Release Notes

IBM

IBM® Tivoli® Identity Manager

Oracle e-Business Suite (Oracle eBS) Adapter

Version 5.0.10

First Edition (July 28, 2011)

This edition applies to version 5.0 of Tivoli Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Preface

Welcome to the IBM Tivoli Identity Manager Oracle e-Business Suite Adapter.

These Release Notes contain information for the following products that was not available when the IBM Tivoli Identity Manager manuals were printed:

- Directory Integrator-Based Oracle eBS Adapter Installation and Configuration Guide
- Directory Integrator-Based Oracle eBS Adapter User Guide

Adapter Features and Purpose

The Oracle eBS Adapter is designed to create and manage accounts on the Oracle e-Business Suite application. The adapter runs in "agentless" mode and communicates using JDBC to the systems being managed.

IBM recommends the installation of this Adapter (and the prerequisite Tivoli Directory Integrator) on each node of an Identity Manager WebSphere cluster. A single copy of the adapter can handle multiple ITIM Services. The optimum deployment configuration is based, in part, on the topology of your network domain, but the primary factor is the planned structure of your Identity Manager Provisioning Policies and Approval Workflow process. Please refer to the Identity Manager Information Center for a discussion of these topics.

The Identity Manager Adapters are powerful tools that require administrator level authority. Adapters operate much like a human system administrator, creating accounts, permissions and home directories. Operations requested from the Identity Manager server will fail if the adapter is not given sufficient authority to perform the requested task. IBM recommends that this adapter run with administrative (root) permissions.

Contents of this Release

Adapter Version

Component	Version
Release Date	July 28, 2011
Adapter Version	5.0.10
Component Versions	AL version: 5.0.1012 Profile: 5.0.1010 Connector: none (uses TDI JDBC connector) Dispatcher: 5.125
Documentation	Directory Integrator-Based Oracle eBS Adapter Installation and Configuration Guide SC23-6156-00 Directory Integrator-Based Oracle eBS Adapter User Guide SC23-9920-00

New Features

Enhancement # (FITS)	Description
	Items included in current release
MR111110213	Add ability to require SSL connection from OracleEBS Adapter to Oracle
	See "Configuration Notes" for more information.
MR0817103443 MR0715114436	Need adapter support for administering new RBAC feature of Oracle EBS 12. Roles Provisioning Support for Oracle eBusiness Suite Adapter v5.1.7 with ITIM 5.1 Adapter. See "Configuration Notes" for more information.
	Added support for Oracle eBS 12.1.1.
	Items included in 5.0.8 – 5.0.9 release
MR0908093426	Oracle EBS should support start/end dates at responsibility level. **Note:** Run full reconciliation before performing any other operation with this version of adapter.
MR0121104331	Oracle EBS adapter ability to filter user responsibility by language. **Note:** Run full reconciliation before performing any other operation with this version of adapter.
Internal 37461	Unable to add securing attributes to the user (duplicate securing attributes, varying only by mixed-case)
MR0820105833	Oracle EBS Adapter having more debug statement with INFO level logging **Note:** Run full reconciliation before performing any other operation with this version of adapter.
MR041210570	Oracle EBS Adapter recon warning about security attributes - G/OB **Note:** Run full reconciliation before performing any other operation with this version of adapter.
	Items included in 5.0.7 release
MR0908094757	OracleEBS should support changing eruid.
	Items included in 5.0.6 release

Enhancement # (FITS)	Description
MR0408095034	Oracle EBS: adapter must support securing attributes on responsibilities. Please see the "Configuration" section of this document for additional information.
	Items included in 5.0.5 release
	1) Changes in profile for Max Connection Count. A feature of Dispatcher. 2) Changes in profile for AL FileSystem Path. A feature of Dispatcher.
	Items included in 5.0.4 release
	None
	Items included in 5.0.3 release
N/A	Updated adapter profile to include the new Dispatcher option to Disable AL Caching.
	Items included in 5.0.2 release
MR0912073842	Oracle eBS v12 support
N/A	PASSWORD_DATE attribute in OracleEBS will reflect the system date when the account's password is set or changed.
	Items included in 5.0.1 release
MR032007687	Enhance the adapter so that it does not require the APPS account.
	Initial release for Tivoli Identity Manager v5.0

Closed Issues

Internal#	APAR#	PMR# / Description
		Items closed in current version
		None
		Items closed in 5.0.5 – 5.0.9 version
		None
		Items closed in 5.0.4 version
	IZ3155	71834,500,000 ADAPTER HAS ISSUE WITH ATTRIBUTE VALUES WITH (single) QUOTES.
	IZ34103	70244,500,000 Oracle eBS Adapter restore operation does not work if password contains quotes.
	IZ37738	73344,500,000 ORACLEEBS LOSES RESPONSIBILITIES Oracle eBS adapter provisions multiple responsibilities on a transaction correctly but does not report success correctly to TIM. Roles are removed on TIM but provisioned correctly on target.
		Items closed in 5.0.3 version
	IZ31941	05412,707,707 Recons duplicate entries for responsibility when multiple languages are active on the Oracle eBS system.
		Items closed in 5.0.2 version
32500		Oracle eBS Adapter Profile cannot be exported.
32524		Oracle eBS Adapter Delete Responsibility Fails.
		Items closed in 5.0.2 version
		None

Known Issues

Internal#	APAR#	PMR# / Description
N/A	N/A	**Deprovisioning user accounts** Account deprovisioning is not supported natively (no stored procedure) in Oracle e-Business Suite and is therefore not available in the adapter.
N/A	N/A	**Changing a Password on a Suspended Account** On Oracle eBS 12i if account is suspended (end dated) then password change operation will fail with following error: "ORA-20001: APP-FND-02602: Unabled to change password for user XXXXXXX for this following reason: Your account does not exist or has expired…" **Work Around:** 1. You must enable the account first by setting future end date or deleting the end date and then perform password change. 2. Use restore operation and specify new password.

N/A	N/A	**Anonymous Record History**
		
		Assigning or modifying responsibilities through ITIM results in the audit fields ("Created By" and "Updated By") showing an anonymous value.
		
		Workaround:
		
		To have the "SYSADMIN" value show in the audit fields for the responsibility record of an Oracle eBS user account, modify OracleEBSManageUserAL.xml and nonAPPS.sql (if using a non-APPS user) as follows:
		
		Step 1. Changes required for OracleEBSManageUserAL.xml:
		
		In the *conOracleEBSManageUser* connector, add the following piece of code to the *After Initialize* hook of the *Prolog* section:
		
		`if (g_bIsAppsUser) {`
		`    task.logmsg("DEBUG","Initialized session parameters APPS");`
		`    result = thisConnector.connector.execSQL("Begin FND_GLOBAL.APPS_INITIALIZE( 0, -1, -1, 0, -1); end;");`
		`} else {`
		`    task.logmsg("DEBUG","Initialize session parameters Non-APPS");`
		`    result = thisConnector.connector.execSQL("Begin APPS.ITIM_APPS_INITIALIZE(0, -1, -1, 0, -1); end;");`
		`}`
		`if (result != "") {`
		`    task.logmsg("ERROR","Could not initialize the session parameters");`
		`    if(g_bIsAPPSUser) task.logmsg("DEBUG","FND_GLOBAL.APPS_INITIALIZE Failed. Error: " + result);`
		`    else task.logmsg("DEBUG","APPS.ITIM_APPS_INITIALIZE Failed. Error: " + result);`
		`}`
		
		After making the changes, recreate the OraEBSProfile.jar. Import the modified OraEBSProfile.jar to ITIM.
		
		Step 2. Changes required in nonAPPS.sql:
		
		Add the following lines to the nonAPPS.sql and execute the file.

Internal#	APAR#	PMR# / Description
| | | ```
create or replace PROCEDURE "APPS"."ITIM_APPS_INITIALIZE" (

    user_id in number,
    resp_id in number,
    resp_appl_id in number,
    security_group_id in number default 0,
    server_id in number default -1

) AS begin

    FND_GLOBAL.APPS_INITIALIZE (

        user_id => user_id,
        resp_id => resp_id,
        resp_appl_id => resp_appl_id,
        security_group_id => security_group_id,
        server_id => server_id);

end ITIM_APPS_INITIALIZE;

grant execute on APPS.ITIM_APPS_INITIALIZE to nonapps;
``` |

Installation and Configuration Notes

See the IBM Tivoli Identity Manager Adapter Installation Guide for detailed instructions.

Corrections to Installation Guide

The following corrections to the Installation Guide apply to this release:

A. Make the following changes to Chapter 2: Installing the Oracle eBS Adapter.

The prerequisites in the release notes take precedence over the prerequisites listed in the Installation Guide.

After "Importing the adapter profile into the Tivoli Identity Manager server", add

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the OraEBSSubForms.zip file.

To deploy the subforms, place the contents of OraEBSSubForms.zip in the subforms folder of the installed IBM Tivoli Identity Manager web application. For a Self Service console installation this will be *WAS_PROFILE_HOME*/installedApps/*nodeName*/ITIM.ear/itim_self_service.war and for an Administrative Console installation this will be *WAS_PROFILE_HOME*/installedApps/*nodeName*/ITIM.ear/itim_console.war. Note that the subform must be deployed on each WebSphere application server if you have a clustered setup.

If WebSphere version 6.1 is being used, the jdkSourceLevel JSP engine configuration parameter must be set to "15" for each web application that the subforms are deployed to. Perform the following steps:

1. Open the WEB-INF/ibm-web-ext.xmi file from the configuration directory *WAS_PROFILE_HOME*/config/cells/*cellName*/applications/ITIM.ear/deployments/ITIM/*webModuleName*, where webModuleName is itim_self_service.war and/or itim_console.war.
2. Add the following tag within the content of the webappext:webAppExtension tag: <jspAttributes xmi:id="JSPAttribute_1" name="jdkSourceLevel" value="15"/>. Note that the integer n in JSPAttribute_n has to be unique within the file.
3. Save the file.
4. Restart the ITIM application from the WebSphere Administrative Console, or restart the service.

Creating an Oracle eBS Adapter service

The IBM Tivoli Identity Manager Adapter service on the Tivoli Directory Integrator server only needs to be restarted when the password field is changed.

To support connecting to the Oracle eBS database via an SSL connection, several fields have been added to the Oracle eBS Adapter service form on the Oracle EBS Profile tab:

> **Use SSL communication with Oracle?**
>
>> Check the checkbox to force an SSL connection from the adapter to the Oracle eBS database.
>
> **Oracle EBS Server Distinguished Name**
>
>> Optional. Specify the distinguished name contained in the Oracle eBS database's certificate. If SSL communication is enabled and this field is not blank, the connection will only succeed if the distinguished names match.

B. Make the following changes to Chapter 3. Configuring the Oracle eBS Adapter.

Customizing the Oracle eBS Adapter profile

OracleEBSAdapter.xml is no longer included in OraEBSProfile.jar.

To import the file, the commands for the first step should be:

```
cd /tmp
jar -cvf OraEBSProfile.jar OraEBSProfile
```

C. Make the following changes to Appendix A. Adapter attributes.

Attribute descriptions

The attribute "erOraEBSStartDate" should be changed to "erOraEBSUserStartDate".

The following attributes should be added/updated in Table 7:

Attribute	Description	Constraints	Permissions
erOraEBSResp	Specifies a directly granted responsibility formatted as "*Application_Name␣|␣Responsibility_Name|Start_Date| End_Date*", where ␣ denotes a space character and dates are formatted as "dd/mm/yyyy" (e.g. 31/12/2001) or empty to omit. E.g. "Sales Foundation | Customer Relationship Mgmt| 13/01/2001|"	Only *End_Date* may be omitted.	Read and Write
erOraEBSIndirectResp	Specifies an inherited responsibility formatted like that of erOraEBSResp.		Read
erOraEBSSecAttr	Specifies an associated securing attribute formatted as "*Application_ID|Attribute_Code|Value*". Note that no extra spaces should be added anywhere. E.g. "454| ONE_DAY_BOOK_TO_SHIP_PERCENT|2342". If *Value* is of DATE type, it should be formatted as "dd-mm-yyyy" (e.g. "31-12-2001"); if it is of DATETIME type, it should be formatted as "dd-mm-yyyy hh24:mi:ss" (e.g. "31-12-2001 13:45:00").		Read and Write
erOraEBSDirectRoles	Specifies a directly granted role formatted as a JSON object with the fields *role* (object), *startDate* (string), *endDate* (string), and *reason* (string). *role* is a JSON object with fields *name* (string), *origSystem* (string), and *origSystemId* (string). The date fields (startDate and endDate) are represented as strings with the format "yyyymmddhh24mi'Z'" (e.g. "200112311345Z"). E.g. "{"endDate":null,"reason":"Granted by XX","role":{"name":"UMX| SECURITY_ADMIN", "origSystem":"UMX","origSystemId":"0"}, "startDate":"201103150000Z"}".	Only the *endDate* and *reason* fields may be null.	Read and Write
erOraEBSIndirectRoles	Specifies an inherited role formatted like that of erOraEBSDirectRoles.		Read

Configuration Notes

The following configuration notes apply to this release:

Running the adapter as a non-APPS user

The account APPS owns the Oracle eBS database and the Oracle eBS Adapter must run as the APPS user unless special configuration steps are followed.

If "APPS" is specified as **Administrator Name** on the Oracle EBS service form within TIM, then no configuration changes are required on Oracle eBS.

If your security standards do not permit the use of APPS as the administrator account for the Oracle eBS adapter, then you must create a new user and grant required permissions as shown in the nonAPPS.sql file shipped with the adapter. No changes are required in the adapter profile.

NOTE: The adapter depends on wrapper stored procedures when an account other than APPS is used. Create the wrapper stored procedures specified in the nonAPPS.sql file.

Updating Adapters from Version 4.6

Tivoli Directory Integrator version 6.1.1 is a prerequisite to run the 5.0 adapters. To upgrade the adapter from a Tivoli Identity Manager 4.6 installation, perform the following:

1. If the Tivoli Directory Integrator is not version 6.1.1, take the appropriate actions to upgrade it.
2. Install all the adapter's components, as described in the installation guide, on the Tivoli Directory Integrator version 6.1.1. The installer will replace any previous installation.
3. Import the adapter profile into the Tivoli Identity Manager 5.0.

MR111110213 – Add ability to require SSL connection from OracleEBS Adapter to Oracle

The adapter has been enhanced to allow a secure connection from the adapter to the Oracle eBS database.

The following new attributes are defined in the schema.dsml file:

1. "erOraEBSUseSSL" (OID 1.3.6.1.4.1.6054.3.144.2.30) is added for the "erOraEBSRMIService" class.
   a. A new label (eroraebsusessl = **Use SSL communication with Oracle?**) is added for this attribute in the CustomLabels.properties file.
   b. This attribute is visible on the service form.
2. "erOraEBSServerDN" (OID 1.3.6.1.4.1.6054.3.144.2.31) is added for the "erOraEBSRMIService" class.
   a. A new label (eroraebsserverdn = **Oracle EBS Server Distinguished Name**) is added for this attribute in the CustomLabels.properties file.
   b. This attribute is visible on the service form.

JDBC driver location for SSL

SSL support in the JDBC Thin driver was first included in the 10g Release 2 of the driver. The driver may be obtained from either:

- The *ORACLE_HOME*/jdbc/lib directory of the database tier, or
- The JDBC Driver Downloads page on the Oracle Technology Network (OTN) website.

The driver for use with JRE 1.5 (TDI 6.1.1) is ojdbc5.jar. The appropriate driver should be copied to the *TDI_HOME*/jars/3rdparty/others directory on the Tivoli Directory Integrator (TDI) server.

Furthermore, previous versions of the JDBC Thin driver should be removed from the TDI server directory. These include:

- ojdbc14.jar
- classes12.zip
- nls_charset12.zip
- classes111.zip
- nls_charset11.zip

Note that the zip files listed above may alternatively have been named as jar files, e.g. classes12.jar.

Configure the SSL connection

To enable SSL communication between the Oracle eBS adapter and the Oracle eBS database, a truststore and optionally a keystore need to be configured for the RMI dispatcher.

A keystore will have to be configured if the Oracle eBS database is configured to require SSL client authentication.

To configure the truststore for the RMI dispatcher, you must minimally import the Certification Authority (CA) certificate that is used to sign the certificate for the Oracle eBS database.

All the files in the example steps below are in the Tivoli Identity Manager solutions directory (*TDI_HOME*/timsol by default).

TDI configuration for Oracle eBS database tier authentication

The command to import a CA certificate into the truststore is as follows:

```
keytool -import -v -alias OACA -file CA.cer -keystore truststore.jks -storetype JKS
    -storepass "ThePwd12"
```

In the solutions.properties file, the following properties must be set:

```
javax.net.ssl.trustStore=truststore.jks
javax.net.ssl.trustStorePassword=ThePwd12
javax.net.ssl.trustStoreType=jks
```

If the javax.net.ssl.trustStore property is already set to a truststore other than truststore.jks, then the CA certificate should be imported into that file instead.

Note that the store password, ThePwd12, is for illustrative purposes only.

If a keystore is not required and the keystore properties have not been set in the solution.properties file, then set the properties to the same values as the truststore properties:

```
javax.net.ssl.keyStore=truststore.jks
javax.net.ssl.keyStorePassword=ThePwd12
javax.net.ssl.keyStoreType=jks
```

TDI configuration for Oracle eBS adapter authentication

If the Oracle eBS database is configured for SSL client authentication, a keystore will have to be configured. The following commands set up a JKS type keystore:

```
keytool -genkey -alias OADB -dname "CN=client,C=US" -storetype JKS -keystore client.jks
    -keyalg RSA -storepass "ThePwd12"
keytool -certreq -alias OADB -file creq.cer -keystore client.jks -storepass "ThePwd12"
orapki cert create -wallet ./authority -request creq.cer -cert signed.cer -validity 3650
    -pwd=ThePwd12
keytool -import -v -alias OACA -file CA.cer -keystore client.jks -storepass "ThePwd12"
keytool -import -v -alias OADB -file signed.cer -keystore client.jks -storepass "ThePwd12"
```

The above commands assume that you have created a self-signed certification authority as described in the Oracle eBS database tier configuration section later in this document.

In the solutions.properties file, the following properties must be set:

```
javax.net.ssl.keyStore=client.jks
javax.net.ssl.keyStorePassword=ThePwd12
javax.net.ssl.keyStoreType=jks
```

Note that the store password, ThePwd12, is for illustrative purposes only.

Oracle eBS database tier configuration

To configure both the truststore and keystore on the Oracle eBS database tier, Oracle tools, such as the Oracle Wallet Manager and the orapki command, are used. The following commands set up a self-signed certification authority, truststore, and keystore. Note that the passwords, ThePwd12, are only for illustrative purposes only.

Self-signed certification authority

```
mkdir authority
orapki wallet create -wallet ./authority -pwd=ThePwd12
orapki wallet add -wallet ./authority -dn "CN=authority, C=US" -keysize 2048 -self_signed
    -validity 3650 -pwd=ThePwd12
orapki wallet export -wallet ./authority -dn "CN=authority, C=US" -cert CA.cer
    -pwd=ThePwd12
```

The CA.cer file is the trusted certificate that is used in the keytool command to import a CA certificate into the truststore for the RMI dispatcher.

Stores for Oracle eBS database tier authentication

```
mkdir server
orapki wallet create -wallet ./server -auto_login -pwd=ThePwd12
orapki wallet add -wallet ./server -trusted_cert -cert CA.cer -pwd=ThePwd12
orapki wallet add -wallet ./server -dn "CN=server, C=US" -keysize 2048 -pwd=ThePwd12
orapki wallet export -wallet ./server -dn "CN=server, C=US" -request creq.cer
-pwd=ThePwd12
orapki cert create -wallet ./authority -request creq.cer -cert signed.cer -validity 3650
-pwd=ThePwd12
orapki wallet add -wallet ./server -user_cert -cert signed.cer -pwd=ThePwd12
```

Oracle Network configuration

The listener.ora and sqlnet.ora files need to be configured on the Oracle eBS database tier to enable SSL. These files are located in the *ORACLE_HOME*/network/admin/*instance* directory of the database tier. These files are often edited through the Oracle Net Manager, but may also be edited through a text editor.

The following show the relevant lines for a sample configuration:

listener.ora:

```
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION = (SOURCE = (METHOD = FILE)(METHOD_DATA =
        (DIRECTORY = SERVER_WALLET_LOCATION)
))
LISTENER = (DESCRIPTION_LIST = (DESCRIPTION =
        (ADDRESS = (PROTOCOL = TCPS)(HOST = HOSTNAME)(PORT = 2484))
))
```

sqlnet.ora:

```
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION = (SOURCE = (METHOD = FILE)(METHOD_DATA =
        (DIRECTORY = SERVER_WALLET_LOCATION)
))
```

Make sure that *SERVER_WALLET_LOCATION* is substituted with the directory where the server wallet is on the database server. Substitute *HOSTNAME* with your hostname. Port *2484* is often the port used for SSL communication (protocol TCPS). If authentication of the Oracle eBS adapter is desired, SSL_CLIENT_AUTHENTICATION should be set to TRUE instead (the given configuration does not require authentication of the adapter).

Oracle eBS adapter service form

To enable SSL communication between the Oracle eBS adapter and the Oracle eBS database, the following changes are needed on the Oracle eBS adapter service form:

- Check the checkbox labeled **Use SSL communication with Oracle?**
- Update the value of **Oracle EBS Service Port** to the TCPS port, e.g. 2484, listed in the listener.ora file.
- Optionally provide a value for the **Oracle EBS Server Distinguished Name** field.

When a value is entered for the **Oracle EBS Server Distinguished Name** field, the entry will be verified against the Oracle eBS database server certificate.

Notes

1. Start both the listener and database services with the same user who has created the wallet, so that they are both able to access the wallet successfully.

2. The wallet location is provided in both the sqlnet.ora and the listener.ora files. In the most common case, both files contain the same wallet location, but this is not necessarily the case; the listener could use its own wallet.

    a. The distinguished name of the certificate pointed by the wallet in the sqlnet.ora file is the name to which the Oracle eBS adapter must verify (when we include a distinguished name in the service form).

    b. It is recommended that you include a distinguished name in the service form as an extra measure of security, so that you avoid the risk of another server faking its identity.

3. For more details about how to configure SSL with the Oracle JDBC Thin driver, refer to the Oracle technical white paper SSL with Oracle JDBC Thin Driver on Oracle's website (http://www.oracle.com/).

MR0817103443 and MR0715114436 – Oracle eBS RBAC role support

The adapter has been enhanced to support addition, modification and reconciliation of RBAC role information associated with an Oracle eBS user.

The following new classes are defined in the schema.dsml file:

1. "erOraEBSRoleAccount" (OID 1.3.6.1.4.1.6054.3.144.1.8) is added for support data reconciliation.

The following new attributes are defined in the schema.dsml file:

1. "erOraEBSRole" (OID 1.3.6.1.4.1.6054.3.144.2.32, type Directory String) is added to the "erOraEBSRoleAccount" class.
2. "erOraEBSRoleName" (OID 1.3.6.1.4.1.6054.3.144.2.33, type Directory String) is added to the "erOraEBSRoleAccount" class.
3. "erOraEBSRoleSystem" (OID 1.3.6.1.4.1.6054.3.144.2.34, type Directory String) is added to the "erOraEBSRoleAccount" class.
4. "erOraEBSRoleDisplayName" (OID 1.3.6.1.4.1.6054.3.144.2.35, type Directory String) is added to the "erOraEBSRoleAccount" class.
5. "erOraEBSRoleDescription" (OID 1.3.6.1.4.1.6054.3.144.2.36, type Directory String) is added to the "erOraEBSRoleAccount" class.
6. "erOraEBSRoleDisplay" (OID 1.3.6.1.4.1.6054.3.144.2.37, type Directory String) is added to the "erOraEBSRoleAccount" class.
7. "erOraEBSDirectRoles" (OID 1.3.6.1.4.1.6054.3.144.2.38, type Directory String) is added to the "erOraEBSAccount" class.
8. "erOraEBSIndirectRoles" (OID 1.3.6.1.4.1.6054.3.144.2.38, type Directory String) is added to the "erOraEBSAccount" class.

The attribute formats for the account class may be found in the Corrections to Installation Guide section of this document.

Subforms have been created to administer a user's directly granted roles via the web interfaces. Details on how to install and use the subforms may be found in the Corrections to Installation Guide and Corrections to User Guide sections of this document.

Changes to nonAPPS.sql to support roles

To support roles the following grants are required for a non APPS user:

• An execute grant on the package APPS.WF_LOCAL_SYNCH.
• A select grant on the tables/views/synonyms APPS.WF_ALL_USER_ROLES, APPS.WF_ROLES.

Corrections to User Guide

The following corrections to the User Guide apply to this release:

A. Make the following changes to Chapter 3. Oracle eBS Adapter user account management tasks.

Reconciling user accounts

To the list of supporting data for an Oracle eBS user account, add the following:
- Securing attributes
- Roles

Adding user accounts

To the list of optional attributes on the Oracle eBS account form, add the following:
- Securing attributes
- Roles

Replace the subsection "Assigning responsibilities to a user account" with the following:

You can assign responsibilities to the Oracle eBS user account by using the Responsibilities subform, accessed by clicking the "Details..." button under the Reponsibilities field.

The subform shows the responsibilities that are slated for assignment in the table "Direct Responsibilities".

To save all changes that have been made, click the "Save changes and Close Current Window" button. If a validation error occurs, the changes will not be saved and the subform will continue to be displayed. Otherwise, the subform window will be closed. Note that saving the subform's values merely prepares them for main form submission. If the main form is cancelled, any changes will not be effected.

To abort all changes made since the most recent savepoint, click the "Cancel" button. The subform window will be closed.

To add responsibilities, click the "Add" button. A search window will pop up. Enter the search criteria and click the "Search" button. On the search results page, the "Name" column shows the responsibility in the form "Application_Name | Responsibility_Name". Select any number of rows using the checkboxes, and click Add. The search window will be closed and the added responsibilities will appear in the subform.

To modify the start and/or end dates of a responsibility, enter the date in the appropriate input boxes. The date format is "dd/mm/yyyy" (e.g. "31/12/2001"). The start date of a responsibility is a compulsory field. An empty end date denotes a responsibility that continues indefinitely.

A responsibility cannot be deleted. However, it can be disabled by setting the end date to a date prior to the current date. Note that the end date cannot be before the start date.

Add the following subsections after the "Assigning responsibilities to a user account" subsection:

Assigning securing attributes to a user account

You can assign securing attributes to the Oracle eBS user account by using the Securing Attributes subform, accessed by clicking the "Details..." button under the Securing Attributes field.

The subform shows the securing attributes that are slated for assignment in a table.

To save all changes that have been made, click the "Save changes and Close Current Window" button. If a validation error occurs, the changes will not be saved and the subform will continue to be displayed. Otherwise, the subform window will be closed. Note that saving the subform's values merely prepares them for main form submission. If the main form is cancelled, any changes will not be effected.

To abort all changes made since the most recent savepoint, click the "Cancel" button. The subform window will be closed.

To add securing attributes, click the "Add" button. A search window will pop up. Enter the search criteria and click the "Search" button. On the search results page, the "Name" column shows the securing attribute in the form "Attribute_Name | Attribute_Code | Application_Name | Application_ID | Attribute_Type". Select any number of rows using the checkboxes, and click Add. The search window will be closed and the added securing attributes will appear in the subform.

To delete securing attributes, select the attributes using the checkboxes in the subform, and click the "Delete Selected" button. The attributes will be removed from the table.

To modify the securing attribute value, enter the appropriate data into the corresponding input box. For an attribute type of DATE, the value's format should be "dd-mm-yyyy" (e.g. "31-12-2001"). For an attribute type of DATETIME, the value's format should be "dd-mm-yyyy hh24:mi:ss" (e.g. "31-12-2001 13:45:00").

Assigning roles to a user account

You can assign roles to the Oracle eBS user account by using the Roles subform, accessed by clicking the "Details..." button under the Roles field.

The subform shows the roles that are slated for assignment in the table "Direct Roles".

To save all changes that have been made, click the "Save changes and Close Current Window" button. If a validation error occurs, the changes will not be saved and the subform will continue to be displayed. Otherwise, the subform window will be closed. Note that saving the subform's values merely prepares them for main form submission. If the main form is cancelled, any changes will not be effected.

To abort all changes made since the most recent savepoint, click the "Cancel" button. The subform window will be closed.

To add roles, click the "Add" button. A search window will pop up. Enter the search criteria and click the "Search" button. On the search results page, the "Name" column shows the role in the form Name | ID | System | Display_Name | Description. Select any number of rows using the checkboxes, and click Add. The search window will be closed and the added roles will appear in the subform.

To modify the start and/or end dates of a role, enter the date in the appropriate input boxes. The date format is "dd/mm/yyyy hh24:mi" (e.g. "31/12/2001 13:45"). The start date of a role is a compulsory field. An empty end date denotes a role that continues indefinitely. The assignment reason may be entered in the appropriate input box.

A role cannot be deleted. However, it can be disabled by setting the end date to a date prior to the current date. Note that the end date cannot be before the start date.

Modifying user accounts

Remove the phrase "but cannot delete the values" from the sentence introducing the list of modifiable attributes.

"User ID" should be removed from the list of unmodifiable attributes and placed in the list of modifiable attributes. In addition, the following attributes should be added to the list of modifiable attributes:

- Description
- Email
- Fax
- User Start Date (you may not delete the value)
- User End Date
- Responsibilities
- Securing attributes
- Roles

B. Make the following changes to Chapter 4. Troubleshooting the Oracle eBS Adapter errors.

Add the following rows to Table 3:

Error Message	Recommended Action
CTGIMT008W The account was added, but some attributes failed. ERROR: java.sql.SQLException: ORA-01861: literal does not match format string	Ensure that a value specified to this attribute should match the data format of the securing attribute.
CTGIMT008W The account was added, but some attributes failed. Error: ERROR: java.sql.SQLException: ORA-01843: not a valid month	Ensure that a value specified to this attribute should match the data format of the securing attribute.

CTGIMT008W The account was added, but some attributes failed.
ERROR: java.sql.SQLException: ORA-06550: PLS-00103: Encountered the symbol "x" when expecting one of the following:
) , * & | = - + < / > at in is mod not rem => ..
  <an exponent (**)> <> or != or ~= >= <= <> and or like
  between ||
The symbol "," was substituted for "x" to continue.
	Ensure that a value specified to this attribute should match the data format of the securing attribute.

CTGIMT008W The account was added, but some attributes failed. ERROR: java.sql.SQLException: ORA-01858: a non-numeric character was found where a numeric was expected	Ensure that a value specified to this attribute should match the data format of the securing attribute.
CTGIMT013E A system error occurred while modifying the account.	Ensure that the user name is not already in use and does not exceed the allowed number of characters.

Replace the following rows in Table 3:

Error Message	Recommended Action
CTGIMT014W: The account was modified, but some attributes failed. erUid Error: See Adapter log for detailed error.	Ensure that the user name is not already in use and does not exceed the allowed number of characters.

C. Make the following changes to Appendix A. APIs used by the adapter.

Add the following rows to Table 4.

Oracle eBS API	Operation
ICX_USER_SEC_ATTR_PUB.create_user_sec_attr	Add securing attribute
ICX_USER_SEC_ATTR_PUB.delete_user_sec_attr	Delete securing attribute
FND_USER_PKG.change_user_name	Change user name
WF_LOCAL_SYNCH.propagateUserRole	Add/modify user roles

Customizing or Extending Adapter Features

The Identity Manager adapters can be customized and/or extended. The type and method of this customization may vary from adapter to adapter.

Getting Started

Customizing and extending adapters requires a number of additional skills. The developer must be familiar with the following concepts and skills prior to beginning the modifications:

- Tivoli Identity Manager administration
- Tivoli Directory Integrator management
- Tivoli Directory Integrator assemblyline development
- LDAP schema management
- Working knowledge of Javascript scripting language
- Working knowledge of LDAP object classes and attributes
- Working knowledge of XML document structure

Note: If the customization requires a new Tivoli Directory Integrator connector, the developer must also be familiar with Tivoli Directory Integrator connector development and working knowledge of Java programming language.

Tivoli Identity Manager Resources:

> Check the "Learn" section of the Tivoli Identity Manager Support web site for links to training, publications, and demos.

Tivoli Directory Integrator Resources:

> Check the "Learn" section of the Tivoli Directory Integrator Support web site for links to training, publications, and demos.

Tivoli Identity Manager Adapter Development:

> Adapter Development Tool
>
> > The Adapter Development Tool, ADT, is a tool used by IBM Tivoli Identity Manager (ITIM) customers and consultants to create custom TIM adapters. It reduces adapter delivery time by about 50% and it helps in the development of custom adapters. The Adapter development tool is available on the IBM Integrated Service Management Library.

Support for Customized Adapters

The integration to the Identity Manager server – the adapter framework – is supported. However, IBM does not support the customizations, scripts, or other modifications. If you experience a problem with a customized adapter, IBM Support may require the problem to be demonstrated on the GA version of the adapter before a PMR is opened.

Supported Configurations

Installation Platform

The IBM Tivoli Identity Manager Adapter was built and tested on the following product versions.

Adapter Installation Platform:

> This adapter installs into Tivoli Directory Integrator (TDI) and may be installed on any platform supported by the TDI product and supported by the target system libraries or client, where applicable. IBM recommends installing TDI on each node of the ITIM WAS Cluster and then installing this adapter on each instance of TDI. Supported TDI versions include:

- TDI 6.1.1 with Fix Pack 10 or higher

Managed Resource:

- Oracle e-Business Suite   12.0
- Oracle e-Business Suite   12.1.1

IBM Tivoli Identity Manager:

- Identity Manager v5.0

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.
IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

IBM Corporation
2ZA4/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
IBM logo
DB2
Tivoli
Universal Database
WebSphere.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the U.S., other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

End of Release Notes