"Zero Sign-on" to EBS - Enabling 96000 Users to Login to EBS Without User Maintenance

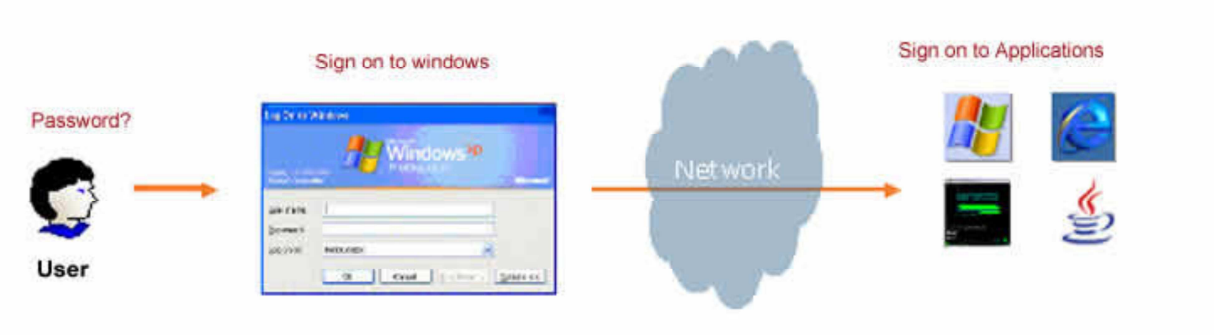
Doug Pepka
Comcast Cable Communications

Abhishek Chandan
Ideametrics LLC

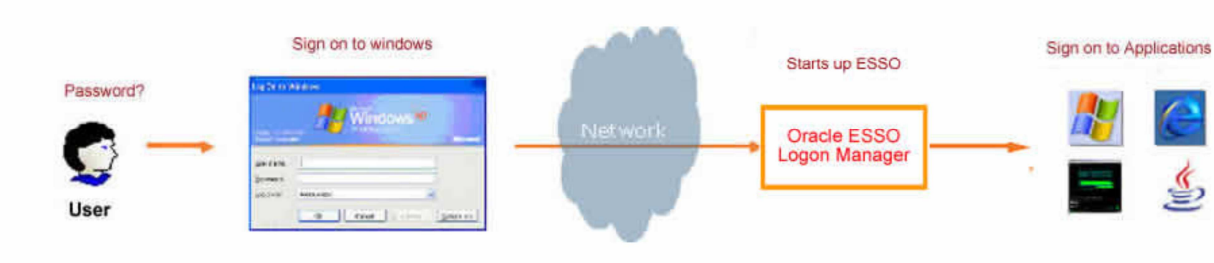
Steve Miller
Ideametrics LLC

Executive Summary

Enterprises these days generally have Microsoft Windows desktop users accessing diverse enterprise applications on a daily basis. Each enterprise application often has different security requirements and, as a consequence, users in many organizations are forced to remember multiple different passwords for various applications. In many organizations, users are often forced to remember more than six different passwords for various enterprise resources. As a result, there is a need to enable a simple and secure way for enterprise users to access heterogeneous applications (e.g. Microsoft Windows, Java, Mainframe applications etc) by signing on just once to their windows desktop. This should not only circumvent the need to remember credentials for individual applications but also enhance user productivity by eliminating helpdesk calls associated with forgotten passwords.



The Oracle Enterprise Single Sign-on (Oracle ESSO) Suite facilitates a way for desktop users to access enterprise applications by signing on just once to their desktops using a single set of credentials.



This eliminates the challenge for users to know application credentials for all the enterprise applications that they are entitled to access based on their roles and responsibilities.

This presentation focuses on integration of Oracle E-Business Suite with Oracle Single Sign-On suite.

Introduction

In large organizations, users often have a large number of userids for a variety of network-based resources such as corporate websites and custom applications. As the number of available resources grows, users and security administrators are faced with the increasingly-difficult challenge of managing a proliferation of userids and passwords across different systems.

Enterprise identity management solutions allow security administrators to define a user in a single location such as an Lightweight Directory Access Protocol (LDAP) directory, and share that common user definition throughout multiple parts of their enterprise. Microsoft Active Directory (AD) is one of the many commonly used LDAP directories to store and manage corporate user authentication information.

Oracle Identity Management, part of Oracle Application Server 10g, may be integrated with the E-Business Suite to support centralized user management via Oracle Internet Directory, and to support single sign-on functionality via Oracle Single Sign-On.

In its default configuration, the Oracle E-Business Suite Release 11i allows registered users to log in using credentials stored directly in the E-Business Suite. In this default configuration, E-Business Suite system administrators are responsible for maintaining the local repository of registered E-Business Suite users.

When optionally integrated with Oracle Application Server 10g, E-Business Suite system administrators can reconfigure their environments to delegate both user administration and user authentication to Oracle Application Server 10g.

This integration with Oracle Application Server 10g requires significant changes to how Oracle E-Business Suite Release 11i handles authentication. Instead of performing authentication natively, via the local E-Business Suite FND_USER table, the E-Business Suite Release 11i now delegates this functionality to the Oracle Single Sign-On server. In this configuration, Oracle E-Business Suite Release 11i can direct unauthenticated users to an Oracle Single Sign-On server for identity verification, and securely accept identities vouched for by the Single Sign-On mechanism.

Oracle Single Sign-On may, in turn, be integrated with existing third-party authentication systems such as Microsoft Windows (Kerberos), and Oracle Internet Directory may be integrated with existing third-party LDAP directories such as Microsoft Active Directory.

Oracle Single Sign-On either performs authentication against information stored in Oracle Internet Directory (an LDAP server), or delegates authentication to a third-party authentication mechanism.

Note that where a third-party authentication mechanism is in use, Oracle Single Sign-On server and Oracle Internet Directory are still required, to provide bridge functionality between Oracle E-Business Suite Release 11i and the third-party single sign-on solution.

Enterprise User Management

Oracle Internet Directory is the integration point that allows Oracle E-Business Suite Release 11i to participate in enterprise level user management. Each Oracle E-Business Suite instance must still maintain a record of registered users, in the form of the traditional application accounts. However, the level of abstraction needed for an enterprise level user requires a mechanism that can uniquely identify a user across the enterprise. This is accomplished via a globally unique identifier (GUID). Oracle Internet Directory and Oracle E-Business Suite Release 11i store GUID information for each enterprise level user; the GUID can be considered as an identity badge that is recognized by both Oracle Internet Directory and Oracle E-Business Suite Release 11i.

Another requirement in such an environment is for user enrollment to be done only once, at well-defined places, with the user subsequently being known to the rest of the enterprise. Two additional features enable support for automatic propagation of user information across an enterprise:

• A synchronization process between Oracle Internet Directory and a third-party LDAP server.

•A provisioning process between Oracle Internet Directory and Oracle E-Business Suite Release 11i.

Much of the complexity involved with integrating Oracle E-Business Suite into a single sign-on environment arises because of the need to consolidate fragmented or duplicated user data in the single sign-on environment, as a legacy of integrating previously isolated systems. The solution described in this document provides mechanisms to link the existing data together using the GUID. In addition, bulk migration tools are provided to move a large number of users between Oracle Internet Directory and Oracle E-Business Suite during the transition to a single sign-on environment.

Authorization

The solution described here does not address the issue of authorization. After a user has been authenticated, Oracle E-Business Suite Release 11i retrieves the authorization information associated with the application account the user is logged into.

Authorization information for application accounts is managed through Applications responsibilities. Oracle E-Business Suite Release 11i applies authorization checks as and when required during the user's session.

Summary of Key Identity Management Configuration Options Configuration Option

	Possible Settings	Configured Via
Initial Source of User Information	1. E-Business Suite 2. Oracle Internet Directory 3. Third-Party LDAP Directory 4. Combination of above	Manual initial provisioning steps executed
Master Source of Truth for Updates to User Information	1. E-Business Suite 2. Oracle Internet Directory 3. Third-Party LDAP Directory 4. Combination of above	Provisioning profile selected for Directory Integration & Provisioning Platform

New Userids Created in Oracle Internet Directory …	1. Are automatically created in E-Business Suite with subscriptions for user attribute updates
	2. Have manually-created equivalent userids in E-Business Suite, and are manually linked by the end-user at the time of first logon
	3. Have manually-created equivalent userids in E-Business Suite, and are automatically linked at the time of first logon
	4. Are automatically created in a third-party LDAP directory, combined with either of the two above options
		Related E-Business Suite Profile Options:
		`APPS_SSO_OID_IDENTITY`
		`APPS_SSO_AUTO_LINK_USER`

New Userids Created in E-Business Suite …	1. Are automatically created in Oracle Internet Directory with subscriptions for user attribute updates
	2. Have manually-created equivalent userids in Oracle Internet Directory, and are manually linked by the end-user at the time of first logon
	3. Have manually-created equivalent userids in Oracle Internet Directory, and are automatically linked at the time of first logon
		Related E-Business Suite Profile Options:
		`APPS_SSO_LDAP_SYNC`
		`APPS_SSO_AUTO_LINK_USER`

Specific E-Business Suite Userids …	1. Log on to E-Business Suite via Single Sign-On 10g 2. Log on to E-Business Suite directly, bypassing Single Sign-On 10g	`APPS_SSO_LOCAL_LOGIN` profile option

	3. Both of the above	
All Oracle Internet Directory Userids …	1. Are linked to a single E-Business Suite userid 2. Are linked to multiple E-Business Suite accounts	`APPS_SSO_ALLOW_MULTIPLE_ACCOUNTS` profile option

Starting Point

- Oracle E-Business Suite Release 11i is in use, and has existing users populated in an up-to-date FND_USER repository.
- There is no corporate single-sign solution is in use. An upcoming I-Expense implementation will increase the number of EBS users by one hundred thousand (100,000). Tradition EBS managed user authentication will result in significantly higher support requirements.
- Microsoft Active Directory (AD) is in use as a corporate user directory.
- At the start of the implementation, all users existed in both EBS and AD. Most users exist with a different user name in each.
- Oracle Portal is not implemented.

Solution Outline and Other Details

These are included in the session presentations. For implementation specific detail questions, please email achandan@ideametrics.com.