



# Oracle® Single Sign-On for JD Edwards® EnterpriseOne®:

## Part I – Oracle Internet Directory Integration with Microsoft Active Directory

By Charles Anderson

**Editor's Note:** *If your company's IT security policy requires users to change passwords at a frequent rate, and each user averages, say, five to ten passwords—one for each vendor's application—that can be a time consuming process for them. It's an even greater challenge for those tasked with managing User IDs and passwords. This is where the beauty of Oracle Single Sign-On for JD Edwards® EnterpriseOne and other Oracle applications comes into play. By following the steps provided by Charles Anderson, you can shorten the time for both users and administrators by creating a single sign-on that requires one User ID and one password per user to access their JDE and Oracle applications. This is Part I of a three-part series. In this white paper, Charles discusses installation of the Oracle Internet Directory, including special considerations you'll want to keep in mind.*

### Introduction

In today's environment, with SOX compliance and access audits on the mind of many publicly traded companies, Single Sign-On for critical business applications (your ERP systems, for example) can help ease some of the tension between IT Security Administrators, Managers, and IT Auditors. When Single Sign-On products are integrated with Microsoft Active Directory, user access can be controlled at the Windows Domain level and strict policies can be created and enforced, often more visibly and more effectively than from within the applications themselves.

I'm often asked about the integration of EnterpriseOne with Microsoft Active Directory. More specifically, how does one go about an Oracle Single Sign-On implementation for JD Edwards EnterpriseOne? Let's not forget the special instructions to make this work with EnterpriseOne Tools 8.97. Such a feat, on the surface, appears to be quite complex, and make no mistake – to some degree it is. But armed with the proper knowledge, just about any CNC should be able to make a Single Sign-On dream a reality. In this white paper, the first of three parts, I will walk you through the process of installing Oracle Internet Directory (OID). Future articles will show you how to integrate OID with Microsoft Active Directory and then implement Oracle Single Sign-On security for the JD Edwards EnterpriseOne HTML.

There are distinct advantages for users of any single sign-on product, and when you have an open system that supports adding multiple disparate applications to your single sign-on portfolio, such as Oracle Single Sign-On, support costs will most likely decrease. Such an implementation of Oracle Single Sign-On would typically include Oracle Internet Directory (OID) integrating with an *existing* Microsoft Active Directory server.

The business justification for this is quite simple: Microsoft Active Directory (MSAD) has evolved into what is probably the *de facto* LDAP (Lightweight Directory Access Protocol) directory server standard for most corporations. A fair number of CIOs and IT Managers have chosen to standardize on Active Directory for centralized account creation and maintenance for several reasons, one being that more than 90% of business desktops are running an Active Directory compatible version of Microsoft Windows (Windows 2000, Windows XP, and Vista). So why would you not want to leverage the capabilities you probably already have at your disposal?

You can do so much more with Active Directory than simply manage accounts, but in this paper we'll focus on the identity management features. I suspect that Active Directory is often the only LDAP server many companies might have in operation. For many IT organizations, introducing a competing product into the environment can be challenging. They may already have the right to



# Oracle Single Sign-On for JD Edwards EnterpriseOne:

## Part I – Oracle Internet Directory Integration with Microsoft Active Directory

use the product by way of an Oracle Technology Foundation license for EnterpriseOne, but there are other costs involved besides the upfront purchase cost, such as implementation, database administration requirements, and sustaining support.

You may run into the same situation if there is already more than one LDAP server in place. If so, the folks who manage the directory services in your organization might be inclined to keep costs down and control infrastructure sprawl. While this is understandable, if the directive is to implement Oracle SSO technology, there really is no choice but to introduce the Oracle OID server, because non-Oracle LDAP servers are not, *at this time*, supported by Oracle Single Sign-On. A future release may introduce this much desired enhancement, but for now, this is but a pipe dream.

### Understanding Oracle Single Sign-On Requirements

Oracle Single Sign-On is one of the components included with the Red Stack for use specifically with EnterpriseOne and Oracle Portal. While Oracle Portal requires Single Sign-On, EnterpriseOne does not. In fact, EnterpriseOne supports several sign on methods, one of which even happens to be a “portlet”, or many different published portlets, within Oracle Portal. Oracle Portal is limited for use with EnterpriseOne as a portlet consumer for self service applications, EnterpriseOne menu, etc. A limited use installation of Oracle Internet Directory (which I will refer to as OID from this point forward) is in turn supplied with a limited use edition of the Oracle Database Enterprise Edition. Now that that’s out of the way...

JD Edwards EnterpriseOne now provides support for several different authentication methods. The most basic and probably the most familiar is the standard JD Edwards HTML client logon screen. The logon screen shown in Figure 1 is specific to the release of EnterpriseOne Tools you happen to be running, though it has not changed cosmetically since the initial release of Tools 8.96. This logon screen is *functionally* equivalent to the Windows client logon screen. It should be noted that with the use of this access method, long usernames and passwords can *not* be implemented with the EnterpriseOne HTML client.



User ID:

Password:

[Details](#)

This system is intended for limited (authorized) use and is subject to company policies.

Figure 1: Oracle Standard Security for EnterpriseOne HTML client

## This Article Continues...

**Subscribers**, log in from our main search page to access the full article:

[www.JDEtips.com/MyAccess.html](http://www.JDEtips.com/MyAccess.html)

**Not a Subscriber? Gain access to our full library of JDE topics:**

[www.JDEtips.com/JD-Edwards-Library](http://www.JDEtips.com/JD-Edwards-Library)

Visit [www.JDEtips.com](http://www.JDEtips.com) for information on the JDEtips University schedule, private training and consulting, and our Knowledge Express Document Library.

License Information: The use of JDE is granted to JDEtips, Inc. by permission from J.D. Edwards World Source Company. The information on this website and in our publications is the copyrighted work of JDEtips, Inc. and is owned by JDEtips, Inc.

NO WARRANTY: This documentation is delivered as is, and JDEtips, Inc. makes no warranty as to its accuracy or use. Any use of this documentation is at the risk of the user. Although we make every good faith effort to ensure accuracy, this document may include technical or other inaccuracies or typographical errors. JDEtips, Inc. reserves the right to make changes without prior notice.

Oracle and J.D. Edwards EnterpriseOne and World are trademarks or registered trademarks of Oracle Corporation. All other trademarks and product names are the property of their respective owners.

Copyright © by JDEtips, Inc.