

Who, what, where, why and how?

Oracle Identity Management Solutions

Manpreet Singh Johal, Inatech Solutions Limited

This article gives an overview of Oracle Identity Management solutions and how to quickly deploy Oracle Enterprise Single Sign-On, using Oracle Internet Directory as a user profile and credential repository.

Identity management is the process by which the complete security lifecycle for end-users and network entities is managed for an organisation. Identity management most commonly refers to the management of an organisation's users, where steps in the security life cycle include account creation, deletion, suspension, privilege modification, and attribute management. The network entities managed include devices, processes, applications, servers, or anything else that needs to interact in a networked environment. Entities managed by an identity management process may also include users outside of the organisation, for example customers, suppliers, or trading partners.

Identity Management System Components

A complete identity management solution includes the following components:

- Scalable, secure, and standards compliant directory service for storing and managing the user information
- User-provisioning framework that can either be linked to the enterprise provisioning system (such as HR application), or that can be operated stand-alone
- Delegated administration model and application that allows the administrator of the identity management system to selectively delegate access rights to the administrator of the individual application or to the end-user directly. An appropriate security model, and user-interface model that can support various requirements is critical
- Directory integration platform that enables the enterprise to connect the Identity Management directory with legacy or application specific directory
- Run-time model and application for user authentication
- System to create and manage PKI certificates

Benefits

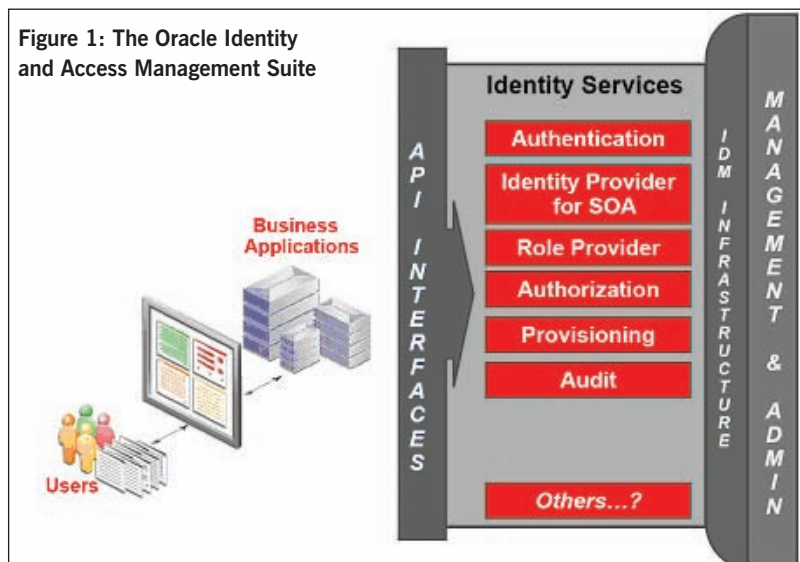
- **Identity management saves money.** For most enterprises, application user administration is a very expensive, laborious and error-prone process
- **Identity management enables faster deployments.** Typically, provisioning of a new application means creating and managing separate user accounts and their privileges. Identity Management enables the new applications to leverage the existing infrastructure for its user management, and thus reduces the time it takes to deploy and manage new applications
- **Identity management improves the end-user experience.** An identity management strategy allows new users to gain access to their applications quickly, eliminating wasted employee time. It also allows the users to modify any of their attributes or preferences at only one place, instead of changing it for every application
- **Identity management improves application security.** An identity management strategy allows users to have their passwords and security credentials managed centrally

Oracle Identity and Access Management Suite

Oracle Identity and Access Management Suite allows enterprises to manage end-to-end lifecycle of user identities across all enterprise resources within and beyond the firewall. Administrators can deploy applications faster, apply the most granular protection to enterprise resources, and automatically eliminate latent access privileges. The Oracle Identity and Access Management Suite is a member of Oracle Fusion Middleware family of products, which brings greater agility, better decision-making, and reduced cost and risk to diverse IT environments. (See Figure 1.)

The Oracle Identity and Access Management Suite include the following components:

- **Oracle Access Manager** delivers critical functionality for access control, single sign-on, and user profile management in heterogeneous application environments
- **Oracle Identity Manager** is a powerful and flexible enterprise identity provisioning and compliance monitoring solution that automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases and so on
- **Oracle Identity Federation** enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the box



- **Oracle Internet Directory**, a scalable, robust LDAP V3-compliant directory service that leverages the high availability capabilities of the Oracle 10g Database platform
- **Oracle Virtual Directory** provides internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronising or moving data from its native locations
- **Oracle Web Services Manager** is a comprehensive solution for adding policy-driven security and management capabilities to existing or new Web services
- **Oracle Enterprise Single Sign-On** provides users with unified single sign-on and authentication across all their enterprise resources, including desktops, client-server, and custom and host-based mainframe applications
- **Oracle Adaptive Access Manager** provides web access real-time fraud detection and multifactor online authentication security for the enterprise
- **Oracle Role Manager** is an authoritative source for role lifecycle management that leverages business policy and organisational data to automate role based provisioning and access control

Oracle Enterprise Single Sign-On (eSSO) Example Deployment

Oracle Enterprise Single Sign-On (eSSO) provides single sign-on functionality for all the enterprise applications i.e. web based, client-server and legacy applications. Users are able to use eSSO functionality whether they are connected to corporate network, traveling, or roaming between workstations.

Oracle Enterprise Single Sign-On uses any LDAP directory or any SQL database as its user profile and credential repository. It accepts primary authentication from Windows logon.

Oracle Enterprise Single Sign-On has the following components:

- i) **Oracle Enterprise Manager Single Sign-On Logon Manager**: allows users to securely use a single login credentials for all web based, client-server and legacy applications.
- ii) **Oracle Enterprise Single Sign-On Password Reset**: helps in reducing helpdesk calls by enabling users to manage Microsoft Windows password through self-service interfaces.
- iii) **Oracle Enterprise Single Sign-On Authentication Manager**: allows organisations to use a combination of tokens, smart cards, biometrics and password for strong authentication.

- iv) **Oracle Enterprise Single Sign-On Provisioning Gateway**: enables organisations to distribute single sign-on credentials to Oracle eSSO Manager based on provisioning instructions from Oracle Identity Manager.
- v) **Oracle Enterprise Single Sign-On Kiosk Manager**: allows users to securely access enterprise applications at distributed workstations.

For the purpose of this article, we shall demonstrate how to deploy **Oracle Enterprise Manager Single Sign-On Logon Manager (eSSO-LM)**, using Oracle Internet Directory as user profile and credential repository at Windows environment.

Step 1: Enterprise Single Sign-On Logon Manager (eSSO-LM) Admin Console Setup

This section assumes that Oracle Internet Directory is already installed and functional in your network.

1. Download Oracle Enterprise Manager Single Sign-On (eSSO) Suite from Oracle Technology Network (<http://www.oracle.com/technology/software/products/ias/htdocs/101401.html>)
2. Extract the software at C:\esso directory. Extraction will create sub-directories for each of Oracle eSSO sub-components under C:\esso directory.
3. Go to C:\esso\ESSO Logon Manager 10.1.4.0.5 and click on "ESSO-LM Admin Console.exe".
4. At **Welcome** screen, click **Next**.
5. At **License Agreement** screen, accept the agreement and click **Next**.
6. At **Setup Type** screen, select **Complete** option and click **Next**.
7. At **Ready to Install** screen, click at **Install**.
8. Click **Finish**, once installation is completed.

Step 2: Extend Oracle Internet Directory schema for eSSO-LM

1. Launch eSSO-LM Administration Console. Start -> Programs -> Oracle -> ESSO-LM -> ESSO-LM Console
2. Click on Repository -> Extend Schema menu option. (See Figure 2.)

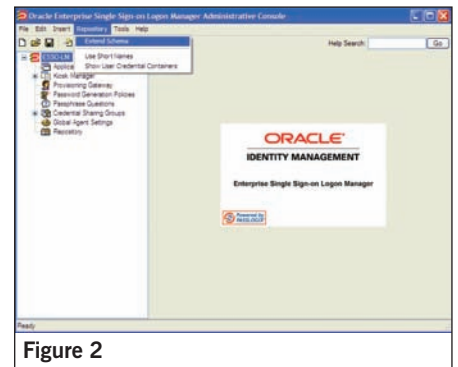


Figure 2

3. Connect to Oracle Internet Directory by entering following information, and click OK.

Server Name: lon-int-lap0586 or name of the server where OID is running.

Repository Type: Oracle Internet Directory.

Port: 389

Use secure channel (SSL): Uncheck Username/ID: cn=orcladmin

Password: <orcladmin password> (See Figure 3.)

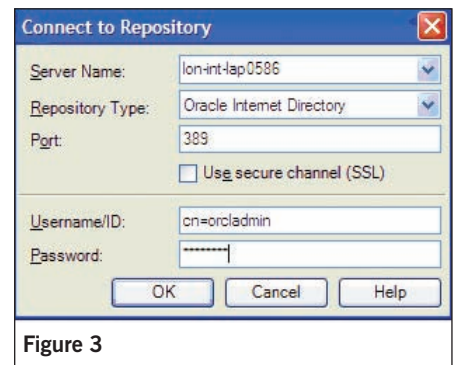


Figure 3

4. After successful extension of OID schema, following dialog will appear. Click on **Close**.
5. In order to store user credentials under respective OID user objects, an additional schema change and rights assignment is required. The OID user object needs to allow the creation of a child object of type eSSO-LM. A user also needs the right to create this object and credential objects under their own OID user object. Click at **Repository** link at left navigation of eSSO-LM Admin Console, and click on the link **Click here to connect** in right hand side pane. (See Figure 4.)

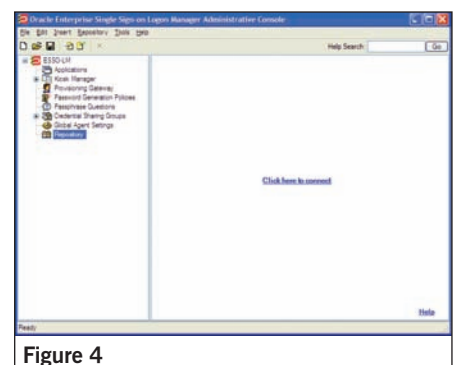


Figure 4

6. Enter OID connection information, as specified in Step 3. After successful authentication, OID schema information will appear in eSSO-LM Admin Console as following: (See Figure 5.)

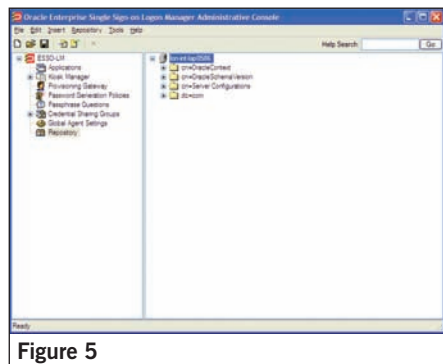


Figure 5

Step 3: Install eSSO-LM Agent

1. Go to C:\esso\ESSO Logon Manager 10.1.4.0.5 and click on “ESSO-LM.exe”.
2. At **Welcome** screen, click **Next**.
3. At **License Agreement** screen, accept the agreement and click **Next**.
4. At **Setup Type** screen, select **Custom** option and click **Next**.
5. At Custom Setup screen, four options will appear.

- a. **Application:** installs all necessary files and settings that serve as the core foundation of the application.
- b. **Logon Methods:** This option provides plug-ins for different methods of logging on to eSSO-LM. Choose **Windows Logon**.
- c. **Extensions:** This option provides plug-ins that enhance and extend the functionality of eSSO-LM.
 - i. **Backup/Restore Manager:** allows a user or administrator to backup a user’s passwords and settings to file and restore, if required. This feature should not be used along with synchroniser, due to conflicts in credentials time stamp.
 - ii. **Logon Manager:** this is a required component for credential management, request and delivery. It includes support for web application accessed through Internet Explorer or Firefox. Mainframe applications, console window applications such as Telnet and JAVA applications.
 - iii. **Setup Manager:** This plug-in provides the initial first time use experience when setting up the SSO application.
 - iv. Expand **Extensions -> Synchronisation Manage -> LDAP Synchroniser.** It will allow eSSO-LM to synchronise administration configuration, mobility and

- backup. Administrators can deploy configuration overrides to provide new registry, application template, and first-time use settings or to update existing settings. eSSO-LM synchronises credentials to a central repository i.e. OID, in this example.
- v. Expand **Event Manager** and choose **Windows Event Extension**. This plug-in supports logging of events to Windows Event Manager.
 - d. **Languages:** provides localised language support for various international languages.

6. At **Ready to Install** screen, click **Install**.
7. Click **Finish**, once installation is completed.

Step 4: Configuring OID with eSSO-LM

This section contains steps that enable credentials to be stored in and retrieved from Oracle Internet Directory. This section includes:

- Configure logon manager agent to connect to OID
- Create a container in OID for storing SSO information
- Configure a test application
- First time agent setup and confirmation of OID sync

1. Start the eSSO-LM Admin Console
2. Right click **Global Agent Settings** from left hand pane of Administrative Console. Select **Import**, and select **From Live HKLM**. This step imports current configuration from the local-machine registry entry on your system. Additional entries will appear in Administrative Console
3. Expand **Live -> Synchronisation**
4. Set **Enable role/group security support** by checking the appropriate box and selecting **Use role/group security** from the appropriate drop down box. Set **Sync Order** to **LDAPEXT** and **Interval for automatic re-sync** to 5. (See Figure 6.)

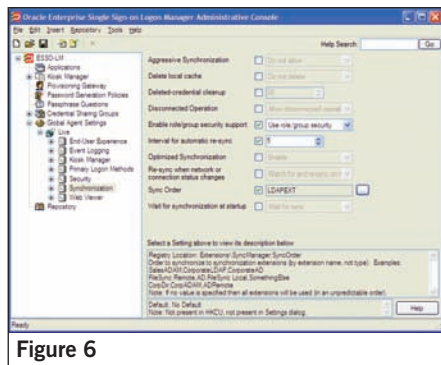


Figure 6

5. Navigate to **Global Agent Settings -> Live -> Synchronisation -> LDAPEXT -> Required**. Select **Directory Type** check box and specify value as **Oracle Internet Directory**. Select check box named **Servers** and specifies OID server hostname/IP address along with Port. (See Figure 7.)

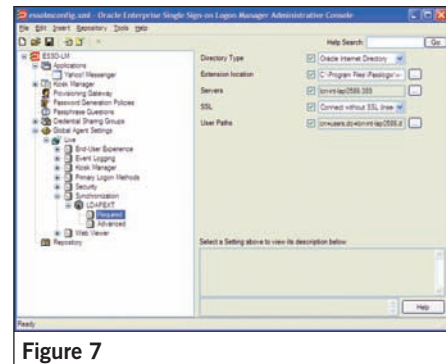


Figure 7

6. After configuring the eSSO-LM agent, we need to configure OID to store eSSO-LM application templates and configuration settings in OID. Login into **Repository** by clicking at link in left pane.
7. Right click on container named **dc=lon-int-lap0586, dc=com** and select **New Container**. Specify container name as **SSOConfig** and click **OK**. New container will appear in OID schema as following. (See Figure 8.)

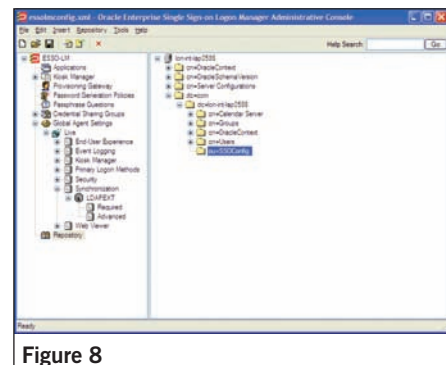


Figure 8

8. Update the eSSO-LM agent configuration to make use of container defined in earlier step to store application templates and configuration information. Navigate to **Global Agent Settings -> Live -> Synchronisation -> LDAPEXT -> Advanced**.
9. Check the check box next to **Configuration Objects Base Locations**, and click on button on right hand side of field. Specify container location as **ou=SSOConfig,dc=lon-int-lap0586,dc=com** and click **OK**.

10. Update the configuration information to OID. Click on **Repository** entry in left window pane. In right window pane, right click on container **ou=SSOConfig** and choose **Configure SSO Support** option.
11. At **Configure SSO Support** screen, select **Administrative Console** as data source, as we are uploading application template defined in eSSO-LM Administrative Console.
12. Choose configuration mode as **Advanced**, and click **Next**.
13. Click **Next**.
14. At **Global Agent Settings** screen, choose **Live** and click **Next**.
15. At summary screen, review the information and click **Finish**. **Yahoo! Messenger** application template information is uploaded in OID.
16. To update the client systems registry entries with updated information from OID container, choose menu option **Tools -> Write Global Agent Settings to HKLM**.
17. Restart client desktop.

Step 5: First Time Use (FTU) Agent Setup

1. After the system restart, login into your desktop/laptop. Since this is first time we are logging in after installing eSSO-LM Agent, First Time Use (FTU) wizard will appear and prompt for OID username/password to update the user information. (See Figure 9.)

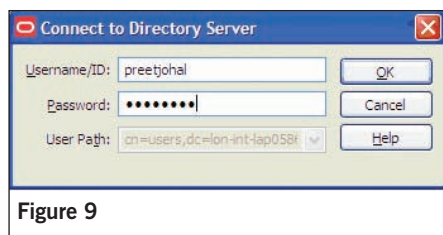


Figure 9

3. At **Primary Logon** screen, click **Next** and at next screen, choose **Windows Logon** and click **Next**. It will prompt for user's Windows credentials.
4. Provide the credentials and click **Next**.
5. Click **Finish** and eSSO-LM is ready for use.

Step 6: Add applications to eSSO-LM

In this section, we will demonstrate that how we can add a web application to eSSO-LM.

1. Launch Internet Explorer and open <http://metalink.oracle.com>
2. Click at Login to Metalink link. (See Figure 10.)

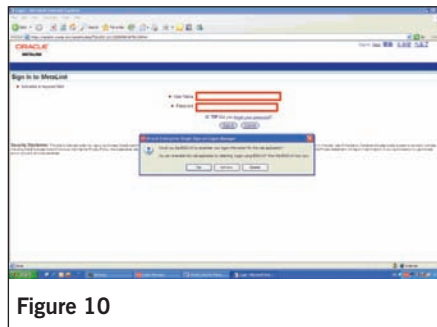


Figure 10

3. eSSO-LM will automatically detect web login page and will prompt user to enable ESSO-LM to remember the login details. Click **Yes**.
4. A **New Logon for Login** dialog will appear. Provide Metalink Username/Password details and click **Finish**. (See Figure 11.)

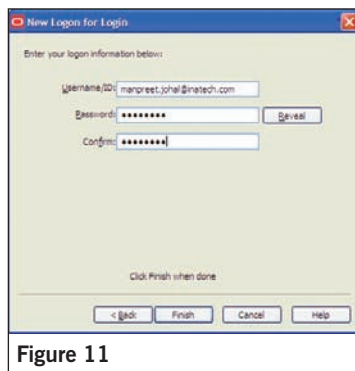


Figure 11

5. ESSO-LM will implicitly login user into Metalink with credentials provided.
6. Next time, whenever the user will access Metalink Login page, ESSO-LM will login user with credentials provided during application registration.
7. User can view the registered applications information by right clicking at ESSO-LM icon, which appears in system tray and choose **Configuration-> Logon Manager**. (See Figure 12.)

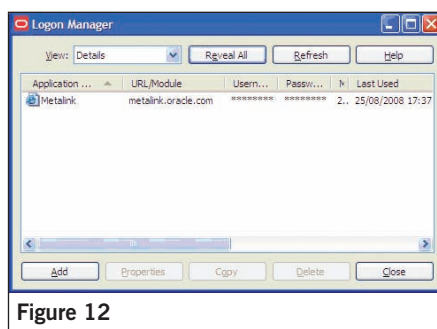


Figure 12

8. Similarly, users can add other desktop and web applications to Logon Manager.

Conclusion

Oracle Identity Management enables customers to manage life cycle of user identities by providing products which manage different stages of user identity life cycle. Customers can choose the products that fulfill their business requirement and integrate with existing in-house identity management products. Thus, providing a unified and integrated identity management solution.

Inatech Value Add

The following services can be provided for Identity Management Solution:

- Enterprise Single Sign On for Web Application
- Single Sign On integration with Microsoft Active Directory
- Synchronisation of Users' Account from Microsoft Active Directory to Oracle Internet Directory and vice versa
- Integration functionality with 3rd party Directory Services using out-of-box with available Integration Functions, and using LDAP APIs where standard integration function is not available (provided Directory Service should support LDAP interface)
- Available directory connectivity solutions for Peoplesoft and Oracle Human Resources
- High Availability and Scalability deployment and support

About the Author



Manpreet Singh Johal, Solution Architect – Inatech Solutions Limited
Manpreet Singh Johal is an Oracle Certified Associate – AS

10g with nearly 8 years of cumulative work experience. He has excellent technical experience in Oracle Applications 11i/R12; Fusion Middleware - Application Server, Identity Management, Enterprise Management, OCS Implementation, Portal Administration/Development, and Software Development/System Analysis. He has worked with various teams successfully across multiple projects globally. He has also conducted a presentation at UKOUG 2007 on "Designing Disaster Recovery Site with OracleAS Guard 10g".