Implementing Oracle Identity Management Using External Authentication Plug-In

Dinesh Gupta

Lucidity Consulting Group

Corporate Information:



The better way to make business decisions.









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.

C Oracle Relationship

Lucidity works exclusively with Oracle products and has achieved Oracle's highest partner status. Lucidity was named Oracle's <u>"Partner of the Year"</u> 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 "<u>Certified Advantage Partner</u>" 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	From third-party user repository to OID
information with external directory	
Method for initial population of user	From third-party user repository to OID to
information in OID and Release 11i	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	From third-party user repository to OID to
information	Release 11i

<u>Exhibit 1</u>

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.

Oracle Universal Installer: Select a Product to Install	🧐 _ ×
Select a Product to Install	10^{g}
COracle Identity Federation 10g	
Oracle Identity Federation is a standalone, standards-based feo enterprises to form trusted relationships across disparate secu	derated identity management solution enabling urity domains quickly and securely.
Oracle Application Server Infrastructure 10g	
Application Server Certificate Authority and others.	
	Product Languages)
Help Installed Products Back	Next Install Cancel

Exhibit 3

🔀 Oracle Universal Installer: Select Installation Type	_ ×
10	8
Select Installation Type	
Oracle Application Server Infrastructure 10g 10.1.4.0.1	
What type of installation do you want?	
Identity Management and Metadata Repository (4.01GB)	
This option installs and configures Identity Management services (Oracle Internet Directory, Single Sign- Delegated Administration Service, Directory Integration Platform, and Certificate Authority) and an Orac 10.1.0.5.0 database containing the Oracle Application Server Metadata Repository. (Requires 1024 MB R configured on your machine)	-On, Ie AM
C Identity Management (1.26GB)	
This option installs and configures Identity Management services (see above for component list). To configure Oracle Internet Directory or Certificate Authority, you need an existing Oracle Application Ser Metadata Repository. (Requires 1024 MB RAM configured on your machine)	ver
C Metadata Bepository (4.01GB)	
This option installs a new Oracle 10.1.0.5.0 database containing the Oracle Application Server Metadata Repository. This Repository can be used by Oracle Application Server Instances and/or Identity Manager services. (Requires 1024 MB RAM configured on your machine)	ment
- Help) Installed Products) Back Next Install (ncel)
ORACLE	

<u>Exhibit 4</u>

Sel	ect Configuration Options		
Selec nstal	t the components that you would like to configure llation.	and automatically start at the end of the	
Dracl f you hen	le Application Server Metadata Repository is alwa I want to use an existing Oracle Internet Directory prompt you to enter the location of the existing O	ys configured. ; then do not select it below. The installer will racle Internet Directory.	
	Available Components:	Description	-
	Oracle Application Server Metadata Repository	Configures Oracle Application Server Metadat	
	Oracle Application Server Metadata Repository Oracle HTTP Server	Configures Oracle Application Server Metadat Serves static and dynamic Web content.	
	Oracle Application Server Metadata Repository Oracle HTTP Server Oracle Application Server Containers for J2EE	Configures Oracle Application Server Metadat Serves static and dynamic Web content. Runs Enterprise Java applications.	
	Oracle Application Server Metadata Repository Oracle HTTP Server Oracle Application Server Containers for J2EE Oracle Internet Directory	Configures Oracle Application Server Metadat Serves static and dynamic Web content. Runs Enterprise Java applications. Configures an LDAP server for identity and se	
	Oracle Application Server Metadata Repository Oracle HTTP Server Oracle Application Server Containers for J2EE Oracle Internet Directory Oracle Application Server Single Sign-On	Configures Oracle Application Server Metadat Serves static and dynamic Web content. Runs Enterprise Java applications. Configures an LDAP server for identity and se Configures a directory-enabled single sign-or	r
	Oracle Application Server Metadata Repository Oracle HTTP Server Oracle Application Server Containers for J2EE Oracle Internet Directory Oracle Application Server Single Sign-On Oracle Application Server Delegated Administr	Configures Oracle Application Server Metadat Serves static and dynamic Web content. Runs Enterprise Java applications. Configures an LDAP server for identity and se Configures a directory-enabled single sign-or Provides web-based identity and security add	r r
	Oracle Application Server Metadata Repository Oracle HTTP Server Oracle Application Server Containers for J2EE Oracle Internet Directory Oracle Application Server Single Sign-On Oracle Application Server Delegated Administr Oracle Directory Integration Platform	Configures Oracle Application Server Metadat Serves static and dynamic Web content. Runs Enterprise Java applications. Configures an LDAP server for identity and se Configures a directory-enabled single sign-or Provides web-based identity and security add Enables directory synchronization and user additional security and security and security and security and security additional security synchronization and user additional security and security and security and security and security additional security synchronization and user additional security and security additional security synchronization and user additional security additional security synchronization and user additional security additional security additional security additional security synchronization and user additional security addit	r r
	Oracle Application Server Metadata Repository Oracle HTTP Server Oracle Application Server Containers for J2EE Oracle Internet Directory Oracle Application Server Single Sign-On Oracle Application Server Delegated Administr Oracle Directory Integration Platform Oracle Application Server Certificate Authority (Configures Oracle Application Server Metadat Serves static and dynamic Web content. Runs Enterprise Java applications. Configures an LDAP server for identity and se Configures a directory-enabled single sign-or Provides web-based identity and security add Enables directory synchronization and user an Creates and manages security certificates.	r r

<u>Exhibit 5</u>

🗽 Oracle Universal Installer	: Specify Namespace in Internet Directory	() _ ×
R		
Specify Namespa	ace in Internet Directory	
Specify a location, or namesp Management policies. This na	ace, in Oracle Internet Directory to contain user amespace will be the default Identity Manageme	rs, groups, and Identity ant Realm.
Suggested Namespace:	dc=pecousa, dc=com	
C Custom Namespace:	Example: dc=acme,dc=com	
Help Installed Pr	oducts Back Next	Install <u>Cancel</u>

<u>Exhibit 6</u>

Oracle Universal Installe	er: Specify Database Configuration Options
Specify Databa	se Configuration Options
Database Naming A Global Database Name, database. In addition, eac Specify the Global Databas	typically of the form "name.domain", uniquely identifies an Oracle ch datalyase is referenced by at least one Oracle System Identifier (SID). se Name ^a and SID for this database.
Global Database Name:	infradb.pecousa.com SID: infradb
"Help" for the definition of Standard UTF-8 AL32UTF8	Incups to be stored determine which database character set to use. See Ianguage groups. For the Unicode database character set, select "Unicode 8"
Select Database Characte	er set: Unicode standard UTF-8 AL32UTF8 🔹
 Database File Location Use the file system for data recommends installing data 	abase storage. For best database organization and performance, Oracle tabase files and Oracle software on separate disks.
Specify Database File Loc	cation: /home/oraas/oradata/ Browse
Help Installed [Products) Back Next Install Cancel

<u>Exhibit 7</u>

pecify Instance Name and ias_admin Password I oracle Application Server Infrastructure instances installed on a host must have unique names. The installated of the instance name. ach Oracle Application Server Infrastructure instance has its own password; regardless of which user efformed the installation. Passwords are not shared across instances, even if the instances were stalled by the same user. he password must have a minimum of 5 alphanumeric characters, maximum 30 characters, and at as to ne of the characters must be a number. administrator Username: las_admin istance Name: identity as admin Password: method installed products Back Best install orAccle Exhibit 8 recise Universal Installer: Specify Database Schema Passwords Install on stall ston. After the installation is complete, you must unlock and se asswords for these accounts will not expire. Specify the same undoked at the end of installation. After the installation is complete, you must unlock and se asswords for these accounts will not expire. Specify the same undoked at the end of installation. After the installation is complete, you must unlock and se asswords for these accounts will not expire. Specify the same used for these accounts will not expire. Specify the same user. If use different passwords for these accounts Installed confirm Password If use different passwords for these accounts Installed on the spire. Specify the same used for these accounts will not expire. Specify the same user.	Specify Instance Name and ias_admin Password. And Oracle Application Server Infrastructure instances installed on a host must have unique names in the instance mane of the host are appended to the instance mane. Each Oracle Application Server Infrastructure instance has its own password, regardless of which berformed 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, an east one of the characters must be a number. Administrator Username: ias_admin Instance Name: Indentity Ias_admin Password: Free password is installed Products Back Next Install Concole	. The
Proceeding and the set of the se	A confirm Password:	. The
Perception of the control of the set of the	Becify instance warme and has_addrive the instances installed on a host must have unique names ostname and domain name of the host are appended to the instances name. ach Oracle Application Server Infrastructure Instances has its own password, regardless of which erformed the installation. Passwords are not shared across instances, even if the instances were stalled by the same user. The password must have a minimum of S alphanumeric characters, maximum 30 characters, and the instance Name is a number. The password must have a minimum of S alphanumeric characters, maximum 30 characters, and the the for the characters must be a number. The password must have a minimum of S alphanumeric characters, maximum 30 characters, and the instance Name is identity as_admin Passyord: The password installed Products Back Next Install Definition Exhibit 8 Definition Def	. The
I Oracle Application Server Infrastructure instances installed on a host must have unique names. The astheme and domain name of the host are appended to the instance name. ach Oracle Application Server Infrastructure instance has its own password, regardless of which user erformed the installation. Passwords are not shared across instances, even if the instances were stalled by the same user. The password must have a minimum of 5 alphanumeric characters, maximum 30 characters, and at ast one of the characters must be a number. administrator Username: i.a_admin instance Name: [identity a_a_admin Password: ************************************	Il Oracle Application Server Infrastructure instances installed on a host must have unique names ostname and domain name of the host are appended to the instance name. Application Server Infrastructure instance has its own password, regardless of which erformed the installation. Passwords are not shared across instances, even if the instances were stalled by the same user. In the password must have a minimum of 5 alphanumeric characters, maximum 30 characters, an east one of the characters must be a number. Identity as_admin Password: "************************************	. The
ach Oracle Application Server Infrastructure Instance has its own password, regardless of which user stalled by the same user. The password must have a minimum of S alphanumeric characters, maximum 30 characters, and at ast one of the characters must be a number. Imministrator Username: las, admin Instance Name: [Identity as, admin Password: ******* centime Password: ******* centime Password: ******* centime Device The Section	ach Oracle Application Server Infrastructure instance has its own password, regardless of which erformed the installation. Passwords are not shared across instances, even if the instances were stalled by the same user. he password must have a minimum of 5 alphanumeric characters, maximum 30 characters, an hast one of the characters must be a number. dministrator Username: ias_admin Instance Ngme: Identity as_admin Password: enter Passwords for these accounts enter Passwords for these accounts. enter Password confirm Password for france accounts. enter Password for france account for the for the for the for the for the for the for th	
he password must have a minimum of 5 alphanumeric characters, maximum 30 characters, and at ast one of the characters must be a number. dministrator Username: las_admin instance Name: [Identity] as_admin Password: [*******] Help Installed Products Back Next Install Cancel CRACLE Pecify Database Contents Passwords Pecify Database Schema Passwords Tacke Universal Installer: Specify Database Schema Passwords Pecify Database Contains pre-loaded schemas, most of which have passwords that will expire the blocked at the end of installation. After the installation is complete, you must unlock and se asswords for those accounts you wish to use. Schema used for the database management and stall functions are left unlocked, and passwords for these accounts will not expire. Specify the asswords for these accounts. Cy Lise different passwords for these accounts User Name Enter Password SYSTEM SYSTEM SYSTEM SYSTEM SYSTEM SYSTEM	he password must have a minimum of S alphanumeric characters, maximum 30 characters, an hast one of the characters must be a number. dministrator Username: las_admin nstance Name: [identity as_admin Password: *******	user e
dministrator Username: ias_admin instance Name: identity as_admin Password: ******* ignfirm Password: ******* Exhibit 8 reacle Universal Installer: Specify Database Schema Passwords Pecify Database Contains pre-loaded schemas, most of which have passwords that will expir to be locked at the end of installation. After the installation is complete, you must unlock and se asswords for these accounts you wish to use. Schemas used for the database management and the locked at the end of installation. After the installation is complete, you must unlock and se asswords for these accounts will not expire. Specify the asswords for these accounts	dministrator Username: ias_admin nstance Name: identity as_admin Password: ******* Egnfirm Password: ******* Egnfirm Password: ******* Eleip Installed Products Back Next Install C CRACLE DracLE DracLE DracLE DracLE DracLE DracLE DracL	id at
Instance Name: Identity as_admin Password: Improvement	Instance Name: Identity as_admin Password: ****** Confirm Password: ****** Dentify Password: ****** Dentify Password: ****** Dentify Datable Products Back Next Install C Dentify Datable Products Back Next Install Dentify Datable Products Dentify Datable Products Product Products	
Instance Name: Identity as_admin Password: Important Password:	Instance Name: Identity as_admin Password: ****** Confirm Password: ****** Dentify Password: ****** Dentify Database Passwords (******* Dentify Database Schema Passwords Dentify Database Contains pre-loaded schemas, most of which have passwords that will not be locked at the end of installation. After the installation is complete, you must unlock at asswords for those accounts you wish to use. Schemas used for the database management istall functions are left unlocked, and passwords for these accounts will not expire. Specify to asswords for these accounts. Contains the end of these accounts Contains are left unlocked, and passwords for these accounts will not expire. Specify to asswords for these accounts Contains are left unlocked and passwords for these accounts will not expire. Specify to asswords for these accounts Contains are left unlocked and passwords for these accounts will not expire. Specify to asswords for these accounts Contains are left unlocked and passwords for these accounts will not expire. Specify to asswords for these accounts Contains are left unlocked at the end of these accounts Contains are left unlocked and passwords for these accounts will not expire. Specify to asswords for these accounts Contains are left unlocked and passwords for these accounts will not expire. Specify to asswords for these accounts Contains are left unlocked and passwords for these accounts will not expire. Specify to asswords for these accounts Contains are left and and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left and a passwords for these accounts Contains are left a	
Identity as_admin Password:	Identity as_admin Password: Identity as_admin Password: Installed Products Back Next Install DracLe Installed Products Back Next Install DracLe Exhibit 8 Dracle Universal Installer: Specify Database Schema Passwords Specify Database Contains pre-loaded schemas, most of which have passwords that will not be locked at the end of installation. After the installation is complete, you must unlock at asswords for those accounts you wish to use. Schema used for the database management Istall functions are left unlocked, and passwords for these accounts will not expire. Specify to asswords for these accounts. Cuse different passwords for these accounts Diser Name Enter Password Sys	
as_admin Password:	as_admin Password: ****** Ignfirm Password: ******* Ignfirm Password: ******* Ignfirm Password: ******** Ignfirm Password: ******* Ignfirm Password: ******** Ignfirm Password: ************************************	
entre Password:	Installed Products Back Next Install Install CRACLE Installed Products Back Next Install Exhibit 8 Dracle Universal Installer: Specify Database Schema Passwords Specify Database Schema Passwords Specify Database Contains pre-loaded schemas, most of which have passwords that will the Starter Database contains pre-loaded schemas, most of which have passwords that will the Starter Database contains pre-loaded schemas, most of which have passwords that will the Starter Database contains pre-loaded schemas, most of which have passwords that will the Starter Database contains pre-loaded schemas, most of which have passwords that will the be locked at the end of installation. After the installation is complete, you must unlock at asswords for those accounts you wish to use. Schemas used for the database management tstall functions are left unlocked, and passwords for these accounts will not expire. Specify t asswords for these accounts. Cuse different passwords for these accounts User Name Enter Password Confirm Password	
Help Installed Products Back Next Install Cancel ORACLE Exhibit 8 Practe Universal Installer: Specify Database Schema Passwords Image: Specify Content of the second schema Schema Passwords Image: Specify Content of the second schema Schema Passwords Image: Specify Content of the second schema Schema Passwords Pecify Database Schema Passwords Image: Specify Content of the second schema	Help Installed Products Back Next Install C CRACLE Exhibit 8 Oracle Universal Installer: Specify Database Schema Passwords Oracle Universal Installer: Specify Database Schema Passwords Specify Database Schema Passwords Oracle Universal Installer: Specify Database Schema Passwords Oracle Universal Installation. After the Installation is complete, you must unlock at asswords for those accounts you wish to use. Schemas used for the database management istall functions are left unlocked, and passwords for these accounts will not expire. Specify tasswords for these accounts. Or Use different passwords for these accounts User Name Oracle Password Onfirm Password Oracle Password	
asswords for those accounts you wish to use. Schemas used for the database management and stall functions are left unlocked, and passwords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the asswords for these accounts will not expire. Specify the assword for these accounts will not expire. Specify the assword for these accounts will not expire. Specify the assword for these accounts will not expire. Specify the assword for these accounts will not expire. Specify the assword for these accounts will not expire. Specify the assword for these accounts will not expi	asswords for those accounts you wish to use. Schemas used for the database management stall functions are left unlocked, and passwords for these accounts will not expire. Specify t asswords for these accounts. C Use different passwords for these accounts User Name Enter Password Confirm Password SYS	
C Use different passwords for these accounts User Name Enter Password Confirm Password SYS SYSTEM SYSMAN DBSNMP C	C Use different passwords for these accounts User Name Enter Password Confirm Password SYS	expire
Cuse different passwords for these accounts User Name Enter Password SYS SYSTEM SYSMAN DBSNMP Image: State of the second secon	User Name Enter Password Confirm Password	expire nd set and p the
User Name Enter Password Confirm Password SYS SYSTEM SYSMAN DBSNMP	User Name Enter Password Confirm Password SYS	expire nd set and p the
SYS SYSTEM SYSMAN DBSNMP	SYS	expire nd set and p the
SYSTEM SYSMAN DBSNMP		expire nd set and p the
	STSTEM	expire nd set and p the
	SYSMAN	expire nd set and p the
	DESNMP	expire nd set and p the
		expire nd set and p the

<u>Exhibit 9</u>

Back

Next

) [nstall] (

Installed Products...)

Help

ORACLE

⊆ancel

×



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
- 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 \diamond 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
 - Idapbind -h 192.168.10.100 -h 389 -D "cn=admin,o=peco" -p *****
 - Connect to OID
 - Idapbind -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 expression fig -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/Idap/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/Idap/odi/conf/eDirectoryImport.map odip.profile.status=ENABLE

🔀 Oixcle Directory Manager Connect 🥃)	N	_ 🗆 🗙
	💂 Credentials	E SSL	
	User:	orcladmin	&
	Server:		
Oracle	Derver.	Oracleapidev	
In the second Dimension	Port:	13060	
Internet Directory		SSL Enabled	
	Help)	Login	Cancel)
	Copyright (C) 199	8, 2006, Oracle. All rights resen	/ed.



Exhibit 12

National Providence of the second sec			
ile Edit View Operation Help			
CE 19 😒 🗞 🖉 🗛 🕤 🖆 🖻		? 💊 🗑 🧐	ORACLE
System Objects 🦳 🔵 🤇	/orcladmin@oracleap1dev:	13060/Server Management/Inte	gration Server/Configuration Set1
🖯 🛅 Oracle Internet Directory Servers	Relintegration Connectors		
🕁 🚉 orcladmin@oracleap1dev.13060			
🖻 🐴 Access Control Management	Connector Name	Synchronization Mode	Connector Status
🕈 🛱 Attribute Uniqueness Managemer	eDirectoryImport	IMPORT	ENABLE
- 🚛 Audit Log Management	eDirectoryExport	EXPORT	DISABLE
🕁 🔄 Change Log Management	🛃 eDirectoryExp	EXPORT	DISABLE
🗈 📶 Entry Management	🚱 TaggedExport	EXPORT	DISABLE
🕀 🧟 Garbage Collection Management	Ca LdifExport	EXPORT	DISABLE
Password Policy Management	🚱 OracleHRAgent	IMPORT	DISABLE
Password Verifier Management	🚱 ActiveChgImp	IMPORT	DISABLE
🗈 🚉 Plug-in Management	🚱 OpenLDAPImport	IMPORT	DISABLE
E Replication Management	🚱 eDirectoryImp	IMPORT	DISABLE
Schema Management	🛃 TaggedImport	IMPORT	DISABLE
G	🚱 Idifimport	IMPORT	DISABLE
Directory Server	🚱 IplanetExport	EXPORT	DISABLE
E Replication Server	🚱 ActiveExport	EXPORT	DISABLE
Elintegration Server	🛃 ActiveImport	IMPORT	DISABLE
	🚱 OpenIdapExport	EXPORT	DISABLE
Separa Chaining Management	🚱 IplanetImport	IMPORT	DISABLE
			Create Edit Delete Befresh
	Help		

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:

	dmin) Provisioning	g Console - Users - Microsoft Intern	et Explorer				
File E	dit View Favorites	Tools Help					<u></u>
О В	ack • 🕥 - 💌	😰 🏠 🔎 Search 🔶 Favorite	s 😧 🎯 - 🎽 🔳 - 📘] 除 🋍 🧐 📅			
Address	http://oracleap1de	v.pecousa.com:7777/oiddas/ui/oracle/idap/d	las/pages/UserSearch			💌 🔁 Go 🛛 Lir	nks 🎽 🍯 Snagit 🔁 📷
O Norto	n 360 🖪 🛞		(Fraud monitoring is on			Options 👻
Provis	CLE Identity Ma ioning Console	ces Applications				Home My Profile Dire	t Realm Management Help Ctory Configuration
Users		(G) 11-1-1-1	Courts Designation Courts				Logged in as orcladmin
Dearch	Search is conducted	over attributes listed below.	Search Provisioning Search				
View	(Edit) (Privileges	Delete Unlock Enable Di	sable) (Create) (Bulk)			© Previous 1-2	5 of 268 💉 Next 25 🛞
(View Select	Edit Privileges	Delete Unlock Enable Di Email Address	sable) Create) Bulk	Last Name	Job Title	Previous 1-2 Work Phone	5 of 268 Vext 25 S
View Select) (Edit) (Privileges User ID / aarhei	5) Delete) Unlock) Enable) Di Email Address	sable) Create) Bulk) First Name	Last Name HEINE	Job Title	O Previous 1-2 Work Phone	5 of 268 Vext 25 S Locked Enabled
View Select) (Edit) (Privileges User ID / aarhei admin	Email Address	sable) Create) Bulk) First Name	Last Name HEINE admin	Job Title	Previous 1-2 Work Phone	5 of 268 V Next 25 S Locked Enabled
View Select) Edit (Privileges User ID / aarhei admin admin_oid	Delete Unlock Enable Di Email Address orcladmin	sable) Create) (Bulk) First Name orcladmin	Last Name HEINE admin orcladmin	Job Title	Previous 1-2 Work Phone	5 of 268 V Next 25 S Locked Enabled
View Select	Edit) (Privileges) User ID aarhei admin admin_oid adrdel	5) Delete Unlock Enable Di Email Address orcladmin	sable) (Create) (Bulk) First Name orcladmin	Last Name HEINE admin orcladmin DeLeon	Job Title	O Previous 1-2	5 of 268 V Next 25 S Locked Enabled
View Select	Edit Privileges User ID A aarhei admin admin_oid adrdel albtam	5 Delete Uniock Enable Di Email Address orcladmin	sable) (Create) (Bulk) First Name orcladmin	Last Name HEINE admin orcladmin DeLeon tamayo	Job Title	O Previous 1-2	5 of 268 V Next 25 3 Locked Enabled
View Select O O O O	Edit Privileges User ID A aarhei admin admin_oid adrdel albtam allwal	i) Delete) Unlock) (Enable) (Di Email Address orcladmin	sable) Create) (Bulk) First Name orcladmin	Last Name HEINE admin orcladmin DeLeon tamayo walker	Job Title	O Previous 1-2	5 of 268 VNext 25 3
View Select O O O O O O O	Edit) (Privileges User ID aarhei admin admin_oid adrdel albtam allwal anggon	Eletete) (Uniock) (Enable) (Di Email Address orcladmin	sable) Create) (BUIK) First Name orcladmin	Last Name HEINE admin DeLeon tamayo walker gonzales	Job Title	O Previous 1-2	5 of 268 V Next 25 S Locked Enabled V V V V V V V V V V V V V V V V V V V
View Select O O O O O O O O	Edit (Privileges User ID aarhei admin admin_oid adrdel albtam allwal anggon anhmei	j) Delete) (Unlock) (Enable) (Di Ermall Address orcladmin	sable) (Create) (Bulk) First Name orcladmin	Last Name HEINE admin orcladmin DeLeon tamayo walker gonzales mei	Job Title	OPrevious 1-2	5 of 268 V Next 25 S Locked Enabled
View Select	Edit (Privileges User ID aarhei admin admin_oid adridel albtam allwal anggon anhmei annhop	i) Delete) (Uniock) (Enable) (Di Email Address orcladmin	sable) Create) (Bulk.) First Name orcladmin	Last Name HEINE admin orcladmin DeLeon tamayo walker gonzales mei hopkins	Job Title	OPrevious 12	5 of 268 V Next 25 © Locked Enabled
(View Select ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	Edit (Privileges User ID ~ aarhei admin_oid admin_oid addel albtam albtam albtam anbmei annhmei annhmep anothertest	 Delete) (Uniock) (Enable) (Di Email Address orcladmin 	sable Create) Bulk First Name orcladmin	Last Name HEINE admin orcladmin DeLeon tamayo walker gorzales mei hopkins Test	Job Title	OPrevious 1-2	5 of 268 Y Next 25 (*) Locked Enabled
(View Select ⊙ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	Cetit) (Privileges User ID ▲ aarhei admin_oid adridel albtam ankwai ankmei annhmei annhmei anshbar	Eletete) (Unick) (Enable) (Di Email Address orcladmin	sable) (Create) (Bulk) First Name orcladmin	Last Name HEINE admin orclatmin DeLeon tamayo walker gonzales mei hopkins Test barham	Job Title	OPrevious 1-2	5 of 268 V Next 25 S Locked Enabled
(View Select ⊙ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	CERT Q Privileges User ID ▲ aarhei admin admin_oid adrdel albtam albtam albtam anhmei annhop anothertest ashbar ashkan	5) Delete) (Uniock) (Enable) (Di Email Address orcladmin	sable) Create) (Bulk) First Name orcladmin	Last Name HEINE admin orcladmin DeLeon tamayo walker gonzales mei hopkins Test barham kendrick	Job Title	OPrevious 1-2	5 of 268 V Next 25 © Locked Enabled
(View Select 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	(Edit) (Privileges User ID ∧ aarhei admin admin_oid adrdel albtam altwal anggon anhmei annhop annhop anothertest ashbar astken assuzam	Enable (Unick) (Enable) (Di Email Address orcladmin	sable Create) Bulk First Name orcladmin	Last Name HEINE admin orcladmin DeLeon tamayo walker gozzales mei hopkins Test barham kendrick zam	Job Title	OPrevious 1-2	5 of 268 Y Next 25 (*) Locked Enabled

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 Idapbind 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/Idap/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 Idapbind, 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 🥯			_ 🗆 ×
Eile ⊑dit ⊻iew Operation Help			
(@ 🧐 😘 🖉 🗛 😚 👈	6 3 V 🔀 📎 19	? 😂 🗃 🧐	ORACLE
(System Objects	(/orcladmin@oracleap1dev:13)	060/Plug-in Management/oidexplg_compare_edirect	ory
⊖ Gacle Internet Directory Servers	💽 🕈 Mandatory Properties 🗍 📦	SOptional Properties	
	Plug-in Version: Plug-in Subscriber DN List: Plug-in Attribute List:	Plug-in Class Reload Enabled Cn=users, dc=pecousa, dc=com Userpassword	Browse
Bit oidexplg_compare_openida Bit oidexplg_compare_iplanet Bit oidexplg_compare_edirecto Bit oidexplg_compare_edir_mir Bit oidexplg_compare_edir_mir Bit oidexplg_compare_edir_mir Bit oidexplg_bind_openidap Bit oidexplg_bind_openidap	Plug-in Result Code: Plug-in Entry Properties: Plug-in Request Group: Plug-in Binary Flex Field:	(+) (((&(objectclass = orcindsobject)(objectclass = o	Prowse Browse Browse Browse
Soidexplg_bind_edirectory	Flex Fields Flex Field Name host2 Help	Flex Field Value host.domain.com	Apply Bevert

Exhibit 16



Exhibit 17

🙀 Oracle Directory Manager 🧕			
Eile Edit ⊻iew Operation Help			
🕑 🧐 🐚 🗞 📈 🗛 🕤 👘		? 💊 🗑 🧐	ORACLE
(System Objects)	/orcladmin@oracleap1dev.1	3060/Plug-in Management/oidexplg_bind	d_edirectory
⊖ 🕞 Oracle Internet Directory Servers 🛛 🛋	Mandatory Properties	S Optional Properties	
🖯 🚉 orcladmin@oracleap1dev:13060	Containation y Properties		
⊕ Ccess Control Management		🗌 Plug-in Class Reload Enabled	—
🕀 🖀 Attribute Uniqueness Managerr	Plug-in Version:	1.0.1	
-🌆 Audit Log Management	Plug-in Subscriber DN List:	cn=users dc=pecousa dc=com	Browse
⊕ ^{_1} t _l Change Log Management	-		Browse
🕀 📶 Entry Management			- 2
🕀 쪒 Garbage Collection Manageme			
⊕ 🕾 Password Policy Management	Plua-in Attribute List:		Drouuro
🕀 🔐 Password Verifier Management			Erowse
🖓 🏥 Plug-in Management			
- to be a compare openida - to be a compare		a	
- iplanet	Plug-in Result Code:		
- Soidexplg_compare_edirecto			
- idexplg_compare_edir_mir	Plug-In Entry Properties:	(!(&(objectclass=orcIndsobject)(o	bjectclass=orclusen Browse
- Compare_ad	Plug-in Request Group:		Browse
- Boidexplg_bind_openIdap	Blue in Dinon (Flow Field)		
- Soidexplg_bind_iplanet	Flug-In Binary Flex Fleid.		Browse
- Contemporation Contemporatio Contemporation Contemporation Contemporation Contemporation Conte	Flex Fields		
- Boodexplg_bind_edir_min	Flex Field Name	Flex Field Value	A
	host2	host.domain.com	Add
Replication Management	Cantallau.	/tmn	
- Korema Management	Halp		Marriel Rowert
⊕ Server Manaαement			ShbiA Reast

Sign in Microsoft Internet Explore:				
Net RX Were You Revolte Total You Revolte You Rev	Sign In	- Microsoft Internet Explorer		
Index is probled and new subjed you be child and orthinal prosecution. Copyright 0 1599, 2000 Cnack. All rights reserved.	File Edi	View Favorites Tools Help		A
Anderes <	G Bad	🔹 💿 - 🖹 🗟 🏠 🔎 Search 👷 Favorites	🔗 🍛 🗷 · 🖵 除 🏭 💙 📅	
Notrand 30	Address 🧔	http://oracleap1dev.pecousa.com:7777/sso/pages/login.jsp?site2p	storetoken=v1.4~72723BAC~B66D50700711A70942F1524D8837DC167A274C5E6699A468A	49631B8ED97F290BD60422F4 🔽 🋃 Go 🛛 Links 🍟 🍃 Snaglt 🛐 🔡
CRACE identity Management PECO_TEST eff& - 0 E V L Instance Sign In CK Cancel Sign In CK Cancel User Name orcladmin Password CK Cancel CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL CK CANCEL	O Norton	360 💶 🌐	No fraud detected	Options •
Sign In C Cancel Sign In Enter your Single Sign-On user name and password to sign in. User Name orcladmin Password C Cancel C C C Cancel C C C Cancel C C C Cancel C C C Cancel C C C Cancel C C C Cancel C C C Cancel C C C Cancel C C C C C C C C C C C C C C C C C C C		ORACLE Identity Management PECo_TEST eDir - D E V L Instance		
Enter your Single Sign-On user name and password to sign in. User Name orcladmin Password •••••• User Name orcladmin Password •••••• OK Cancel Unadhritzed use of this ate is prohibited and may subject you to civil and criminal prosecution. Copyright © 1999, 2006 Oracle. All rights reserved.		Sign In Sign In		OK Cancel
User Name orcitadmin Password •••••• Uhauthorized use of this site is prohibited and may subject you to civil and criminal prosecution: Copyright @ 1989, 2006 Grade. All rights reserved.		Enter your Single Sign-On user name and	password to sign in.	
Password Cancel OK Cancel Unadhorized use of this stells prohibited and may subject you to civil and criminal prosecution. Copyright @ 1999, 2006 Oracle. All rights reserved. To Done To Done The met			User Name orcladmin	
OK Cancel Unauthorized use of this 3te is prohibited and may subject you to civil and criminal prosecution. Copyright © 1989, 2006 Oracle. All rights reserved.			Password ••••••	
Unadhorized use of this site is prohibited and may subject you to civil and criminal prosecution. Copyright © 1399, 2006 Oracle. All rights reserved.				OK Cancel
🗿 Done		Uneuthorized use of this site is prohibited and may subject you to ci Copyright © 1999, 2006 Oracle. All rights reserved.	ivil and criminal prosecution;	2
	🕘 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.