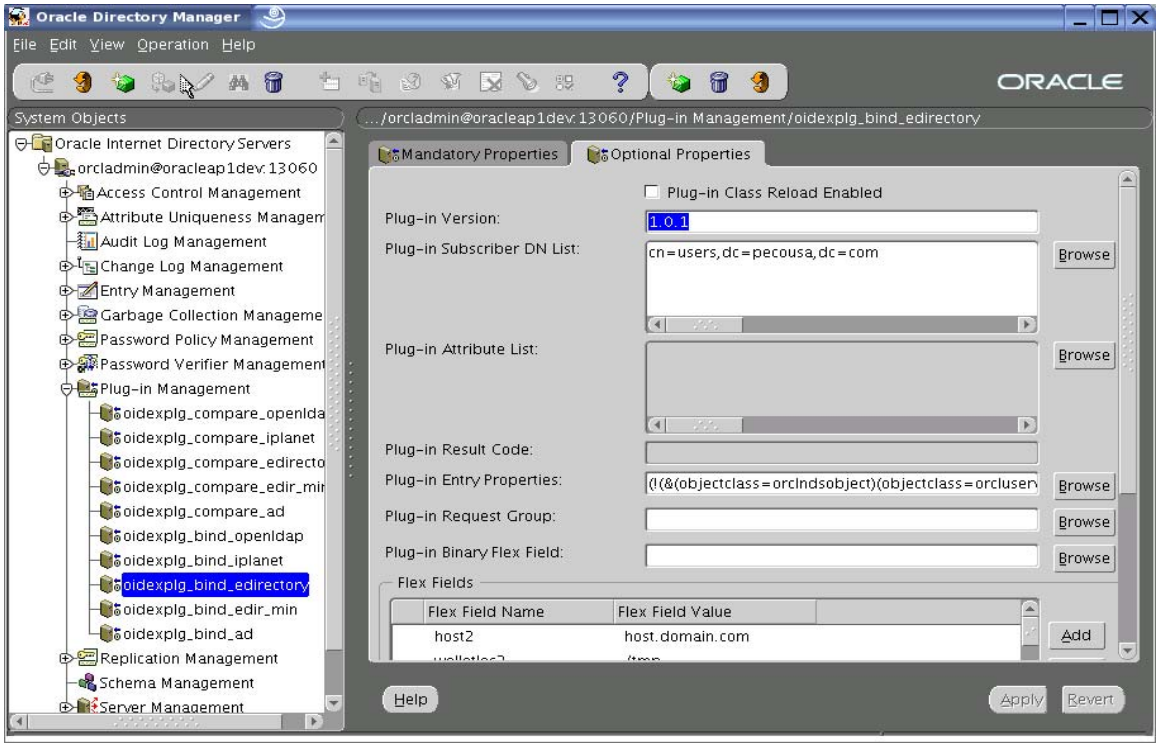

Exhibit 18

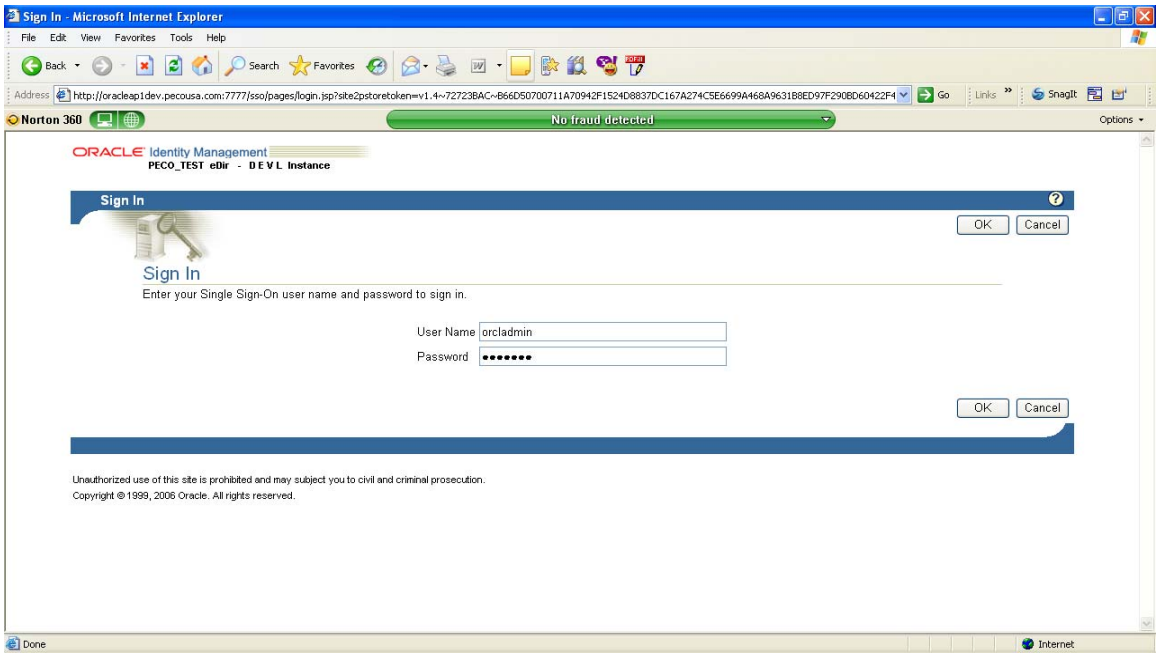

Exhibit 19

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.