Long User ID and Password Support
In JD Edwards EnterpriseOne

An Oracle JD Edwards EnterpriseOne Red Paper

November 2007
PURPOSE STATEMENT

This document outlines the steps that existing JD Edwards EnterpriseOne customers would take to support long user IDs and passwords using Oracle Application Server Single Sign-on or Oracle Access Manager.

This document is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle. Updates and enhancements are provided in accordance with Oracle’s Technical Support Policies at:

www.oracle.com/support/collateral/oracle-technical-support-policies.pdf
Overview

Managing Long User IDs and Passwords in Oracle Application Server Single Sign-On

Prerequisite ................................................................. 6
Configuring LDAP for Longer User IDs .................................................... 6
Map Long User IDs in JD Edwards EnterpriseOne .................................... 7

Managing Long User IDs and Passwords in Oracle Access Manager

Overview ....................................................................................... 8
Prerequisites ...................................................................................... 8
Configuring LDAP for Longer User IDs ................................................. 8
Configure Oracle Access Manager for Long User IDs ......................... 9
  Create an Authentication Scheme ...................................................... 9
  Configure the Authentication Scheme ............................................. 11
  Enable the Authentication Scheme ................................................ 12
  Configure a Policy Domain ............................................................ 13
Test Signing into JD Edwards EnterpriseOne Using a Long User ID ....... 14
OVERVIEW
This red paper provides an overview of long user ID and password support in JD Edwards EnterpriseOne.

To support more than 10 characters in a user name or password in JD Edwards EnterpriseOne, you must use an LDAP server to centrally manage long user IDs and passwords. You can then map the user IDs and passwords to JD Edwards EnterpriseOne user IDs.

Note: You cannot use or map long user IDs and passwords for JD Edwards EnterpriseOne non-web users (such as Windows client, WSG, and Java Connector users).

You can support long user IDs in either of the following single sign-on configurations:

- Single Sign-On into JD Edwards EnterpriseOne using OSSO.
  
  In this configuration, you can either use LDAP or the JD Edwards EnterpriseOne application to map LDAP longer user IDs to JD Edwards EnterpriseOne user IDs.

- JD Edwards EnterpriseOne single sign-on configuration through Oracle Access Manager.
MANAGING LONG USER IDS AND PASSWORDS IN ORACLE APPLICATION SERVER SINGLE SIGN-ON

When LDAP support is enabled in a JD Edwards EnterpriseOne and Oracle Application Server Single Sign-On (OSSO) configuration, JD Edwards EnterpriseOne uses the LDAP server settings to search for user profiles in the LDAP server, as illustrated in this diagram:

In this diagram, the JD Edwards EnterpriseOne application requests a search of the Directory Information Tree for a JD Edwards EnterpriseOne user in the United States with an ab12345 user ID. The user can only be found if these attributes contain valid values:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USRSRCHBASE (User Search Base)</td>
<td>o=enterpriseone, c=us</td>
</tr>
<tr>
<td>USRSRCHSCP (User Search Scope)</td>
<td>subtree</td>
</tr>
<tr>
<td>USRSRCHFLT (User Search Filter)</td>
<td>objectclass=inetOrgperson</td>
</tr>
<tr>
<td>USRSRCHATR (User Search Attribute)</td>
<td>uid</td>
</tr>
<tr>
<td>E1USRIDATR (EnterpriseOne User ID Attribute)</td>
<td>uid</td>
</tr>
</tbody>
</table>
In LDAP, the user ID (uid) is configured as the value for both User Search Attribute and EnterpriseOne User ID Attribute, which is used by the Security Server as the login user ID.

Other attributes and values, such as mail=orcladmin@host.com, can be used as a long user ID for third-party systems that need to use the same LDAP configuration. However, note that the user password still is limited to 10 characters as the LDAP record is the same for both uid=ab12345 and mail=orcladmin@host.com. The following example shows the configuration of the mail attribute:

When the mail attribute is used by a third-party system, the uid attribute can be used for JD Edwards EnterpriseOne security. Note that the user password still is limited to 10 characters. An alternative is to set up JD Edwards EnterpriseOne to use the sn attribute instead of uid, as illustrated in this example:
In this configuration, the third-party system can use the UID attribute for login.

After you add the long user ID in the LDAP server, you must map this ID to the EnterpriseOne user ID using JD Edwards EnterpriseOne. See “Managing User ID Mapping in JD Edwards EnterpriseOne” in the JD Edwards EnterpriseOne Tools 8.97 Security Administration Guide.

**Prerequisite**

Successful integration between Oracle Single Sign-On with JD Edwards EnterpriseOne has been established.


**Configuring LDAP for Longer User IDs**

To configure LDAP for long user IDs, you must specify an attribute that you want to use for long user IDs and then use that attribute to configure all the users with long user IDs.

1. On the LDAP Server, log in as an administrator.
2. On Oracle Directory Manager, expand the Entry Management node and select a user account.

3. Choose and note the attribute that you want to use to configure each long user ID.

4. Use this attribute to set up each JD Edwards Enterprise HTML client user with a long user ID.

5. Log out and close Oracle Directory Manager.

**Map Long User IDs in JD Edwards EnterpriseOne**


1. Click the Configure the UserID Mapping link.

2. To add a user ID mapping, on the Work with SSO E/E1 UserID Mapping form, click Add.

3. On the SSO E/E1 userID Mapping Revisions form, complete the EnterpriseOne UserID and Enterprise UserID fields. Use the new longer user ID created in LDAP for the Enterprise UserID fields.

   The system saves the record in the F00927 table.

   **Note:** If the EnterpriseOne user ID is not in the F0092 table, the system generates an error stating that it cannot add the mapping record.
MANAGING LONG USER IDS AND PASSWORDS IN ORACLE ACCESS MANAGER

This section provides an overview and discusses how to:

- Configure LDAP for longer user IDs.
- Configure Oracle Access Manager for longer user IDs.
- Test signing into JD Edwards EnterpriseOne using a longer user ID.

Overview

Oracle Access Manager enables you to manage long user IDs and passwords in a single sign-on configuration with JD Edwards EnterpriseOne. Using Oracle Directory Manager, a component of Oracle Access Manager, you can configure and map JD Edwards EnterpriseOne user IDs to longer user IDs.

In addition to mapping user IDs, you must set up an authorization policy in Oracle Access Manager so that the system is directed to authorize the long user IDs when accessing JD Edwards EnterpriseOne in a single sign-on configuration.


Prerequisites

Before you configure long user ID and password support between Oracle Access Manager and JD Edwards EnterpriseOne, you must:

- Establish integration between Oracle Access Manager and JD Edwards EnterpriseOne.
- Ensure all services have been started including Oracle Access Manager Identity Server, Oracle Access Manager Access Server, Oracle Application Server, and JD Edwards EnterpriseOne HTML Web Server.
- Configure the web browser to allow cookies, according to vendor instructions.

Configuring LDAP for Longer User IDs

To configure LDAP for long user IDs, you must specify an attribute that you want to use for long user IDs and then use that attribute to configure all the users with long user IDs.

1. On the LDAP Server, log in as an administrator.
2. On Oracle Directory Manager, expand the Entry Management node and select a user account.

3. Choose and note the attribute that you want to use to configure each long user ID. You use this attribute when you configure the authentication scheme.

   **Note:** When you set up JD Edwards EnterpriseOne HTML client users with long user IDs, you must use this attribute for the long user ID.

4. Log out and close Oracle Directory Manager.

**Configure Oracle Access Manager for Long User IDs**

To set up and configure Oracle Access Manager single sign-on to use longer user IDs for JD Edwards EnterpriseOne, you must:

- Create an authentication scheme.
- Configure the authentication scheme.
- Enable the authentication scheme.
- Configure a policy domain.

**Create an Authentication Scheme**

1. Log in to Oracle Access System Console.
2. Navigate to Authentication Management.
3. Click the Add button.

4. On the General tab, complete these fields, and then click Save:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the authentication scheme.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description.</td>
</tr>
<tr>
<td>Level</td>
<td>1</td>
</tr>
<tr>
<td>Challenge Method</td>
<td>Select the Basic option.</td>
</tr>
<tr>
<td>Challenge Parameter</td>
<td>realm:Oracle Access and Identity</td>
</tr>
<tr>
<td>SSL Required</td>
<td>Select the No option.</td>
</tr>
<tr>
<td>Challenge Redirect</td>
<td>Leave blank.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select No.</td>
</tr>
<tr>
<td>Update Cache</td>
<td>Select this check box.</td>
</tr>
</tbody>
</table>

5. On the dialog box, click OK to commit the changes.
Configure the Authentication Scheme

1. Click the new authentication scheme and click the Plugins tab.

2. On the Plugins tab, click Modify.

3. Enter the following parameters for the two plugins. You must click the Add button to add the parameters for the second plugin.

<table>
<thead>
<tr>
<th>Plugin Name</th>
<th>Plugin Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>credential_mapping</td>
<td><code>obMappingBase=&lt;mappingbase&gt;,obMappingFilter=('(&amp;(objectclass=interorgperson)(&lt;ldap_attribute&gt;=%userid%))(!(obuseraccountcontrol=*))')(obuseraccountcontrol=ACTIVATED)</code></td>
</tr>
<tr>
<td></td>
<td>where <code>&lt;mappingbase&gt;</code> is the LDAP mapping base.</td>
</tr>
<tr>
<td></td>
<td>and</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ldap_attribute&gt;</code> is the user LDAP attribute used for the long user ID. For example, if you used the “mail” attribute to enter long user IDs, you would enter email here.</td>
</tr>
</tbody>
</table>

| validate_password | `obCredentialPassword=password`                                                 |

4. Click Save.

   This screen shows the added plugins:
Enable the Authentication Scheme

1. Click the General tab and then click the Modify button.
2. Select Yes for Enabled.

3. Click Save.

4. On the dialog box, click OK to commit the changes.

**Configure a Policy Domain**

1. Log in to Oracle Policy Manager.
2. Navigate to the Policy Domain that protects JD Edwards EnterpriseOne URLs.

3. Under the Policies tab, click the Authentication Rule tab and then click Modify.

4. Click OK on the dialog box to continue.

5. In the Authentication Scheme field, select the name of the newly created Authentication Scheme, and then click Save.


**Test Signing into JD Edwards EnterpriseOne Using a Long User ID**

After you configure Oracle Access Manager single sign-on to use long user IDs for JD Edwards EnterpriseOne, you should use a long user ID that you configured in the previous section to test the configuration.

1. In a web browser, enter the URL for the JD Edwards EnterpriseOne web client.

   The Oracle Access and Identity screen appears.

2. On Oracle Access and Identity, enter a long user ID that was configured in the previous section, along with the associated password.
If the authentication with Oracle Access Manager SSO was successful, the JD Edwards EnterpriseOne form for selecting an environment and role appears.