

Oracle® Identity Manager

Connector Guide for Oracle E-Business User Management

Release 9.1.0

E11203-17

July 2015

Copyright © 2013, 2015, Oracle and/or its affiliates. All rights reserved.

Primary Author: Gowri.G.R

Contributing Authors: Prakash Hulikere, Gauhar Khan, Alankrita Prakash, Deena Purushothaman

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	xi
Audience	xi
Documentation Accessibility	xi
Related Documents	xi
Documentation Updates	xi
Conventions	xii
 What's New in Oracle Identity Manager Connector for Oracle E-Business User Management?	xiii
Software Updates	xiii
Documentation-Specific Updates.....	xxiv
 1 About the Connector	
1.1 Certified Components	1-1
1.2 Usage Recommendations.....	1-2
1.3 Certified Languages.....	1-3
1.4 Connector Architecture.....	1-3
1.5 Features of the Connector	1-4
1.5.1 Oracle E-Business User Management Connectors.....	1-4
1.5.1.1 User Management	1-5
1.5.1.2 User Management with HR Foundation.....	1-5
1.5.1.3 User Management with TCA Foundation	1-7
1.5.1.4 Similarities Between the Three Connectors	1-7
1.5.1.5 Differences Between the Connectors	1-8
1.5.2 Management of Entitlements	1-9
1.5.3 SoD Validation of Entitlement Provisioning	1-10
1.5.4 Support for an SSO-Enabled Target System Installation	1-10
1.5.5 Reconciliation of Effective-Dated Events	1-11
1.5.6 Account Status Reconciliation and Provisioning	1-11
1.5.7 Configurable Reconciliation Queries	1-12
1.5.8 Account Password Management.....	1-12
1.5.9 Support for Full and Incremental Reconciliation.....	1-12
1.5.10 Support for Limited (Filtered) Reconciliation	1-12
1.5.11 Support for Batched Reconciliation	1-12
1.5.12 Connection Pooling	1-13

1.6	Reconciliation Process	1-13
1.6.1	Reconciliation Queries	1-14
1.6.2	Target System Columns Used in Reconciliation	1-15
1.6.3	Reconciliation Rule	1-18
1.6.4	Reconciliation Action Rules for Target Resource Reconciliation.....	1-19
1.7	Provisioning Process.....	1-20
1.7.1	Request-Based Provisioning of Entitlements.....	1-22
1.7.2	Attribute Mappings for Provisioning	1-23
1.7.3	Provisioning Functions	1-25
1.8	Lookup Definitions Used During Connector Operations.....	1-27
1.8.1	Lookup Definitions That Are Common to All Three Connectors	1-27
1.8.2	Lookup Definitions That Are Specific to the User Management Connector	1-29
1.8.3	Lookup Definitions That Are Specific to the User Management with HR Foundation Connector 1-30	
1.8.4	Lookup Definitions That Are Specific to the User Management with TCA Foundation Connector 1-32	
1.9	Roadmap for Deploying and Using the Connector	1-34

2 Deploying the Connector

2.1	Preinstallation.....	2-1
2.1.1	Preinstallation on Oracle Identity Manager.....	2-1
2.1.1.1	Files and Directories on the Installation Media	2-1
2.1.1.2	Determining the Release Number of the Connector	2-4
2.1.1.3	Creating a Backup of the Existing Common.jar File	2-4
2.1.2	Preinstallation on the Target System	2-5
2.1.2.1	Creating a Target System User Account for Connector Operations	2-6
2.1.2.2	Compiling Custom Wrapper Packages	2-9
2.1.2.3	Setting the Employee Number Creation Mode.....	2-9
2.2	Installation	2-10
2.2.1	Running the Connector Installer	2-10
2.2.2	Copying Files to the Oracle Identity Manager Host Computer.....	2-13
2.3	Postinstallation	2-14
2.3.1	Configuring SoD	2-14
2.3.1.1	Configuring the Oracle Applications Access Controls Governor to Act As the SoD Engine 2-14	
2.3.1.2	Specifying a Value for the TopologyName IT Resource Parameter	2-14
2.3.1.3	Disabling and Enabling SoD	2-15
2.3.2	Configuring Secure Communication Between the Target System and Oracle Identity Manager 2-20	
2.3.2.1	Configuring Data Encryption and Integrity in Oracle Database.....	2-20
2.3.2.2	Configuring SSL Communication in Oracle Database.....	2-20
2.3.3	Postinstallation on Oracle Identity Manager	2-21
2.3.3.1	Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server 2-22	
2.3.3.2	Configuring Oracle Identity Manager 11.1.2 or Later.....	2-31
2.3.3.2.1	Creating and Activating a Sandbox.....	2-31
2.3.3.2.2	Creating a New UI Form	2-32
2.3.3.2.3	Creating an Application Instance	2-32

2.3.3.2.4	Publishing a Sandbox	2-32
2.3.3.2.5	Harvesting Entitlements and Sync Catalog.....	2-33
2.3.3.2.6	Updating an Existing Application Instance with a New Form	2-33
2.3.3.3	Clearing Content Related to Connector Resource Bundles from the Server Cache ... 2-33	
2.3.3.4	Enabling Logging	2-35
2.3.3.4.1	Enabling Logging on Oracle Identity Manager Release 9.1.0.x.....	2-35
2.3.3.4.2	Enabling Logging on Oracle Identity Manager Releases 11.1.x and 11.1.2.x 2-36	
2.3.3.5	Determining Values for the JDBC URL and Connection Properties Parameters..... 2-39	
2.3.3.5.1	Supported JDBC URL Formats.....	2-39
2.3.3.5.2	Only Data Encryption and Integrity Is Configured	2-40
2.3.3.5.3	Only SSL Communication Is Configured	2-40
2.3.3.5.4	Both Data Encryption and Integrity and SSL Communication Are Configured . 2-42	
2.3.3.6	Configuring the IT Resource.....	2-43
2.3.3.7	SSO IT Resource.....	2-49
2.3.3.8	Disabling the Auto Save Form Feature on Oracle Identity Manager Releases 11.1.x and 11.1.2.x 2-50	
2.3.3.9	Enabling Request-Based Provisioning.....	2-50
2.3.3.9.1	Enabling Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x 2-50	
2.3.3.9.2	Enabling Request-Based Provisioning on Oracle Identity Manager Releases 11.1.x and 11.1.2.x: 2-53	
2.3.4	Localizing Field Labels in UI Forms	2-55
2.4	Postcloning Steps	2-56

3 Using the Connector

3.1	Setting Up Lookup Definitions in Oracle Identity Manager	3-1
3.1.1	Setting Up the Configuration Lookup Definition for SSO Password Update	3-1
3.1.2	Setting Up the Configuration Lookup Definition.....	3-2
3.1.2.1	Setting Up the Lookup.EBS.UM.Configuration Lookup Definition	3-2
3.1.2.2	Setting Up the Lookup.EBS.UMHRMS.Configuration Lookup Definition	3-4
3.1.2.3	Setting Up the Lookup.EBS.UMTCA.Configuration Lookup Definition.....	3-6
3.2	Scheduled Task for Lookup Field Synchronization.....	3-7
3.3	Configuring Reconciliation.....	3-9
3.3.1	Reconciliation Time Stamp.....	3-9
3.3.2	Batched Reconciliation	3-10
3.3.3	Configuring Limited Reconciliation	3-10
3.3.4	Reconciliation Scheduled Tasks.....	3-11
3.4	Configuring Scheduled Tasks	3-13
3.5	Attributes for Which You Can Specify Values During New Resource and Entitlement Provisioning 3-16	
3.5.1	Resource Provisioning Using the User Management Connector	3-17
3.5.2	Resource Provisioning Using the User Management with TCA Foundation Connector . 3-17	

3.5.3	Resource Provisioning Using the User Management with HR Foundation Connector....	3-17
3.5.4	Entitlement Provisioning Using All Three Connectors.....	3-18
3.6	Provisioning Operations Performed in an SoD-Enabled Environment.....	3-18
3.6.1	Overview of the Provisioning Process in an SoD-Enabled Environment	3-19
3.6.2	Direct Provisioning in an SoD-Enabled Environment	3-19
3.6.2.1	Prerequisites	3-19
3.6.2.2	Performing Direct Provisioning	3-20
3.6.3	Request-Based Provisioning in an SoD-Enabled Environment	3-30
3.6.3.1	End-User's Role in Request-Based Provisioning.....	3-30
3.6.3.1.1	End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x	3-30
3.6.3.1.2	End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.x	3-35
3.6.3.2	Approver's Role in Request-Based Provisioning	3-37
3.6.3.2.1	Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x	3-37
3.6.3.2.2	Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.x	3-39
3.7	Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.x	3-39
3.8	Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later.....	3-41
3.9	Uninstalling the Connector.....	3-41

4 Extending the Functionality of the Connector

4.1	Guidelines on Extending the Functionality of the Connector	4-1
4.1.1	Guidelines for Configuring Queries Used in Lookup Field Synchronization.....	4-2
4.1.2	Guidelines for Configuring Queries Used in Reconciliation.....	4-2
4.1.3	Guidelines Common to Configuring Both Types of Queries.....	4-3
4.1.4	Guidelines on Modifying Predefined Attribute Mappings for Provisioning	4-4
4.2	Adding or Removing Attributes for Reconciliation	4-5
4.2.1	Adding New Attributes for Reconciliation.....	4-5
4.2.2	Removing Attributes Used for Reconciliation.....	4-8
4.3	Adding or Removing Attribute Mappings for Provisioning.....	4-13
4.3.1	Adding New Attributes for Provisioning	4-14
4.3.2	Removing Attributes for Provisioning	4-20
4.4	Adding Filter Parameters in a Reconciliation Query.....	4-25
4.5	Modifying Field Lengths on the Process Form.....	4-27
4.6	Configuring Validation of Data During Reconciliation	4-27
4.7	Configuring Transformation of Data During User Reconciliation.....	4-29
4.8	Configuring Validation of Data During Provisioning.....	4-30
4.9	Configuring the Connector for Multiple Installations of the Target System	4-32
4.10	Customizing the Connector to Handle Timezone Differences	4-34

5 Testing and Troubleshooting

5.1	Running Test Cases.....	5-1
5.2	Troubleshooting	5-4

6 Known Issues

A Special Characters Supported by Oracle E-Business Suite 11.5.10

Index

List of Tables

1-1	Certified Components	1-2
1-2	Differences Between the Connectors.....	1-9
1-3	Attribute Mappings for Reconciliation in the User Management Connector.....	1-16
1-4	Attribute Mappings for Reconciliation in the User Management with HR Foundation Connector 1-16	
1-5	Attribute Mappings for Reconciliation in the User Management with TCA Foundation Connector 1-17	
1-6	Relationship Between Process Form Fields for Responsibilities and Target System Data Fields 1-17	
1-7	Relationship Between Process Form Fields for Roles and Target System Data Fields.	1-18
1-8	Action Rules for Target Resource Reconciliation.....	1-19
1-9	Attribute Mappings for Provisioning	1-23
1-10	Provisioning Functions	1-25
1-11	Lookup Definitions Common to All Three Connectors	1-28
1-12	Lookup Definitions Specific to the User Management Connector	1-30
1-13	Lookup Definitions Specific to the User Management with HR Foundation Connector	1-31
1-14	Lookup Definitions Synchronized with the Target System.....	1-33
2-1	Files and Directories on the Installation Media.....	2-1
2-2	Files to Be Copied to the Oracle Identity Manager Host Computer	2-13
2-3	Certificate Store Locations	2-21
2-4	Queries for Lookup Field Synchronization.....	2-23
2-5	Log Levels and ODL Message Type:Level Combinations	2-37
2-6	IT Resource Parameters.....	2-45
3-1	Date Formats That Can Be Entered as the Values of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT Entries 3-3	
3-2	Date Formats That Can Be Entered as the Values of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT Entries 3-5	
3-3	Date Formats That Can Be Entered as the Values of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT Entries 3-6	
3-4	Attributes of the eBusiness UM Lookup Definition Reconciliation Scheduled Task	3-8
3-5	Attributes of the eBusiness UM Target Resource User Reconciliation Scheduled Task	3-12
4-1	Connector Objects	4-32
A-1	Special Characters Supported by Oracle E-Business Suite 11.5.10	A-1

List of Figures

1-1	Architecture of the Connector	1-4
1-2	Architecture of the Connector with Configured to Work with an SSO Solution	1-11

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Oracle E-Business User Management.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit
<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

<http://www.oracle.com/technology/documentation/oim.html>

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

<http://www.oracle.com/technology/documentation/oim.html>

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in Oracle Identity Manager Connector for Oracle E-Business User Management?

This chapter provides an overview of the updates made to the software and documentation for the Oracle E-Business User Management connector in release 9.1.0.7.14.

The updates discussed in this chapter are divided into the following categories:

- [Software Updates](#)
This section describes updates made to the connector software.
- [Documentation-Specific Updates](#)
This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following sections discuss software updates:

- [Software Updates in Release 9.1.0.7.14](#)
- [Software Updates in Release 9.1.0.7](#)
- [Software Updates in Release 9.1.0.5](#)
- [Software Updates in Release 9.1.0.4](#)
- [Software Updates in Release 9.1.0.3](#)
- [Software Updates in Release 9.1.0.1](#)
- [Software updates in Release 9.1.0](#)

Software Updates in Release 9.1.0.7.14

The following are software updates in release 9.1.0.7.14:

- [Resolved Issues in Release 9.1.0.7.14](#)

Resolved Issues in Release 9.1.0.7.14

The following table lists issues resolved in release 9.1.0.7.14:

Bug Number	Issue	Resolution
12715982	<p>When an attempt to reconcile one record in the SSO-enabled mode was made, the SSO GUID of the user was reconciled successfully.</p> <p>However, when an attempt to reconcile more than one user was made, only the first record reconciled the SSO User ID. The subsequent records logged the following warning:</p> <p>"Could not find SSO User ID corresponding to user."</p>	<p>This issue has been resolved. During a reconciliation run, the SSO GUIDs of all user records being reconciled are fetched.</p>
12956783	Enabling a disabled user record did not work as expected.	This issue has been resolved. Enabling a disabled user records works as expected.
12980532	<p>Consider an Oracle Identity Manager environment with a large number of target system user accounts. Revoking a target system resource from an Oracle Identity Manager User account worked as expected. However, provisioning the target system resource to the same Oracle Identity Manager User account resulted in a timeout.</p>	<p>This issue has been resolved. The connector does not timeout while trying to provision a revoked resource in an Oracle Identity Manager environment with a large number of user accounts.</p> <p>In addition, the searching criteria is optimized to get a revoked status before a new user is provisioned.</p>
13070641	Child form fields such as Application Name, Responsibility Name, and Security Group displayed encoded values that were difficult to decipher.	<p>This issue has been resolved. The Lookup Column Name property has been modified from "lkv_encoded" to "lkv_decoded". Therefore, the connector displays decoded values in the child form fields.</p>

Bug Number	Issue	Resolution
13593940	The scripts/script1/OIM.sh and scripts/script2/OIM.sh scripts did not function as expected due to shell syntax errors.	This issue has been resolved. The OIM.sh scripts work as expected as all syntax errors in the scripts have been corrected.
13997216	When you specified a value for the Context User ID parameter of the IT resource, the CREATED_BY and LAST_UPDATE_BY columns of the FND_USR table were not set to contain the right value.	This issue has been resolved. CREATED_BY and LAST_UPDATE_BY columns of the FND_USER table are updated correctly.
14126858	The value of the SSO identifier was not updated after an EBS resource was reprovisioned to an Oracle Identity Manager User. In addition, the Oracle Identity Manager User could not use the SSO password through OID, although SSO was enabled. As a result, the user was unable to log in to the EBS target system.	This issue has been resolved. The value of the SSO identifier is updated after reprovisioning an EBS resource. OIM Users can now successfully log in to the EBS target system.
14176597	The OIM.sh scripts had misleading headers that prompted the use of an incorrect OIM.sh script version.	This issue has been resolved. The headers in the OIM.sh scripts have been corrected. In addition, these scripts do not mention the target system.
14826572	The HRMS Revoke and TCA Revoke provisioning operations and cross-provisioning features were missing.	This issue has been resolved. The HRMS Revoke and TCA Revoke provisioning functions have been added. This addition provides a configuration option to delete employee records or party records.

Bug Number	Issue	Resolution
14827165	<p>Create User provisioning operation was rejected with the "USER_EXISTS" status if you provisioned a TCA resource to the OIM User after revoking an HR resource.</p> <p>This issue was encountered because the CUSTOMER_ID column of the FND_USER table was not checked while provisioning a TCA resource.</p>	<p>This issue has been resolved. The connector has been enhanced to check the CUSTOMER_ID column value and update the same while provisioning or deprovisioning TCA resource.</p>
15996977	<p>While provisioning an EBS account, if the Hire Date was in the past, the connector created two records in the PER_ALL_PEOPLE_F table.</p> <p>While updating an employee record, the date track mode was set to "UPDATE" if the hire date was not the same as the start date, which created two employee records.</p>	<p>This issue has been resolved. Connector does not create two employee records if the employee hire date has a past value.</p> <p>The date track update mode is set to "CORRECTION" to ensure that only one record is created for each employee.</p>
16015896	<p>The value of the START_DATE column in the target system was incorrectly updated when a Remove Role provisioning operation was performed.</p>	<p>This issue has been resolved. The role start date is not modified when a role is revoked from a user.</p>
16458228	<p>Updating any OIM User process form field (for example Email), updated the Person ID field also.</p> <p>This was because the already existing Person ID values were overwritten in the target system and the same person ID field was not modified in the process form.</p>	<p>This issue has been resolved. The Person ID field is updated only when it is modified in the OIM User process form.</p>

Bug Number	Issue	Resolution
16692869	<p>The connector was able to perform cross-provisioning operations to both the TCA and HRMS resource. This allowed a single user account to be provisioned with both the TCA and HRMS resources at the same time.</p> <p>This issue was encountered because the connector did not check whether the resource being provisioned (HRMS or TCA) was revoked.</p>	<p>This issue has been resolved. Before performing a cross-provisioning operation, the connector check whether the resource being provisioned (HRMS or TCA) has been revoked.</p>
16808397	<p>Creation of a target system user account for connector operations failed if your target system was running on an Oracle RAC implementation.</p> <p>This issue was encountered because the scripts used for creating the user account were creating a tablespace.</p>	<p>This issue has been resolved. Creation of a target system user account for connector operations works as expected.</p> <p>Tablespace related commands have been removed to ensure that the user account gets created successfully.</p>
16892131	<p>During a reconciliation run, the connector created a new user account in Oracle Identity Manager even if the status of the corresponding user in the target system was "disabled".</p>	<p>This issue has been resolved. The connector does not create OIM User accounts for target system accounts that are in the "disabled" state.</p>
17055095	<p>After a reconciliation run from the target system to Oracle Identity Manager, the connector set an incorrect value for the Effective Date To field.</p> <p>This issue was encountered because fields storing date values did not use the correct date format.</p>	<p>This issue has been resolved. Fields containing date values are now reconciled correctly. The connector now uses the dd-Mon-yyyy format instead of the dd-Mon-yy format.</p>

Bug Number	Issue	Resolution
17252551	Inconsistencies in expected behavior were observed while handling entitlements through access policy-based provisioning. For example, if an application name was not provided in an access policy, then issues were encountered after reconciliation.	This issue has been resolved. Application Name is no longer a key field in reconciliation mappings.

Software Updates in Release 9.1.0.7

The following are the major enhancements in this release:

- [Added Security Groups Support to Oracle e-Business User Management Connectors](#)
- [Added Support for Validation and Transformation](#)
- [Resolved Issues in Release 9.1.0.7](#)

Added Security Groups Support to Oracle e-Business User Management Connectors

From this release onward, the security groups are added for provisioning and reconciliation in User Management connector, User Management with HR Foundation connector, and User Management with TCA Foundation connectors. During provisioning, the user can select a security group for any responsibility. If the user does not select any security group, then by default Standard security group is selected.

Added Support for Validation and Transformation

From this release onward, support for validation and transformation are added for provisioning and reconciliation.

Resolved Issues in Release 9.1.0.7

The following table lists issues resolved in release 9.1.0.7:

Bug Number	Issue	Resolution
10353797	Target User Reconciliation run stopped in between due to <code>IllegalArgumentException</code>	This issue has been resolved. Target User Reconciliation now will not be stopped even if user fields contain special characters. It will log the warning message with exception stack trace details of that user record and continue the reconciliation run for the next user records.

Bug Number	Issue	Resolution
11890859	Java command is incorrect in the test utility script oracleebiz.sh	This issue has been resolved. The Java command typo is now corrected in the test utility script, oracleebiz.sh
11829671	Logs do not display proper error for password expiration type	This issue has been resolved. The logs now display proper error message when password expiration type is selected, but password expiration interval value is not provided while updating the user task.

Software Updates in Release 9.1.0.5

The following are the software updates in release 9.1.0.5:

- [Resolved Issues in Release 9.1.0.5](#)

Resolved Issues in Release 9.1.0.5

The following table lists issues resolved in release 9.1.0.5:

Bug Number	Issue	Resolution
9779250	The scripts to create a target system user account for connector operations were not divided according to connector type.	This issue has been resolved. The scripts to create a target system user account for connector operations are now divided according to connector type.
9938336	During reconciliation, if a date field in a child table contained a NULL value, then that date field was not included in the reconciliation data.	This issue has been resolved. The connector correctly processes date fields into which NULL values are brought during reconciliation.
9467030	During provisioning operations, roles and responsibilities displayed in lookup fields on the Administrative and User Console were not filtered according to the selected IT resource.	This issue has been resolved. The list of roles or responsibilities is now filtered according to the selected IT resource.
9925468	An incorrect error message was displayed when an invalid configuration lookup definition name was specified in the IT resource.	This issue has been resolved. The message displayed when an invalid configuration lookup definition name is specified accurately describes the issue.

Software Updates in Release 9.1.0.4

The following are the software updates in release 9.1.0.4:

- [Support for New Oracle Identity Manager Release](#)
- [Support for Request-Based Provisioning](#)

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11g release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See [Section 1.1, "Certified Components"](#) for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11g release 1 (11.1.1).

See [Section 3.6.3, "Request-Based Provisioning in an SoD-Enabled Environment"](#) for more information.

Software Updates in Release 9.1.0.3

The following table lists issues resolved in release 9.1.0.3:

Bug Number	Issue	Resolution
6086572	On Oracle E-Business Suite 11.5.10, the target system user account for performing connector operations did not work as expected.	This issue has been resolved. See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for information about the procedure to create the target system user account.
8502490	To update an entitlement, the connector revoked and then added the entitlement.	This issue has been resolved. From this release onward, the connector can update the start date and end date values of an entitlement. The entitlement need not be revoked and then added.
9389768	The scheduled task for lookup field synchronization did not use the updateLookupValue method to update existing values in lookup definitions.	This issue has been resolved. The scheduled task now uses the updateLookupValue method to update existing values in lookup definitions.

Software Updates in Release 9.1.0.1

The following table lists issues resolved in release 9.1.0.1:

Bug Number	Issue	Resolution
8509529	In earlier releases, lookup field synchronization could be run in one of two modes: Refresh or Update. The Mode attribute of the eBusiness UM Lookup Definition Reconciliation scheduled task was used to store your choice.	From this release onward, lookup field synchronization is always run in the Update mode. The Mode attribute has been removed.
8969251	The connector created reconciliation events even for records that had not changed since the last reconciliation run.	This issue has been resolved. The connector now creates reconciliation events only for records that are added or modified after the last reconciliation run.
8798992	The Create User provisioning operation failed if you entered a value in the Person ID field.	This issue has been resolved. During the Create User provisioning operation, you can now enter a value in the Person ID field.
8783010	The Javadocs did not provide documentation on the public methods for the connector.	The Javadocs have been updated.
9004591	In an SSO-enabled environment, the default password set through a Create User operation was not configurable.	<p>This issue has been resolved. The FND_WEB_SEC.EXTERNAL_PWD entry has been added in the configuration lookup definition. In an SSO-enabled environment, you can use this entry to specify the default password for new users.</p> <p>Note: The "s" at the end of the name of the configuration lookup definitions has been removed in this release.</p>

Bug Number	Issue	Resolution
9000721	For Create User operations, the minimum password length for new users was set at 5 characters.	This issue has been resolved. You can now use the Minimum Password Length parameter of the IT resource to set the minimum password length.
8999921	During a Create User operation, you had to specify a password even when SSO communication was enabled.	This issue has been resolved. If SSO is enabled, then you need not specify a password during Create User operations.
8916172	In earlier releases, the connector required the ojdbc14.jar during reconciliation and provisioning. You had to copy this file from an external source.	<p>This issue has been resolved. The connector can now work with the ojdbc6.jar file. This file is present in the application server installation directory.</p> <p>As part of the fix implemented for this bug, the RECON_DATE_FORMAT and TO_CHAR_DATE_FORMAT entries have been introduced in the Lookup.EBS.ER.Configurations lookup definition. See Section 3.1, "Setting Up Lookup Definitions in Oracle Identity Manager" for more information about these entries.</p>
9003839	<p>The target system user account for connector operations was unable to perform the required connector operations. The following error message was displayed on the server console:</p> <p>ORA-04030: out of process memory</p>	<p>This issue has been resolved. The target system user account is now able to perform all connector operations successfully. However, a target system user account created on Oracle E-Business Suite 11.5.10 is unable to perform connector operations. This point has also been mentioned in the "Known Issues" chapter.</p>

Software updates in Release 9.1.0

The following are software updates in release 9.1.0:

- [Support for New Target System Versions and Configurations](#)
- [Dedicated Support for Target Resource Reconciliation](#)
- [Support for Provisioning Basic Person Records in Oracle E-Business HRMS and Basic Party Records in Oracle E-Business TCA](#)
- [Support for Managing Oracle E-Business Suite UMX Roles](#)
- [Support for SoD Validation of Entitlement Provisioning](#)
- [Support for SSO-Enabled Oracle E-Business Suite Installations](#)
- [Support for Oracle E-Business Suite Role and Responsibility Navigation Catalog](#)
- [Support for Effective-Dated Target System Events](#)
- [Support for Account Status Reconciliation and Provisioning](#)
- [Support for Configurable Reconciliation Queries](#)
- [Support for Creating Copies of Connector Objects](#)
- [Support for Target System Account with Minimum Permissions for Connector Operations](#)
- [Support for Connection Pooling](#)
- [Support for SSL Communication](#)
- [Support for the Multiple Trusted Source Reconciliation Feature of Oracle Identity Manager](#)
- [Inclusion of Javadocs in the Connector Deployment Package](#)

Support for New Target System Versions and Configurations

From this release onward, the connector supports the following new target system versions and configurations:

- Oracle E-Business Suite 11.5.10, 12.0.1 through 12.0.6 running on Oracle Real Application Clusters 10g and 11g
- Oracle E-Business Suite 12.1.1 running on Oracle Database 10g or Oracle Database 11g, as either single database or Oracle RAC implementation

These target systems are listed in the [Section 1.1, "Certified Components"](#) section.

Dedicated Support for Target Resource Reconciliation

The connector provides all the features required for setting up Oracle E-Business Suite as a managed (target) resource of Oracle Identity Manager. If you want to use Oracle E-Business Suite as a trusted source of identity data for Oracle Identity Manager, then use the Oracle E-Business Employee Reconciliation connector.

Support for Provisioning Basic Person Records in Oracle E-Business HRMS and Basic Party Records in Oracle E-Business TCA

Along with creation of a user record in Oracle E-Business Suite, the connector can be used to create a basic person record in Oracle E-Business HRMS. This feature enables access to Oracle E-Business Suite applications that require a user to have an account in Oracle E-Business HRMS.

In addition, the connector can be used to create a basic person-type party record in Oracle E-Business TCA. This feature enables access to Oracle E-Business Suite applications that require a user to have an account in Oracle E-Business TCA.

See [Section 1.5.1, "Oracle E-Business User Management Connectors"](#) for more information.

Support for Managing Oracle E-Business Suite UMX Roles

UMX role assignments can now be managed during reconciliation and provisioning.

Support for SoD Validation of Entitlement Provisioning

From this release onward, the connector supports the Segregation of Duties (SoD) feature introduced in Oracle Identity Manager release 9.1.0.2. Requests for Oracle E-Business Suite role and responsibility entitlements can be validated with Oracle Application Access Controls Governor. Entitlements are provisioned into Oracle E-Business Suite only if the request passes the SoD validation process. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to users.

See [Section 1.5.3, "SoD Validation of Entitlement Provisioning"](#) for more information.

Support for SSO-Enabled Oracle E-Business Suite Installations

The connector can be used to integrate Oracle Identity Manager with an SSO-enabled Oracle E-Business Suite installation.

See [Section 1.5.4, "Support for an SSO-Enabled Target System Installation"](#) for more information.

Support for Oracle E-Business Suite Role and Responsibility Navigation Catalog

You can use the connector to fetch data about responsibilities and roles definitions from each target system application and store this data in lookup definitions on Oracle Identity Manager. During a provisioning operation, these lookup definitions are

populated with responsibilities and roles that are specific to the Oracle E-Business Suite application you select for the operation. This feature leverages the dependent lookup capability of Oracle Identity Manager.

See [Section 1.8, "Lookup Definitions Used During Connector Operations"](#) for more information.

Support for Effective-Dated Target System Events

Oracle E-Business Suite allows future-dating (effective-dating) of account disable and account enable operations. The connector can detect and respond to these effective-dated lifecycle events.

Similarly, the connector can also respond to effective-dated operations in which roles and responsibilities are granted or revoked.

See [Section 1.5.5, "Reconciliation of Effective-Dated Events"](#) for an overview of the process.

Support for Account Status Reconciliation and Provisioning

The connector can now be used for reconciliation and provisioning account status data. During reconciliation, changes to the Effective Date From and Effective Date To fields on the target system are duplicated in Oracle Identity Manager. The same effect can be achieved through provisioning operations performed on Oracle Identity Manager.

See [Section 1.5.6, "Account Status Reconciliation and Provisioning"](#) for more information.

Support for Configurable Reconciliation Queries

Reconciliation involves running a SQL query on the target system database to fetch the required user account records to Oracle Identity Manager. From this release onward, predefined SQL queries are stored in a file in the connector deployment package. You can modify these SQL queries or add your own SQL queries for reconciliation.

See [Section 1.6.1, "Reconciliation Queries"](#) for information about the reconciliation queries.

Support for Creating Copies of Connector Objects

To meet the requirements of specific use cases, you might need to create multiple copies of the Oracle Identity Manager objects that constitute the connector. The connector can work with multiple instances of these objects.

See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for more information.

Support for Target System Account with Minimum Permissions for Connector Operations

In earlier releases, you had to use the APPS user for connector operations. From this release onward, you can create and use an Oracle E-Business Suite user with the minimum permissions required for connector operations.

See [Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"](#) for more information.

Support for Connection Pooling

The connector supports the connection pooling feature introduced in Oracle Identity Manager release 9.1.0.2. In earlier releases, a connection with the target system was

established at the start of a reconciliation run and closed at the end of the reconciliation run. With the introduction of connection pooling, multiple connections are established by Oracle Identity Manager and held in reserve for use by the connector.

See [Section 1.5.12, "Connection Pooling"](#) for more information.

Support for SSL Communication

From this release onward, you can configure SSL to secure communication between Oracle Identity Manager and the target system.

See [Section 2.3.2, "Configuring Secure Communication Between the Target System and Oracle Identity Manager"](#) for more information.

Support for the Multiple Trusted Source Reconciliation Feature of Oracle Identity Manager

The connector now supports the multiple trusted source reconciliation feature of Oracle Identity Manager. See Oracle Identity Manager Design Console Guide for detailed information about multiple trusted source reconciliation.

Inclusion of Javadocs in the Connector Deployment Package

To facilitate reuse and customization of some parts of the connector code, Javadocs are included in the connector deployment package.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- [Documentation-Specific Updates in Release 9.1.0.7.14](#)
- [Documentation-Specific Updates in Release 9.1.0.7](#)
- [Documentation-Specific Updates in Release 9.1.0.5](#)
- [Documentation-Specific Updates in Release 9.1.0.4](#)
- [Documentation-Specific Updates in Release 9.1.0.3](#)
- [Documentation-Specific Updates in Release 9.1.0.1](#)
- [Documentation-Specific Updates in Release 9.1.0](#)

Documentation-Specific Updates in Release 9.1.0.7.14

The following documentation-specific update has been made in revision "17" of release 9.1.0.7.14:

- The "Oracle Identity Manager" and "Target system" rows of [Table 1–1, "Certified Components"](#) have been updated.
- The "ResourceConnection class definition" row of [Table 2–6, "IT Resource Parameters"](#) has been updated.

The following documentation-specific update has been made in revision "16" of release 9.1.0.7.14:

The "Target System" row of [Table 1–1, "Certified Components"](#) has been updated.

The following documentation-specific update has been made in revision "15" of release 9.1.0.7.14:

[Section 3.9, "Uninstalling the Connector"](#) has been added.

The following documentation-specific updates have been made in revision "14" of release 9.1.0.7.14:

- A "Note" has been added to [Section 2.3.3.2.2, "Creating a New UI Form."](#)
- The "Admin Id" row of Step 2 has been modified in [Section 2.3.3.7, "SSO IT Resource."](#)

The following documentation-specific updates have been made in the revision "13" of release 9.1.0.7.14:

- Added [Section 2.3.3.7, "SSO IT Resource."](#)
- The first point has been added to the first note of [Section 3.3.4, "Reconciliation Scheduled Tasks."](#)
- Added [Section 2.4, "Postcloning Steps."](#)
- The "External code" row has been removed from [Table 1–1, " Certified Components"](#).
- A note has been added to [Section 1.7.3, "Provisioning Functions."](#)
- "Update Role" and "Update Responsibility" have been removed from [Table 1–10, " Provisioning Functions"](#).
- Information related to wrapper package for revoke role operation has been added to [Section 2.1.2.2, "Compiling Custom Wrapper Packages."](#)
- [Section 3.1.1, "Setting Up the Configuration Lookup Definition for SSO Password Update"](#) has been added.
- Revoke role provisioning operation related information has been added to the following Sections:
 - [Section 3.1.2.1, "Setting Up the Lookup.EBS.UM.Configuration Lookup Definition"](#)
 - [Section 3.1.2.2, "Setting Up the Lookup.EBS.UMHRMS.Configuration Lookup Definition"](#)
 - [Section 3.1.2.3, "Setting Up the Lookup.EBS.UMTCA.Configuration Lookup Definition"](#)
- Added the first point to the "Note" present in [Section 3.3.4, "Reconciliation Scheduled Tasks."](#)
- A "Note" has been added to Step 4 of [Section 4.3.1, "Adding New Attributes for Provisioning."](#)
- Step 6 has been added to [Section 4.3.1, "Adding New Attributes for Provisioning."](#)
- Steps 5 and 6 have been added to [Section 4.3.2, "Removing Attributes for Provisioning."](#)

Documentation-Specific Updates in Release 9.1.0.7

The following are the documentation-specific updates in this release:

- The following sections have been added:
 - [Section 1.2, "Usage Recommendations"](#)
 - [Section 2.3.3.2, "Configuring Oracle Identity Manager 11.1.2 or Later"](#)
 - [Section 3.8, "Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later"](#)

- [Section 4.10, "Customizing the Connector to Handle Timezone Differences"](#)
- Instructions specific to Oracle Identity Manager release 11.1.2.x have been added as required throughout the guide.
- The "Target System" row in [Table 1–1, "Certified Components"](#) has been updated.
- Information about CUSTOMER ID and PARTY ID has been added to [Section 1.5.1.3, "User Management with TCA Foundation"](#).
- Steps 1, 2, and 3 have been added to the procedure to "Enable SoD" in [Section 2.3.1.3, "Disabling and Enabling SoD."](#)
- The "Reinstallation of the connector is unsuccessful" row has been added to the table in [Section 5.2, "Troubleshooting."](#)

Documentation-Specific Updates in Release 9.1.0.5

The following is a documentation-specific update in this release:

- [Section 2.3.3.8, "Disabling the Auto Save Form Feature on Oracle Identity Manager Releases 11.1.x and 11.1.2.x"](#) has been added.

Documentation-Specific Updates in Release 9.1.0.4

The following are documentation-specific updates in release 9.1.0.4:

- [Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File"](#) has been added.
- [Section 3.6.2.1, "Prerequisites"](#) has been added.
- Some of the text in [Section 3.6, "Provisioning Operations Performed in an SoD-Enabled Environment"](#) has been moved to [Section 3.6.2.1, "Prerequisites."](#)

Documentation-Specific Updates in Release 9.1.0.3

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.1.0.1

The following are documentation-specific updates in release 9.1.0.1:

- In [Section 1.1, "Certified Components,"](#) changes have been made in the "External code" row.
- The "Using External Code Files" section has been removed from [Chapter 2, "Deploying the Connector."](#)
- All occurrences of "Lookup.EBS.UM.Configurations" have been replaced with "Lookup.EBS.UM.Configuration".
- In the [Chapter 6, "Known Issues":](#)
 - The following issue tracked by bug 8535215 has been removed as it was fixed in an earlier release:

The "ORA-00904 OBJ_UDF_KEYFIELD is invalid" error is thrown during reconciliation. To resolve this problem, deselect the Sequence Recon check box on the Resource Objects form of the Design Console. See *Oracle Identity Manager Design Console Guide* for more information about this flag.
 - A known issue tracked by bug 6086572 has been added.

- In [Section 2.1.1.1, "Files and Directories on the Installation Media,"](#) information about the script/OimUserAppstablesSynonyms.sql file and documentation/javadoocs directory has been added.
- In [Section 2.3.3.6, "Configuring the IT Resource,"](#) the Minimum Password Length IT resource parameter has been added.
- In the [Section 2.1.2.1, "Creating a Target System User Account for Connector Operations,"](#) the information that you must enter while running the script to create a target system user account for connector operations has been updated.
- In the [Section 3.2, "Scheduled Task for Lookup Field Synchronization,"](#) the Mode attribute has been removed.
- From this release onward:
 The minimum certified release of Oracle Identity Manager is release 9.1.0.2 or later.
 The minimum certified release of JDK is release 1.5.
 See [Section 1.1, "Certified Components"](#) for the complete listing of certified components.

Documentation-Specific Updates in Release 9.1.0

The following are documentation-specific updates in release 9.1.0:

- Major changes have been made in the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of information provided by the guide.
 See [Section 1.9, "Roadmap for Deploying and Using the Connector"](#) for detailed information about the organization of content in this guide.
- In [Section 1.1, "Certified Components,"](#) changes have been made in the "Target system" row.

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to use Oracle E-Business Suite as a managed (target) resource for Oracle Identity Manager.

In the account management (target resource) mode of the connector, information about users created or modified directly on Oracle E-Business Suite can be reconciled into Oracle Identity Manager. This data is used to provision (assign) resources to or update resources already assigned to OIM Users. In addition, you can use Oracle Identity Manager to provision or update resources assigned to OIM Users. These provisioning operations performed on Oracle Identity Manager translate into the creation of or updates to the corresponding target system accounts.

Note: At some places in this guide, Oracle E-Business Suite is referred to as the **target system**.

This chapter is divided in the following sections:

- [Section 1.1, "Certified Components"](#)
- [Section 1.2, "Usage Recommendations"](#)
- [Section 1.3, "Certified Languages"](#)
- [Section 1.4, "Connector Architecture"](#)
- [Section 1.5, "Features of the Connector"](#)
- [Section 1.6, "Reconciliation Process"](#)
- [Section 1.7, "Provisioning Process"](#)
- [Section 1.8, "Lookup Definitions Used During Connector Operations"](#)
- [Section 1.9, "Roadmap for Deploying and Using the Connector"](#)

1.1 Certified Components

[Table 1–1](#) lists the certified components for the connector.

Table 1–1 Certified Components

Component	Requirement
Oracle Identity Manager	<p>You can use one of the following releases of Oracle Identity Manager:</p> <ul style="list-style-type: none"> Oracle Identity Manager release 9.1.0.2 BP02 and any later BP in this release track Note: In this guide, Oracle Identity Manager release 9.1.0.x has been used to denote Oracle Identity Manager release 9.1.0.2 BP02 and future releases in the 9.1.0.x series that the connector supports. Oracle Identity Manager 11g release 1 (11.1.x) Note: In this guide, Oracle Identity Manager release 11.1.x has been used to denote Oracle Identity Manager 11g release 1 (11.1.x) and future releases in the 11.1.1.x series that the connector supports. Oracle Identity Manager 11g Release 2 (11.1.2.0.1) and any later BP in this release track Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)
Target system	<p>You can use one of the following releases of Oracle E-Business Suite:</p> <ul style="list-style-type: none"> Oracle E-Business Suite 11.5.10 Oracle E-Business Suite 12.0.0 through 12.0.6 Oracle E-Business Suite 12.1.0 through 12.1.3 Oracle E-Business Suite 12.2.0 through 12.2.4 <p>These applications may run on Oracle Database 10g or Oracle Database 11g, as either single database or Oracle RAC implementation.</p> <p>Note: Communication between Oracle Identity Manager and the target system can be in SSL or non-SSL mode.</p>
SoD engine	<p>If you want to enable and use the Segregation of Duties (SoD) feature of Oracle Identity Manager with this target system, then install one of the following:</p> <ul style="list-style-type: none"> If you are using Oracle Identity Manager release 9.1.0.x, then install Oracle Applications Access Controls Governor release 8.2.1 along with the latest patch set. Note: Contact Oracle Support for information about the patch set for release 8.2.1. If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then install Oracle Applications Access Controls Governor release 8.5.1. <p>See Section 1.5.3, "SoD Validation of Entitlement Provisioning" for more information about the SoD feature.</p>
SSO system	<p>The target system can use one of the following single sign-on (SSO) solutions:</p> <ul style="list-style-type: none"> Oracle Single Sign-On with Oracle Internet Directory as the LDAP-based repository Oracle Access Manager with Microsoft Active Directory, Sun Java System Directory, or Novell eDirectory as the LDAP-based repository
JDK	<p>The JDK requirement is as follows:</p> <ul style="list-style-type: none"> For Oracle Identity Manager release 9.1.0.x, use JDK 1.5 or later For Oracle Identity Manager release 11.1.x, use JDK 1.6 or later For Oracle Identity Manager release 11.1.2 or later, use JDK 1.6 or later

1.2 Usage Recommendations

If you are using Oracle Identity Manager 11g Release 2 (11.1.2), then you must perform the steps mentioned in Metalink note 1535369.1 to ensure the connector works as expected.

1.3 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

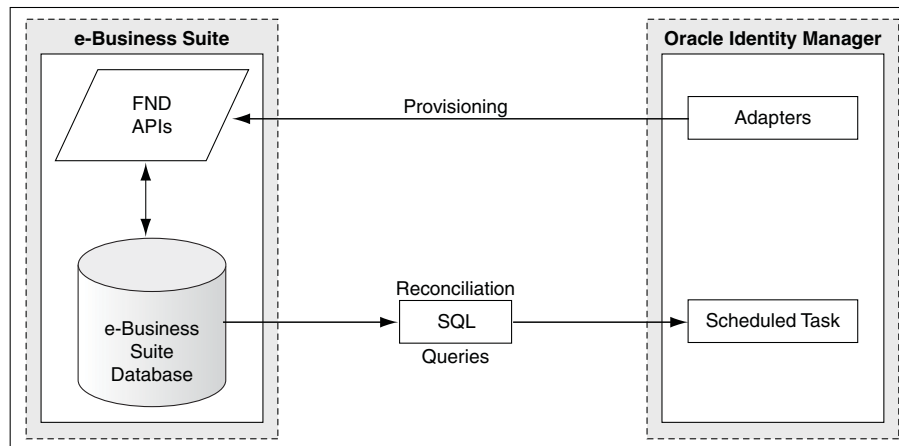
1.4 Connector Architecture

Note: In Oracle Identity Manager releases 11.1.x and 11.1.2.x, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.x is the same as the term **scheduled job** in the context of Oracle Identity Manager releases 11.1.x and 11.1.2.x.

See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

The basic function of the connector is to enable management of user data on Oracle E-Business Suite through Oracle Identity Manager. In other words, Oracle E-Business Suite (the target system) is used as a managed or target resource of Oracle Identity Manager. You can create and manage target system accounts (resources) for OIM Users through provisioning. In addition, data related to newly created and modified target system accounts can be reconciled (using scheduled tasks) and linked with existing OIM Users and provisioned resources.

Figure 1–1 shows the basic architecture of the connector. Data flow between the various components shown in this diagram is explained later in this chapter.

Figure 1–1 Architecture of the Connector

1.5 Features of the Connector

The following are features of the connector:

- [Section 1.5.1, "Oracle E-Business User Management Connectors"](#)
- [Section 1.5.2, "Management of Entitlements"](#)
- [Section 1.5.3, "SoD Validation of Entitlement Provisioning"](#)
- [Section 1.5.4, "Support for an SSO-Enabled Target System Installation"](#)
- [Section 1.5.5, "Reconciliation of Effective-Dated Events"](#)
- [Section 1.5.6, "Account Status Reconciliation and Provisioning"](#)
- [Section 1.5.7, "Configurable Reconciliation Queries"](#)
- [Section 1.5.8, "Account Password Management"](#)
- [Section 1.5.9, "Support for Full and Incremental Reconciliation"](#)
- [Section 1.5.10, "Support for Limited \(Filtered\) Reconciliation"](#)
- [Section 1.5.11, "Support for Batched Reconciliation"](#)
- [Section 1.5.12, "Connection Pooling"](#)

1.5.1 Oracle E-Business User Management Connectors

An FND_USER record represents an Oracle E-Business Suite account. This record is the main component of the account data whose management is enabled by the connector. Depending on your configuration of the target system, there may be other user data components that must be managed by the connector:

- Some applications in Oracle E-Business Suite require a user to have a person record in Oracle E-Business HRMS.

These users are either full-time employees of the organization or users (such as contract or part-time employees) who have been provided with access that is similar to the access provided to full-time employees. iExpense is an example of an application that requires users to have person (HRMS) records.

- Some applications in the Oracle E-Business Suite require a user to have a record in Oracle E-Business TCA.

Typically, these users are representatives or employees of customers and vendors of your organization. iStore and iProcurement are examples of applications that require users to have TCA records.

The connector can be used to manage any one or a combination of FND_USER, HRMS, and TCA records. Three separate versions of the connector have been provided for this purpose. The following sections provide information about these three connectors:

- [Section 1.5.1.1, "User Management"](#)
- [Section 1.5.1.2, "User Management with HR Foundation"](#)
- [Section 1.5.1.3, "User Management with TCA Foundation"](#)

The following section provides information that is common to all three connectors:

- [Section 1.5.1.4, "Similarities Between the Three Connectors"](#)
- [Section 1.5.1.5, "Differences Between the Connectors"](#)

1.5.1.1 User Management

In the User Management connector, you can use the connector to create Oracle E-Business Suite accounts (FND_USER records) for OIM Users and to grant roles and responsibilities to these accounts. You can also reconcile newly created and modified FND_USER records from the target system. These reconciled records are used to create and update Oracle E-Business Suite accounts assigned to OIM Users. These provisioning and reconciliation operations constitute the basic functions of the User Management connector.

The process form stores the User ID of the FND_USER record. All subsequent update operations (through reconciliation or provisioning) on the FND_USER record are performed on the basis of the User ID value.

If required, you can also *link* an FND_USER record with an existing HRMS person record. Use of this feature arises when the FND_USER record is required to be linked with an HRMS person record for access to intranet applications such as iExpense.

On the target system, the person ID forms the link between the FND_USER record and HRMS person record. For an FND_USER record that is linked with an HRMS record, the value in the EMPLOYEE_ID column of the FND_USER table is the same as the value in the PERSON_ID column of the PER_ALL_PEOPLE_F table.

While provisioning or modifying an already provisioned Oracle E-Business Suite account (FND_USER record), you can specify the person ID of the HRMS person record with which you want to link the FND_USER record. If a match is found, then the person record is linked with the FND_USER record. This person ID constitutes the link between the FND_USER record and the HRMS person record.

1.5.1.2 User Management with HR Foundation

In the User Management with HR Foundation connector, you can use the connector to create FND_USER records for OIM Users and to grant roles and responsibilities to these accounts. You can also reconcile newly created and modified FND_USER records from the target system. This is the same as the basic function of the connector in the User Management connector. In addition, you can create a basic HRMS person record for the user in Oracle E-Business HRMS and link that record with the FND User. As mentioned earlier in this chapter, the existence of an HRMS record is a prerequisite for using some applications in the Oracle E-Business Suite, such as iExpense and iRecruitment. This linking of records can also take place during reconciliation.

Note: In this guide, the basic HRMS record created by the connector is referred to as the **HR Foundation record**.

During a Create User provisioning operation, the FND_USER record is created first and then the employee record is created. Next, the link between the FND_USER record and employee record is established. The connector does not check for an existing employee record with the First Name and Last Name values provided during the provisioning operation.

For FND_USER records that are linked with HRMS person records, the value in the EMPLOYEE_ID column in the FND_USER table is the same as the value in the PERSON_ID column of the PER_ALL_PEOPLE_F table.

Note: You use the Manage HR Records parameter of the IT resource to enable the linking of HRMS Person records with FND_USER records. The IT resource is discussed later in this guide.

The process form stores the User ID of the FND_USER record and the Person ID of the HRMS record. All subsequent update operations (through reconciliation or provisioning) on the FND_USER record are performed on the basis of the User ID value. Similarly, all subsequent update operations (through reconciliation or provisioning) on the HRMS record are performed on the basis of the person ID value.

Guidelines on selecting the User Management with HR Foundation connector

You use the Oracle E-Business Employee Reconciliation connector to configure Oracle E-Business HRMS as a trusted source of Oracle Identity Manager. Ideally, Oracle Identity Manager only reconciles data from a trusted source. You do not perform provisioning (account management) operations on a trusted source.

The User Management with HR Foundation connector creates an HR Foundation record on Oracle E-Business HRMS. This is an account creation (that is, provisioning) operation.

As mentioned earlier, the HR Foundation record is a very basic HRMS person record. The connector supports only creation of and updates to this basic HRMS person record. These provisioning operations cannot be effective dated. For these reasons, you cannot use the connector to manage records on an Oracle E-Business HRMS installation.

In addition, to avoid conflicting data flows, it is strongly recommended that you do not configure a particular Oracle E-Business HRMS installation as *both* of the following:

- A trusted source, by using the Oracle E-Business Employee Reconciliation connector
- A target resource, by using the User Management with HR Foundation connector

Note: If you want the connector to recognize links between HRMS person records and FND_USER records, then use the User Management connector.

1.5.1.3 User Management with TCA Foundation

In the User Management with TCA Foundation connector, you can use the connector to create FND_USER records for OIM Users and to grant roles and responsibilities to these accounts. You can also reconcile newly created and modified FND_USER records from the target system. This is the same as the basic function of the User Management connector. In addition, you can create a basic TCA person-type party record for the user in Oracle E-Business TCA and link that record with the FND User. As mentioned earlier in this chapter, the existence of a TCA party record is a prerequisite for using some applications in the Oracle E-Business Suite, such as iStore. This linking of records can also take place during reconciliation.

Note: In this guide, the basic TCA person-type party record created by the connector is referred to as the **TCA Foundation record**.

During a create or modify FND_USER provisioning operation for a particular OIM User, the TCA party record is created the first time you specify First Name and Last Name values for that record. While creating the TCA party record, the connector does not check if another record with the same First Name and Last Name values exists. After the connector creates the TCA party record, the link established through the Party ID returned by Oracle E-Business TCA is used during subsequent updates of the TCA party record.

For FND_USER records that are linked with TCA party records, the value in the PERSON_PARTY_ID column in the FND_USER table is the same as the value in the PARTY_ID column of the HZ_PARTIES table.

Creating a person party ID internally creates or derives customer ID which is same as party ID and links this customer ID, party ID to the CUSTOMER_ID and PERSON_PARTY_ID columns of the FND_USER table, respectively. This connector supports provisioning and reconciliation of customer parties, but does not support provisioning and reconciliation of Suppliers or Vendors.

Note: You use the Manage TCA Records parameter of the IT resource to enable the linking of TCA party records with FND_USER records. The IT resource is discussed later in this guide.

The process form stores the User ID of the FND_USER record and the Party ID of the TCA record. All subsequent update operations (through reconciliation or provisioning) on the FND_USER record are performed on the basis of the User ID value. Similarly, all subsequent update operations (through reconciliation or provisioning) on the TCA record are performed on the basis of the Party ID value.

1.5.1.4 Similarities Between the Three Connectors

The following are similarities between the three connectors:

- The basic provisioning and reconciliation function is the same in all three connectors:
The connector creates and updates FND_USER records.
- Connector objects, such as process forms and resource objects, store data related to target system resources assigned to OIM Users. Each connector has its own set of these data objects.
- Each connector can be installed independently of the other connectors.

- Any combination of the connectors can be installed, in any order.
- All three connectors support standard features such as SoD and integration with an SSO-enabled target system. These features are discussed in detail later in this chapter.

1.5.1.5 Differences Between the Connectors

[Table 1–2](#) summarizes the differences between the connectors.

Table 1–2 Differences Between the Connectors

Feature	User Management	User Management with HR Foundation	User Management with TCA Foundation
Provisioning function in addition to the basic provisioning function	The connector can establish a link between an FND_USER record and an existing HRMS person record. The person ID of the FND_USER is used to establish and store the link. You specify the person ID during provisioning operations.	<p>The connector can establish a link between an FND_USER record and an HRMS person record.</p> <p>The existence of an HRMS person record is determined through the Employee Number and Business Group ID attributes of the HRMS person record.</p> <p>If an HRMS person record does not exist, then a basic HRMS person record (HR Foundation record) is created and then linked to the FND_USER record. If an HRMS person record exists, then the person record is linked with the FND_USER record. The person ID of the PER_ALL_PEOPLE_F is used to establish the link.</p> <p>You cannot specify the person ID while provisioning or modifying a provisioned resource. This value is displayed in the process form as a display-only field.</p>	<p>The connector can establish a link between an FND_USER record and a TCA party (person-type) record.</p> <p>The party (person type) record is always created when you run a provisioning process. The PARTY_ID column of the HZ_PARTIES is brought back to Oracle Identity Manager by the API and is used to establish the link with the FND_USER record.</p> <p>You cannot specify the party ID while provisioning or modifying a provisioned resource. This value is displayed in the process form as a display-only field.</p>
Additional reconciliation function	None	<p>During reconciliation, if the connector detects a link between an existing HRMS person record and an FND_USER record, then the same link is established in Oracle Identity Manager.</p> <p>After a link is established with an existing HRMS person record or an HR Foundation record (through provisioning or reconciliation), the connector fetches changes to the FND_USER record and the HRMS person/HR Foundation record during reconciliation.</p>	<p>During reconciliation, if the connector detects a link between an existing TCA party record and an FND_USER record, then the same link is established in Oracle Identity Manager.</p> <p>After a link is established with an existing TCA party record or a TCA Foundation record (through provisioning or reconciliation), the connector fetches changes to the FND_USER record and the TCA party/TCA Foundation record during reconciliation.</p>
Other features	The additional provisioning function is always enabled. You cannot enable or disable that feature.	You can enable and disable the additional provisioning and reconciliation functions by using the Manage HR Records parameter of the IT resource.	You can enable and disable the additional provisioning and reconciliation functions by using the Manage TCA Records parameter of the IT resource.

1.5.2 Management of Entitlements

UMX roles and responsibilities are an integral part of the features offered by the target system. These roles and responsibilities are entitlements granted to target system users. An entitlement enables a user to access and use features of the target system to meet the user's job requirements.

Note: A role can be seen as an alias for a particular responsibility or set of responsibilities. The connector provides similar features for working with both roles and responsibilities.

You can use the connector to:

- Synchronize data about entitlements available for assignment to users
See [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#) for more information.
- Reconcile data about entitlements assigned to users
See [Section 3.3.4, "Reconciliation Scheduled Tasks"](#) for more information.

1.5.3 SoD Validation of Entitlement Provisioning

This connector supports the SoD feature. The following are the focal points of this software update:

- The SoD Invocation Library (SIL) is bundled with Oracle Identity Manager release. The SIL acts as a pluggable integration interface with any SoD engine.
- The Oracle E-Business User Management connector is preconfigured to work with Oracle Applications Access Controls Governor as the SoD engine. To enable this, changes have been made in the approval and provisioning workflows of the connector.
- The SoD engine processes role and responsibility entitlement requests that are sent through the connector. Potential conflicts in role and responsibility assignments can be automatically detected.

See Also:

Oracle Identity Manager Tools Reference for Release 9.1.0.2 for detailed information about the SoD feature

[Section 2.3.1, "Configuring SoD"](#) in this guide

1.5.4 Support for an SSO-Enabled Target System Installation

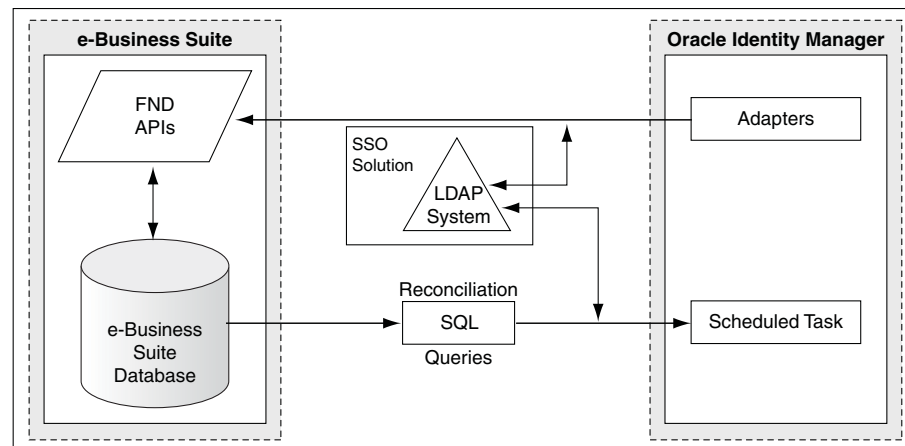
Note: This feature is available in all three connectors.

Oracle E-Business Suite can be configured to use a single sign-on solution, such as Oracle Single Sign-On or Oracle Access Manager, to authenticate users. Oracle Single Sign-On uses Oracle Internet Directory as an LDAP-based repository for storing user records. Oracle Access Manager can use Microsoft Active Directory, Sun Java System Directory, or Novell eDirectory as the LDAP-based repository. You can configure the connector to work with either one of these SSO solutions during reconciliation and provisioning operations.

[Figure 1–2](#) shows the architecture of the connector with the LDAP system. Data flow between the various components shown in this diagram is explained later in this chapter.

Note: In this guide, the generic term **LDAP system** is used to refer to the LDAP system used by the SSO solution in your operating environment.

Figure 1–2 Architecture of the Connector with Configured to Work with an SSO Solution



1.5.5 Reconciliation of Effective-Dated Events

Oracle E-Business Suite allows future-dating (effective-dating) of account disable and account enable operations. For example, an administrator on the target system can specify that user John Doe's account must be disabled on 1-April-2009 by setting the Effective Date To that date for the account. This date is stored in the `END_DATE` column of the target system database table. Similarly, the day an account is revoked can be set in advance. The date for an event of this type is stored in the `END_DATE` column. For a particular future-dated change, when the current date equals the date stored in the `START_DATE` or `END_DATE` column, the appropriate change is made in the person's record on the target system.

The connector can detect and respond to these future-dated lifecycle events.

When you run any of the predefined queries, only records for which changes fall within the `START_DATE` and `END_DATE` range are fetched into Oracle Identity Manager.

Similarly, the connector can also respond to future-dated operations in which roles and responsibilities are granted or revoked.

1.5.6 Account Status Reconciliation and Provisioning

When you enable an account on the target system, the Effective Date From field is set to the current date and the Effective Date To field is set to NULL on the target system.

When you disable an account on the target system, the Effective Date To field is set to the current date on the target system.

The same effect can be achieved through provisioning operations performed on Oracle Identity Manager. In addition, status changes made directly on the target system can be copied into Oracle Identity Manager during reconciliation.

See [Section 3.6, "Provisioning Operations Performed in an SoD-Enabled Environment"](#) for more information.

1.5.7 Configurable Reconciliation Queries

Reconciliation involves running a SQL query on the target system database to fetch the required user account records to Oracle Identity Manager. Predefined SQL queries are stored in a file in the connector deployment package. You can modify these SQL queries or add your own SQL queries for reconciliation.

See [Section 1.6.1, "Reconciliation Queries"](#) for information about the reconciliation queries.

1.5.8 Account Password Management

The connector supports basic password management features. For a particular user, you can specify when the user's password must expire by using the following process form fields:

- Password Expiration Type

You use the Password Expiration Type field to specify the factor (or measure) that you want to use to set a value for password expiration. You can select either `Accesses` or `Days` as the password expiration type.

- Password Expiration Interval

In the Password Expiration Interval field, you specify the number of access or days for which the user must be able to use the password.

For example, if you specify `Accesses` in the Password Expiration Type field and enter 20 in the Password Expiration Interval field, then the user is prompted to change the user's password at the twenty-first login. Similarly, if you specify `Days` in the Password Expiration Type field and enter 100 in the Password Expiration Interval field, then the user is prompted to change the user's password on the hundred and first day after setting a new password.

1.5.9 Support for Full and Incremental Reconciliation

In full reconciliation, all user records are fetched from the target system to Oracle Identity Manager. In incremental reconciliation, user records that are added or modified after the last reconciliation run are fetched into Oracle Identity Manager.

The Last Execution Time and Batch Size scheduled task attributes are used to implement full and incremental reconciliation. If the Last Execution Time attribute is set to 0 and the Batch Size attribute is set to a non-zero value, then full reconciliation is performed. If the Last Execution Time attribute holds a non-zero value, then incremental reconciliation is performed.

See [Section 3.3.4, "Reconciliation Scheduled Tasks"](#) for more information.

1.5.10 Support for Limited (Filtered) Reconciliation

To limit or filter the records that are fetched into Oracle Identity Manager during a reconciliation run, you can add conditions in the WHERE clause of the reconciliation query that you run.

See [Section 3.3.3, "Configuring Limited Reconciliation"](#) for more information.

1.5.11 Support for Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See [Section 3.3.2, "Batched Reconciliation"](#) for more information.

1.5.12 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

The configuration properties of the connection pool are part of the IT resource definition. [Section 2.3.3.6, "Configuring the IT Resource"](#) provides information about setting up the connection pool.

1.6 Reconciliation Process

See Also: The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about target resource reconciliation

The connector is configured to perform target resource reconciliation with the target system. Data from newly created and updated target system records is brought to Oracle Identity Manager and used to create and update Oracle E-Business Suite resources provisioned to OIM Users.

Note: The reconciliation process is the same for all three connectors. There are three scheduled tasks, one for each connector.

The following is an overview of the steps involved in target resource reconciliation:

1. A SQL query is used to fetch target system records during reconciliation. All predefined SQL queries are stored in a properties file. Each query in the file is identified by a name. While configuring the scheduled tasks described in [Section 3.3.4, "Reconciliation Scheduled Tasks"](#), you specify the name of the query that you want to run as the value of the Query Name attribute.
2. The scheduled task is run at the time (frequency) that you specify. This scheduled task contains details of the mode of reconciliation you want to perform.
3. The scheduled task establishes a connection with the target system.
4. The scheduled task reads values that you set for the task attributes, maps the task attributes to parameters of the reconciliation query, formats the query, and then runs the query on the target system database.
5. The SQL query is run on the target system database. Target system records that meet the query criteria are fetched into Oracle Identity Manager. In addition:

- If the target system is SSO-enabled, then the USER_GUID value is first read from the target system record. This USER_GUID value is then used to fetch the SSO User ID value from the LDAP system.

Note: The USER_GUID and SSO User ID values are fetched by a query that is internal to the connector. The reconciliation query is not used for this purpose.

- If you use the User Management with HR Foundation connector, then HRMS Foundation data from HRMS person records is also fetched for all FND_USER users that are linked with HRMS users.
 - If you use the User Management with TCA Foundation connector, then TCA Foundation data from TCA Party records is also fetched for all FND_USER users that are linked with TCA users.
6. Each user record fetched from the target system is compared with existing target system resources assigned to OIM Users. The reconciliation rule is applied during the comparison process.

See Also: [Section 1.6.3, "Reconciliation Rule"](#)

7. The next step of the process depends on the outcome of the matching operation:
- If a match is found between the target system record and a resource provisioned to an OIM User, then the resource is updated with changes made to the target system record.
 - If no match is found, then the target system user record is compared with existing OIM Users. The next step depends on the outcome of the matching operation:
 - If a match is found, then the target system record is used to provision a resource for the OIM User.
 - If no match is found, then the status of the reconciliation event is set to No Match Found.

The rest of this section discusses connector objects used during reconciliation:

- [Section 1.6.1, "Reconciliation Queries"](#)
- [Section 1.6.2, "Target System Columns Used in Reconciliation"](#)
- [Section 1.6.3, "Reconciliation Rule"](#)
- [Section 1.6.4, "Reconciliation Action Rules for Target Resource Reconciliation"](#)

1.6.1 Reconciliation Queries

As mentioned earlier in this chapter, a SQL query is used to fetch target system records during reconciliation. All predefined SQL queries are stored in the ebsUMQuery.properties file.

Note: Depending on your requirements, you can modify existing queries or add your own query in the properties file. Alternatively, you can create and use your own properties file. [Section 4.1, "Guidelines on Extending the Functionality of the Connector"](#) provides more information.

The predefined queries are used in conjunction with the Last Execution Time scheduled task attribute. This attribute stores the time stamp at which the last reconciliation run started. When the next reconciliation run begins, only target system records for which the LAST_UPDATE_DATE column value is greater than the value of the Last Execution Time attribute are fetched into Oracle Identity Manager. In other words, only records that were added or modified after the last reconciliation run started are considered for the current reconciliation run.

Note: If the effective end date of a responsibility granted to a user is changed directly on the target system, then that account will not be reconciled in the next reconciliation run unless some other attribute of the account is also modified.

You can specify a value for the Last Execution Time attribute. See [Section 3.3.1, "Reconciliation Time Stamp"](#) for more information.

The following are predefined queries in the ebsUMQuery.properties file:

- **UM_USER_RECON**
This query is used to fetch users' FND_USER records. It is used in the User Management connector.
- **UM_USER_HRMS_RECON**
This query is used to fetch users' FND_USER records and HRMS person records. It is used in the User Management with HR Foundation connector.
- **UM_USER_TCA_RECON**
This query is used to fetch users' FND_USER records and TCA party records. It is used in the User Management with TCA Foundation connector.
- **UM_USER_RESPONSIBILITIES**
This query is used to fetch data about users' responsibility entitlements.
- **UM_USER_ROLES**
This query is used to fetch data about users' role entitlements.

1.6.2 Target System Columns Used in Reconciliation

Columns in the SELECT clause of each predefined query other than the ones for entitlements are directly mapped to process form fields by lookup definitions in Oracle Identity Manager.

For the User Management connector, [Table 1–3](#) lists the target system columns and the process form fields to which they are mapped for reconciliation. These mappings are stored in the Lookup.EBS.UM.UserRecon lookup definition.

Table 1–3 Attribute Mappings for Reconciliation in the User Management Connector

Process Form Field	Target System Column	Description
Person ID	PERSON_ID	Person ID
User ID	USER_ID	User ID This is a mandatory attribute.
User Name	USER_NAME	User name This is a mandatory attribute.
Description	DESCRIPTION	Description
Email	EMAIL_ADDRESS	E-mail address
Fax	FAX	Fax number
Effective Date From	START_DATE	Date from which the account is active This is a mandatory attribute.
Effective Date To	END_DATE	Date up to which the account is active

For the User Management with HR Foundation connector, [Table 1–4](#) lists the target system columns and the process form fields to which they are mapped for reconciliation. These mappings are stored in the Lookup.EBS.UM.UserHRMSRecon lookup definition.

Table 1–4 Attribute Mappings for Reconciliation in the User Management with HR Foundation Connector

Process Form Field	Target System Column	Description
User ID	USER_ID	User ID This is a mandatory attribute.
User Name	USER_NAME	User name This is a mandatory attribute.
Description	DESCRIPTION	Description
Email	EMAIL_ADDRESS	E-mail address
Fax	FAX	Fax number
Effective Date From	START_DATE	Start date of the account This is a mandatory attribute.
Effective Date To	END_DATE	End date of the account
Note: The remaining attributes listed in this table are HR Foundation record attributes.		
Employee Number	EMPLOYEE_NUMBER	Employee number
First Name	FIRST_NAME	First name
Last Name	LAST_NAME	Last name
Gender	SEX	Gender
Person Type ID	PERSON_TYPE_ID	Person type ID
Business Group ID	BUSINESS_GROUP_ID	Business group ID
Hire Date	ORIGINAL_DATE_OF_HIRE	Hire date
Person ID	PERSON_ID	Person ID

For the User Management with TCA Foundation connector, [Table 1–5](#) lists the target system columns and the process form fields to which they are mapped for reconciliation. These mappings are stored in the Lookup.EBS.UM.UserTCARecon lookup definition.

Table 1–5 Attribute Mappings for Reconciliation in the User Management with TCA Foundation Connector

Process Form Field	Target System Column	Description
User ID	USER_ID	User ID This is a mandatory attribute.
User Name	USER_NAME	User name This is a mandatory attribute.
Description	DESCRIPTION	Description
Email	EMAIL_ADDRESS	E-mail address
Fax	FAX	Fax number
Effective Date From	START_DATE	Start date of the account This is a mandatory attribute.
Effective Date To	END_DATE	End date of the account
Note: The remaining attributes listed in this table are TCA Foundation record attributes.		
First Name	PERSON_FIRST_NAME	First name
Last Name	PERSON_LAST_NAME	Last name
Party ID	PERSON_PARTY_ID	Party ID

For all three connectors, [Table 1–6](#) lists mappings between the target system columns and the process form fields for responsibilities defined on the target system.

Table 1–6 Relationship Between Process Form Fields for Responsibilities and Target System Data Fields

Process Form Field	Target System Column	Description
Application Name	Format of the value: <i>IT_RESOURCE_KEY~APPLICATION_ID</i> Sample value: 1~810	Combination of the IT resource key and the application ID on the target system Note: The IT resource key is a numeric value.
Responsibility Name	Format of the value: <i>IT_RESOURCE_KEY~APPLICATION_ID~RESPONSIBILITY_ID</i> Sample value: 1~810~2751	Combination of the IT resource key, application ID, and responsibility ID on the target system

Table 1–6 (Cont.) Relationship Between Process Form Fields for Responsibilities and Target System Data

Process Form Field	Target System Column	Description
Effective Start Date	START_DATE	Start date of the responsibility assignment
Effective End Date	END_DATE	End date of the responsibility assignment
Security Group	Format of the value: IT_RESOURCE_KEY~SECURITY_GROUP_ID Sample value: 1~1	Combination of the IT resource key and the security group ID on the target system. Note: The IT resource key is a numeric value.

For all three connectors, [Table 1–7](#) lists mappings between the target system columns and the process form fields for roles defined on the target system.

Table 1–7 Relationship Between Process Form Fields for Roles and Target System Data Fields

Process Form Field	Target System Column	Description
Application Name	Format of the value: IT_RESOURCE_KEY~APPLICATION_ID Sample value: 1~260	Combination of the IT resource key and the application ID on the target system Note: The IT resource key is a numeric value.
Role Name	Format of the value: IT_RESOURCE_KEY~APPLICATION_ID~ROLE_ID Sample value: 1~260~UMX UMX_TEST_ROLE	Combination of the IT resource key, application ID, and role ID on the target system
Start Date	start_date	Start date of the role assignment
Expiration Date	expiration_date	End date of the role assignment

1.6.3 Reconciliation Rule

See Also: *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following is the reconciliation rule:

- Rule name for the User Management connector:
EBS UM Target Resource
- Rule name for the User Management with HR Foundation connector:
EBS UM HRMS Target Resource
- Rule name for the User Management with TCA Foundation connector:
EBS UM TCA Target Resource

Rule element for all three connectors: User Login Equals User Name

In this rule:

- User Login is the field on the OIM User form.
- User Name is the target system field.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for the rule name.

1.6.4 Reconciliation Action Rules for Target Resource Reconciliation

[Table 1–8](#) lists the action rules for target resource reconciliation.

Table 1–8 Action Rules for Target Resource Reconciliation

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the resource object. The following are the names of the resource objects for each connector:
 - Resource object for the User Management connector:
eBusiness Suite User
 - Resource object for the User Management with HR Foundation connector:
eBusiness Suite User HR Foundation
 - Resource object for the User Management with TCA Foundation connector:
eBusiness Suite User TCA Foundation
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector.

1.7 Provisioning Process

See Also: The "Provisioning" section in *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning

Provisioning involves management of user accounts and assignment of responsibilities and roles to users in the target system. When you allocate (or provision) an Oracle E-Business Suite resource to an OIM User, the operation results in the creation of an account on Oracle E-Business Suite for that user. Similarly, when you update the resource on Oracle Identity Manager, the same update is made to the account on the target system.

You can enable the Segregation of Duties (SoD) feature in Oracle Identity Manager for validation of role and responsibility provisioning. When SoD is enabled, a role or responsibility is granted to an OIM User's resource (account) only after the request for the role or responsibility clears the SoD validation process. If a conflicting role or responsibility is detected by the SoD engine, then the role or responsibility request is rejected.

Note: the SoD validation process is asynchronous. The response from the SoD engine must be brought to Oracle Identity Manager by a scheduled task.

The provisioning process can be started through one of the following events:

- Direct provisioning
A user uses the Administrative and User Console to create a target system account for another user.
- Request-based provisioning
A user creates a request for a target system account, role, or responsibility, and another user approves this request.
- Provisioning triggered by access policy changes
An access policy related to accounts on the target system is modified. When an access policy is modified, it is reevaluated for all users to which it applies.

The following is an overview of the provisioning process:

1. The provisioning process is started through direct provisioning, request-based provisioning, or an access policy change.
2. If the target system is configured to work with Oracle Single Sign-On, then:

Note: There must be a GUID for the user on the LDAP system before the user can be created on the target system. In other words, the user for whom the provisioning operation is being performed must have a record on the LDAP system.

- a. The connector first establishes a connection with the LDAP system used by Oracle Single Sign-On. To establish a connection, the connector uses information stored in the IT resource for the LDAP system.

- b. From the LDAP system, the connector reads the GUID of the user for whom the provisioning operation is being performed and then adds the GUID to the provisioning data that will be passed on to the target system.
3. The connector establishes a connection with the target system, and passes the provisioning data to the FND APIs of the target system.
4. The target system APIs use the provisioning data to perform the required operation (create or update user). The actual steps performed depend on the connector that you are using:
 - In the User Management connector, the FND_USER record is created or updated. If the person ID is provided on the process form and a record with the same person ID exists on the target system, then that record is linked with the FND_USER record.
 - In the User Management with HR Foundation connector:
 - a. The HRMS person record (containing only HRMS Foundation data) is created or updated.
 - b. The FND_USER record is created or updated.

Note: If the HRMS record is created, then the value in the Person_ID column of the PER_ALL_PEOPLE_F table is copied into the Employee_ID column in the FND_USER table.

- In the User Management with TCA Foundation connector:
 - a. The FND_USER record is created or updated.
 - b. The TCA Party record (containing only TCA Party foundation data) is created or updated.

Note: If the TCA record is created, then the value in the PARTY_ID column of the HZ_PARTIES table is copied into the PERSON_PARTY_ID column in the FND_USER table.

5. The target system APIs return the status of the operation to the connector.
6. The connector translates and displays (or logs) the status message returned by the FND APIs.
7. In an SoD-enabled Oracle Identity Manager system, the connector cannot grant roles or responsibilities directly to the provisioned user account. When a user performs the procedure to provision a role or responsibility, the details of the entitlement request (sent through direct or request-based provisioning) are sent to an SoD engine for conflict analysis. Based on the outcome of the SoD validation process, the entitlement request is either accepted or rejected.

The rest of this section discusses connector objects used during provisioning:

- [Section 1.7.1, "Request-Based Provisioning of Entitlements"](#)
- [Section 1.7.2, "Attribute Mappings for Provisioning"](#)
- [Section 1.7.3, "Provisioning Functions"](#)

1.7.1 Request-Based Provisioning of Entitlements

Note: On Oracle Identity Manager release 9.1.0.x, you can create separate requests for provisioning:

- Target system resources to OIM Users.
- Entitlements to OIM Users who have been provisioned target system resources.

On Oracle Identity Manager releases 11.1.x and 11.1.2.x, you can provision entitlements while provisioning a target system resource to an OIM User. In other words, you need not create a new request for provisioning entitlements.

Therefore, information provided in this section is applicable only if you are using Oracle Identity Manager release 9.1.0.x. If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then skip this section.

Roles and responsibilities defined on the target system are entitlements that can be assigned to a user during the Create User provisioning operation. In addition, an existing user can create requests for responsibilities and roles. If you enable SoD in your Oracle Identity Manager installation, then an entitlement is granted only after the SoD validation clears the request for the entitlement. Users can create entitlement requests for themselves. Alternatively, administrators can submit entitlement requests on behalf of a user.

Note: The connector supports the scenario in which a single request is created for multiple responsibilities and a single approver is assigned the entire request.

Request-based provisioning of responsibilities involves the following steps:

1. A request for a role or responsibility is created.
[Section 3.6, "Provisioning Operations Performed in an SoD-Enabled Environment"](#) describes the procedure to create the request.
2. The request data is written to an object form.
3. When the object form is populated with data, it is sent for approval.
4. After the standard approval process, the SoD Checker process task is triggered. This process task is completed by running the GetSODCheckResultApproval scheduled task from the task scheduler.

Note: The approver should not approve/deny this task manually while approving the request.

After the SoD Checker process task is run and the SoD Check result is passed, the Human Approval task (if it has been defined) is triggered.

5. If the approval process clears the request, then the request data is sent to the process form. When this data reaches the target system, the responsibility is assigned to the user.

Note: If SoD is not enabled or if the provisioning operation does not include entitlement provisioning, then the SODCheckStatus field remains in the SODCheckNotInitiated state.

If the approval process does not clear the request, then the status of the request is set to Denied.

1.7.2 Attribute Mappings for Provisioning

Table 1–9 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations. The third column of this table specifies the connector in which the function is supported.

Note: During a Create User provisioning operation, the EBS Create User adapter is used to populate values in all the target system attributes. Similarly, during an Update User provisioning operation, the EBS Update User performs this function.

Table 1–9 Attribute Mappings for Provisioning

Process Form Attribute	Target System Attribute	Connector	Mandatory?
User Name	User Name	All	Yes
Password	Password	All	Yes
Description	Description	All	
Email	E-Mail	All	
Fax	Fax	All	
Password Expiration Type This is a lookup field.	Password Expiration Type	All	
Password Expiration Interval	Password Expiration Interval	All	
Effective Date From	Effective Dates From	All	Yes
Effective Date To	Effective Dates To	All	
Person ID Note: This field can be edited in the User Management connector. It is a display-only field in the User Management with HR Foundation connector.	Person ID Note: The Full Name corresponding to the person ID in HRMS person record is displayed on the UI with the label <code>Person ID</code> .	User Management and User Management with HR Foundation	
SSO User ID	SSO User ID from the LDAP system Note: This attribute is not displayed on the target system UI.	All	
User ID This is a display-only field.	User ID Note: This attribute is not displayed on the target system UI.	All	

Table 1–9 (Cont.) Attribute Mappings for Provisioning

Process Form Attribute	Target System Attribute	Connector	Mandatory?
SSO GUID This is a display-only field.	GUID fetched from the LDAP system used by Oracle Single Sign-On This value is stored in the USER_GUID column of the FND_USER table. Note: This attribute is not displayed on the target system UI.	All	
Employee Number	Employee Number	User Management with HR Foundation	
First Name	First Name (in the User Management with HR Foundation connector) First Name (in the User Management with TCA Foundation connector)	User Management with HR Foundation and User Management with TCA Foundation	
Last Name	Last Name (in the User Management with HR Foundation connector) Last Name (in the User Management with TCA Foundation connector)	User Management with HR Foundation and User Management with TCA Foundation	
Gender This is a lookup field.	Sex	User Management with HR Foundation	
Person Type ID	Person Types	User Management with HR Foundation	
Business Group ID	Business Group ID Note: This attribute is not displayed on the target system UI.	User Management with HR Foundation	
Party ID This is a display-only field.	Party ID Note: The full name corresponding to the party ID in the TCA Party record is displayed on the target system UI with the label <i>Customer</i> .	User Management with TCA Foundation	
Hire Date	Latest Start Date	User Management with HR Foundation	
Responsibility Child Form Fields (for all three connectors)			
Application Name	IT_RESOURCE_KEY~APPLICATION_ID	All	
Responsibility Name	IT_RESOURCE_KEY~APPLICATION_ID~RESPONSIBILITY_ID	All	Yes
Effective Start Date	Effective Dates From	All	
Effective End Date	Effective Dates To	All	

Table 1–9 (Cont.) Attribute Mappings for Provisioning

Process Form Attribute	Target System Attribute	Connector	Mandatory?
Security Group	IT_RESOURCE_KEY~SECURITY_ GROUP_ID All	All	
Roles Child Form Fields (for all three connectors)			
Application Name	IT_RESOURCE_KEY~APPLICATI ON_ID	All	
Role Name	IT_RESOURCE_KEY~APPLICATI ON_ID~ROLE_ID	All	Yes
Start Date	Start Date	All	
Expiration Date	Expiration Date	All	

1.7.3 Provisioning Functions

Table 1–10 lists provisioning functions and the corresponding adapters.

Note: An Update provisioning operation on child data is not supported.

Table 1–10 Provisioning Functions

Provisioning Function	Adapter	Stored Procedure in Wrapper Package
Create user	EBS Create User	OIM_FND_USER_PKG.CreateUser
Create SSO-enabled user	EBS Create User	OIM_FND_USER_PKG.CreateUser
Disable user	EBS Disable User	OIM_FND_USER_PKG.DisableUser
Update Email	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update Fax	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update Password	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update Description	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update Effective Date From	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update Effective Date To	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update SSO User ID	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update Password Expiration Type	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update Password Expiration Interval	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Update Person ID	EBS Update User	OIM_FND_USER_PKG.UpdateUser
Note: This is applicable only in the User Management connector.		
Enable User	EBS Enable User	OIM_FND_USER_PKG.EnableUser
Add Responsibility	EBS Add Responsibility	OIM_FND_USER_PKG.AddResp
Remove Responsibility	EBS Revoke Responsibility	OIM_FND_USER_PKG.DelResp
Add Role	EBS Add Role	WF_LOCAL_SYNCH_PKG.PropagateUserRole
Remove Role	EBS Revoke Role	WF_LOCAL_SYNCH_PKG.PropagateUserRole

Table 1–10 (Cont.) Provisioning Functions

Provisioning Function	Adapter	Stored Procedure in Wrapper Package
Update User Name	EBS Update Username	OIM_FND_USER_PKG.change_user_name
Functions Specific to the User Management with HR Foundation Connector		
Create Employee	EBS Create User HRMS	OIM_EMPLOYEE_WRAPPER.create_emp_api
Delete User	EBS Revoke Employee	OIM_EMPLOYEE_WRAPPER.terminate_emp_api
Delete User	EBS Revoke Employee	OIM_EMPLOYEE_WRAPPER.delete_emp_api
<p>Note: It is recommended not to perform a delete employee operation on the target system.</p> <p>However, delete employee operation is configurable by setting the value of DELETE_EMP_RECORD to "Yes" in the Lookup.EBS.UMHRMS.Configuration lookup definition.</p> <p>The default value of DELETE_EMP_RECORD is set to "No" and hence needs to be changed to "Yes".</p>		
Update First Name	EBS Update Employee	OIM_EMPLOYEE_WRAPPER.update_person_api
Update Last Name	EBS Update Employee	OIM_EMPLOYEE_WRAPPER.update_person_api
Update Gender	EBS Update Employee	OIM_EMPLOYEE_WRAPPER.update_person_api
Update Person Type ID	EBS Update Employee	OIM_EMPLOYEE_WRAPPER.update_person_api
Update Business Group ID	EBS Update Employee	OIM_EMPLOYEE_WRAPPER.update_person_api
Update Hire Date	EBS Update Employee	OIM_EMPLOYEE_WRAPPER.update_person_api
Functions Specific to the User Management with TCA Foundation Connector		
Create Party of Person Type	EBS Create User TCA	OIM_TCA_WRAPPER.create_person_party_api
Delete User	EBS Revoke Party	OIM_TCA_WRAPPER.disable_person_party_api

Table 1–10 (Cont.) Provisioning Functions

Provisioning Function	Adapter	Stored Procedure in Wrapper Package
Delete User Note: It is recommended not to perform a delete employee operation on the target system. However, delete employee operation is configurable by setting the value of DELETE_EMP_RECORD to "Yes" in the Lookup.EBS.UMHRMS.Configuration lookup definition. The default value of DELETE_EMP_RECORD is set to "No" and hence needs to be changed to "Yes".	EBS Revoke Party	OIM_TCA_WRAPPER.delete_person_party_api
Update First Name	EBS Update Party	OIM_TCA_WRAPPER.update_person_party_api
Update Last Name	EBS Update Party	OIM_TCA_WRAPPER.update_person_party_api

1.8 Lookup Definitions Used During Connector Operations

When you deploy the connector, lookup definitions of the following types are created in Oracle Identity Manager:

- Lookup definitions corresponding to lookup fields on the target system
- Lookup definitions that store configuration information

The following sections discuss lookup definitions used by the connector:

- [Section 1.8.1, "Lookup Definitions That Are Common to All Three Connectors"](#)
- [Section 1.8.2, "Lookup Definitions That Are Specific to the User Management Connector"](#)
- [Section 1.8.3, "Lookup Definitions That Are Specific to the User Management with HR Foundation Connector"](#)
- [Section 1.8.4, "Lookup Definitions That Are Specific to the User Management with TCA Foundation Connector"](#)

1.8.1 Lookup Definitions That Are Common to All Three Connectors

[Table 1–11](#) describes lookup definitions that are common to all three connectors.

Table 1–11 Lookup Definitions Common to All Three Connectors

Lookup Definition	Code Key	Decode	Input Source
Lookup.EBS.Applicat ion	<p>Combination of the following elements:</p> <ul style="list-style-type: none"> ■ A number assigned to the IT resource for the target system installation from which values are synchronized ■ Application ID on the target system <p>Sample value: 1~694</p> <p>In this example, 1 is the number assigned to the IT resource for the target system installation and 694 is the application ID assigned to the application in the target system.</p>	<p>Short name for the application in the target system</p> <p>Sample value: PRP</p>	<p>You configure and run the eBusiness UM Lookup Definition Reconciliation scheduled task to populate this lookup definition with values from the target system.</p>
Lookup.EBS.Security Group	<p>Combination of the following elements:</p> <ul style="list-style-type: none"> ■ A number assigned to the IT resource for the target system installation from which values are synchronized ■ Security Group Name on the target system <p>Sample value: 1~1</p> <p>In this example, 1 is the number assigned to the IT resource for the target system installation and 1 is the application ID assigned to the application in the target system.</p>	<p>Short name for the Security Group Name in the target system</p> <p>Sample value: GOVERNMENT</p>	<p>You configure and run the eBusiness UM Lookup Definition Reconciliation scheduled task to populate this lookup definition with values from the target system.</p>

Table 1–11 (Cont.) Lookup Definitions Common to All Three Connectors

Lookup Definition	Code Key	Decode	Input Source
Lookup.EBS.Responsibility	<p>Combination of the following elements:</p> <ul style="list-style-type: none"> Number assigned to the IT resource for the target system installation from which values are synchronized Application ID on the target system Responsibility ID on the target system <p>Sample value: 1~694~20903</p> <p>In this sample value, 1 is the number assigned to the IT resource for the target system installation, 694 is the application ID, and 20903 is the responsibility ID.</p>	<p>Responsibility name of the corresponding application in the target system</p> <p>Sample Value: MRC Purchasing Manager</p>	You configure and run the eBusiness UM Lookup Definition Reconciliation scheduled task to populate this lookup definition with values from the target system.
Lookup.EBS.UMX.Roles	<p>Combination of three elements:</p> <ul style="list-style-type: none"> A number assigned to the IT resource for the target system installation from which values are synchronized Application ID on the target system Role name on the target system <p>Sample value: 1~694~UMX UMX_EXT_ADMN</p> <p>In this example, 1 is the number assigned to the IT resource for the target system installation, FND-UMX is the short name for the application, and UMX_EXT_ADMN is the role name.</p>	<p>Display name of the role on the target system</p> <p>Sample Value: Customer Administrator</p>	You configure and run the eBusiness UM Lookup Definition Reconciliation scheduled task to populate this lookup definition with values from the target system.
Lookup.EBS.PasswordExpirationType	<p>Unit of measurement for specifying the password expiration type</p> <p>The value can be one of the following:</p> <p>Accesses</p> <p>Days</p> <p>None</p>	<p>Unit of measurement for specifying the password expiration type</p> <p>The value can be one of the following:</p> <p>Accesses</p> <p>Days</p> <p>None</p>	This lookup definition is preconfigured. You must not modify this lookup definition.

1.8.2 Lookup Definitions That Are Specific to the User Management Connector

Table 1–12 describes lookup definitions that are specific to the User Management connector.

Table 1–12 Lookup Definitions Specific to the User Management Connector

Lookup Definition	Code Key	Decode	Input Source
Lookup.EBS.UM.UserProvisioning	Process form field name Sample value: UD_EBS_USER_USRNAME	Corresponding argument of the stored procedure used for user provisioning Sample Value: x_user_name,1,vvarchar2,IN	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for provisioning. Chapter 4, "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.UM.UserRecon	Reconciliation field of resource object Sample value: User Name	Corresponding column names or column alias names used in reconciliation query Sample value: USER_NAME	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for reconciliation. Chapter 4, "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.Responsibility.Mapping Note: This lookup definition is used for entitlement provisioning.	Name of the process form column for the responsibility attributes in the eBusiness Suite User Responsibility resource object	Name of the process form column for the responsibility attribute in the eBusiness Suite User resource object	This lookup definition is preconfigured. You must not modify this lookup definition.
Lookup.EBS.Role.Mapping	Name of the process form column for the role attributes in eBusiness Suite User Role resource object	Name of the process form column for the role attribute in the eBusiness Suite User resource object	This lookup definition is preconfigured. You must not modify this lookup definition.
Lookup.EBS.UM.Query Filters	Filter parameters that you want to append to the reconciliation SQL query	See Section 3.3.3, "Configuring Limited Reconciliation" for detailed information about the Decode value.	See Section 3.3.3, "Configuring Limited Reconciliation" for detailed information about this lookup definition.
Lookup.EBS.UM.Configuration	Configurable data items used by the connector during both reconciliation and provisioning	Values of the configurable parameters	You can modify some of entries in this lookup definition. See Section 3.1, "Setting Up Lookup Definitions in Oracle Identity Manager" for more information.

1.8.3 Lookup Definitions That Are Specific to the User Management with HR Foundation Connector

[Table 1–13](#) describes lookup definitions that are specific to the User Management with HR Foundation connector.

Table 1–13 Lookup Definitions Specific to the User Management with HR Foundation Connector

Lookup Definition	Code Key	Decode	Input Source
Lookup.EBS.Gender	Code for gender Sample value: M	Display name of gender Sample value: Male	This lookup definition is preconfigured. You must not modify this lookup definition.
Lookup.EBS.UM.UserHRMSProvisioning	Process form field name Sample value: UD_EBSH_USR_USRNAME	Information about the corresponding argument in the stored procedure used for user provisioning Sample Value: x_user_name,1,vvarchar2, IN	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for provisioning. Chapter 4, "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.UM.UserHRMSRecon	Reconciliation fields of resource object Sample value: Employee Number	Column names or column name alias used in the reconciliation query Sample value: EMPLOYEE_NUMBER	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for reconciliation. Chapter 4, "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.UM.CreateEmployee	Process form field name Sample value: UD_EBSH_USR_EMPNUM	Information about the corresponding argument in the stored procedure used for HRMS person record provisioning Sample Value: p_employee_number,7,vvarchar2, IN OUT	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for provisioning. Chapter 4, "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.UM.UpdateEmployee	Process form field name Sample value: UD_EBSH_USR_EMPNUM	Information about the corresponding argument in the stored procedure used for HRMS person record provisioning Sample Value: p_employee_number,8,vvarchar2, IN OUT	You must not modify or remove existing attributes in this lookup definition. However, you can add or remove new attributes for provisioning.
Lookup.EBS.HRMSResponsibility.Mapping	Name of the process form column for the responsibility attributes in the eBusiness Suite User HR Foundation Responsibility resource object Note: This lookup definition is used for request-based responsibility provisioning.	Name of the process form column for the responsibility attribute in the eBusiness Suite User HR Foundation resource object	You must not modify this lookup definition.
Lookup.EBS.HRMSRoles.Mapping	Name of the process form column for the role attributes in the eBusiness Suite User HR Foundation Role resource object Note: This lookup definition is used for request-based provisioning.	Name of the process form column for the role attribute in the eBusiness Suite User HR Foundation resource object	You must not modify this lookup definition.

Table 1–13 (Cont.) Lookup Definitions Specific to the User Management with HR Foundation Connector

Lookup Definition	Code Key	Decode	Input Source
Lookup.EBS.UMHRMS. QueryFilters	Filter parameters that you want to append to the reconciliation SQL query	See Section 3.3.3, "Configuring Limited Reconciliation" for detailed information about the Decode value.	See Section 3.3.3, "Configuring Limited Reconciliation" for detailed information about this lookup definition.
Lookup.EBS.UMHRMS. EmployeeInfoMapping	Name of the process form column for information about the HR Foundation person record	Name of the column used for fetching the person record data from the target system database	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for provisioning. Chapter 4, "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.UMHRMS. Configuration	Configurable data items used by the connector during both reconciliation and provisioning	Values of the configurable parameters	You can modify some of entries in this lookup definition. See Section 3.1, "Setting Up Lookup Definitions in Oracle Identity Manager" for more information.

1.8.4 Lookup Definitions That Are Specific to the User Management with TCA Foundation Connector

[Table 1–14](#) describes lookup definitions that are specific to the User Management with TCA Foundation connector.

Table 1–14 Lookup Definitions Synchronized with the Target System

Lookup Definition	Code Key	Decode	Input Source
Lookup.EBS.UM.UserT CAProvisioning	Process form field name Sample value: UD_EBST_USR_USRNAME	Information about the corresponding argument in the stored procedure used for user provisioning Sample Value: x_user_name,1,varchar2 , IN	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for provisioning. Chapter 4 , "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.UM.PartyP rovisioning	Process form field name Sample value: UD_EBST_USR_FNAME	Information about the corresponding argument in the stored procedure used for HRMS Person provisioning Sample Value: p1_a1,9,varchar2, IN	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for provisioning. Chapter 4 , "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.UM.Updat eParty	Process form field name Sample value: UD_EBST_USR_FNAME	Information about the corresponding argument in the stored procedure used for HRMS Person provisioning Sample Value: p1_a1,9,varchar2, IN	You must not modify or remove existing attributes in this lookup definition. However, you can add or remove new attributes for provisioning.
Lookup.EBS.UM.UserT CARecon	Reconciliation field of resource object Sample value: First Name	Column name or column alias name used in reconciliation query Sample value: FIRST_NAME	This lookup definition is preconfigured. You modify this lookup definition only if you are adding or removing attributes for reconciliation. Chapter 4 , "Extending the Functionality of the Connector" discusses the procedure.
Lookup.EBS.UserTCAR esponsibility.Mapping Note: This lookup definition is used for entitlement provisioning.	Name of the process form column for the responsibility attributes in the eBusiness Suite User TCA Foundation Responsibility	Name of the process form column for the responsibility attribute in the eBusiness Suite User TCA Foundation resource object	You must not modify this lookup definition.

Table 1–14 (Cont.) Lookup Definitions Synchronized with the Target System

Lookup Definition	Code Key	Decode	Input Source
Lookup.EBS.TCARoles.Mapping	Name of the process form column for the role attributes in the eBusiness Suite User TCA Foundation Role resource object	Name of the process form column for the role attribute in the eBusiness Suite User TCA Foundation resource object	You must not modify this lookup definition.
Lookup.EBS.UMTCA.QueryFilters	Name of the process form column for information about the TCA Foundation person record	Name of the column used for fetching the person record data from the target system database	See Section 3.3.3, "Configuring Limited Reconciliation" for detailed information about this lookup definition
Lookup.EBS.UMTCA.Configuration	Configurable data items used by the connector during both reconciliation and provisioning	Values of the configurable parameters	You can modify some of entries in this lookup definition. See Section 3.1, "Setting Up Lookup Definitions in Oracle Identity Manager" for more information.

1.9 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- [Chapter 2, "Deploying the Connector"](#) describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- [Chapter 3, "Using the Connector"](#) describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- [Chapter 4, "Extending the Functionality of the Connector"](#) describes procedures that you can perform if you want to extend the functionality of the connector.
- [Chapter 5, "Testing and Troubleshooting"](#) describes the procedure to use the connector testing utility and the Diagnostic Dashboard for testing the connector.
- [Chapter 6, "Known Issues"](#) lists known issues associated with this release of the connector.

Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- [Section 2.1, "Preinstallation"](#)
- [Section 2.2, "Installation"](#)
- [Section 2.3, "Postinstallation"](#)
- [Section 2.4, "Postcloning Steps"](#)

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- [Section 2.1.1, "Preinstallation on Oracle Identity Manager"](#)
- [Section 2.1.2, "Preinstallation on the Target System"](#)

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- [Section 2.1.1.1, "Files and Directories on the Installation Media"](#)
- [Section 2.1.1.2, "Determining the Release Number of the Connector"](#)
- [Section 2.1.1.3, "Creating a Backup of the Existing Common.jar File"](#)

2.1.1.1 Files and Directories on the Installation Media

[Table 2–1](#) lists the files and directories on the installation media.

Table 2–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
config/ebsUMQuery.properties	This file contains SQL queries that are used for target resource reconciliation.
config/ebsUMLookupQuery.properties	This file contains SQL queries that are used for lookup field synchronization.
Files in the configuration directory	This directory contains the configuration files that are used by the Connector Installer during installation of each connector.
Oracle_EBS_User-Management-CI.xml	
Oracle_EBS_User-HRMS-Management-CI.xml	
Oracle_EBS_User-TCA-Management-CI.xml	

Table 2–1 (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
lib/EBSUM.jar	<p>This JAR file contains the class files that are used during reconciliation and provisioning operations. During connector installation, this file is copied to the following location:</p> <ul style="list-style-type: none"> For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/JavaTasks</i> For Oracle Identity Manager releases 11.1.x and 11.1.2.x or later: <i>Oracle Identity Manager database</i>
lib/EBSCCommon.jar	<p>This JAR file contains utility classes that support provisioning and reconciliation operations. During connector installation, this file is copied to the following location:</p> <ul style="list-style-type: none"> For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/JavaTasks</i> For Oracle Identity Manager releases 11.1.x and 1.1.2.x or later: <i>Oracle Identity Manager database</i>
lib/Common.jar	<p>This JAR file contains classes that are used by all release 9.1.0 connectors. During connector installation, this file is copied to the following location:</p> <ul style="list-style-type: none"> For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/JavaTasks</i> For Oracle Identity Manager releases 11.1.x and 1.1.2.x or later: <i>Oracle Identity Manager database</i>
Files in the resources directory	<p>Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied to the following location:</p> <ul style="list-style-type: none"> For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/connectorResources</i> For Oracle Identity Manager releases 11.1.x and 1.1.2.x or later: <i>Oracle Identity Manager database</i> <p>Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.</p>
scripts/script1/OIM.bat scripts/script1/OIM.sh	<p>This file contains commands to run the SQL scripts for creating a target system user and granting the required rights to the user.</p> <p>See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information about this user.</p>
scripts/script1/OIM_FND_GLOBAL.pck	This is the customized apps.fnd_global package.
scripts/script1/OIM_FND_USER_PKG.pck	This is the customized apps.fnd_user package.
scripts/script1/OIM_EMPLOYEE_WRAPPER.pck	This is a customized wrapper package for creating and updating employee records.
scripts/script1/OIM_TCA_WRAPPER.pck	This is a customized wrapper package for creating and updating party records.

Table 2–1 (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
scripts/script1/OimUser.sql	These file contains the SQL scripts to create a target system user account in a new tablespace, grant the required rights to the user, and create synonyms of various database objects to be used by the connector.
scripts/script1/OimUserGrants.sql	
scripts/script1/OimUserSynonyms.sql	
script/script1/OimUserAppstablesSynonyms.sql	See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for more information about this user.
scripts/script1/WL_LOCAL_SYNCH_PKG	This is the customized version of the apps.wf_local_synch package. It is used for role management.
scripts/script1/EXECUTE ON APPS.UMX_ACCESS_ROLES_PVT	This is a customized wrapper package for updating user roles.
scripts/script1/EXECUTE ON APPS.FND_USER_RESP_GROUPS_API	This is a customized wrapper package for updating user responsibilities.
scripts/script2/ . . .	This directory contains copies of the files in the scripts/script1 directory. You use the contents of either the script1 or script2 directory depending on the target system release that you are using. Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" provides more details.
test/config/config_um_prov.properties	This properties file contains data that is used by the testing utility. See Section 5.1, "Running Test Cases" for more information.
test/config/config_um_prov_fileOption.properties	This properties file contains data that is used by the testing utility. See Section 5.1, "Running Test Cases" for more information.
test/config/log.properties	This file contains properties that you use to enable log4j logging.
test/scripts/OracleEbiz.bat	This file is used to run the testing utility.
test/scripts/OracleEbiz.sh	
xml/Oracle-eBusinessSuite-Main-ConnectorConfig.xml	This XML file contains configuration information about the User Management connector. The Connector Installer uses this XML file to create connector components that are used for both direct and request-based user account creation.
xml/Oracle-eBusinessSuite-HRMS-Main-ConnectorConfig.xml	This XML file contains configuration information about the User Management with HR Foundation connector. The Connector Installer uses this XML file to create connector components that are used for both direct and request-based creation of user records and person records.
xml/Oracle-eBusinessSuite-TCA-Main-ConnectorConfig.xml	This XML file contains configuration information about the User Management with TCA Foundation connector. The Connector Installer uses this XML file to create connector components that are used for both request-based creation of user records and TCA party records.
xml/Oracle-eBusinessSuite-HRMS-RequestApproval-ConnectorConfig.xml	This XML file is used for request-based entitlement provisioning in the User Management with HR Foundation connector.
xml/Oracle-eBusinessSuite-RequestApproval-ConnectorConfig.xml	This XML file is used for request-based entitlement provisioning in the User Management connector.
xml/Oracle-eBusinessSuite-TCA-RequestApproval-ConnectorConfig.xml	This XML file is used for request-based entitlement provisioning in the User Management with TCA Foundation connector.
documentation/javadocs	This directory contains information about the Java APIs used by the connector.

2.1.1.2 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the connector JAR file that is in the *OIM_HOME/xellerate/JavaTasks* directory.

For 11.1.x and 11.1.2.x server, download Connector JAR file from OIM database using DownloadJars utility.

2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the connector JAR file.

In the Manifest.mf file, the release number of the connector is displayed as the value of the Version property.

2.1.1.3 Creating a Backup of the Existing Common.jar File

The Common.jar file is in the deployment package of each 9.1.x release of the connector. With each new release, code corresponding to that particular release is added to the existing code in this file. For example, the Common.jar file shipped with Connector Y on 12-July contains:

- Code specific to Connector Y
- Code included in the Common.jar files shipped with all other 9.1.x release of the connectors that were released before 12-July

If you have installed a release 9.1.x connector that was released after the current release of the Oracle E-Business User Management connector, back up the existing Common.jar file, install the Oracle E-Business User Management connector, and then restore the Common.jar file. The steps to perform this procedure are as follows:

Caution: If you do not perform this procedure, then your release 9.1.x connectors might not work.

1. Determine the release date of your existing release 9.1.x connector as follows:
 - a. Extract the contents of the following file in a temporary directory:
OIM_HOME/xellerate/JavaTasks/Common.jar

Note: On Oracle Identity Manager releases 11.1.x and 11.1.2.x or later, use the Oracle Identity Manager Download JARs utility to download the Common.jar file from the database, and then extract the contents of this file into a temporary directory.

See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager 11g Release 1 (11.1.1)* for instructions about using the Download JARs utility.

- b. Open the Manifest.mf file in a text editor.
 - c. Note down the Build Date and Build Version values.
2. Determine the Build Date and Build Version values of the current release of the Oracle E-Business User Management connector as follows:

- a. On the installation media for the connector, extract the contents of the lib/Common.jar and then open the Manifest.mf file in a text editor.
 - b. Note down the Build Date and Build Version values.
3. If the Build Date and Build Version values for the Oracle E-Business User Management connector are less than the Build Date and Build Version values for the connector that is installed, then:
 - If you are using Oracle Identity Manager release 9.1.0.x, then:
 - a. Copy the `OIM_HOME/xellerate/JavaTasks/Common.jar` to a temporary location.
 - b. After you perform the procedure described in [Section 2.2, "Installation"](#) overwrite the new Common.jar file in the `OIM_HOME/xellerate/JavaTasks` directory with the Common.jar file that you backed up in the preceding step.
 - If you are using Oracle Identity Manager release 11.1.x, then run the Oracle Identity Manager Upload JARs utility to post the Common.jar file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

Note: Before you run this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

For Microsoft Windows:

`OIM_HOME/server/bin/UploadJars.bat`

For UNIX:

`OIM_HOME/server/bin/UploadJars.sh`

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the procedure described in the following sections:

- [Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"](#)
- [Section 2.1.2.2, "Compiling Custom Wrapper Packages"](#)
- [Section 2.1.2.3, "Setting the Employee Number Creation Mode"](#)

2.1.2.1 Creating a Target System User Account for Connector Operations

Note: You must have DBA privileges to grant the required permissions to the target system user account.

You must have Oracle Database Client installed on the computer on which you perform the procedure described in this section. The Oracle Database Client release must be the same as the database release. In addition, if Oracle Database Client is not installed on the database host computer, then the tnsnames.ora file on the Oracle Database Client host must contain an entry for the SID of the database.

Oracle Identity Manager requires a target system user account to access the target system during connector operations. You provide the credentials of this user account while performing the procedure described in [Section 2.3.3.6, "Configuring the IT Resource."](#)

To create a target system user account for connector operations:

1. From the installation media, copy one of the following directories to a temporary directory on either the target system host computer or a computer on which the Oracle Database Client has been installed:

See Also: [Section 2.1.1.1, "Files and Directories on the Installation Media"](#) for information about the contents of the scripts directory

- scripts/script1

The scripts in this directory create wrapper packages in the APPS schema. These wrapper packages are used for connector provisioning operations.

- scripts/script2

The scripts in this directory create wrapper packages in the schema of the user that you are creating. These wrapper packages are used for connector provisioning operations.

To determine whether to copy the scripts in the script1 or the script2 directory:

- a. If you are using the User Management connector, then run the following queries:

```
SELECT text FROM user_source WHERE name = 'FND_USER_PKG' AND type =
'PACKAGE' AND UPPER(text) LIKE '%AUTHID%';
SELECT text FROM user_source WHERE name = 'FND_GLOBAL' AND type = 'PACKAGE'
AND UPPER(text) LIKE '%AUTHID%';
SELECT text FROM user_source WHERE name = 'WF_LOCAL_SYNCH' AND type =
'PACKAGE' AND UPPER(text) LIKE '%AUTHID%';
SELECT text FROM user_source WHERE name = 'UMX_ACCESS_ROLES_PVT' AND type =
'PACKAGE' AND UPPER(text) LIKE '%AUTHID%';
SELECT text FROM user_source WHERE name = 'FND_USER_RESP_GROUPS_API' AND
type = 'PACKAGE' AND UPPER(text) LIKE '%AUTHID%';
```

- b. If you are using the User Management with HR Foundation connector, then run the following queries:

```
SELECT text FROM user_source WHERE name = 'OIM_EMPLOYEE_WRAPPER' AND type =
'PACKAGE' AND UPPER(text) LIKE '%AUTHID%';
```

- c. If you are using the User Management with TCA Foundation connector, then run the following queries:

```
SELECT text FROM user_source WHERE name = 'OIM_TCA_WRAPPER' AND type =
'PACKAGE' AND UPPER(text) LIKE '%AUTHID%';
```

- d. If any of the queries that you run returns a row containing the text AUTHID CURRENT_USER, then use the script1 directory. Otherwise, use either the script1 or the script2 directory.
2. On the computer where you copy the scripts directory, verify that there is a TNS entry in the tnsnames.ora file for the target system database.
 3. Depending on the host platform, run either the OIM.sh or OIM.bat file.
 4. When you run the script, you are prompted for the following information:
 - ORACLE_HOME path
This prompt is displayed only if the ORACLE_HOME environment variable has not been set on the computer on which you are running the script.
 - Enter the system user name
Enter the login (user name) of a DBA account with the privileges to create and configure a new target system user.
 - Enter the name of the database
Enter the connection string or service name given in the tnsnames.ora file to connect to the target system database.
 - Enter the name of the tablespace to be created
Enter a name for the tablespace to be created for the user.
 - Enter the name of the datafile to be created
Enter a name for the datafile to be created for the user.
 - Enter the path for the datafile to be created
Enter the path where the datafile must be created. The path is relative to the repository of the directory in which the target system is installed. If you do not enter a value at this prompt, then the default directory is created.
 - Enter New database Username to be created
Enter a user name for the target system account that you want to create.
 - Enter the New user password
Enter a password for the target system account that you want to create.
 - Connecting with newly created database user
Enter the connection string or service name that you provided earlier.

At the end of the operation, a log file (OIM_APPS_USER.log) is created in the scripts directory. If the user is successfully created, then a message to this effect is recorded in the log file.

During the account creation process, the following privileges are granted:

- [Privileges Granted to the Account for All 3 Connectors](#)
- [Additional Privileges Granted to the Account for the User Management with HR Foundation Connector](#)

- [Additional Privileges Granted to the Account for the User Management with TCA Foundation Connector](#)

Privileges Granted to the Account for All 3 Connectors

The following privileges are granted to the new database user account for all 3 connectors:

```
EXECUTE ON APPS.WF_LOCAL_SYNCH
EXECUTE ON APPS.FND_USER_PKG
EXECUTE ON APPS.FND_API
EXECUTE ON APPS.FND_GLOBAL
EXECUTE ON APPS.UMX_ACCESS_ROLES_PVT
EXECUTE ON APPS.FND_USER_RESP_GROUPS_API
SELECT ON APPS.FND_APPLICATION
SELECT ON APPS.FND_RESPONSIBILITY
SELECT ON APPS.FND_RESPONSIBILITY_TL
SELECT ON APPS.FND_RESPONSIBILITY_VL
SELECT ON APPS.FND_USER_RESP_GROUPS_DIRECT
SELECT ON APPS.PER_ALL_PEOPLE_F
SELECT ON APPS.FND_APPLICATION_TL
SELECT ON APPS.WF_LOCAL_USER_ROLES
SELECT ON APPS.WF_USER_ROLES
SELECT ON APPS.WF_LOCAL_ROLES
SELECT, UPDATE ON APPS.FND_USER
SELECT ON APPS.FND_SECURITY_GROUPS
SELECT ON APPS.FND_SECURITY_GROUPS_TL
EXECUTE ON APPS.OIM_FND_USER_PKG
EXECUTE ON APPS.OIM_FND_GLOBAL
EXECUTE ON APPS.WF_LOCAL_SYNCH_PKG
EXECUTE ON APPS.OIM_UMX_ACCESS_ROLES_PVT
EXECUTE ON APPS.OIM_FND_USER_RESP_GROUPS_API
```

Additional Privileges Granted to the Account for the User Management with HR Foundation Connector

In addition to the privileges listed in the "[Privileges Granted to the Account for All 3 Connectors](#)" section, the following privileges are granted to the account for the User Management with HR Foundation connector:

```
EXECUTE ON APPS.HR_EMPLOYEE_API
EXECUTE ON APPS.HR_PERSON_API
SELECT ON APPS.PER_ALL_ASSIGNMENTS_F
SELECT ON APPS.PER_PEOPLE_F
```

```
SELECT ON APPS.PER_PERSON_TYPES
SELECT ON APPS.PER_PERIODS_OF_SERVICE
```

Additional Privileges Granted to the Account for the User Management with TCA Foundation Connector

In addition to the privileges listed in the ["Privileges Granted to the Account for All 3 Connectors"](#) section, the following privileges are granted to the account for the User Management with TCA Foundation connector:

```
EXECUTE ON APPS.FND_OID_USERS
EXECUTE ON APPS.FND_OID_UTIL
SELECT, UPDATE ON APPS.HZ_PARTIES
SELECT, UPDATE ON APPS.HZ_PERSON_PROFILES
REVOKE SELECT ON APPS.PER_ALL_PEOPLE_F
```

2.1.2.2 Compiling Custom Wrapper Packages

The following custom wrapper packages are used during the Person Create and Update operations:

- OIM_EMPLOYEE_WRAPPER
- OIM_TCA_WRAPPER

OIM_UMX_ACCESS_ROLES_PVT.pck wrapper package is used during the Revoke Role operation.

If you plan to use the APPS account for reconciliation, provisioning, and revoke role operations, then:

Note: Do *not* perform these steps if you plan to use the account described in [Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"](#).

1. Copy the packages from the scripts directory on the installation media into a directory on the target system host computer.
2. Log in to the database as the APPS user.
3. Run the following commands at the SQL prompt:

Note: See [Section 2.1.1.1, "Files and Directories on the Installation Media"](#) for information about the location of the packages containing these SQL scripts.

```
@<DIRECTORY_PATH_WHERE_THE_PACKAGES_ARE_SAVED>/OIM_EMPLOYEE_WRAPPER.pck
@<DIRECTORY_PATH_WHERE_THE_PACKAGES_ARE_SAVED>/OIM_TCA_WRAPPER.pck
@<DIRECTORY_PATH_WHERE_THE_PACKAGES_ARE_SAVED>/OIM_UMX_ACCESS_ROLES_PVT.pck
```

2.1.2.3 Setting the Employee Number Creation Mode

Note: Perform the procedure described in this section only if you plan to use the User Management with HR Foundation connector.

If you plan to use the User Management with HR Foundation connector, then the target system must be configured to manual mode for generating employee numbers. By default, employee numbers are automatically generated. To set the employee number generation mode to manual:

1. Log in to the target system.
2. Select the Oracle E-Business HRMS responsibility. For example: Human Resource Vision Enterprise.
3. Navigate to **Workstructures > Organization > Description**.
4. Search for and select the business group,
5. Click **Others**.
6. Select **Business Group Info** from the list of values.
7. Open the flexfield to view the setting for employee number generation
8. Set the value of Employee Number Generation to **Manual**.
9. Click **OK**.

2.2 Installation

Installing the connector on Oracle Identity Manager release 9.1.0 or later involves the following procedures:

Note: You can perform these procedures to install each connector, in any order.

- [Section 2.2.1, "Running the Connector Installer"](#)
- [Section 2.2.2, "Copying Files to the Oracle Identity Manager Host Computer"](#)

2.2.1 Running the Connector Installer

Note:

In this guide, the term Connector Installer has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

Direct provisioning is automatically enabled after you run the Connector Installer. If required, you can enable request-based provisioning in the connector. See [Section 2.3.3.9, "Enabling Request-Based Provisioning"](#) if you want to use the request-based provisioning feature for this target system.

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

Note: In an Oracle Identity Manager cluster, perform this step on each node of the cluster.

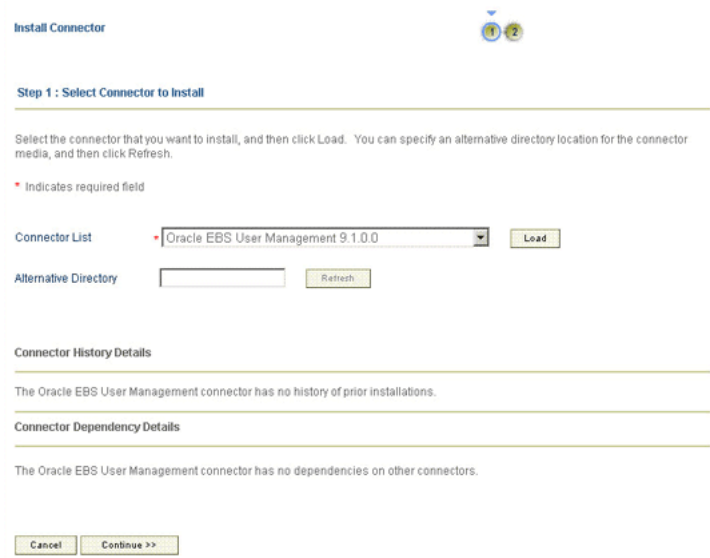
- For Oracle Identity Manager release 9.1.0.x:
OIM_HOME/xellerate/ConnectorDefaultDirectory
 - For Oracle Identity Manager releases 11.1.x and 11.1.2.x or later:
OIM_HOME/server/ConnectorDefaultDirectory
2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:
 - For Oracle Identity Manager release 9.1.0.x:
Oracle Identity Manager Administrative and User Console Guide
 - For Oracle Identity Manager releases 11.1.x and 11.1.2.x or later:
Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager
 3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
 - For Oracle Identity Manager release 9.1.0.x:
Click **Deployment Management**, and then click **Install Connector**.
 - For Oracle Identity Manager release 11.1.x:
On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.
 - For Oracle Identity Manager release 11.1.2.x or later:
 - a. Log in to Oracle Identity System Administration by using the user account described in the "Creating the User Account for Installing Connectors" section *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
 - b. In the left pane, under System Management, click **Manage Connector**.
 4. The Connector List list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

You can select one of the following options:

- For the User Management connector:
Oracle EBS User Management RELEASE_NUMBER
- For the User Management with HR Foundation connector:
Oracle EBS HR Foundation User Management RELEASE_NUMBER
- For the User Management with TCA Foundation connector:
Oracle EBS TCA Foundation User Management RELEASE_NUMBER

If you have copied the installation files into a different directory, then:

- a. In the **Alternative Directory** field, enter the full path and name of that directory.
 - b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
 - c. From the **Connector List** list, select the connector that you want to install.
5. Click **Load**. The following screenshot shows this page:



Install Connector

Step 1 : Select Connector to Install

Select the connector that you want to install, and then click Load. You can specify an alternative directory location for the connector media, and then click Refresh.

* Indicates required field

Connector List: Oracle EBS User Management 9.1.0.0 Load

Alternative Directory: Refresh

Connector History Details

The Oracle EBS User Management connector has no history of prior installations.

Connector Dependency Details

The Oracle EBS User Management connector has no dependencies on other connectors.

Cancel Continue >>

6. To start the installation process, click **Continue**.

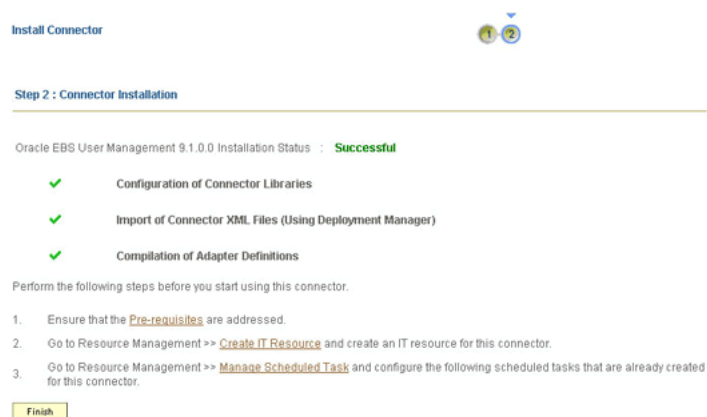
The following tasks are performed in sequence:

- a. Configuration of connector libraries
- b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager).
- c. Compilation of adapters

On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

- Retry the installation by clicking **Retry**.
- Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. The following screenshot shows this page for Oracle Identity Manager release 9.1.0.x:



Install Connector

Step 2 : Connector Installation

Oracle EBS User Management 9.1.0.0 Installation Status : **Successful**

- ✓ Configuration of Connector Libraries
- ✓ Import of Connector XML Files (Using Deployment Manager)
- ✓ Compilation of Adapter Definitions

Perform the following steps before you start using this connector.

1. Ensure that the [Pre-requisites](#) are addressed.
2. Go to Resource Management >> [Create IT Resource](#) and create an IT resource for this connector.
3. Go to Resource Management >> [Manage Scheduled Task](#) and configure the following scheduled tasks that are already created for this connector.

Finish

In addition, a list of steps that you must perform after the installation is displayed. These steps are as follows:

- a. Ensuring that the prerequisites for using the connector are addressed

Note: At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See [Section 2.3.3.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#) for information about running the PurgeCache utility.

The prerequisites for this connector are also described later in this guide.

- b. Configuring the IT resource for the connector

Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

- c. Configuring the scheduled tasks that are created when you installed the connector

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in [Table 2-1](#).

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See [Section 2.1.1.1, "Files and Directories on the Installation Media"](#) for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.2.2 Copying Files to the Oracle Identity Manager Host Computer

After you run the Connector Installer, you must manually copy the files listed in [Table 2-2](#).

Note: If a particular destination directory does not exist on the Oracle Identity Manager host computer, then create it.

Table 2-2 Files to Be Copied to the Oracle Identity Manager Host Computer

Files on the Installation Media	Destination Directory on the Oracle Identity Manager Release 9.1.0.x Host Computer	Destination Directory on the Oracle Identity Manager releases 11.1.x and 11.1.2.x Host Computer
Files in the config directory	<code>OIM_HOME/xellerate/XLIntegrations/EBSUM/config</code>	<code>OIM_HOME/server/XLIntegrations/EBSUM/config</code>
Files in the test/config directory	<code>OIM_HOME/xellerate/XLIntegrations/EBSUM/config</code>	<code>OIM_HOME/server/XLIntegrations/EBSUM/config</code>
Files in the test/scripts directory	<code>OIM_HOME/xellerate/XLIntegrations/EBSUM/scripts</code>	<code>OIM_HOME/server/XLIntegrations/EBSUM/scripts</code>

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- [Section 2.3.1, "Configuring SoD"](#)
- [Section 2.3.2, "Configuring Secure Communication Between the Target System and Oracle Identity Manager"](#)
- [Section 2.3.3, "Postinstallation on Oracle Identity Manager"](#)
- [Section 2.3.4, "Localizing Field Labels in UI Forms"](#)

2.3.1 Configuring SoD

This section discusses the following procedures:

- [Section 2.3.1.1, "Configuring the Oracle Applications Access Controls Governor to Act As the SoD Engine"](#)
- [Section 2.3.1.2, "Specifying a Value for the TopologyName IT Resource Parameter"](#)
- [Section 2.3.1.3, "Disabling and Enabling SoD"](#)

Note: The ALL USERS group has INSERT, UPDATE, and DELETE permissions on the UD_EBS_USER, UD_EBS_RESP, UD_EBS_RLS, UD_EBSH_USR, UD_EBSH_RSP, UD_EBST_RLS, UD_EBST_USR, UD_EBST_RSP, and UD_EBST_RLS process forms. This is required to enable the following process:

During SoD validation of an entitlement request, data first moves from a dummy object form to a dummy process form. From there, data is sent to the SoD engine for validation. If the request clears the SoD validation, then data is moved from the dummy process form to the actual process form. Because the data is moved to the actual process forms through APIs, the ALL USERS group must have INSERT, UPDATE, and DELETE permissions on the three process forms.

2.3.1.1 Configuring the Oracle Applications Access Controls Governor to Act As the SoD Engine

If you are using Oracle Identity Manager release 9.1.0.x, then see the "Configuring Oracle Application Access Controls Governor" section in the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in *Oracle Identity Manager Tools Reference* for information about this procedure.

If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x or later, then see the "Configuring Oracle Application Access Controls Governor" section of the "Configuring SoD Validation" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about this procedure.

2.3.1.2 Specifying a Value for the TopologyName IT Resource Parameter

The TopologyName IT resource parameter holds the name of the combination of the following elements that you want to use for SoD validation of entitlement provisioning operations:

- Oracle Identity Manager installation
- Oracle Applications Access Controls Governor installation

- Oracle E-Business Suite installation

The value that you specify for the `TopologyName` parameter must be the same as the value of the `TopologyName` element in the `SILConfig.xml` file. For Oracle Identity Manager releases 11.1.x and 11.1.2.x or later, if you are using default SIL registration, then specify `sodoaacg` as the value of the `TopologyName` parameter.

See one of the following for more information about this element:

- For Oracle Identity Manager release 9.1.0.x, the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in *Oracle Identity Manager Tools Reference*.
- For Oracle Identity Manager releases 11.1.x and 11.1.2.x or later, the "Configuring SoD Validation" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

See [Section 2.3.3.6, "Configuring the IT Resource"](#) section for information about specifying values for parameters of the IT resource.

2.3.1.3 Disabling and Enabling SoD

This section describes the procedures to disable and enable SoD.

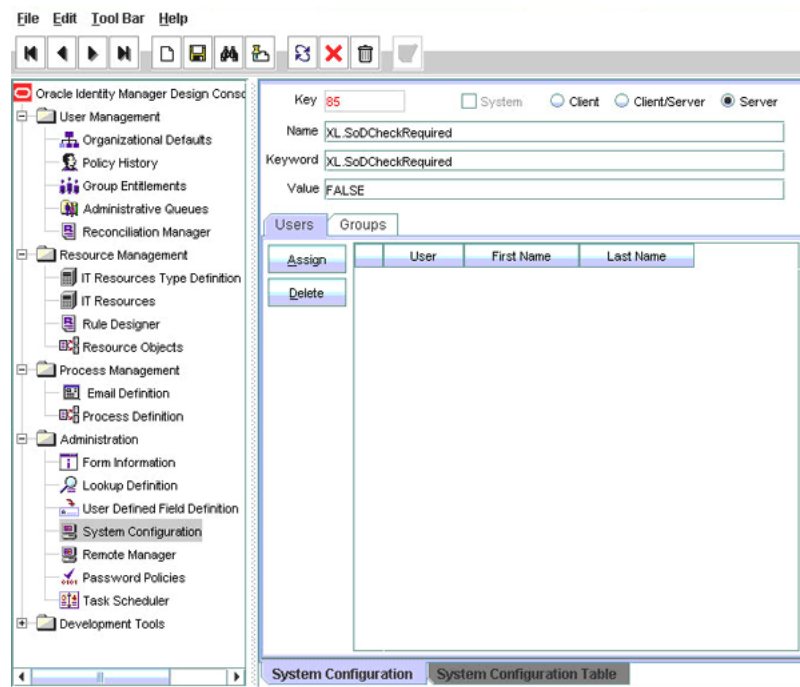
To disable SoD:

Note: The SoD feature is disabled by default. Perform the following procedure only if the SoD feature is currently enabled and you want to disable it.

1. Log in to one of the following consoles:
 - If you are using Oracle Identity Manager release 9.1.0.x, then log in to the Design Console.
 - If you are using Oracle Identity Manager release 11.1.x, then log in to the Administrative and User Console.
 - If you are using Oracle Identity Manager release 11.1.2.x or later, then log in to the System Administration console.
2. Set the `XL.SoDCheckRequired` system property to `FALSE` as follows:

For Oracle Identity Manager release 9.1.0.x:

 - a. Expand **Administration**, and then double-click **System Configuration**.
 - b. Search for and open the `XL.SoDCheckRequired` system property.
 - c. Set the value of the system property to `FALSE`. The following screenshot shows this page:



Note: You need not change the values of the XL.SIL.Home.Dir and Triggers Synchronous SoD checks offline system properties.

- d. Click the Save icon.

For Oracle Identity Manager releases 11.1.x:

- a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
- b. On Welcome to Identity Manager Advanced Administration page, in the System Management section, click **Search System Properties**.
- c. On the left pane, in the **Search System Configuration** field, enter XL.SoDCheckRequired, which is the name of the system property as the search criterion.
- d. In the search results table on the left pane, click the XL.SoDCheckRequired system property in the Property Name column.
- e. On the System Property Detail page, in the Value field, enter FALSE.
- f. Click **Save** to save the changes made.

A message confirming that the system property has been modified is displayed.

For Oracle Identity Manager releases 11.1.2.x:

- a. In the left pane, under System Management, click **System Configuration**. The Advanced Administration is displayed with the System Configuration section in the System Management tab is active.
- b. On the left pane, in the **Search System Configuration** field, enter XL.SoDCheckRequired, which is the name of the system property as the search criterion.

- c. In the search results table on the left pane, click the XL.SoDCheckRequired system property in the Property Name column.
- d. On the System Property Detail page, in the Value field, enter FALSE.
- e. Click **Save** to save the changes made.

A message confirming that the system property has been modified is displayed.

3. If you are going to perform the procedure described in [Section 2.3.3.9, "Enabling Request-Based Provisioning"](#), then for all approval process definitions, the human approval tasks must be made unconditional as follows:
 - Log in to the Design Console.
 - Expand Process Management, and then double-click Process Definition.
 - Search for and open the approval-type process definition for the connector that you are using. See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for information about the connector objects.
 - On the Task tab, search for the Manager Approval task.
 - Make this task unconditional by deselecting the Conditional check box. See the following screenshot:

The screenshot shows the 'Manager Approval' task configuration in the Design Console. The 'Task Properties' section is expanded, showing the following settings:

- Conditional:** ☐ (unchecked)
- Disable Manual Insert:** ☐ (unchecked)
- Retry Period in Minutes:** (empty)
- Required for Completion:** ☒ (checked)
- Allow Cancellation while Pending:** ☒ (checked)
- Retry Count:** (empty)
- Constant Duration:** ☐ (unchecked)
- Allow Multiple Instances:** ☒ (checked)
- Task Effect:** (dropdown menu)
- Child Table:** (dropdown menu)
- Trigger Type:** (dropdown menu)

- Save the changes to the process definition.

4. Restart Oracle Identity Manager.

To enable SoD:

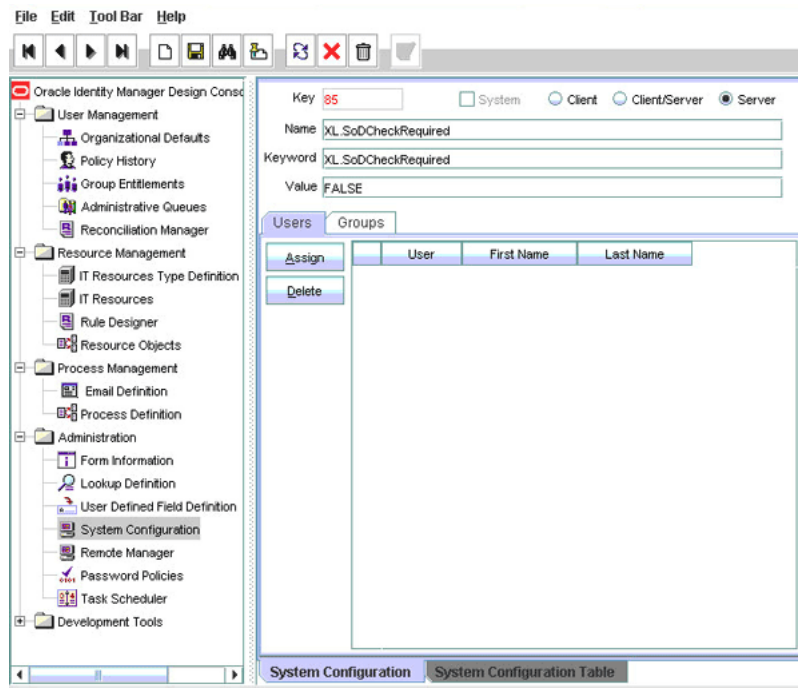
Note: If you are enabling SoD for the first time, then see one of the following documents for detailed information:

- Oracle Identity Manager release 9.1.0.x:
Oracle Identity Manager Readme for Release 9.1.0.2
 - Oracle Identity Manager releases 11.1.x and 11.1.2.x:
Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager
-

1. Log in to one of the following consoles:
 - If you are using Oracle Identity Manager release 9.1.0.x, then log in to the Design Console.
 - If you are using Oracle Identity Manager release 11.1.x, then log in to the Administrative and User Console.
 - If you are using Oracle Identity Manager release 11.1.2.x, then log in to the System Administration console.
2. Set the XL.SoDCheckRequired system property to TRUE as follows:

For Oracle Identity Manager release 9.1.0.x:

 - a. Expand **Administration**, and then double-click **System Configuration**.
 - b. Search for and open the **XL.SoDCheckRequired** system property.
 - c. Set the value of the system property to **TRUE**. The following screenshot shows this page:



Note: You need not change the values of the XL.SIL.Home.Dir and Triggers Synchronous SoD checks offline system properties.

- d. Click the Save icon.

For Oracle Identity Manager releases 11.1.x:

- a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
- b. On Welcome to Identity Manager Advanced Administration page, in the System Management section, click **Search System Properties**.
- c. On the left pane, in the **Search System Configuration** field, enter **XL.SoDCheckRequired**, which is the name of the system property as the search criterion.

- d. In the search results table on the left pane, click the `XL.SoDCheckRequired` system property in the Property Name column.
- e. On the System Property Detail page, in the Value field, enter `FALSE`.
- f. Click **Save** to save the changes made.

A message confirming that the system property has been modified is displayed.

For Oracle Identity Manager releases 11.1.2.x or later:

- a. In the left pane, under System Management, click **System Configuration**. The Advanced Administration is displayed with the System Configuration section in the System Management tab is active.
 - b. On the left pane, in the **Search System Configuration** field, enter `XL.SoDCheckRequired`, which is the name of the system property as the search criterion.
 - c. In the search results table on the left pane, click the `XL.SoDCheckRequired` system property in the Property Name column.
 - d. On the System Property Detail page, in the Value field, enter `FALSE`.
 - e. Click **Save** to save the changes made.
- A message confirming that the system property has been modified is displayed.
3. If you are using Oracle Identity Manager release 9.1.0.x, then:
 - a. In the Design Console, expand **Administration**, and then double-click **System Configuration**.
 - b. Search for and open the `XL.SIL.Home.Dir` system property.
 - c. Verify that the value of this system property is set to the full path and name of the `SIL_HOME` directory. Here, `SIL_HOME` is the directory in which you have copied the SIL XML files.
 4. If you are going to perform the procedure described in [Section 2.3.3.9, "Enabling Request-Based Provisioning"](#), then for all approval process definitions, the human approval tasks must be made conditional as follows:
 - On the Design Console.
 - Expand Process Management, and then double-click Process Definition.
 - Search for and open the approval-type process definition for the connector that you are using. See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for information about the connector objects.
 - On the Task tab, search for the Manager Approval task.
 - Make this task conditional by selecting the Conditional check box. See the following screenshot:

The screenshot shows the Oracle Identity Manager configuration console. The 'General' tab is selected, displaying the 'Manager Approval' task configuration. The 'Task Name' is 'Manager Approval' and the 'Task Description' is 'Manager Approval task'. The 'Duration' section has fields for Days, Hours, and Minutes. The 'Task Properties' section includes checkboxes for 'Conditional', 'Required for Completion', 'Constant Duration', 'Disable Manual Insert', 'Allow Cancellation while Pending', 'Allow Multiple Instances', 'Retry Period in Minutes', and 'Retry Count'. The 'Task Effect' is set to 'No Effect'. The 'Child Table' and 'Trigger Type' are also visible.

- Save the changes to the process definition.
5. Restart Oracle Identity Manager.

2.3.2 Configuring Secure Communication Between the Target System and Oracle Identity Manager

To secure communication between Oracle Database and Oracle Identity Manager, you can perform either one or both of the following procedures:

Note: To perform the procedures described in this section, you must have the permissions required to modify the TNS listener configuration file.

- [Section 2.3.2.1, "Configuring Data Encryption and Integrity in Oracle Database"](#)
- [Section 2.3.2.2, "Configuring SSL Communication in Oracle Database"](#)

2.3.2.1 Configuring Data Encryption and Integrity in Oracle Database

See *Oracle Database Advanced Security Administrator's Guide* for information about configuring data encryption and integrity.

2.3.2.2 Configuring SSL Communication in Oracle Database

To enable SSL communication between Oracle Database and Oracle Identity Manager:

1. See *Oracle Database Advanced Security Administrator's Guide* for information about enabling SSL communication between Oracle Database and Oracle Identity Manager.
2. Export the certificate on the Oracle Database host computer.
3. Copy the certificate to Oracle Identity Manager.
4. Import the certificate into the JVM certificate store of the application server on which Oracle Identity Manager is running.

To import the certificate into the certificate store, run the following command:

```
keytool -import -file FILE_LOCATION -keystore TRUSTSTORE_LOCATION -storepass TRUSTSTORE_PASSWORD -trustcacerts -alias ALIAS
```

In this command:

- Replace *FILE_LOCATION* with the full path and name of the certificate file.
- Replace *ALIAS* with an alias for the certificate.
- Replace *TRUSTSTORE_PASSWORD* with a password for the certificate store.
- Replace *TRUSTSTORE_LOCATION* with one of the certificate store paths given in [Table 2–3](#). This table shows the location of the certificate store for each of the supported application servers.

Note: In an Oracle Identity Manager cluster, you must import the file into the certificate store on each node of the cluster.

Table 2–3 Certificate Store Locations

Application Server	Certificate Store Location
Oracle WebLogic Server	<ul style="list-style-type: none"> ■ If you are using Oracle jrockit_R27.3.1-jdk, then copy the certificate into the following directory: <i>JROCKIT_HOME</i>/jre/lib/security ■ If you are using the default Oracle WebLogic Server JDK, then copy the certificate into the following directory: <i>WEBLOGIC_HOME</i>/java/jre/lib/security/cacerts
IBM WebSphere Application Server	<ul style="list-style-type: none"> ■ For a nonclustered configuration of any supported IBM WebSphere Application Server release, import the certificate into the following certificate store: <i>WEBSphere_HOME</i>/java/jre/lib/security/cacerts ■ For IBM WebSphere Application Server 6.1.x, in addition to the <i>cacerts</i> certificate store, you must import the certificate into the following certificate store: <i>WEBSphere_HOME</i>/Web_Sphere/profiles/<i>SERVER_NAME</i>/config/cells/<i>CELL_NAME</i>/nodes/<i>NODE_NAME</i>/trust.p12 For example: C:/Web_Sphere/profiles/AppSrv01/config/cells/tcs055071Node01Cell/nodes/tcs055071Node01/trust.p12 ■ For IBM WebSphere Application Server 5.1.x, in addition to the <i>cacerts</i> certificate store, you must import the certificate into the following certificate store: <i>WEBSphere_HOME</i>/etc/DummyServerTrustFile.jks
JBoss Application Server	<i>JAVA_HOME</i> /jre/lib/security/cacerts
Oracle Application Server	<i>ORACLE_HOME</i> /jdk/jre/lib/security/cacerts

2.3.3 Postinstallation on Oracle Identity Manager

Configuring Oracle Identity Manager involves performing the following procedures:

- [Section 2.3.3.1, "Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server"](#)
- [Section 2.3.3.2, "Configuring Oracle Identity Manager 11.1.2 or Later"](#)
- [Section 2.3.3.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#)

- [Section 2.3.3.4, "Enabling Logging"](#)
- [Section 2.3.3.5, "Determining Values for the JDBC URL and Connection Properties Parameters"](#)
- [Section 2.3.3.6, "Configuring the IT Resource"](#)
- [Section 2.3.3.7, "SSO IT Resource"](#)
- [Section 2.3.3.8, "Disabling the Auto Save Form Feature on Oracle Identity Manager Releases 11.1.x and 11.1.2.x"](#)
- [Section 2.3.3.9, "Enabling Request-Based Provisioning"](#)

2.3.3.1 Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server

Note: Perform the procedure described in this section only if your Oracle Identity Manager installation is running on Microsoft SQL Server.

In this connector, the child forms of a resource implement the dependent lookup feature of Oracle Identity Manager. By default, the queries for synchronization of lookup field values from the target system are based on Oracle Database SQL. If your Oracle Identity Manager installation is running on Microsoft SQL Server, then you must modify the lookup queries for synchronization of lookup definitions as follows:

1. On the Design Console, expand **Development Tools** and double-click **Form Designer**.
2. Search for and open the process form for the connector that you are using.
3. Click **Create New Version** to create a version of the process form. Then, enter a version name and click the Save icon.
4. Go to the Properties tab.
5. Select the properties of the attribute according to your requirement.
6. Modify the Lookup Query property for the field. Existing and new values are listed in [Table 2-4](#). The following screenshot shows this page:

The screenshot shows the 'Component Property' dialog box. It has a title bar with standard window controls. The main area contains several labeled fields: 'Column Name' with the value 'Application Name', 'Column Type' with the value 'LookupField', 'Property Name' with a dropdown menu showing 'Lookup Query', 'Property Value' with the text 'data.UD_EBS_USER_EBS_ITRES\$,'-')>0', 'Filter Column' with an empty dropdown, 'Source' with an empty dropdown, and 'Field' with an empty dropdown. There are also some icons at the top of the dialog.

7. Click the Save icon.
8. Click **Make Version Active** to activate the new version of the process form.

9. Create a new version of the parent form for the child form you modified and make that version active.

See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for information about the process forms.

Table 2–4 Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
User Management connector		
UD_EBS_RLO_APP_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded, concat('\$Form data.UD_EBS_UO_EBS_ITRES\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBS_UO_EBS_ITRES\$' + '~', lkv_encoded)>0
UD_EBS_RLO_ROLE_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and instr(lkv_encoded, concat('\$Form data.UD_EBS_RLO_APP_NAME\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBS_RLO_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBS_RLS_APP_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded, concat('\$Form data.UD_EBS_USER_EBS_ITRES\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBS_USER_EBS_ITRES\$' + '~', lkv_encoded)>0
UD_EBS_RLS_ROLE_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and instr(lkv_encoded, concat('\$Form data.UD_EBS_RLS_APP_NAME\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBS_RLS_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBS_RSO_APP_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded, concat('\$Form data.UD_EBS_UO_EBS_ITRES\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBS_UO_EBS_ITRES\$' + '~', lkv_encoded)>0
UD_EBS_RSO_RESP_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and instr(lkv_encoded, concat('\$Form data.UD_EBS_RSO_APP_NAME\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBS_RSO_APP_NAME\$' + '~', lkv_encoded)>0

Table 2–4 (Cont.) Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_EBS_RSO_SEC_GROUP	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. SecurityGroup' and instr(lkv_encoded, concat('\$Form data.UD_EBS_UO_EBS_ITRES\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.SecurityGroup' and CHARINDEX('\$Form data.UD_EBS_UO_EBS_ITRES\$' + '~' , lkv_encoded)>0
UD_EBS_RESP_APP_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded, concat('\$Form data.UD_EBS_USER_EBS_ITRES\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBS_USER_EBS_ITRES\$' + '~' , lkv_encoded)>0
UD_EBS_RESP_SEC_GROUP	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. SecurityGroup' and instr(lkv_encoded, concat('\$Form data.UD_EBS_USER_EBS_ITRES\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.SecurityGroup' and CHARINDEX('\$Form data.UD_EBS_USER_EBS_ITRES\$' + '~' , lkv_encoded)>0
UD_EBS_RESP_RESP_APP_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Responsibility' and instr(lkv_encoded, concat('\$Form data.UD_EBS_RESP_APP_NAMES\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBS_RESP_APP_NAMES\$' + '~' , lkv_encoded)>0
UD_EBS_RLCO_APP_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded, concat('\$Form data.UD_EBS_RLPO_EBS_INST\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBS_RLPO_EBS_INST\$' + '~' , lkv_encoded)>0
UD_EBS_RLCO_ROLE_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. UMX.Roles' and instr(lkv_encoded, concat('\$Form data.UD_EBS_RLCO_APP_NAMES\$' , '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBS_RLCO_APP_NAMES\$' + '~', lkv_encoded)>0
UD_EBS_RLCP_APP_NAME	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded, concat('\$Form data.UD_EBS_RLPP_EBS_INST\$', '~'))>0	select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBS_RLPP_EBS_INST\$' + '~', lkv_encoded)>0

Table 2–4 (Cont.) Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_EBS_RLCP_ROLE_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBS_RLCP_APP_NAME\$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBS_RLCP_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBS_RSCO_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded,concat('\$Form data.UD_EBS_RSPO_EBS_INST\$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBS_RSPO_EBS_INST\$' + '~', lkv_encoded)>0
UD_EBS_RSCO_RESP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBS_RSCO_APP_NAME\$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBS_RSCO_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBS_RSCP_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded,concat('\$Form data.UD_EBS_RSPP_EBS_INST\$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBS_RSPP_EBS_INST\$' + '~', lkv_encoded)>0
UD_EBS_RSCP_RESP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBS_RSCP_APP_NAME\$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBS_RSCP_APP_NAME\$' + '~', lkv_encoded)>0
User Management with HR Foundation connector		
UD_EBSH_RLO_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_UO_EBS_ITRES\$','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBSH_UO_EBS_ITRES\$' + '~', lkv_encoded)>0

Table 2–4 (Cont.) Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_EBSH_RLO_ROLE_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_RLO_APP_NAME \$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBSH_RLO_APP_NAME\$' + '~',lkv_encoded)
UD_EBSH_RLS_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_USR_EBS_ITRES\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBSH_USR_EBS_ITRES\$' + '~', lkv_encoded)>0
UD_EBSH_RLS_ROLE_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_RLS_APP_NAME\$' , '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBSH_RLS_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBSH_RSO_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_UO_EBS_ITRES\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBSH_UO_EBS_ITRES\$' + '~' ,lkv_encoded)>0
UD_EBSH_RSO_SECURITY_GROUP	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. SecurityGroup' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_UO_EBS_ITRES\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.SecurityGroup' and CHARINDEX('\$Form data.UD_EBSH_UO_EBS_ITRES\$' + '~' ,lkv_encoded)>0
UD_EBSH_RSO_RESP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_RSO_APP_NAME\$' , '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBSH_RSO_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBSH_RSP_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_USR_EBS_ITRES\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBSH_USR_EBS_ITRES\$' + '~' ,lkv_encoded)

Table 2–4 (Cont.) Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_EBSH_RSP_SEC_GROUP	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.SecurityGroup' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_USR_EBS_ITRES\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.SecurityGroup' and CHARINDEX('\$Form data.UD_EBSH_USR_EBS_ITRES\$' + '~', lkv_encoded)
UD_EBSH_RSP_RESP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBSH_RESP_APP_NAME\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBSH_RESP_APP_NAME\$' + '~', lkv_encoded)
UD_EBH_RLCO_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded,concat('\$Form data.UD_EBH_RLPO_EBS_INST\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBH_RLPO_EBS_INST\$' + '~', lkv_encoded)>0
UD_EBH_RLCO_ROLE_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBH_RLCO_APP_NAME\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBH_RLCO_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBH_RLCP_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded,concat('\$Form data.UD_EBH_RLPP_EBS_INST\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBH_RLPP_EBS_INST\$' + '~', lkv_encoded)>0
UD_EBH_RLCP_ROLE_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBH_RLCP_APP_NAME\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBH_RLCP_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBH_RSCO_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and instr(lkv_encoded,concat('\$Form data.UD_EBH_RSPO_EBS_INST\$', '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBH_RSPO_EBS_INST\$' + '~', lkv_encoded)>0

Table 2–4 (Cont.) Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_EBH_RSCO_RESP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Responsibility' and instr(lkv_encoded,concat('\$Form data. UD_EBH_RSPO_APP_NAME\$','~')) >0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data. UD_EBH_RSPO_APP_NAME\$' + '~' , lkv_encoded)>0
UD_EBH_RSCP_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBH_RSPP_EBS_INST\$',' ~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBH_RSPP_EBS_INST\$' + '~' , lkv_encoded)>0
UD_EBH_RSCP_RESP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBH_RSCP_APP_NAME\$ ','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBH_RSCP_APP_NAME\$' + '~' , lkv_encoded)>0
User Management with TCA Foundation connector		
UD_EBST_RLO_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBST_UO_EBS_ITRES\$',' ~'))>0	select lkv_encoded,lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBST_UO_EBS_ITRES\$' + '~' , lkv_encoded)>0
UD_EBST_RLO_ROLE_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBST_RLO_APP_NAME\$ ','~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBST_RLO_APP_NAME\$' + '~' ,lkv_encoded)
UD_EBST_RLS_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBST_USR_EBS_ITRES\$',' ~'))>0	select lkv_encoded,lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBST_USR_EBS_ITRES\$' + '~' , lkv_encoded)>0

Table 2–4 (Cont.) Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_EBST_RLS_ROL E_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBST_RLS_APP_NAMES\$' ,~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBST_RLS_APP_NAMES\$' + '~', lkv_encoded)>0
UD_EBST_RSO_APP _NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBST_UO_EBS_ITRES\$','~ '>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBST_UO_EBS_ITRES\$' + '~', lkv_encoded)>0
UD_EBST_RSO_SEC _GROUP	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. SecurityGroup' and instr(lkv_encoded,concat('\$Form data.UD_EBST_UO_EBS_ITRES\$','~ '>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.SecurityGroup' and CHARINDEX('\$Form data.UD_EBST_UO_EBS_ITRES\$' + '~', lkv_encoded)>0
UD_EBST_RSO_RES P_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBST_RSO_APP_NAME\$' ,~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBST_RSO_APP_NAME\$' + '~', lkv_encoded)>0
UD_EBST_RSP_APP _NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBST_USR_EBS_ITRES\$',' ~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBST_USR_EBS_ITRES\$' + '~', lkv_encoded)>0
UD_EBST_RSP_SEC_ GROUP	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. SecurityGroup' and instr(lkv_encoded,concat('\$Form data.UD_EBST_USR_EBS_ITRES\$',' ~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.SecurityGroup' and CHARINDEX('\$Form data.UD_EBST_USR_EBS_ITRES\$' + '~', lkv_encoded)>0
UD_EBST_RSP_RESP _NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBST_RSP_APP_NAME\$' ,~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBST_RSP_APP_NAME\$' + '~', lkv_encoded)>0

Table 2–4 (Cont.) Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_EBT_RLCO_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBT_RLPO_EBS_INST\$', ~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBT_RLPO_EBS_INST\$' + '~' , lkv_encoded)>0
UD_EBT_RLCO_ROLE_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBT_RLCO_APP_NAMES\$ '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBT_RLCO_APP_NAMES\$' + '~' , lkv_encoded)>0
UD_EBT_RLCP_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBT_RLPP_EBS_INST\$', ~'))>0	select lkv_encoded,lkv_decoded from lkv lkv, lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBT_RLPP_EBS_INST\$' + '~' , lkv_encoded)>0
UD_EBT_RLCP_ROLE NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. UMX.Roles' and instr(lkv_encoded,concat('\$Form data.UD_EBT_RLCP_APP_NAME\$ '~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.UMX.Roles' and CHARINDEX('\$Form data.UD_EBT_RLCP_APP_NAME\$' + '~' , lkv_encoded)>0
UD_EBT_RSCO_APP_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBT_RSPO_EBS_INST\$', ~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBT_RSPO_EBS_INST\$' + '~' , lkv_encoded)>0

Table 2–4 (Cont.) Queries for Lookup Field Synchronization

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
UD_EBT_RSCO_RES P_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBT_RSCO_APP_NAME\$,~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBT_RSCO_APP_NAME\$' + '~' , lkv_encoded)>0
UD_EBT_RSPP_APP _NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Application' and instr(lkv_encoded,concat('\$Form data.UD_EBT_RSPP_EBS_INST\$', '~')>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Application' and CHARINDEX('\$Form data.UD_EBT_RSPP_EBS_INST\$' + '~' , lkv_encoded)>0
UD_EBT_RSPP_RES P_NAME	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS. Responsibility' and instr(lkv_encoded,concat('\$Form data.UD_EBT_RSPP_APP_NAME\$' ,~'))>0	select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Lookup.EBS.Responsibility' and CHARINDEX('\$Form data.UD_EBT_RSPP_APP_NAME\$' + '~' , lkv_encoded)>0

2.3.3.2 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2.x or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

- [Section 2.3.3.2.1, "Creating and Activating a Sandbox"](#)
- [Section 2.3.3.2.2, "Creating a New UI Form"](#)
- [Section 2.3.3.2.3, "Creating an Application Instance"](#)
- [Section 2.3.3.2.4, "Publishing a Sandbox"](#)
- [Section 2.3.3.2.5, "Harvesting Entitlements and Sync Catalog"](#)
- [Section 2.3.3.2.6, "Updating an Existing Application Instance with a New Form"](#)

2.3.3.2.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see the "Managing Sandboxes" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes**. The Manage Sandboxes page is displayed.
2. On the toolbar, click **Create Sandbox**. The Create Sandbox dialog box is displayed.
3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.

5. Click **Save and Close**. A message is displayed with the sandbox name and creation label.
6. Click **OK**. The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. Select the sandbox that you created.
8. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
9. On the toolbar, click **Activate Sandbox**.
The sandbox is activated.

2.3.3.2.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see the "Managing Forms" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer**.
2. Under Search Results, click **Create**.
3. Select the resource type for which you want to create the form, for example, `eBusiness User`.
4. Enter a form name and click **Create**.

Note:

- While creating a new UI form, the form type should be Parent Form + Child Tables (Master/Detail).
 - Ensure that you select the **Generate Entitlement Forms** check box.
-

2.3.3.2.3 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see the "Managing Application Instances" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances**.
2. Under Search Results, click **Create**.
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save**.
4. In the Form drop-down list, select the newly created form and click **Apply**.
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See the "Managing Organizations Associated With Application Instances" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed instructions.

2.3.3.2.4 Publishing a Sandbox

To publish the sandbox that you created in [Section 2.3.3.2.1, "Creating and Activating a Sandbox"](#):

1. Close all the open tabs and pages.
2. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in [Section 2.3.3.2.1, "Creating and Activating a Sandbox."](#)
3. On the toolbar, click **Publish Sandbox**. A message is displayed asking for confirmation.
4. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

2.3.3.2.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about this scheduled job.

2.3.3.2.6 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in [Section 2.3.3.2.1, "Creating and Activating a Sandbox."](#)
2. Create a new UI form for the resource as described in [Section 2.3.3.2.2, "Creating a New UI Form."](#)
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in [Section 2.3.3.2.4, "Publishing a Sandbox."](#)

2.3.3.3 Clearing Content Related to Connector Resource Bundles from the Server Cache

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the `OIM_HOME/xellerate/connectorResources` directory for Oracle Identity Manager release 9.1.0.x and Oracle Identity Manager database for Oracle Identity Manager releases 11.1.x and 11.1.2.x or later. Whenever you add a new resource bundle to the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, perform one of the following steps:
 - If you are using Oracle Identity Manager release 9.1.0.x, then switch to the *OIM_HOME/xellerate/bin* directory.
 - If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x or later, then switch to the *OIM_HOME/server/bin* directory.

Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

For Oracle Identity Manager release 9.1.0.x:

OIM_HOME/xellerate/bin/SCRIPT_FILE_NAME

For Oracle Identity Manager releases 11.1.x and 11.1.2.x or later:

OIM_HOME/server/bin/SCRIPT_FILE_NAME

2. Enter one of the following commands:

- For Oracle Identity Manager release 9.1.0.x:
On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`
On UNIX: `PurgeCache.sh ConnectorResourceBundle`

Note: You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

In this command, `ConnectorResourceBundle` is one of the content categories that you can delete from the server cache. See the following file for information about the other content categories:

OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager releases 11.1.x and 11.1.2.x:

On Microsoft Windows: `PurgeCache.bat All`

On UNIX: `PurgeCache.sh All`

When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

`t3://OIM_HOST_NAME:OIM_PORT_NUMBER`

In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about the `PurgeCache` utility.

2.3.3.4 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform instructions in one of the following sections:

- [Section 2.3.3.4.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"](#)
- [Section 2.3.3.4.2, "Enabling Logging on Oracle Identity Manager Releases 11.1.x and 11.1.2.x"](#)

2.3.3.4.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.x

Note: In an Oracle Identity Manager cluster, you must perform this procedure on each node of the cluster. Then, restart each node.

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- ALL
This level enables logging for all events.
- DEBUG
This level enables logging of information about fine-grained events that are useful for debugging.
- INFO
This level enables logging of messages that highlight the progress of the application at a coarse-grained level.
- WARN
This level enables logging of information about potentially harmful situations.
- ERROR
This level enables logging of information about error events that might allow the application to continue running.
- FATAL
This level enables logging of information about very severe error events that could cause the application to stop functioning.
- OFF
This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **IBM WebSphere Application Server**

To enable logging:

1. Add the following line in the `OIM_HOME/xellerate/config/log.properties` file:

```
log4j.logger.OIMCP.EBSUM=log_level
```

2. In this line, replace `log_level` with the log level that you want to set.

For example:

```
log4j.logger.OIMCP.EBSUM=INFO
```

After you enable logging, log information is written to the following file:

`WEBSPHERE_HOME/AppServer/logs/SERVER_NAME/SystemOut.log`

■ JBoss Application Server

To enable logging:

1. In the `JBOSS_HOME/server/default/conf/jboss-log4j.xml` file, add the following lines if they are not already present in the file:

```
<category name="ADAPTER.OIMCP.EBSUM">
  <priority value="log_level"/>
</category>
```

2. In the second XML code line, replace `log_level` with the log level that you want to set. For example:

```
<category name="ADAPTER.OIMCP.EBSUM">
  <priority value="INFO"/>
</category>
```

After you enable logging, log information is written to the following file:

`JBOSS_HOME/server/default/log/server.log`

■ Oracle Application Server

To enable logging:

1. Add the following line in the `OIM_HOME/xellerate/config/log.properties` file:

```
log4j.logger.OIMCP.EBSUM=log_level
```

2. In this line, replace `log_level` with the log level that you want to set.

For example:

```
log4j.logger.OIMCP.EBSUM=INFO
```

After you enable logging, log information is written to the following file:

`OC4J_HOME/opmn/logs/default_group~home~default_group~1.log`

■ Oracle WebLogic Server

To enable logging:

1. Add the following line in the `OIM_HOME/xellerate/config/log.properties` file:

```
log4j.logger.OIMCP.EBSUM=log_level
```

2. In this line, replace `log_level` with the log level that you want to set.

For example:

```
log4j.logger.OIMCP.EBSUM=INFO
```

After you enable logging, log information is displayed on the server console.

2.3.3.4.2 Enabling Logging on Oracle Identity Manager Releases 11.1.x and 11.1.2.x

Note: In an Oracle Identity Manager cluster, you must perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager releases 11.1.x and 11.1.2.x or later uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100
This level enables logging of information about fatal errors.
- SEVERE
This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.
- WARNING
This level enables logging of information about potentially harmful situations.
- INFO
This level enables logging of messages that highlight the progress of the application.
- CONFIG
This level enables logging of information about fine-grained events that are useful for debugging.
- FINE, FINER, FINEST
These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in [Table 2-5](#).

Table 2-5 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

- a. Add the following blocks in the file:

```
<log_handler name='ebs-um-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off' />
  <property name='path' value='[FILE_NAME]' />
  <property name='format' value='ODL-Text' />
  <property name='useThreadName' value='true' />
  <property name='locale' value='en' />
  <property name='maxFileSize' value='5242880' />
  <property name='maxLogSize' value='52428800' />
  <property name='encoding' value='UTF-8' />
</log_handler>

<logger name="OIMCP.EBSUM" level="[LOG_LEVEL]" useParentHandlers="false">
  <handler name="ebs-um-handler" />
  <handler name="console-handler" />
</logger>
```

- b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. [Table 2-5](#) lists the supported message type and level combinations.

Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]** :

```
<log_handler name='ebs-um-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off' />
  <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log' />
  <property name='format' value='ODL-Text' />
  <property name='useThreadName' value='true' />
  <property name='locale' value='en' />
  <property name='maxFileSize' value='5242880' />
  <property name='maxLogSize' value='52428800' />
  <property name='encoding' value='UTF-8' />
</log_handler>

<logger name="OIMCP.EBSUM" level="NOTIFICATION:1"
useParentHandlers="false">
  <handler name="ebs-um-handler" />
  <handler name="console-handler" />
</logger>
```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

Replace **FILENAME** with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

2.3.3.5 Determining Values for the JDBC URL and Connection Properties Parameters

This section discusses the JDBC URL and Connection Properties parameters. You apply the information in this section while performing the procedure described in [Section 2.3.3.6, "Configuring the IT Resource"](#).

The values that you specify for the JDBC URL and Connection Properties parameters depend on the security measures that you have implemented:

- [Section 2.3.3.5.1, "Supported JDBC URL Formats"](#)
- [Section 2.3.3.5.2, "Only Data Encryption and Integrity Is Configured"](#)
- [Section 2.3.3.5.3, "Only SSL Communication Is Configured"](#)
- [Section 2.3.3.5.4, "Both Data Encryption and Integrity and SSL Communication Are Configured"](#)

2.3.3.5.1 Supported JDBC URL Formats

The following are the supported JDBC URL formats:

- Multiple database instances support one service (Oracle RAC)

JDBC URL format:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=HOST1_NAME.DOMAIN)(PORT=PORT1_NUMBER))(ADDRESS=(PROTOCOL=TCP)(HOST=HOST2_NAME.DOMAIN)(PORT=PORT2_NUMBER))(ADDRESS=(PROTOCOL=TCP)(HOST=HOST3_NAME.DOMAIN)(PORT=PORT3_NUMBER)) . . . (ADDRESS=(PROTOCOL=TCP)(HOST=HOSTn_NAME.DOMAIN)(PORT=PORTn_NUMBER))(CONNECT_DATA=(SERVICE_NAME=ORACLE_DATABASE_SERVICE_NAME)))
```

Sample value:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=host1.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host3.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host4.example.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=svrce1)))
```

- One database instance supports one service

JDBC URL format:

```
jdbc:oracle:thin:@HOST_NAME.DOMAIN:PORT_NUMBER:ORACLE_DATABASE_SERVICE_NAME
```

Sample value:

```
jdbc:oracle:thin:@host1.example:1521:svrce1
```

- One database instance supports multiple services (for Oracle Database 10g and later)

JDBC URL format:

```
jdbc:oracle:thin:@//HOST_NAME.DOMAIN:PORT_NUMBER/ORACLE_DATABASE_SERVICE_NAME
```

Sample value:

```
jdbc:oracle:thin:@host1.example.com:1521/srvce1
```

2.3.3.5.2 Only Data Encryption and Integrity Is Configured If you have configured only data encryption and integrity, then enter the following values:

- **JDBC URL parameter**

While creating the connector, the value that you specify for the JDBC URL parameter must be in the following format:

```
jdbc:oracle:thin:@TARGET_HOST_NAME_or_IP_ADDRESS:PORT_NUM:sid
```

The following is a sample value for the JDBC URL parameter:

```
jdbc:oracle:thin:@ten.mydomain.com:1521:cust_db
```

- **Connection Properties parameter**

After you configure data encryption and integrity, the connection properties are recorded in the sqlnet.ora file. The value that you must specify for the Connection Properties parameter is explained by the following sample scenario:

See Also: *Oracle Database Advanced Security Administrator's Guide* for information about the sqlnet.ora file

Suppose the following entries are recorded in the sqlnet.ora file:

```
SQLNET.ENCRYPTION_SERVER=REQUIRED  
SQLNET.ENCRYPTION_TYPES_SERVER=(3DES168, DES40, DES, 3DES112)  
SQLNET.CRYPTO_CHECKSUM_SERVER=REQUESTED  
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER=(SHA1,MD5)
```

While creating the connector, you must specify the following as the value of the Connection Properties parameter:

Note:

- The property-value pairs must be separated by commas.
 - As shown in the following example, for the encryption_types and crypto_checksum_types properties, you can select any of the values recorded in the sqlnet.ora file.
-
-

```
oracle.net.encryption_client=REQUIRED,oracle.net.encryption_types_client=(3DES168),oracle.net.crypto_checksum_client=REQUESTED,oracle.net.crypto_checksum_types_client=(MD5)
```

2.3.3.5.3 Only SSL Communication Is Configured

After you configure SSL communication, the database URL is recorded in the `tnsnames.ora` file. See *Oracle Database Net Services Reference* for detailed information about the `tnsnames.ora` file.

The following are sample formats of the contents of the `tnsnames.ora` file. In these formats, `DESCRIPTION` contains the connection descriptor, `ADDRESS` contains the protocol address, and `CONNECT_DATA` contains the database service identification information.

Sample Format 1:

```
NET_SERVICE_NAME=
(DESCRIPTION=
  (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
  (CONNECT_DATA=
    (SERVICE_NAME=SERVICE_NAME) ) )
```

Sample Format 2:

```
NET_SERVICE_NAME=
(DESCRIPTION_LIST=
  (DESCRIPTION=
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
    (CONNECT_DATA=
      (SERVICE_NAME=SERVICE_NAME) ) )
  (DESCRIPTION=
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
    (CONNECT_DATA=
      (SERVICE_NAME=SERVICE_NAME) ) ) )
```

Sample Format 3:

```
NET_SERVICE_NAME=
(DESCRIPTION=
  (ADDRESS_LIST=
    (LOAD_BALANCE=on)
    (FAILOVER=off)
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) ) )
  (ADDRESS_LIST=
    (LOAD_BALANCE=off)
    (FAILOVER=on)
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) )
    (ADDRESS= ( PROTOCOL_ADDRESS_INFORMATION) ) )
  (CONNECT_DATA=
    (SERVICE_NAME=SERVICE_NAME) ) )
```

If you have configured only SSL communication and imported the certificate that you create on the target system host computer into the JVM certificate store of Oracle Identity Manager, then enter the following values:

JDBC URL parameter

While creating the connector, the value that you specify for the JDBC URL parameter must be derived from the value of `NET_SERVICE_NAME` in the `tnsnames.ora` file. For example:

Note: As shown in this example, you must include only the
 (ADDRESS= (PROTOCOL=TCPS) (HOST=*HOST_NAME*) (PORT=2484))
 element because you are configuring SSL. You need not include other
 (ADDRESS= (*PROTOCOL_ADDRESS_INFORMATION*)) elements.

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS) (HOST=myhost)
(PORT=2484))) (CONNECT_DATA=(SERVER=DEDICATED) (SERVICE_NAME=mysid)))
```

Connection Properties parameter

Whether or not you need to specify a value for the Connection Properties parameter depends on the certificate store into which you import the certificate:

- If you import the certificate into the certificate store of the JVM that Oracle Identity Manager is using, then you need not specify a value for the Connection Properties parameter.
- If you import the certificate into any other certificate store, then while creating the connector, specify a value for the Connection Properties parameter in the following format:

```
javax.net.ssl.trustStore=STORE_LOCATION, javax.net.ssl.trustStoreType=JKS, javax.net.ssl.trustStorePassword=STORE_PASSWORD
```

When you specify this value, replace *STORE_LOCATION* with the full path and name of the certificate store, and replace *STORE_PASSWORD* with the password of the certificate store.

2.3.3.5.4 Both Data Encryption and Integrity and SSL Communication Are Configured

If both data encryption and integrity and SSL communication are configured, then:

- **JDBC URL parameter**

While creating the connector, to specify a value for the JDBC URL parameter, enter a comma-separated combination of the values for the JDBC URL parameter described in [Section 2.3.3.5.2, "Only Data Encryption and Integrity Is Configured"](#) and [Section 2.3.3.5.3, "Only SSL Communication Is Configured"](#). For example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS) (HOST=myhost) (PORT=2484))) (CONNECT_DATA=(SERVER=DEDICATED) (SERVICE_NAME=mysid)))
```

- **Connection Properties parameter**

While creating the connector, to specify a value for the Connection Properties parameter, enter a comma-separated combination of the values for the Connection Properties parameter described in [Section 2.3.3.5.2, "Only Data Encryption and Integrity Is Configured"](#) and [Section 2.3.3.5.3, "Only SSL Communication Is Configured"](#). For example:

```
oracle.net.encryption_client=REQUIRED, oracle.net.encryption_types_client=(3DES168), oracle.net.crypto_checksum_client=REQUESTED, oracle.net.crypto_checksum_type_s_client=(MD5), javax.net.ssl.trustStore=STORE_LOCATION, javax.net.ssl.trustStoreType=JKS, javax.net.ssl.trustStorePassword=STORE_PASSWORD
```

As shown in the following example, for the `encryption_types` and `crypto_checksum_types` properties, you can select any of the values recorded in the `sqlnet.ora` file. When you specify this value, replace *STORE_LOCATION* with the full path and name of the certificate store, and replace *STORE_PASSWORD* with the password of the certificate store.

2.3.3.6 Configuring the IT Resource

The IT resource is automatically created when you run the Connector Installer. You must specify values for the parameters of the IT resource as follows:

Note:

A predefined IT resource is created when you run the Connector Installer:

For the User Management connector: EBS-APPS12

For the User Management with HR Foundation connector:
EBSHF-APPS12

For the User Management with TCA Foundation with connector:
EBSTCAF-APPS12

If you do not want to use this IT resource, then you must create a different IT resource of the eBusiness Suite UM IT resource type.

You must use the Administrative and User Console to configure the IT resource. Values set for the connection pooling parameters will not take effect if you use the Design Console to configure the IT resource.

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.x, expand **Resource Management**, and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.x, then:
 - On the Welcome to Oracle Identity Manager Self Service page, click **Advanced**.
 - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration section, click **Manage IT Resource**.
4. If you are using Oracle Identity Manager release 11.1.2.x or later, then:
 - Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
 - In the left pane, under Configuration, click **IT Resource**.
5. In the IT Resource Name field on the Manage IT Resource page, enter EBS-APPS12 and then click **Search**.
6. Click the edit icon for the IT resource. The following screenshot shows this page:

Manage IT Resource
Select an IT resource and the action that you want to perform on it.

IT Resource Name
IT Resource Type

Results 1-1 of 1 First | Previous | Next | Last

IT Resource Name	IT Resource Type	Edit	Delete
EBS-APPS12	eBusiness Suite UM		

First | Previous | Next | Last

7. From the list at the top of the page, select **Parameters**. The following screenshot shows this page:

Edit IT Resource Details and Parameters

You can view additional information about this IT resource:

IT Resource Name **EBS-APPS12**
IT Resource Type **eBusiness Suite UM**
Remote Manager

Parameter	Value
Retry Interval	<input type="text" value="10000"/>
Context User ID	<input type="text" value="0"/>
SSO Login Attribute	<input type="text"/>
Manage HR Record	<input type="text" value="No"/>
Inactive connection timeout	<input type="text" value="600"/>
Validate connection on borrow	<input type="text" value="true"/>
Statement Timeout	<input type="text" value="1200"/>
SSL Enabled	<input type="text" value="No"/>
Connection wait timeout	<input type="text" value="60"/>
ResourceConnection class definition	<input type="text"/>
Connection Retries	<input type="text" value="3"/>

8. Specify values for the parameters of the IT resource. [Table 2-6](#) describes each parameter.

Note: The ALL USERS group has READ permission on the default IT resource. This is to ensure that end users can select the IT resource during request-based provisioning. If you create another IT resource, then you must assign the READ permission for the ALL USERS group on the IT resource.

Table 2–6 IT Resource Parameters

Parameter	Description
Admin ID	<p>Enter the user name of the target system account to be used for provisioning operations.</p> <p>You create this account by performing the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations".</p> <p>Default value: apps</p>
Admin Password	<p>Enter the password of the target system account specified by the Admin ID parameter.</p>
Connection Properties	<p>Specify the connection properties for the target system database.</p> <p>See Section 2.3.3.5, "Determining Values for the JDBC URL and Connection Properties Parameters" for detailed information.</p>
Connection Retries	<p>Enter the number of consecutive attempts to be made at establishing a connection with the target system.</p> <p>Default value: 3</p>
Connection Timeout	<p>Enter the time in milliseconds within which the target system is expected to respond to a connection attempt.</p> <p>For a particular connection attempt, if the target system does not respond within the time interval specified by the Connection Timeout parameter, then it is assumed that the connection attempt has failed.</p> <p>Default value: 1200</p>
Context Application Name	<p>An application context is a set of elements associated with an artifact in Oracle E-Business Suite. The context implements user preferences and access control on the artifact. The Context Application Name, Context Responsibility Name, and Context User ID parameters define the context that is used for connector operations.</p> <p>For the Context Application Name parameter, enter the name of the application to which this user belongs.</p> <p>Default value: 0</p>
Context Responsibility Name	<p>Enter the responsibility assigned to the user in whose context connector operations are performed on the target system.</p> <p>Default value: 0</p>
Context User ID	<p>Enter the user ID of the user in whose context connector operations are performed on the target system.</p> <p>Default value: 0</p>
Enable Revoked User	<p>Enter yes if you want revoked resources to be enabled when the user name of the revoked resources are used to provision resources. Otherwise, enter no.</p> <p>When you perform a Revoke Account provisioning operation on an OIM User, the account of that user on the target system is disabled. If the Enable Revoked User parameter is set to yes and if you perform a Create Account provisioning operation for the same OIM User, then the account that was previously disabled on the target system is enabled. While performing the provisioning operation, you must specify the same User Name value as the one assigned to the account the first time. Field values that you provide during the Create Account operation are used to overwrite existing field values of the Oracle E-Business Suite account.</p> <p>Default value: yes</p>
JDBC URL	<p>Specify the JDBC URL for the target system database.</p> <p>See Section 2.3.3.5, "Determining Values for the JDBC URL and Connection Properties Parameters" for detailed information.</p>

Table 2–6 (Cont.) IT Resource Parameters

Parameter	Description
Manage HR Record	<p>If you have installed the connector in the User Management with HR Foundation connector, then set this parameter to <i>yes</i>. Otherwise, set the value to <i>no</i>.</p> <p>Note: If you are using the User Management with TCA Foundation connector, then do not set a value for this parameter.</p>
Minimum Password Length	<p>Enter the minimum number of characters that the password must contain.</p> <p>Note: If the minimum password length has been set on the target system, then the value of the Minimum Password Length IT resource parameter and minimum password length on the target system must be the same.</p> <p>Default value: 1</p>
Retry Interval	<p>Enter the interval in milliseconds between consecutive attempts at establishing a connection with the target system.</p> <p>Default value: 10000</p>
SSL Enabled	<p>Enter <i>yes</i> if you plan to configure SSL to secure communication between Oracle Identity Manager and the target system. Otherwise, enter <i>no</i>.</p> <p>Default value: <i>no</i></p>
SSO Enabled	<p>Enter <i>yes</i> if the target system is SSO enabled. Otherwise, enter <i>no</i>.</p> <p>Default value: <i>no</i></p>
SSO IT Resource	<p>This is the name of the IT resource created for the LDAP-based system.</p> <p>See Section 2.3.3.7, "SSO IT Resource" for information related to SSO IT Resource.</p>
SSO Identifier	<p>Enter the name of the attribute that uniquely identifies a user throughout all the systems on the organization. This attribute need not be the same as the attribute specified in the SSO Login Attribute parameter.</p> <p>For Oracle Internet Directory: <i>orclGUID</i></p> <p>For Microsoft Active Directory: <i>objectGUID</i></p> <p>For Sun Java System Directory: <i>nsUniqueID</i></p> <p>During a Create User provisioning operation, the connector takes the SSO Identifier value of the user from the LDAP-based system and populates it in the <i>USER_GUID</i> field of the target system.</p>
SSO Login Attribute	<p>Enter the name of the LDAP system user attribute that stores the user ID of users.</p> <p>For Oracle Internet Directory: <i>uid</i></p> <p>For Microsoft Active Directory: <i>SAMAccountName</i></p> <p>For Sun Java System Directory: <i>uid</i></p> <p>Sun Java System Directory and OID both use different attributes to store the user ID of users. You can specify the name of the attribute as the value of the SSO Login Attribute parameter.</p>
Statement Timeout	<p>Enter the time in milliseconds within which a query run on the target system is expected to return results.</p> <p>If the results of a query are not returned within the specified time, then it is assumed that the connection with the target system has failed. The connector then attempts to reestablish a connection with the target system.</p> <p>Default value: 1200</p>
Manage TCA Record	<p>If you have installed the connector in the User Management with TCA Foundation connector, then set this parameter to <i>yes</i>. Otherwise, set the value to <i>no</i>.</p> <p>Note: If you are using the User Management with HR Foundation connector, then do not set a value for this parameter.</p>

Table 2–6 (Cont.) IT Resource Parameters

Parameter	Description
TopologyName	<p>If you have installed the OAACG SIL provider, then enter the value of the Topology element in the SILConfig.xml file. See the SoD documentation for more information.</p> <p>Default value: None</p>
Configuration Lookup Name	<p>This parameter holds the name of the lookup definition that stores configuration information for connector operations. Depending on the connector that you are using, the value is one of the following:</p> <ul style="list-style-type: none"> ■ For the User Management connector: <code>Lookup.EBS.UM.Configuration</code> ■ For the User Management with HR Foundation connector: <code>Lookup.EBS.UMHRMS.Configuration</code> ■ For the User Management with TCA Foundation connector: <code>Lookup.EBS.UMTCA.Configuration</code> <p>You must not change the value of this parameter. However, if you create a copy of this lookup definition, then you can enter the name of the newly created lookup definition as the value of the Configuration Lookup Name parameter.</p>
Connection Pooling Parameters	
Abandoned connection timeout	<p>Time (in seconds) after which a connection must be automatically closed if it is not returned to the pool</p> <p>Note: You must set this parameter to a value that is high enough to accommodate processes that take a long time to complete (for example, full reconciliation).</p> <p>Default value: 600</p>
Connection wait timeout	<p>Maximum time (in seconds) for which the connector must wait for a connection to be available</p> <p>Default value: 60</p>
Inactive connection timeout	<p>Time (in seconds) of inactivity after which a connection must be dropped and replaced by a new connection in the pool</p> <p>Default value: 600</p>
Initial pool size	<p>Number of connections that must be established when the connection pool is initialized</p> <p>The pool is initialized when it receives the first connection request from a connector.</p> <p>Default value: 1</p> <p>Sample value: 3</p>
Max pool size	<p>Maximum number of connections that must be established in the pool at any point of time</p> <p>This number includes the connections that have been borrowed from the pool.</p> <p>Default value: 100</p> <p>Sample value: 30</p>
Min pool size	<p>Minimum number of connections that must be in the pool at any point of time</p> <p>This number includes the connections that have been borrowed from the pool.</p> <p>Default value: 5</p>

Table 2–6 (Cont.) IT Resource Parameters

Parameter	Description
Validate connection on borrow	<p>Specifies whether or not a connection must be validated before it is lent by the pool</p> <p>The value can be <code>true</code> or <code>false</code>. It is recommended that you set the value to <code>true</code>.</p> <p>Default value: <code>false</code></p>
Timeout check interval	<p>Time interval (in seconds) at which the other timeouts specified by the other parameters must be checked</p> <p>Default value: 30</p>
Pool preference	<p>Preferred connection pooling implementation</p> <p>Value: <code>Default</code></p> <p>Note: Do not change this value of this parameter.</p>
Connection pooling supported	<p>Enter <code>true</code> if you want to enable connection pooling for this target system installation. Otherwise, enter <code>false</code>.</p> <p>Default value: <code>false</code></p>
Target supports only one connection	<p>Indicates whether the target system can support one or more connections at a time</p> <p>Value: <code>false</code></p> <p>Note: Do not change the value of this parameter.</p>
ResourceConnection class definition	<p>Implementation of the ResourceConnection class</p> <p>Value: <code>oracle.iam.connectors.ebs.common.vo.EBSResourceConnectionImpl</code></p> <p>Note: Do not change the value of this parameter. The value in this parameter is used only when the Connection pooling supported IT resource parameter is set to <code>True</code>.</p>
Native connection pool class definition	<p>Wrapper to the native pool mechanism that implements the GenericPool</p> <p>Note: Do not specify a value for this parameter.</p>
Pool excluded fields	<p>Comma-separated list of IT parameters whose change must not trigger a refresh of the connector pool</p> <p>Value: Configuration Lookup Name,Manage TCA Record,Enable Revoked User,Statement Timeout,Context User ID,Context Application Name,Context Responsibility Name,TopologyName,SSO Enabled,SSO Identifier,SSO Login Attribute,SSO IT Resource,Manage HR Record</p> <p>Note:</p> <p>Do not change the value of this parameter unless you are adding or deleting a parameter from the IT resource. You must ensure that the total length of the list does not exceed 2000 characters. If you are adding a parameter to the IT resource, then that parameter name must be added to the above list with a comma separator. If you are deleting a parameter from the IT resource, then that parameter must be removed from the list if it exists in the list.</p> <p>You must restart Oracle Identity Manager for changes that you make to this parameter to take effect.</p>

9. To save the values, click **Save**.

Additional Configuration Step for Connection Pooling

If you are using Oracle Identity Manager release 9.1.0.x that is running on Oracle Application Server, then edit the `opmn.xml` file as follows:

1. Open the following file in a text editor:

OAS_HOME/opmn/conf/opmn.xml

2. Search for the following block of lines:

```
<process-type id="home" module-id="OC4J" status="enabled">
<module-data>
<category id="start-parameters">
```

3. After this block of lines, add the following line:

```
<data id="oc4j-options" value="-userThreads"/>
```

4. Save and close the file.

5. Restart the server.

2.3.3.7 SSO IT Resource

Perform the procedure mentioned below to set the value of SSO IT Resource field to LDAP System:

1. Create a new IT Resource type, named for example LDAP system, with the following fields:

- Server Address
- Port
- Root DN
- Admin Id
- Admin Password

Note: Click the encrypted check box here

- SSL

You can provide default values or populate values as mentioned in the following step.

2. Create a new IT Resource, named for example LDAP system with the following field values:
 - Server Address: Host name or IP address of the machine where LDAP is running
 - Port: LDAP port
 - Root DN: DN of the container under which users are stored in LDAP
 - Admin Id: DN to bind to LDAP
 - Admin Password: Password of the DN to bind to LDAP
 - SSL: True or False
3. Modify EBS-APPS12 IT resource, and set the value of field SSO IT Resource to be LDAP System.

2.3.3.8 Disabling the Auto Save Form Feature on Oracle Identity Manager Releases 11.1.x and 11.1.2.x

Note: If you want to configure the request-based provisioning feature of the connector on Oracle Identity Manager releases 11.1.x and 11.1.2.x, then skip this section.

The Auto Save Form option is meant for request-based provisioning in Oracle Identity Manager release 9.1.0.x. When you deploy the connector, this option is enabled by default. However, Oracle Identity Manager releases 11.1.x and 11.1.2.x does not use object forms. If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then disable the Auto Save Form option as follows:

1. Log in to the Design Console.
2. Expand **Process Management**, and then double-click **Process Definition**.
3. Search for and open the process definition for the connector that you are using:
See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
4. Deselect the **Auto Save Form** check box.
5. Click the Save icon.

2.3.3.9 Enabling Request-Based Provisioning

In request-based provisioning, an end user creates a request for a resource or entitlement by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource or entitlement on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

Note: Direct provisioning allows the provisioning of multiple Oracle E-Business Suite accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in one of the following sections:

- [Section 2.3.3.9.1, "Enabling Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x"](#)
- [Section 2.3.3.9.2, "Enabling Request-Based Provisioning on Oracle Identity Manager Releases 11.1.x and 11.1.2.x:"](#)

2.3.3.9.1 Enabling Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x

When you run the Connector Installer, the request-based provisioning of accounts is automatically enabled. If you also want to enable request-based provisioning of entitlements, then perform the procedure described in this section.

This section covers the following topics:

Prerequisites

You must run Oracle Identity Manager in INFO mode when you import the XML file for request-based provisioning. If Oracle Identity Manager is running in DEBUG mode when you import the XML file, then the import operation does not work correctly.

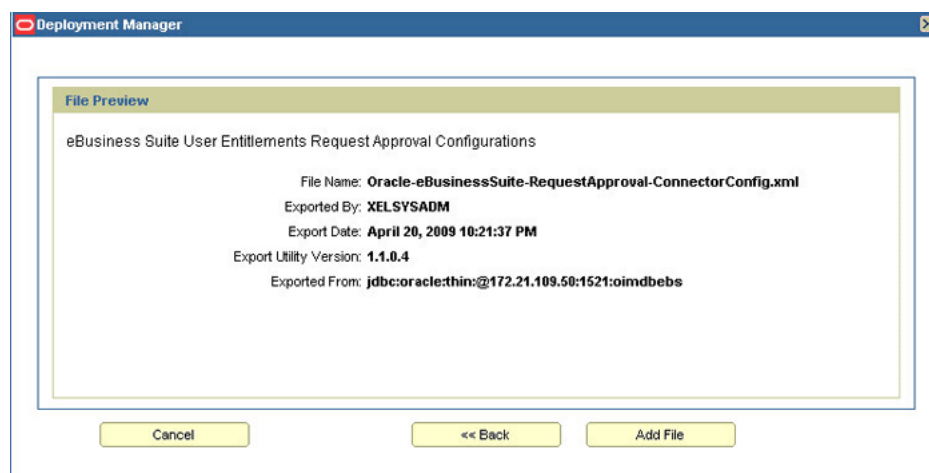
Before you perform this procedure, set your browser to use JRE version 1.6.0_07. If you try to import the XML file with your browser set to any other JRE version, then the browser stops responding.

To enable request-based provisioning of entitlements:

Note: Before you perform this procedure, set your browser to use JRE version 1.6.0_07. If you try to import the XML file with your browser set to any other JRE version, then the browser stops responding.

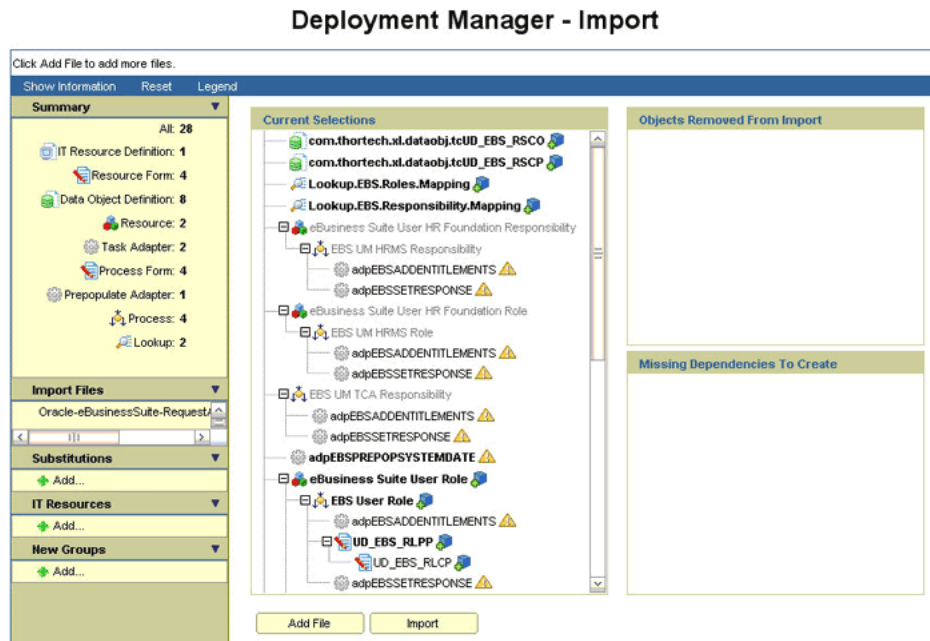
1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open one of the following XML files:
 - For the User Management connector:
Oracle-eBusinessSuite-RequestApproval-ConnectorConfig.xml
 - For the User Management with HR Foundation connector:
Oracle-eBusinessSuite-HRMS-RequestApproval-ConnectorConfig.xml
 - For the User Management with TCA Foundation connector:
Oracle-eBusinessSuite-TCA-RequestApproval-ConnectorConfig.xml

Details of the XML file that you select are shown on the File Preview page. The following screenshot shows this page:



5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **View Selections**.

At this stage, the Deployment Manager Import page should not show an error. See the following screenshot:



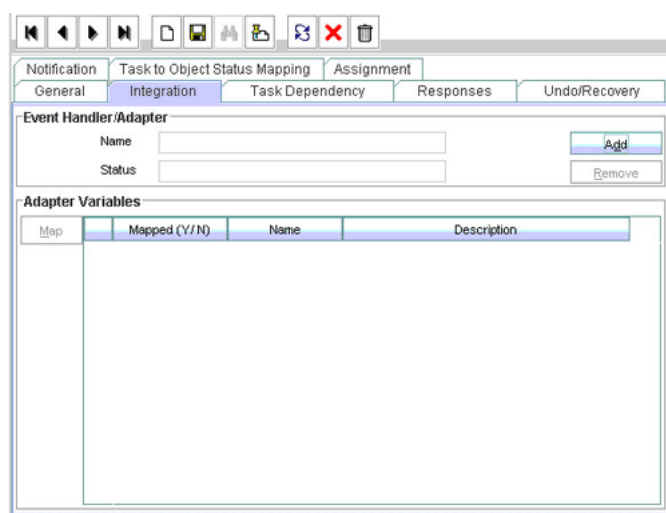
8. Click **Import.**

In the message that is displayed, click **Import** to confirm that you want to import the XML file and then click **OK**.

To suppress the Standard Approval process definition:

Note: The Standard Approval process is common to all resource objects. If you enable request-based provisioning, then you must suppress this process definition.

1. On the Design Console, expand **Process Management** and double-click **Process Definition**.
2. Search for and open the **Standard Approval** process definition.
3. On the Tasks tab, double-click the **Approve** task.
4. On the Integration tab of the Editing Task dialog box, click **Add**. The following screenshot shows this page:



5. In the Handler Selection dialog box:
 Select **System**.
 Select the **tcCompleteTask** handler.
 Click the Save icon, and then close the dialog box.
6. In the Editing Task dialog box, click the Save icon and close the dialog box.
7. Click the Save icon to save changes made to the process definition.

2.3.3.9.2 Enabling Request-Based Provisioning on Oracle Identity Manager Releases 11.1.x and 11.1.2.x:

To enable request-based provisioning, perform the following procedures:

- [Copying Predefined Request Datasets](#)
- [Importing Request Datasets into MDS](#)
- [Enabling the Auto Save Form Feature](#)
- [Running the PurgeCache Utility](#)

Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following is the list of predefined request datasets available in the DataSets directory on the installation media:

- ProvisionResource_eBusinessSuiteUser.xml
- ProvisionResource_eBusinessSuiteUser_HRFoundation.xml
- ProvisionResource_eBusinessSuiteUser_TCAFoundation.xml
- ModifyProvisionedResource_eBusinessSuiteUser.xml
- ModifyProvisionedResource_eBusinessSuiteUser_HRFoundation.xml
- ModifyProvisionedResource_eBusinessSuiteUser_TCAFoundation.xml

Copy the files from the DataSets directory on the installation media to the `OIM_HOME/DataSet/file` directory.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information on modifying request datasets.

Importing Request Datasets into MDS

Note: In an Oracle Identity Manager cluster, perform this step on each node of the cluster.

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into the MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.
2. In a command window, change to the `OIM_HOME/server/bin` directory.
3. Run one of the following commands:
 - On Microsoft Windows
`weblogicImportMetadata.bat`
 - On UNIX
`weblogicImportMetadata.sh`
4. When prompted, enter values for the following:
 - Please enter your username [weblogic]
Enter the username used to log in to the Oracle WebLogic Server
Sample value: `WL_User`
 - Please enter your password [weblogic]
Enter the password used to log in to the Oracle WebLogic Server
 - Please enter your server URL [t3://localhost:7001]
Enter the URL of the application server in the following format:
`t3://HOST_NAME_IP_ADDRESS:PORT`
In this format, replace:
 - `HOST_NAME_IP_ADDRESS` with the host name or IP address of the computer on which Oracle Identity Manager is installed.
 - `PORT` with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS.

Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management**, and then double-click **Process Definition**.
3. Search for and open the process definition for the connector that you are using:
See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See [Section 2.3.3.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#) for instructions.

The procedure to enable request-based provisioning ends with this step.

2.3.4 Localizing Field Labels in UI Forms

Note: Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.x or later and you want to localize UI form field labels.

To localize field label that you add to in UI forms:

1. Publish the sandbox containing application instance form that is supposed to be localized.
2. Export the MDS file, `/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf`. In this file, you can see message keys and messages to be localized.
`sessiondef.oracle.iam.ui.runtime.form.model.testAppInstance.entity.testAppInstanceEO.U`
`D_TES8393_ACCOUNTID__c_LABEL`

See Also: "Deploying and Undeploying Customizations" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*, for more information about exporting metadata files

3. Export the file to localize, for example, for German:
`/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle_de.xlf`

Note: This file may not exist in MDS. If it does not exist, create a new one, but path must be the same.

4. Provide localization for messages in German, follow the same format as in the file exported in step 2.

See Also: *Oracle Fusion Applications Extensibility Guide* for more information about translating resource bundles from metadata services metadata repository

5. Import `/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle_de.xlf` back to MDS.
6. Logout and relogin.

2.4 Postcloning Steps

You can clone this connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

See Also: The "Managing Connector Lifecycle" chapter of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about cloning connectors and the steps mentioned in this section

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- Adapter Tasks

Ensure that all the cloned Oracle E-Business Suite adapter literal variables are referring to the current process form fields. If not, reference the adapter literal variables by correcting them and build the adapter again.

- Lookup Definition

Verify the lookup entries in all lookup definitions to ensure that the code keys of the lookup definition are referring to the appropriate cloned form fields. If not, reference the code keys to the appropriate fields of the cloned form.

You can perform child form related operations by performing the following steps:

1. On the Design Console, expand **Development Tools** and double-click **Form Designer**.
2. Search for and open the process form for the connector that you are using.
3. Click **Create New Version** to create a version of cloned child forms.
For example, UD_EBS_RESP and UD_EBS_RLS.
4. Go to the Properties tab.
5. Select **Lookup Query** from the list to modify the lookup name and column name.
6. Click the Save icon.
7. Click **Make Version Active** to activate the new version of the process form.

Using the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

Note: These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- [Section 3.1, "Setting Up Lookup Definitions in Oracle Identity Manager"](#)
- [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#)
- [Section 3.3, "Configuring Reconciliation"](#)
- [Section 3.4, "Configuring Scheduled Tasks"](#)
- [Section 3.5, "Attributes for Which You Can Specify Values During New Resource and Entitlement Provisioning"](#)
- [Section 3.6, "Provisioning Operations Performed in an SoD-Enabled Environment"](#)
- [Section 3.7, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.x"](#)
- [Section 3.8, "Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later"](#)
- [Section 3.9, "Uninstalling the Connector"](#)

3.1 Setting Up Lookup Definitions in Oracle Identity Manager

This Section discusses the following topics:

- [Section 3.1.1, "Setting Up the Configuration Lookup Definition for SSO Password Update"](#)
- [Section 3.1.2, "Setting Up the Configuration Lookup Definition"](#)

3.1.1 Setting Up the Configuration Lookup Definition for SSO Password Update

Depending on the connector that you are using, add the `IS_SSO_EBS_BIDIRECTIONAL` entry to the following lookup definition:

- For User Management connector: `Lookup.EBS.UM.Configuration`

- For User Management with HR Foundation connector:
Lookup.EBS.UMHRMS.Configuration
- For User Management with TCA Foundation connector:
Lookup.EBS.UMTCA.Configuration

If the target system is configured with SSO, then the password update operation can be controlled by adding the IS_SSO_EBS_BIDIRECTIONAL entry.

If you enter the value as Yes , it will proceed to update the user's password.

If you enter the value as No , the "Password Updated" task will be rejected with the following message:

Password update is not supported if the target system is protected by SSO

3.1.2 Setting Up the Configuration Lookup Definition

Depending on the connector that you are using, you must provide Decode values for some of the entries of the following lookup definition that holds configuration information.

To set a Decode value for an entry in a lookup definition:

1. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
2. Search for and open the lookup definition that you want to modify.
3. Enter the value in the **Decode** column for the Code Key that you want to set.
4. Click the Save icon.

Depending on the connector that you are using, see one of the following section for information about the Code Key entries for which you must specify values:

- [Section 3.1.2.1, "Setting Up the Lookup.EBS.UM.Configuration Lookup Definition"](#)
- [Section 3.1.2.2, "Setting Up the Lookup.EBS.UMHRMS.Configuration Lookup Definition"](#)
- [Section 3.1.2.3, "Setting Up the Lookup.EBS.UMTCA.Configuration Lookup Definition"](#)

3.1.2.1 Setting Up the Lookup.EBS.UM.Configuration Lookup Definition

If you are using the User Management connector, then provide a Decode value for the following entries of the Lookup.EBS.UM.Configuration lookup definition:

- USE_CONNECTION_POOLING

If you want the connector to use connection pooling, then set the value of the USE_CONNECTION_POOLING Code Key to Yes. See [Section 1.5.12, "Connection Pooling"](#) for more information about this feature.

- TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT

You use the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries to specify the format to which you want to convert values that are fetched from the date-type target system columns during reconciliation.

The RECON_DATE_FORMAT entry holds the Java-equivalent date format of the format specified in the TO_CHAR_DATE_FORMAT entry. [Table 3–1](#) lists SQL date formats and the corresponding Java date formats that you can enter as the Decode

value of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries, respectively.

Table 3–1 Date Formats That Can Be Entered as the Values of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT Entries

Value for TO_CHAR_DATE_FORMAT	Value for RECON_DATE_FORMAT
dd-Mon-yy	dd-MMM-yy
dd-Mon-yyyy	dd-MMM-yyyy
dd-mm-yy	dd-MM-yy
dd-mm-yyyy	dd-MM-yyyy

By default, the value of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries is set to dd-Mon-yy and dd-MMM-yy, respectively. Therefore, by default, during reconciliation, all values that are fetched from date-type target system columns are converted to the dd-Mon-yy format.

To convert the format of values fetched from date-type target system columns:

1. In a text editor, open the ebsERQuery.properties file.
2. Specify the date format to which you want to convert values fetched from the date-type target system columns during reconciliation.

Note: See the "TO_CHAR_DATE_FORMAT" column of [Table 3–1](#) for a list of date formats that you can specify.

For example, change:

```
TO_CHAR (PAPF.EFFECTIVE_START_DATE) AS
EFFECTIVE_START_DATE
```

to:

```
TO_CHAR (PAPF.EFFECTIVE_START_DATE, 'dd-Mon-yyyy') AS
EFFECTIVE_START_DATE.
```

3. Save and close the file.
4. Configure the **Lookup.EBS.UM.Configuration** lookup definition as follows:
 - a. In the **Decode** column of the TO_CHAR_DATE_FORMAT Code Key, enter the date format specified in the ebsERQuery.properties file. For example, enter dd-Mon-yyyy.
 - b. In the **Decode** column of the RECON_DATE_FORMAT Code Key, enter the Java-equivalent date format of the format specified in Step 4.e. For example, enter dd-MMM-yyyy.

Note: See [Table 3–1](#) for information about the Java-equivalent date format that must be specified.

- c. Click the Save icon.
- UMX_REVOKE_ROLE_PROC

If you want to perform a revoke role provisioning operation by using the target system account created for performing connector operations, then change the decode value from {CALL

```
OIM_UMX_ACCESS_ROLES_PVT.revokeUserRole(?, ?, ?) } to {CALL  
UMX_ACCESS_ROLES_PVT.revokeUserRole(?, ?, ?) } .
```

Note that you need not perform this change if you are using the APPS account for performing this revoke role provisioning operation, as it points to the custom wrapper package.

3.1.2.2 Setting Up the Lookup.EBS.UMHRMS.Configuration Lookup Definition

If you are using the User Management with HR Foundation connector, then provide Decode values for the following entries of the Lookup.EBS.UMHRMS.Configuration lookup definition:

- **USE_CONNECTION_POOLING**

If you want the connector to use connection pooling, then set the value of the USE_CONNECTION_POOLING Code Key to Yes. See [Section 1.5.12, "Connection Pooling"](#) for more information about this feature.

- **UD_EBSH_USR_BIZGRPID and UD_EBSH_USR_PERTYPEID**

Business Group ID and Person Type ID are two of the attributes on the process form. By entering values for these attributes, you specify the subset of HRMS person records that must be considered for connector operations. The values that you specify for these fields are used during provisioning operations. Alternatively, you can set values for these attributes in the UD_EBSH_USR_BIZGRPID and UD_EBSH_USR_PERTYPEID entries of the Lookup.EBS.UMHRMS.Configuration lookup definition. During a provisioning operation, if you do not enter values for these attributes on the process form, then the connector uses the Decode values of the UD_EBSH_USR_BIZGRPID and UD_EBSH_USR_PERTYPEID entries.

Note: These entries in the lookup definition are also used during request-based provisioning.

To determine the Decode value for the UD_EBSH_USR_BIZGRPID Code Key, run the following query on the target system database:

```
SELECT business_group_id FROM hr_all_organization_units WHERE business_group_id  
= organization_id and hr_all_organization_units.name = 'ORGANIZATION_NAME'
```

To determine the Decode value for the UD_EBSH_USR_PERTYPEID Code Key, run the following query on the target system database:

```
SELECT person_type_id, user_person_type FROM per_person_types WHERE  
business_group_id = BUSINESS_GROUP_ID AND system_person_type = 'EMP'
```

In this query, replace the *BUSINESS_GROUP_ID* with the value returned from the query for the UD_EBSH_USR_BIZGRPID Code Key. This query returns the Person Type ID for records that are of the EMP type, for example, Employee, Retiree, and Contractor.

- **TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT**

You use the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries to specify the format to which you want to convert values that are fetched from the date-type target system columns during reconciliation.

The RECON_DATE_FORMAT entry holds the Java-equivalent date format of the format specified in the TO_CHAR_DATE_FORMAT entry. [Table 3–1](#) lists SQL date formats and the corresponding Java date formats that you can enter as the Decode value of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries, respectively.

Table 3–2 Date Formats That Can Be Entered as the Values of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT Entries

TO_CHAR_DATE_FORMAT	RECON_DATE_FORMAT
dd-Mon-yy	dd-MMM-yy
dd-Mon-yyyy	dd-MMM-yyyy
dd-mm-yy	dd-MM-yy
dd-mm-yyyy	dd-MM-yyyy

By default, the value of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries is set to dd-Mon-yy and dd-MMM-yy, respectively. Therefore, by default, during reconciliation, all values that are fetched from date-type target system columns are converted to the dd-Mon-yy format.

To convert the format of values fetched from date-type target system columns:

1. In a text editor, open the ebsERQuery.properties file.
2. Specify the date format to which you want to convert values fetched from the date-type target system columns during reconciliation.

Note: See the "TO_CHAR_DATE_FORMAT" column of [Table 3–1](#) for a list of date formats that you can specify.

For example, change:

```
TO_CHAR (PAPF.EFFECTIVE_START_DATE) AS
EFFECTIVE_START_DATE
```

to:

```
TO_CHAR (PAPF.EFFECTIVE_START_DATE, 'dd-Mon-yyyy') AS
EFFECTIVE_START_DATE.
```

3. Save and close the file.
4. Configure the **Lookup.EBS.UMHRMS.Configuration** lookup definition as follows:
 - a. In the **Decode** column of the TO_CHAR_DATE_FORMAT Code Key, enter the date format specified in the ebsERQuery.properties file. For example, enter dd-Mon-yyyy.
 - b. In the **Decode** column of the RECON_DATE_FORMAT Code Key, enter the Java-equivalent date format of the format specified in Step 4.e. For example, enter dd-MMM-yyyy.

Note: See [Table 3–1](#) for information about the Java-equivalent date format that must be specified.

c. Click the Save icon.

- **UMX_REVOKE_ROLE_PROC**

If you want to perform a revoke role provisioning operation by using the target system account created for performing connector operations, then change the decode value from {CALL

```
OIM_UMX_ACCESS_ROLES_PVT.revokeUserRole(?, ?, ?) } to {CALL
UMX_ACCESS_ROLES_PVT.revokeUserRole(?, ?, ?) } .
```

Note that you need not perform this change if you are using the APPS account for performing this revoke role provisioning operation, as it points to the custom wrapper package.

3.1.2.3 Setting Up the Lookup.EBS.UMTCA.Configuration Lookup Definition

If you are using the User Management with TCA Foundation connector, then provide Decode values for the following entries of the Lookup.EBS.UMTCA.Configuration lookup definition:

- **USE_CONNECTION_POOLING**

If you want the connector to use connection pooling, then set the value of the USE_CONNECTION_POOLING Code Key to Yes. See [Section 1.5.12, "Connection Pooling"](#) for more information about this feature.

- **TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT**

You use the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries to specify the format to which you want to convert values that are fetched from the date-type target system columns during reconciliation.

The RECON_DATE_FORMAT entry holds the Java-equivalent date format of the format specified in the TO_CHAR_DATE_FORMAT entry. [Table 3–1](#) lists SQL date formats and the corresponding Java date formats that you can enter as the Decode value of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries, respectively.

Table 3–3 Date Formats That Can Be Entered as the Values of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT Entries

TO_CHAR_DATE_FORMAT	RECON_DATE_FORMAT
dd-Mon-yy	dd-MMM-yy
dd-Mon-yyyy	dd-MMM-yyyy
dd-mm-yy	dd-MM-yy
dd-mm-yyyy	dd-MM-yyyy

By default, the value of the TO_CHAR_DATE_FORMAT and RECON_DATE_FORMAT entries is set to dd-Mon-yy and dd-MMM-yy, respectively. Therefore, by default, during reconciliation, all values that are fetched from date-type target system columns are converted to the dd-Mon-yy format.

To convert the format of values fetched from date-type target system columns:

1. In a text editor, open the ebsERQuery.properties file.
2. Specify the date format to which you want to convert values fetched from the date-type target system columns during reconciliation.

Note: See the "TO_CHAR_DATE_FORMAT" column of [Table 3–1](#) for a list of date formats that you can specify.

For example, change:

```
TO_CHAR (PAPF.EFFECTIVE_START_DATE) AS
EFFECTIVE_START_DATE
```

to:

```
TO_CHAR (PAPF.EFFECTIVE_START_DATE, 'dd-Mon-yyyy') AS
EFFECTIVE_START_DATE.
```

3. Save and close the file.
4. Configure the **Lookup.EBS.UMTCA.Configuration** lookup definition as follows:
 - a. In the **Decode** column of the TO_CHAR_DATE_FORMAT Code Key, enter the date format specified in the ebsERQuery.properties file. For example, enter dd-Mon-yyyy.
 - b. In the **Decode** column of the RECON_DATE_FORMAT Code Key, enter the Java-equivalent date format of the format specified in Step 4.e. For example, enter dd-MMM-yyyy.

Note: See [Table 3–1](#) for information about the Java-equivalent date format that must be specified.

- c. Click the Save icon.
- UMX_REVOKE_ROLE_PROC

If you want to perform a revoke role provisioning operation by using the target system account created for performing connector operations, then change the decode value from {CALL

```
OIM_UMX_ACCESS_ROLES_PVT.revokeUserRole(?, ?, ?) } to {CALL
UMX_ACCESS_ROLES_PVT.revokeUserRole(?, ?, ?) }.
```

Note that you need not perform this change if you are using the APPS account for performing this revoke role provisioning operation, as it points to the custom wrapper package.

3.2 Scheduled Task for Lookup Field Synchronization

Note: In Oracle Identity Manager releases 11.1.x and 11.1.2.x, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.x is the same as the term **scheduled job** in the context of Oracle Identity Manager releases 11.1.x and 11.1.2.x.

See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

The eBusiness UM Lookup Definition Reconciliation scheduled task is used for lookup field synchronization.

Note: The procedure to configure this scheduled task is described later in the guide.

The descriptions of some attributes also instruct you not to change the default values. However, if you create a copy of this scheduled task, then you can enter attribute values specific to the target system installation for which you create the copy of scheduled task. See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for more information about creating copies of connector objects.

You must specify values for attributes whose default value is the "Enter a value" string.

[Table 3–4](#) describes the attributes of this scheduled task.

Table 3–4 Attributes of the eBusiness UM Lookup Definition Reconciliation Scheduled Task

Attribute	Description
Query Properties File	Enter the full path and name of the file containing the lookup definition synchronization query that you want to run. Sample value: /usr/temp/ebsUMLookupQuery.properties
IT Resource Name	Enter the name of the IT resource that you configure by performing the procedure described in Section 2.3.3.6, "Configuring the IT Resource" . Sample value: EBS-APPS12
Lookup Definition Name	Enter the name of the lookup definition that you want to synchronize with the target system. You can specify one of the following lookup definitions: <ul style="list-style-type: none"> Lookup.EBS.Application Lookup.EBS.Responsibility Lookup.EBS.UMX.Roles Lookup.EBS.SecurityGroup
Task Name	This attribute holds the name of the scheduled task. Value: eBusiness UM Lookup Definition Reconciliation Note: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that scheduled task as the value of the attribute in that scheduled task.

Note: The `IllegalArgumentException` exception is thrown if lookup field data synchronized by the connector contains characters that are treated as illegal by Oracle Identity Manager. When a record containing an illegal character is encountered, the connector skips that record and proceeds to reconcile other records.

You can search for the string `Skipped code =` in the log to track down the entry that caused the exception.

For information about special characters that are supported by Oracle Identity Manager, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x:
Oracle Identity Manager Globalization Guide
 - For Oracle Identity Manager releases 11.1.x and 11.1.2.x:
Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager
-

3.3 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- [Section 3.3.1, "Reconciliation Time Stamp"](#)
- [Section 3.3.2, "Batched Reconciliation"](#)
- [Section 3.3.3, "Configuring Limited Reconciliation"](#)
- [Section 3.3.4, "Reconciliation Scheduled Tasks"](#)

3.3.1 Reconciliation Time Stamp

This section describes the Last Execution Time attribute of the scheduled task.

The Last Execution Time attribute holds the time stamp at which the last reconciliation run started. This attribute is used in conjunction with the reconciliation query specified by the Query Name attribute. During a reconciliation run, only target system records added or modified after the time stamp value stored in the Last Execution Time attribute are fetched into Oracle Identity Manager for reconciliation.

Apply the following guidelines while deciding on a value for the Last Execution Time attribute:

- For a particular reconciliation mode, if you want to fetch all target system records for reconciliation, then set the value of the attribute to 0.
- If you want to specify a time stamp, then first run the following query to convert the time stamp into the required format:

```
SELECT (TO_DATE('DATE_TO_BE_CONVERTED', 'DD-MON-YYYY') - TO_DATE('01011970',
'DDMMYYYY')) *24*60*60*1000 as ts FROM DUAL
```

In this query, replace `DATE_TO_BE_CONVERTED` with the date that you want to use as the time stamp. For example, if you want to use 5-Dec-2008 as the time stamp, then run the following query:

```
SELECT (TO_DATE('5-Dec-2008','DD-MON-YYYY') - TO_DATE('01011970','DDMMYYYY'))
*24*60*60*1000 as ts FROM DUAL
```

The query returns the following value:

1228435200000

Specify this value as the value of the Last Execution Time attribute.

- The Last Execution Time attribute is updated during each reconciliation run. For example, the Last Execution Time attribute is set to the time stamp at which the run begins.

3.3.2 Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify a value for the Batch Size user reconciliation scheduled task attribute. The value that you specify is the number of records that must be included in each batch. The default value is 1000.

3.3.3 Configuring Limited Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to add filter parameters for reconciliation. The alternative to performing this procedure is to add a condition directly in the WHERE clause of the reconciliation query that you want to run.

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by adding a filter parameter in the reconciliation query and specifying a value for the parameter in the, for example, Lookup.EBS.UM.QueryFilters lookup definition.

For example, you can add a parameter in the WHERE clause of the UM_USER_RECON query so that it returns FND_USER records whose user name is the one that you specify in the lookup definition.

To add a filter parameter in a reconciliation query:

Note: Before you modify a query in the properties file, you must run the query by using any standard database client to ensure that the query produces the required results when it is run against the target system database.

1. Modify the query as follows:
 - a. Open the properties file in a text editor.

- b. Add the condition in the WHERE clause of the query that you want to modify.

Note: The parameter name must begin with the colon (:) as a prefix. In addition, there must be no space between the colon and parameter name and within the parameter name.

For example, in the following snippet of the UM_USER_RECON query, the variable condition highlighted in bold has been added:

```
round((rolegrp.LAST_UPDATE_DATE - to_date('01011970', 'ddmmyyyy'))
* 1440 * 60 * 1000)> :lastExecutionTime \
GROUP BY rolegrp.USER_NAME, fnd.EMPLOYEE_ID, fnd.USER_ID,
fnd.DESCRPTION, fnd.EMAIL_ADDRESS, fnd.FAX, \
fnd.START_DATE, fnd.END_DATE) \
) usr where UPPER(USER_NAME) = UPPER(:username)
```

- c. Save and close the file.
2. Configure the Lookup.EBS.UM.QueryFilters lookup definition as follows:
 - a. Log in to the Design Console.
 - b. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - c. Search for and open the **Lookup.EBS.UM.QueryFilters** lookup definition.
 - d. To add a row, click **Add**.
 - e. In the **Code Key** column, enter the variable name that you specified in the properties file. Do not include the colon (:) character. For example, enter username in the Code Key column.
 - f. In the **Decode** column, enter the value that you want to assign to the parameter for subsequent reconciliation runs. Use one of the following formats to specify a value:

– *value* | DATE | DATE_FORMAT

Sample value: 1-Dec-1975 | DATE | DD-Mon-YYYY

Note: For the USER NAME example, you can enter the following sample value.

– *value* | STRING

Sample value: jdoe | STRING

– *value* | NUMBER

Sample value: 33 | NUMBER

- g. Click the Save icon.

When you next run the query that you have modified, the condition that you add is applied as an additional filter during reconciliation.

3.3.4 Reconciliation Scheduled Tasks

The following scheduled tasks are used to reconcile user data:

- The eBusiness UM Target Resource User Reconciliation scheduled task is used for the User Management connector.
- The eBusiness UM Target Resource User-HRMS Reconciliation scheduled task is used for the User Management with HR Foundation connector.
- The eBusiness UM Target Resource User-TCA Reconciliation scheduled task is used for the User Management with TCA Foundation connector.

[Table 3–5](#) describes the attributes of these scheduled tasks.

Note:

- Any updates made to the First Name and Last Name fields are retrieved only from the FND user form, and not from Oracle E-Business HRMS or Oracle E-Business TCA.
 - Values for most attributes are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
 - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.
 - The descriptions of some attributes also instruct you not to change the default values. However, if you create a copy of this scheduled task, then you can enter attribute values specific to the target system installation for which you create the copy of scheduled task. See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for more information about creating copies of connector objects.
-

Table 3–5 Attributes of the eBusiness UM Target Resource User Reconciliation Scheduled Task

Attribute	Description
Recon Lookup Definition	<p>This attribute holds the name of the lookup definition that holds mappings between the target system with the process form fields.</p> <ul style="list-style-type: none"> ■ Value for the User Management connector: <code>Lookup.EBS.UM.UserRecon</code> ■ Value for the User Management with HR Foundation connector: <code>Lookup.EBS.UM.UserHRMSRecon</code> ■ Value for the User Management with TCA Foundation connector: <code>Lookup.EBS.UM.UserTCAREcon</code> <p>Note: You must not change this value.</p>
Target Date Format	<p>Enter the format of date values stored in the target system database.</p> <p>Default value: <code>MM/dd/yyyy hh:mm:ss</code></p>
Query Properties File	<p>Enter the full path and name of the file containing the user reconciliation query that you want to run.</p> <p>Sample value: <code>/user/temp/ebsUMQuery.properties</code></p>
Query Name	<p>Enter the name of the query in the reconciliation query file that you want to run.</p> <p>Default value:</p> <ul style="list-style-type: none"> ■ Value for the User Management connector: <code>UM_USER_RECON</code> ■ Value for the User Management with HR Foundation connector: <code>UM_USER_HRMS_RECON</code> ■ Value for the User Management with TCA Foundation connector: <code>UM_USER_TCA_RECON</code>

Table 3–5 (Cont.) Attributes of the eBusiness UM Target Resource User Reconciliation Scheduled Task

Attribute	Description
IT Resource Name	<p>Enter the name of the IT resource that you configure by performing the procedure described in Section 2.3.3.6, "Configuring the IT Resource".</p> <p>Sample value: EBS-APPS12</p>
Last Execution Time	<p>This attribute holds the time stamp at which the last reconciliation run started.</p> <p>Default value: 0</p> <p>See Section 3.3.1, "Reconciliation Time Stamp" for information about setting a value for the Last Execution Time attribute.</p>
Batch Size	<p>Enter the number of records that must be included in each batch fetched from the target system.</p> <p>Default value: 1000</p> <p>This attribute is discussed in Section 3.3.2, "Batched Reconciliation".</p>
Task Name	<p>This attribute holds the name of the scheduled task.</p> <ul style="list-style-type: none"> Value for the User Management connector: eBusiness UM Target Resource User Reconciliation Value for the User Management with HR Foundation connector: eBusiness UM Target Resource User-HRMS Reconciliation Value for the User Management with TCA Foundation connector: eBusiness UM Target Resource User-TCA Reconciliation <p>Note: For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that new scheduled task as the value of the Task Name attribute in that scheduled task.</p>
Resource Object Name	<p>This attribute holds the name of the resource object for the connector.</p> <ul style="list-style-type: none"> Value for the User Management connector: eBusiness Suite User Value for the User Management with HR Foundation connector: eBusiness Suite User HR Foundation Value for the User Management with TCA Foundation connector: eBusiness Suite User TCA Foundation <p>Note: Do not change the default value. However, if you create a copy of the resource object, then you can specify the name of the new resource object as the value of the Resource Object attribute.</p>
Query Filter Lookup Definition	<p>This attribute holds the name of the lookup definition that contains information about reconciliation filter parameters.</p> <ul style="list-style-type: none"> Value for the User Management connector: Lookup.EBS.UM.QueryFilters Value for the User Management with HR Foundation connector: Lookup.EBS.UMHRMS.QueryFilters Value for the User Management with TCA Foundation connector: Lookup.EBS.UMTCA.QueryFilters <p>Note:</p> <p>You must ensure that the filter parameters in this lookup definition can be applied along with the query specified by the Query Name attribute. An error is encountered if this condition is not met.</p>

3.4 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Do one of the following:
 - a. If you are using Oracle Identity Manager release 9.1.0.x, expand **Resource Management**, and then click **Manage Scheduled Task**.
 - b. If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then on the Welcome page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
 - If you are using Oracle Identity Manager release 9.1.0.x, then:
 - a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

The following screenshot shows the Scheduled Task Management page:

ORACLE Identity Manager

Welcome System Administrator

Scheduled Task Management

Select a scheduled task and the action that you want to perform on it.

Scheduled Task Name: eBusiness UM Target Res

Task State: [Dropdown]

Search Clear

Results 1-1 of 1

Scheduled Task	Status	Frequency	Last Start	Last Stop	Next Start	Edit	Enable	Disable	Run How
eBusiness UM Target Resource User Reconciliation	Inactive	ONCE	n/a	n/a	n/a	[Edit Icon]	Enable	Disabled	[Run How Icon]

- b. In the search results table, click the edit icon in the Edit column for the scheduled task.

The Edit Scheduled Task Details page is displayed. This is shown in the following screenshot:

ORACLE Identity Manager

Welcome System Administrator

Edit Scheduled Task

* Indicates required field

Task Information

Task Name: eBusiness UM Target Res

Class Name: oracle.iam.connectors.ebs

Status: [Radio Button] Enabled [Radio Button] Disabled

Schedule

Max Retries: 2

Next Start: May 18, 2009 4:21:00

Frequency: [Radio Button] Once [Radio Button] Every [] Minutes

Last Start: n/a

Last Stop: n/a

- If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then:
 - a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management section, click **Search Scheduled Jobs**.
 - b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
 - c. In the search results table on the left pane, click the scheduled job in the Job Name column.
- 4. Modify the details of the scheduled task. To do so:
 - a. If you are using Oracle Identity Manager release 9.1.0.x, then on the Edit Scheduled Task Details page, you can modify the following parameters, and then click **Continue**:
 - **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
 - **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 2.
 - **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
 - **Frequency:** Specify the frequency at which you want the task to run.
 - b. If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then on the Job Details tab, you can modify the following parameters:
 - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
 - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

- 5. Specify values for the attributes of the scheduled task. To do so:

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
 - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
 - Attributes of the scheduled task are discussed in [Section 3.3.4, "Reconciliation Scheduled Tasks."](#)
-

- If you are using Oracle Identity Manager release 9.1.0.x, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

The following screenshot shows the Attributes page. The attributes of the scheduled task that you select for modification are displayed on this page.

The screenshot shows the 'Attributes' page in Oracle Identity Manager. On the left is a navigation menu with options like 'My account', 'My Resources', 'Requests', 'To-Do List', 'Users', 'Organizations', 'User Groups', 'Access Policies', 'Resource Management', 'Deployment Management', 'Reports', 'Generic Technology Connector', and 'Help'. The 'Resource Management' section is expanded, showing 'Manage', 'Create IT Resource', 'Manage IT Resource', 'Create Scheduled Task', and 'Manage Scheduled Task' (which is selected). The main content area is titled 'Attributes' and shows 'Results 1-10 of 10'. It contains a table with the following data:

Attribute Name	Attribute Value	Delete
Batch Size	1000	X
IT Resource Name	EBS-APPS12	X
Last Execution Time	0	X
Query Filter Lookup Definition	Lookup EBS UM QueryFilters	X
Query Name	UM_USER_RECON	X
Query Properties File		X
Recon Lookup Definition	Lookup EBS UM UserRecon	X
Resource Object Name	eBusiness Suite User	X
Target Date Format	MM/dd/yyyy hh:mm:ss	X
Task Name	eBusiness UM Target Resource User Reconciliation	X

Below the table, there are input fields for 'Attribute' and 'Value', and buttons for 'Add' and 'Update'. The 'Attribute' field has a dropdown menu with 'Batch Size' selected. The 'Value' field has '100' entered.

- If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then on the Job Details tab, in the Parameters section, specify values for the attributes of the scheduled task.
6. After specifying the attributes, do one of the following:
- If you are using Oracle Identity Manager release 9.1.0.x, then click **Save Changes** to save the changes.

Note: The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click Stop Execution on the Task Scheduler form of the Design Console.

- If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then click **Apply** to save the changes.

Note: The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.5 Attributes for Which You Can Specify Values During New Resource and Entitlement Provisioning

This section lists the resource and entitlement attributes for which values can be set on the Administrative and User Console during new resource or entitlement provisioning. During an Update Resource or Update Entitlement provisioning operation, all attributes of the resource or entitlement can be updated.

This section is divided into the following topics:

- [Section 3.5.1, "Resource Provisioning Using the User Management Connector"](#)
- [Section 3.5.2, "Resource Provisioning Using the User Management with TCA Foundation Connector"](#)
- [Section 3.5.3, "Resource Provisioning Using the User Management with HR Foundation Connector"](#)
- [Section 3.5.4, "Entitlement Provisioning Using All Three Connectors"](#)

3.5.1 Resource Provisioning Using the User Management Connector

If you are using the User Management connector, then you can set values for the following attributes while provisioning a resource:

- IT resource representing the target system installation on which the provisioning operation is to be performed
- Person ID
- Description
- Email
- Fax
- SSO User ID

3.5.2 Resource Provisioning Using the User Management with TCA Foundation Connector

If you are using the User Management with TCA Foundation connector, then you can set values for the following attributes while provisioning a resource:

- IT resource representing the target system installation on which the provisioning operation is to be performed
- Description
- Email
- Fax
- SSO User ID

The Username and Password fields are pre-populated with OIM User data. The Effective Date From attribute is populated with the current date. Values cannot be set for the Effective Date To, Password Expiration Type and Password Expiration Interval attributes.

In addition the OIM User can set values for the role and responsibility attributes listed later in this section.

3.5.3 Resource Provisioning Using the User Management with HR Foundation Connector

If you are using the User Management with HR Foundation connector, then you can set values for the following attributes while provisioning a resource:

- IT resource representing the target system installation on which the provisioning operation is to be performed
- Description

- Email
- Fax
- SSO User ID
- Gender
- Employee Number

The Username, Password, First Name, and Last Name fields are pre-populated with OIM User data. The Effective Date From, Hire Date fields are populated with the current date. The Business Group ID and Person Type ID attributes have default values of 202 and 13, respectively. The Effective Date To, Password Expiration Type and Password Expiration Interval fields are provisioned without any values. The OIM User cannot enter values for these attributes while submitting a request for a new resource.

3.5.4 Entitlement Provisioning Using All Three Connectors

If you are using any of the three connectors, you can set values for the following entitlement attributes along with values that you set for the resource:

- Application Name
- Role or Responsibility Name
- Start Date
- Security Group Name

The Expiration Date attribute is provisioned without any values. End-users are not allowed to fill in this attribute during new resource provisioning.

3.6 Provisioning Operations Performed in an SoD-Enabled Environment

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create an Oracle E-Business Suite account for the user.

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning of accounts
- Request-based provisioning of entitlements
- Provisioning triggered by policy changes

See Also: *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- [Section 3.6.1, "Overview of the Provisioning Process in an SoD-Enabled Environment"](#)
- [Section 3.6.2, "Direct Provisioning in an SoD-Enabled Environment"](#)
- [Section 3.6.3, "Request-Based Provisioning in an SoD-Enabled Environment"](#)

3.6.1 Overview of the Provisioning Process in an SoD-Enabled Environment

The following is the sequence of steps that take places during a provisioning operation performed in an SoD-enabled environment:

1. The provisioning operation triggers the appropriate adapter.
2. The adapter carries provisioning data to the corresponding BAPI on the target system.
3. If you select an account or entitlements to be provisioned to the OIM User, then the SoD check is initiated. The SoDChecker task submits the User Account and Entitlements details in a form of Duties list to Oracle Application Access Controls Governor. In other words, the SoD validation process takes place asynchronously.
4. The user runs either the Get SOD Check Results Provisioning or Get SOD Check Results Approval scheduled task.
5. The scheduled task passes the entitlement data to the Web service of Oracle Application Access Controls Governor.
6. After Oracle Application Access Controls Governor runs the SoD validation process on the entitlement data, the response from the process is returned to Oracle Identity Manager.
7. The status of the process task that received the response depends on the response itself. If the entitlement data clears the SoD validation process, then the status of the process task changes to Completed. This translates into the entitlement being granted to the user. If the SoD validation process returns the failure response, then status of the process task changes to Canceled.

3.6.2 Direct Provisioning in an SoD-Enabled Environment

This section describes the prerequisites and the procedure to perform direct provisioning. It contains the following sections:

- [Section 3.6.2.1, "Prerequisites"](#)
- [Section 3.6.2.2, "Performing Direct Provisioning"](#)

3.6.2.1 Prerequisites

Note: Perform the procedure in this section *only* in the following situations:

- The first time you perform direct provisioning.
 - If you switch from request-based provisioning to direct provisioning.
-

On Oracle Identity Manager release 9.1.0.x, when you run the Connector Installer, configurations for both direct provisioning and request-based provisioning of Oracle E-Business Suite user accounts are installed. Therefore, during direct provisioning, the process form is suppressed and object form is displayed. If you want to enable the use of the process form during direct provisioning, then perform the procedure described in this section.

On Oracle Identity Manager releases 11.1.x and 11.1.2.x, when you run the Connector Installer, the configuration for direct provisioning of Oracle E-Business Suite user accounts is installed. Although the process form is displayed during direct

provisioning, the connector cannot complete direct provisioning operations unless you enable the use of the process form. If you want to enable the use of the process form during direct provisioning, then perform the procedure described in this section.

To enable the use of the process form during direct provisioning:

Note: Request-based provisioning is disabled when you perform this procedure.

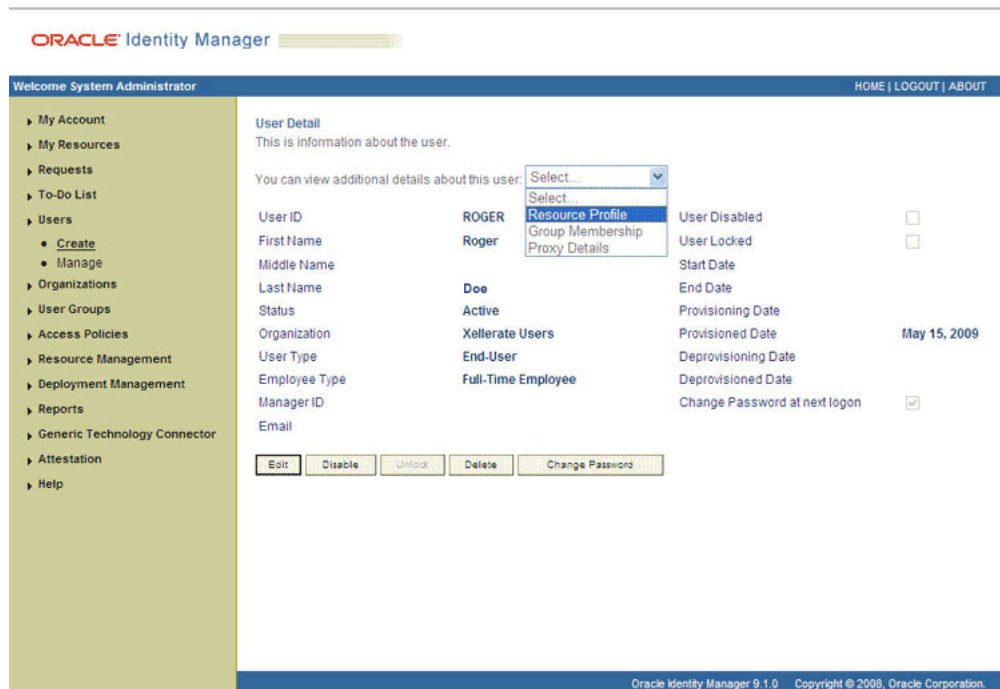
1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the process definition for the connector that you are using:
See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
 - c. Deselect the **Auto Save Form** check box.
 - d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
 - a. Expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the resource object corresponding to the connector that you are using:
 - Resource object for the User Management connector:
eBusiness Suite User
 - Resource object for the User Management with HR Foundation connector:
eBusiness Suite User HR Foundation
 - Resource object for the User Management with TCA Foundation connector:
eBusiness Suite User TCA Foundation
 - c. Deselect the **Self Request Allowed** check box.
 - d. Click the Save icon.

3.6.2.2 Performing Direct Provisioning

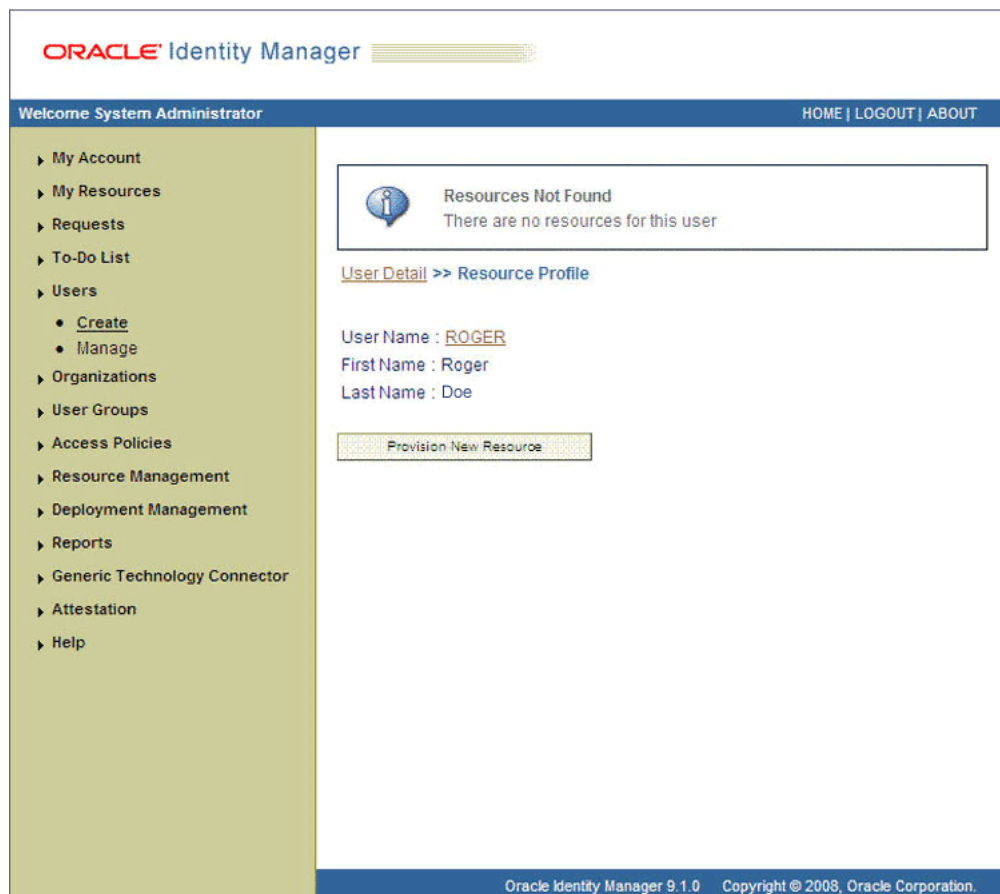
To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
 - If you are using Oracle Identity Manager release 9.1.0.x, then:
 - a. From the Users menu, select **Create**.
 - b. On the Create User page, enter values for the OIM User fields and then click **Create User**. The following screenshot shows the Create User page:

- If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then:
 - a. On the Welcome to Identity Administration page, in the Users section, click **Create User**.
 - b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
- 3. If you want to provision a target system account to an existing OIM User, then:
 - If you are using Oracle Identity Manager release 9.1.0.x, then:
 - a. From the Users menu, select **Manage**.
 - b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.
 - If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then:
 - a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the drop-down list on the left pane.
 - b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
- 4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
 - If you are using Oracle Identity Manager release 9.1.0.x, then:
 - a. On the User Detail page, select **Resource Profile** from the list at the top of the page. The following screenshot shows the User Detail page:



- b. On the Resource Profile page, click **Provision New Resource**. The following screenshot shows the Resource Profile page:



- If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then:

- a. On the user details page, click the **Resources** tab.
 - b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
5. On the Step 1: Select a Resource page, select the resource that you want to provision from the list and then click **Continue**. The following screenshot shows the Step 1: Select a Resource page:

Provision Resource to User
You are provisioning to Roger Doe [ROGER].

Step 1: Select a Resource

Select a resource to provision.

Filter By:

Results 1-7 of 7

	Resource Name	Resource Type	Resource Form
<input type="radio"/>	eBusiness Suite User TCA Foundation Responsibility	Application	Yes
<input type="radio"/>	eBusiness Suite User Responsibility	Application	Yes
<input type="radio"/>	eBusiness Suite User Role	Application	Yes
<input type="radio"/>	AD User	Application	No
<input type="radio"/>	eBusiness Suite User TCA Foundation	Application	Yes
<input checked="" type="radio"/>	eBusiness Suite User	Application	Yes
<input type="radio"/>	eBusiness Suite User TCA Foundation Role	Application	Yes

Exit Continue >>

6. On the Step 2: Verify Resource Selection page, click **Continue**. The following screenshot shows the Step 2: Verify Resource Selection page:

Provision Resource to User
You are provisioning to Roger Doe [ROGER].

Step 2: Verify Resource Selection

You have selected to provision eBusiness Suite User to Roger Doe [ROGER]

Exit << Back Continue >>

7. On the Step 3: Provide Resource Data page for process data, enter the details of the account that you want to create on the target system and then click **Continue**. The following screenshot shows the user details added:

Provision Resource to User
You are provisioning to Roger Doe [ROGER]

Step 3: Provide Resource Data

eBusiness Suite User

Prepopulate

* Indicates required field

EBS Server * EBS-APPS12 [Clear](#)

Description

Email

Fax

SSO User ID

Person ID

SoDCheckStatus SoDCheckNotInitiated

SoDCheckTrackingID

SoDCheckResult

SoDCheckViolation

SoDCheckTimestamp

Exit << Back Continue >>

8. On the Step 3: Provide Process Data page for responsibility data, specify the application name, responsibility name, effective start date, and security group for the account and then click **Add**. If you want to add more than one responsibility, repeat the process. Then, click **Continue**. The following screenshot shows this page:

Welcome System Administrator

HOME | LOGOUT | ABOUT

Provision Resource to User
You are provisioning to ebs10711 ebs10711 [EBS10711]

Step 3: Provide Resource Data

eBusiness Suite Responsibilities

Prepopulate

* Indicates required field

Application Name [Clear](#)

Responsibility Name * [Clear](#)

Effective Start Date [Clear](#)

Security Group [Clear](#)

Add

Application Name	Responsibility Name	Effective Start Date	Security Group	Remove
ALR	Alert Manager, Vision Enterprises		GOVERNMENT	<input type="checkbox"/>
PIQ	Application Developer		000	<input type="checkbox"/>
PJI	Project Intelligence Supervisor		0000	<input type="checkbox"/>
				Remove

Exit << Back Continue >>

9. On the Step 3: Provide Process Data page for role data, specify the application name, role name, and start date for the role assignment and then click **Add**. If you want to add more than one role, repeat the process. Then, click **Continue**. The following screenshot shows this page:

Provision Resource to User
You are provisioning to Roger Doe [ROGER]

1 2 3 4 5 6

Step 3: Provide Resource Data

eBusiness Suite User Role Grants

Prepopulate

* Indicates required field

Application Name Clear

Role Name *

Start Date

Add

Exit << Back Continue >>

10. On the Step 4: Verify Process Data page, verify the data that you have provided and then click **Continue**. The following screenshot shows Step 4: Verify Process Data page.

Provision Resource to User
You are provisioning to Roger Doe [ROGER]

1 2 3 4 5 6

Step 4: Verify Resource Data

You have selected to provision eBusiness Suite User to Roger Doe [ROGER].

Clicking on the Continue button will start provisioning and display the process form (if any). The resource data cannot be changed after that.

eBusiness Suite User Edit

EBS Server	EBS-APP512
Description	
Email	
Fax	
SSO User ID	
Person ID	
SoDCheckStatus	SoDCheckNotInitiated
SoDCheckTrackingID	
SoDCheckResult	
SoDCheckViolation	
SoDCheckTimestamp	

eBusiness Suite User >> eBusiness Suite Responsibilities Edit

Application Name	Responsibility Name	Effective Start Date
EX	Collections Manager	
EX	Collections Agent	
EX	Collections Leasing Agent	

eBusiness Suite User >> eBusiness Suite User Role Grants

This form does not have any entries. Click [Here](#) to add.

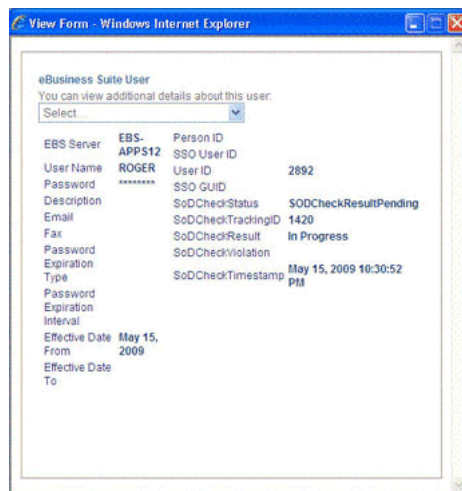
Exit << Back Continue >>

11. The "Provisioning has been initiated" message is displayed. To view the newly provisioned resource, perform one of the following steps:
- If you are using Oracle Identity Manager release 9.1.0.x, then click **Back to User Resource Profile**. The Resource Profile page shows that the resource has been provisioned to the user. The following screenshot shows this page:



- If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then:
 - a. Close the window displaying the "Provisioning has been initiated" message.
 - b. On the Resource tab of the user details page, click **Refresh** to view the newly provisioned resource.
12. To view the process form, perform one of the following steps:
- If you are using Oracle Identity Manager release 9.1.0.x, then on the Resource Profile page, click the **View** link in the Process Form column. The View Form page is displayed.
 - If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then on the Resources tab of the user details page, select the row displaying the newly provisioned resource, and then click **Open**. The Edit Form page is displayed.

The following screenshot shows the page displaying the process form:



In this screenshot, the SODCheckStatus field shows SODCheckPending. The value in this field can be SoDCheckResultPending or SoDCheckCompleted.

Note: If Oracle Identity Manager is not SoD enabled, then SOD Check Status field shows SODCheckNotInitiated.

13. To view the Resource Provisioning Details page, which shows the details of the process tasks that were run, perform the procedure in one of the following steps:
- If you are using Oracle Identity Manager release 9.1.0.x, then on the Resource Profile page, click the resource link in the Resource Name column.
 - If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then on the Resources tab of the user details page, from the Action menu, select **Resource History**.

The following screenshot shows the Resource Provisioning Details page:

User Detail >> Resource Profile >> Resource Provisioning Details
 The following are the provisioning tasks for the resource. You can also enable, disable, or revoke this resource from the user.
 eBusiness Suite User provisioning details for Roger Doe [ROGER]

Results 1-7 of 7 First | Previous | Next | Last

Task Name	Task Status	Date Assigned	Assigned To	Retry
System Validation	Completed	May 15, 2009	System Administrator [KELSY\SADM]	<input type="checkbox"/>
Create User	Completed	May 15, 2009	System Administrator [KELSY\SADM]	<input type="checkbox"/>
Holder	Pending	May 15, 2009	System Administrator [KELSY\SADM]	<input type="checkbox"/>
SODChecker	Pending	May 15, 2009	System Administrator [KELSY\SADM]	<input type="checkbox"/>
Add Responsibility to User	Waiting	May 15, 2009	System Administrator [KELSY\SADM]	<input type="checkbox"/>
Add Responsibility to User	Waiting	May 15, 2009	System Administrator [KELSY\SADM]	<input type="checkbox"/>
Add Responsibility to User	Waiting	May 15, 2009	System Administrator [KELSY\SADM]	<input type="checkbox"/>

First | Previous | Next | Last

Enable Disable Revoke Add Task

This page shows the details of the process tasks that were run. The Holder and SODChecker tasks are in the Pending state. These tasks will change state after the status of the SoD check is returned from the SoD engine. The Add Responsibility and Add Role to User tasks correspond to the responsibilities and roles selected for assignment to this user.

Note: SoD validation by Oracle Application Access Controls Governor is asynchronous. The validation process returns a result as soon as it is completed.

14. After the Get SOD Check Results Provisioning scheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. To view the process form, perform the procedure described in one of the following steps:
- If you are using Oracle Identity Manager release 9.1.0.x, then on the Resource Profile page, click the **View** link in the Process Form column. The View Form page is displayed.
 - If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then on the Resources tab of the user details page, select the row displaying the newly provisioned resource, and then click **Open**. The Edit Form page is displayed.

The following screenshot shows the page displaying this process form:

eBusiness Suite User
You can view additional details about this user:

Select

EBS Server: EBS-APP512
User Name: ROGER
Password: *****
Description: SSO GUID
Email: SSO CheckStatus
Fax: SSO CheckTrackingID 1420
Password Expiration: SSO CheckResult
Type: SSO CheckViolation
Password Expiration Interval: May 15, 2009
Effective Date From: May 15, 2009
Effective Date To: SSO CheckTimestamp May 15, 2009 10:34:56 PM

Person ID
SSO User ID
User ID: 2892
SSO GUID
SoDCheckStatus: SODCheckCompleted
SoDCheckTrackingID: 1420
SoDCheckResult: Failed
[Policy Name]: Conflict
Responsibilities:
[Conflicting Duties]:
Collections Manager:
Collections: Collections
Leasing Agent: Collections
Collections Agent:
Collections

In this screenshot, the SOD Check Status field shows SoDCheckCompleted. Because a violation by the SoD engine in this particular example, the SoD Check Violation field shows the details of the violation.

In addition, the Resource Provisioning Details page shows the status of the SODChecker and Holder tasks as Completed.

The following screenshot shows this page:

User Detail >> Resource Profile >> Resource Provisioning Details
The following are the provisioning tasks for the resource. You can also enable, disable, or revoke this resource from the user.
eBusiness Suite User provisioning details for Roger Doe [ROGER]

Results 1-7 of 7

Task Name	Task Status	Date Assigned	Assigned To	Retry
System Validation	Completed	May 15, 2009	System Administrator [NELSYSADM]	<input type="checkbox"/>
Create User	Completed	May 15, 2009	System Administrator [NELSYSADM]	<input type="checkbox"/>
SODChecker	Completed	May 15, 2009	System Administrator [NELSYSADM]	<input type="checkbox"/>
Holder	Canceled	May 15, 2009	System Administrator [NELSYSADM]	<input type="checkbox"/>
Add Responsibility to User	Canceled	May 15, 2009	System Administrator [NELSYSADM]	<input type="checkbox"/>
Add Responsibility to User	Canceled	May 15, 2009	System Administrator [NELSYSADM]	<input type="checkbox"/>
Add Responsibility to User	Canceled	May 15, 2009	System Administrator [NELSYSADM]	<input type="checkbox"/>

First | Previous | Next | Last

Enable Disable Revoke Add Task

First | Previous | Next | Last

In this screenshot, the status of the Add User Role tasks is Canceled because the request failed the SoD validation process.

15. As the administrator assigning a resource to a user, you can either end the process when a violation is detected or modify the assignment data and then resend it. To modify the assignment data, perform the procedure in one of the following steps:
 - If you are using Oracle Identity Manager release 9.1.0.x, then click the **Edit** link in the Process Form column on the Resource Profile page.
 - If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then on the Resource tab of the user details page, select the row containing the resource, and then click **Open**.
16. In the Edit Form window that is displayed, you can modify the role and profile data that you had selected earlier.

Note: To modify a set of entitlements In the Edit Form window, you must first remove all entitlements and then add the ones that you want to use.

In the following screenshot, one of the roles selected earlier is marked for removal:

Responsibility Name	Effective Start Date	Effective End Date	Update	Remove
Collections Manager			<input type="radio"/>	<input checked="" type="checkbox"/>
Collections Agent			<input type="radio"/>	<input checked="" type="checkbox"/>
Collections Leasing Agent			<input type="radio"/>	<input checked="" type="checkbox"/>

17. Rerun the Get SOD Check Results Provisioning scheduled task to initiate the SoD validation process.
18. After the Get SOD Check Results Provisioning scheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
 - If you are using Oracle Identity Manager release 9.1.0.x, then on the Resource Profile page, click the **View** link in the Process Form column. The process form is displayed.
 - If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then on the Resources tab of the user details page, select the row containing the resource, and then click **Open**. The process form is displayed.

The following screenshot shows the page displaying the process form:

eBusiness Suite User
You can view additional details about this user:

Select

EBS Server	EBS-APP512	Person ID	SSO User ID
User Name	ROGER	User ID	2892
Password	*****	SSO GUID	
Description		SoDCheckStatus	SODCheckCompleted
Email		SoDCheckTrackingID	1423
Fax		SoDCheckResult	Passed
Password		SoDCheckViolation	
Expiration Type		SoDCheckTimestamp	May 15, 2009 10:39:34 PM
Expiration Interval			
Effective Date	May 15, 2009		
From			
Effective Date To			

In this screenshot, the SOD Check Status field shows SoDCheckCompleted. Because no violation was detected by the SoD engine, the SoDCheckResult field shows Passed.

In addition, the Resource Provisioning Details page shows the status of the SODChecker and Holder tasks as Completed.

The following screenshot shows this page:

User Detail >> Resource Profile >> Resource Provisioning Details

The following are the provisioning tasks for the resource. You can also enable, disable, or revoke this resource from the user.

eBusiness Suite User provisioning details for Roger Doe [ROGER]

Results 1-10 of 17 First | Previous | Next | Last

Task Name	Task Status	Date Assigned	Assigned To	Retry
System Validation	Completed	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Create User	Completed	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Holder	Completed	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
SoDChecker	Completed	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Add Responsibility to User	Completed	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
SoDChecker	Completed	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Holder	Completed	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
SoDChecker	Completed	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Revoke Responsibility from User	Rejected	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>
Revoke Responsibility from User	Rejected	May 15, 2009	System Administrator [XELSYSADM]	<input type="checkbox"/>

First | Previous | Next | Last

Enable Disable Revoke Add Task

On the Resource Provisioning Details page, the state of the Add Role to User task is Completed.

3.6.3 Request-Based Provisioning in an SoD-Enabled Environment

See Also: [Section 2.3.1, "Configuring SoD"](#)

The request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The request-based provisioning process described in this section covers steps to be performed by both entities.

In the example used in this section, the end user creates a request for two roles on the target system. The request clears the SoD validation process and is approved by the approver.

Note: To get SoD Violation value updated correctly, change the field label of 'SoDCheckViolation' to 'SoDCheckEntitlementViolation' in the EBS Form on Design Console.

3.6.3.1 End-User's Role in Request-Based Provisioning

Depending on the Oracle Identity Manager release that you are using, end-users perform the procedure described in one of the following sections:

- [Section 3.6.3.1.1, "End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x"](#)
- [Section 3.6.3.1.2, "End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.x"](#)

3.6.3.1.1 End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x

The following are types of request-based provisioning on Oracle Identity Manager release 9.1.0.x:

- Request-based provisioning of accounts: OIM Users are created but not provisioned target system resources when they are created. Instead, the users themselves raise requests for provisioning accounts.

- Request-based provisioning of entitlements: OIM Users who have been provisioned target system resources (either through direct or request-based provisioning) raise requests for provisioning entitlements.

The following steps are performed by the end user in a request-based provisioning operation:

Note: The procedure is almost the same for request-based provisioning of both accounts and entitlements. Differences have been called out in the following sequence of steps.

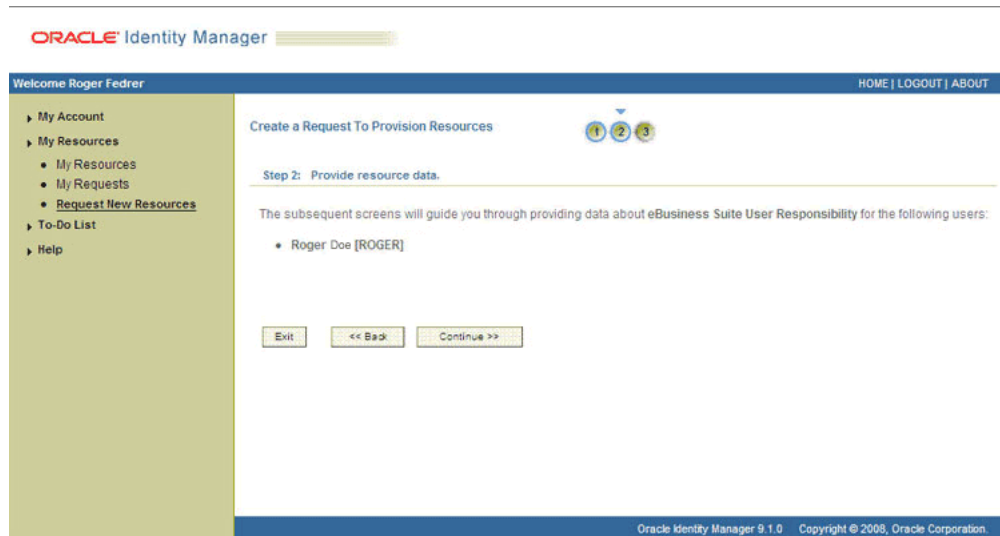
1. Log in to the Administrative and User Console.
2. Expand **My Resources**, and then click **Request New Resources**.
3. On the Step 1: Provide resources page, use the Add button to select one of the following:
 - eBusiness Suite User, if you want to create a request for a target system account
 - eBusiness Suite User Responsibility or eBusiness Suite User Role, if you want to create a request for an entitlement on the target system

The following screenshot shows the eBusiness Suite User Responsibility entitlement selected:



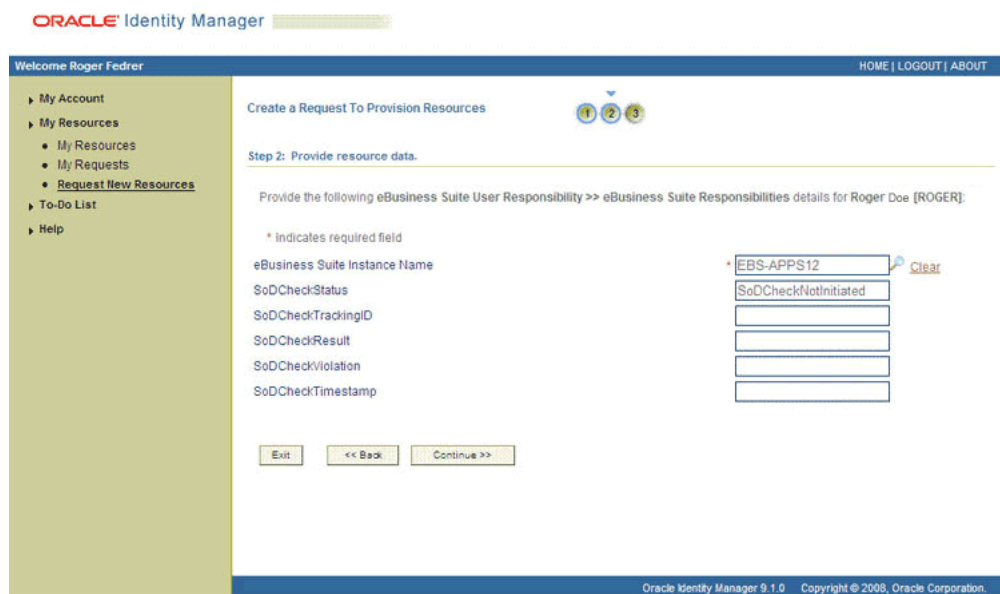
4. On the Step 2: Provide resource data page, click Continue.

The following screenshot shows this page:



5. On the second Step 2: Provide resource data page, select the IT resource corresponding to the target system installation on which you want the selected entitlement.

The following screenshot shows this page:



6. On the third Step 2: Provide resource data page, to add the responsibility data, specify the application name, responsibility name, security group name, and effective start date for the responsibility and then click **Add**. If you want to add more than one responsibility, repeat the process. Then, click **Continue**.

The following screenshot shows two roles selected on this page:

ORACLE Identity Manager

Welcome Roger Fedrer HOME | LOGOUT | ABOUT

My Account
My Resources
My Resources
My Requests
Request New Resources
To-Do List
Help

Create a Request To Provision Resources 1 2 3

Step 2: Provide resource data.

Provide the following eBusiness Suite User Responsibility >> eBusiness Suite Responsibilities detail for Roger Doe [ROGER] and click the Add button to create a new entry.

* Indicates required field

Application Name [Clear](#)

Responsibility Name * [Clear](#)

Effective Start Date [Clear](#)

Security Group [Clear](#)

The following are the existing eBusiness Suite User Responsibility >> eBusiness Suite Responsibilities entries for Roger Doe [ROGER]. You can select specific entries to remove.

Application Name	Responsibility Name	Effective Start Date	Remove
EX	Collections Manager HTML		<input type="checkbox"/>
			<input type="button" value="Remove"/>

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

7. On the Step 3: Verify information page, review the information that you have provided and then submit the request. The following screenshot shows this page:

ORACLE Identity Manager

Welcome Roger Fedrer HOME | LOGOUT | ABOUT

My Account
My Resources
My Resources
My Requests
Request New Resources
To-Do List
Help

Create a Request To Provision Resources 1 2 3

Step 3: Verify information.

Users Selected

User ID	First Name	Last Name
ROGER	Roger	Doe

Resources Selected [Change](#)

Resource Name	Details
eBusiness Suite User Responsibility	Edit

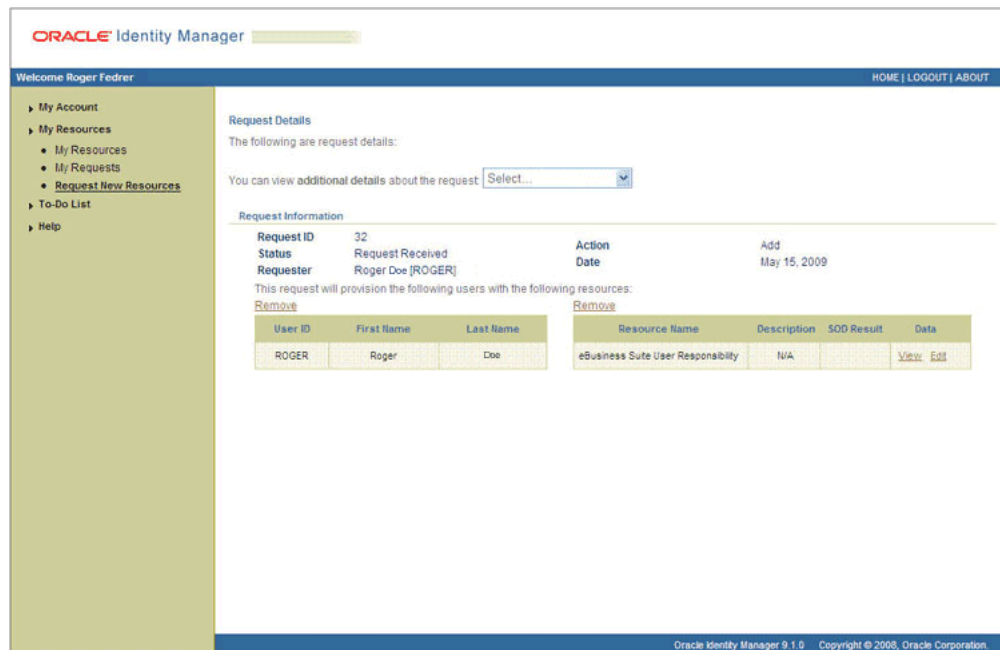
Comments
No comments have been added to this request. [Click here to add a comment.](#)

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

8. If you click Submit Now, then the Request Submitted page shows the request ID. The following screenshot shows this page:



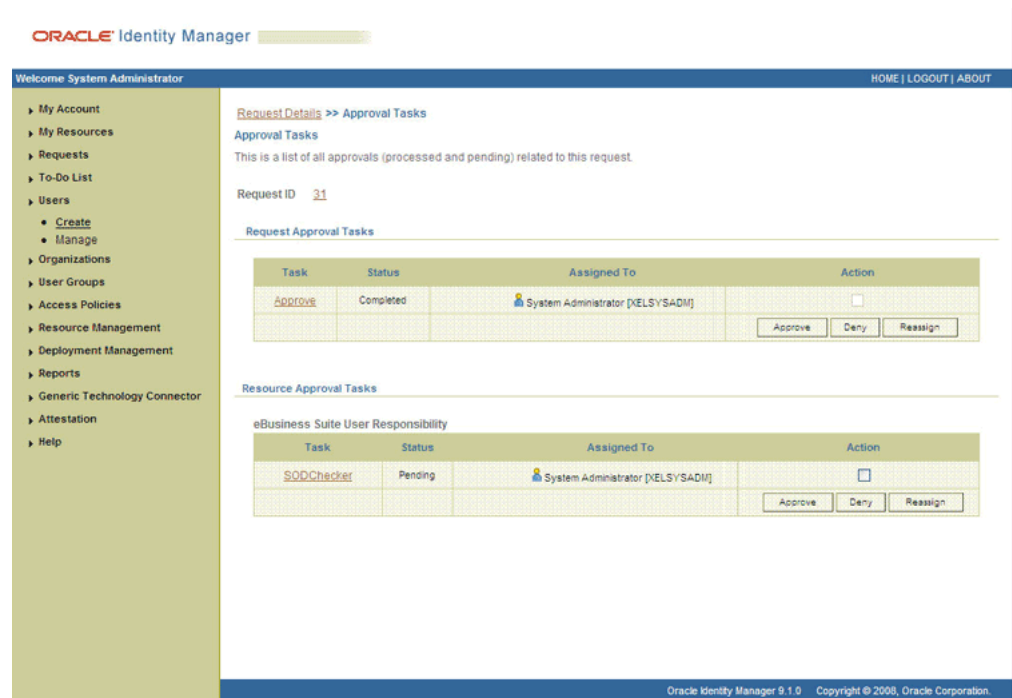
9. If you click the request ID, then the Request Details page is displayed. The following screenshot shows this page:



In this screenshot, the SODCheckStatus field shows SODCheckPending. The value in this field can be SoDCheckResultPending or SoDCheckCompleted.

Note: If Oracle Identity Manager is not SoD enabled, then the SOD Check Status field shows SODCheckNotInitiated.

- To view details of the approval, select Approval Tasks from the list at the top of the page. The Approval Tasks page is displayed. The following screenshot shows this page:



On this page, the status of the SODChecker task is Pending.

- To initiate SoD validation of pending entitlement requests, the approver must run the Get SOD Check Results Approval scheduled task.
- After the Get SOD Check Results Approval scheduled task is run, on the Approvals Task page, the status of the SODChecker task is Completed and the Approval task status is Pending. This page also shows details of the administrator who must now approve the request.

3.6.3.1.2 End User's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.x

The following steps are performed by the end user in a request-based provisioning operation:

See Also: The "Creating and Searching Requests" chapter of *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

- Log in to the Administrative and User Console.
- On the Welcome page, click **Advanced** in the upper-right corner of the page.
- On the Welcome to Identity Manager Advanced Administration page, click the **Administration** tab, and then click the **Requests** tab.
- From the Actions menu on the left pane, select **Create Request**.

The Select Request Template page is displayed.

- From the Request Template list, select **Provision Resource** and click **Next**.

6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specified is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

If you want to create a provisioning request for more than one user, then from the Available Users list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **EBS User**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**:

- Effective Date
- Justification

On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.

13. If you click the request ID, then the Request Details page is displayed.
14. On the Resource tab of the Request Details page, click the View Details link in the row containing the resource for which the request was created. The Resource data page is displayed in a new window.

One of the fields on this page is the SODCheckStatus field. The value in this field can be SoDCheckResultPending or SoDCheckCompleted. When the request is placed, the SODCheckStatus field contains the SoDCheckResultPending status.

Note: If Oracle Identity Manager is not SoD enabled, then the SOD Check Status field shows SODCheckNotInitiated.

15. To view details of the approval, on the Request Details page, click the **Approval Tasks** tab.

On this page, the status of the SODChecker task is pending.
16. To initiate SoD validation of pending requests, the approver must run the Get SOD Check Results Approval scheduled task.
17. After the Get SOD Check Results Approval scheduled task is run, on the Request Details page, click the **Approval Tasks** tab. The status of the SODChecker task is Completed and the Approval task status is Pending. This page also shows details of the administrator who must now approve the request.

3.6.3.2 Approver's Role in Request-Based Provisioning

This section discusses the role of the approver in a request-based provisioning operation.

The approver to whom the request is assigned can use the Pending Approvals feature to view details of the request.

The screenshot displays the Oracle Identity Manager web interface. On the left is a navigation menu with options like 'My Account', 'My Resources', 'Requests', 'To-Do List', 'Users', 'Create', 'Manage', 'Organizations', 'User Groups', 'Access Policies', 'Resource Management', 'Deployment Management', 'Reports', 'Generic Technology Connector', 'Attestation', and 'Help'. The main content area is titled 'Request Details' and shows information for request ID 31. It includes a table for 'Request Information' with columns for Request ID, Status, Requester, Action, and Date. Below this is a table for 'Pending Standard Approval Tasks' with columns for Task, Assigned To, Status, and Approve/Deny. The 'Approve/Deny' column contains buttons for 'Approve', 'Deny', and 'Reassign'.

Request ID	Status	Requester	Action	Date
31	Request Received	Roger Doe [ROGER]	Add	May 15, 2009

User ID	First Name	Last Name	Resource Name	Description	SoD Result	Data
ROGER	Roger	Doe	eBusiness Suite User Responsibility	N/A		View Edit

Task	Assigned To	Status	Approve/Deny
Approve	System Administrator [KLSYSADM]	Pending	<input type="checkbox"/>

In addition, the approver can click the View link to view details of the SoD validation process.

The approver can decide whether to approve or deny the request, regardless of whether the SoD engine accepted or rejected the request. The approver can also modify entitlements in the request.

Depending on the Oracle Identity Manager release that you are using, approvers can perform the procedure described in one of the following sections:

- [Section 3.6.3.2.1, "Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x"](#)
- [Section 3.6.3.2.2, "Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.x"](#)

3.6.3.2.1 Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 9.1.0.x

The following are steps that the approver can perform:

1. As the approver, to edit and approve a request, click the **Edit** link.
2. In the Edit Form window, select the entitlement request data that you want to modify from the list at the top of the window and then make the required change. In the following screenshot, one of the roles that the requester had included in the request has been removed:

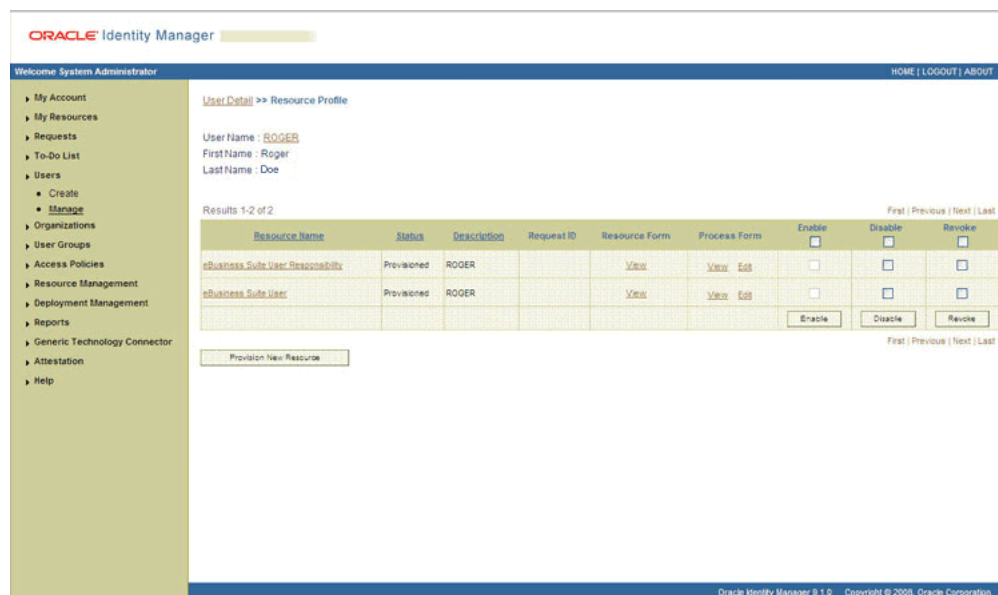
3. Close the Edit Form window, select the check box for the task that you want to approve, and then click **Approve**.

4. On the Confirmation page, click **Confirm**.

The following screenshot shows this page:

5. On the Request Details page, the SOD Status column shows SODCheckCompleted.

If you search for and open the requester's profile, the entitlements granted to the user are shown in the Provisioned state. This is shown in the following screenshot:



3.6.3.2.2 Approver's Role in Request-Based Provisioning on Oracle Identity Manager Release 11.1.x

The following are steps performed by the approver in a request-based provisioning operation:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

A message confirming that the task was approved is displayed.

3.7 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.x

Note: It is assumed that you have performed the procedure described in [Section 2.3.3.9, "Enabling Request-Based Provisioning."](#)

On Oracle Identity Manager release 11.1.x, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the process definition for the connector that you are using:

See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.

- c. Deselect the **Auto Save Form** check box.
 - d. Click the Save icon.
 3. If the Self Request Allowed feature is enabled, then:
 - a. Expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the resource object corresponding to the connector that you are using:
 - Resource object for the User Management connector:
eBusiness Suite User
 - Resource object for the User Management with HR Foundation connector:
eBusiness Suite User HR Foundation
 - Resource object for the User Management with TCA Foundation connector:
eBusiness Suite User TCA Foundation
 - c. Deselect the **Self Request Allowed** check box.
 - d. Click the Save icon.

On Oracle Identity Manager release 11.1.x, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the process definition for the connector that you are using:

See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
 - c. Select the **Auto Save Form** check box.
 - d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
 - a. Expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the resource object corresponding to the connector that you are using:
 - Resource object for the User Management connector:
eBusiness Suite User
 - Resource object for the User Management with HR Foundation connector:
eBusiness Suite User HR Foundation
 - Resource object for the User Management with TCA Foundation connector:
eBusiness Suite User TCA Foundation

- c. Select the **Self Request Allowed** check box.
- d. Click the Save icon.

3.8 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

To perform provisioning operations in Oracle Identity Manager release 11.1.2 or later:

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See the "Managing Users" chapter in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts**.
4. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.
7. If you want to provision entitlements, then:
 - a. On the Entitlements tab, click **Request Entitlements**.
 - b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout**.
 - c. Click **Submit**.

3.9 Uninstalling the Connector

If you want to uninstall the connector for any reason, see "Uninstalling Connectors" in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

Extending the Functionality of the Connector

This chapter describes procedures that you can perform to extend the functionality of the connector for addressing your specific business requirements. This section discusses the following topics:

- [Section 4.1, "Guidelines on Extending the Functionality of the Connector"](#)
- [Section 4.2, "Adding or Removing Attributes for Reconciliation"](#)
- [Section 4.3, "Adding or Removing Attribute Mappings for Provisioning"](#)
- [Section 4.4, "Adding Filter Parameters in a Reconciliation Query"](#)
- [Section 4.5, "Modifying Field Lengths on the Process Form"](#)
- [Section 4.6, "Configuring Validation of Data During Reconciliation"](#)
- [Section 4.7, "Configuring Transformation of Data During User Reconciliation"](#)
- [Section 4.8, "Configuring Validation of Data During Provisioning"](#)
- [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#)
- [Section 4.10, "Customizing the Connector to Handle Timezone Differences"](#)

4.1 Guidelines on Extending the Functionality of the Connector

Note: In Oracle Identity Manager releases 11.1.x and 11.1.2.x, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.x is the same as the term **scheduled job** in the context of Oracle Identity Manager releases 11.1.x and 11.1.2.x.

See Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager for more information about scheduled tasks and scheduled jobs.

As mentioned earlier in this guide, predefined queries are provided for fetching target system user records for reconciliation and entitlement lookup field values for synchronization with Oracle Identity Manager. These predefined queries are in the `ebsUMQuery.properties` and `ebsUMLookupQuery.properties` files, respectively.

You can modify the predefined queries. In addition, you can add your own queries in the same file or a different properties file. The query whose name you specify in the scheduled task is applied during reconciliation or lookup field synchronization.

The following sections discuss guidelines that you must apply while modifying the predefined queries or creating new queries:

- [Section 4.1.1, "Guidelines for Configuring Queries Used in Lookup Field Synchronization"](#)
- [Section 4.1.2, "Guidelines for Configuring Queries Used in Reconciliation"](#)
- [Section 4.1.3, "Guidelines Common to Configuring Both Types of Queries"](#)

The following section discusses guidelines that you must apply while modifying the predefined attribute mappings for provisioning:

- [Guidelines on Modifying Predefined Attribute Mappings for Provisioning](#)

4.1.1 Guidelines for Configuring Queries Used in Lookup Field Synchronization

The following are guidelines that you must apply while modifying or creating queries for lookup field synchronization:

- You must not change the SELECT clause of the predefined query. In other words, the set of target system attributes from which values are fetched for synchronization cannot be modified.
- You must not change existing conditions in the WHERE clause of the predefined query.
- You can add conditions to the WHERE clause of the predefined query.
- If you create a new query, then you must mention the name of the query as the value of the Query Name attribute in the scheduled task.
- If you want to use a new properties file instead of the predefined `ebsUMLookupQuery.properties` file, then specify the name of the file as the value of the Query Properties File attribute in the reconciliation scheduled task. See [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#) for information about this scheduled task.

4.1.2 Guidelines for Configuring Queries Used in Reconciliation

The following are examples of scenarios in which you might want to modify a reconciliation query:

- You want to add a column in the SELECT clause of the reconciliation query.
- You want to remove a column from the SELECT clause of the reconciliation query. For example, you might want to remove the `usr.DESCRPTION` column.
- You want to add conditions to the WHERE clause of the reconciliation query so that only a specified subset of the target system records are considered for reconciliation.

For example, you might want to reconcile records of users with a certain last name.

The following are guidelines that you must apply while modifying or creating queries for reconciliation:

- By adding or removing a column from the SELECT clause of a reconciliation query, you add or remove an attribute from the list of target system attributes for reconciliation. To enable the connector to process a change (addition or removal) in the list of reconciled attributes, you must make corresponding changes in the

provisioning part of the connector. The procedures are described later in this guide.

- You cannot remove columns for attributes that are marked as mandatory attributes in the following tables:
 - [Table 1–3, "Attribute Mappings for Reconciliation in the User Management Connector"](#)
 - [Table 1–4, "Attribute Mappings for Reconciliation in the User Management with HR Foundation Connector"](#)
 - [Table 1–5, "Attribute Mappings for Reconciliation in the User Management with TCA Foundation Connector"](#)
- The queries use inner queries, joins, unions, and the GROUP BY clause. If you add or remove a column from the outer query, you must make corresponding changes in the inner queries, joins, and union queries and the GROUP BY clauses.
- You must ensure that the following conditions are included in the WHERE clause of the inner queries:

Note: The queries for target resource reconciliation contain inner queries, joins, and unions.

```
WHERE((LAST_UPDATE_DATE -TO_DATE('01011970', 'DDMMYYYY')) *24 *60 *60 *1000) >
:lastExecutionTime) \
ROUND((respgrp.LAST_UPDATE_DATE -TO_DATE('01011970', 'DDMMYYYY')) *1440 *60
*1000) > :lastExecutionTime \
((rolegrp.LAST_UPDATE_DATE -TO_DATE('01011970', 'DDMMYYYY')) *1440 *60 *1000) >
:lastExecutionTime \
```

These conditions are used to determine if a target system record, role, or responsibility was added or updated after the time stamp stored in the Last Execution Time scheduled task attribute.

- In the WHERE clause, you must ensure that formats for date literals are specified by the use of the TO_DATE function. For example, instead of specifying a date value as '31-Dec-4712' use TO_DATE('31-Dec-4712', 'DD-Mon-YYYY').
- Changes in attribute mappings for child table (multivalued) data are not supported. Therefore, you must not add or remove columns from the SELECT clause of the UM_USER_RESPONSIBILITIES and UM_USER_ROLES queries in the properties file.
- Before you modify or add a query in the properties file, you must run the query by using any standard database client to ensure that the query produces the required results when it is run against the target system database.
- If you want to use a new properties file instead of the predefined ebsUMQuery.properties file, then specify the name of the file as the value of the Query Name attribute in the reconciliation scheduled task. See [Section 3.3.4, "Reconciliation Scheduled Tasks"](#) for information about this scheduled task.

4.1.3 Guidelines Common to Configuring Both Types of Queries

The following are guidelines that you must apply while modifying or creating queries for either reconciliation or lookup field synchronization:

- The name of the query must not be the same as the name of any other query in the properties file.
- The name of the query must not contain spaces.
- Before you modify or add a query in the properties file, you must run the query by using any standard database client to ensure that it produces the required results.
- Use the number sign (#) to begin each comment line in the properties file.
Add comments to describe changes that you make in existing queries and also to describe new queries that you add in the file.
See existing comments in the properties file for an example.
- If you want to introduce line breaks in the query (to improve readability), then add a backslash (\) at the end of each line.
- You must ensure that the reconciliation does not contain any clause or SQL keyword that modifies or can be used to modify data in the database. For example, an error message is written to the log file if the following keywords are encountered:
 - ALTER
 - CREATE
 - DELETE
 - DROP
 - EXECUTE
 - INSERT
 - UPDATE
- If you create your own reconciliation query or modify an existing query, then you must ensure that the User Name (that is, the login ID), User ID, Effective Start Date From, and Effective Start Date To columns are present in the query. These are mandatory attributes for reconciliation.

4.1.4 Guidelines on Modifying Predefined Attribute Mappings for Provisioning

Apply the following guidelines before you start removing attributes for provisioning:

- You must not remove attributes that are not marked as mandatory in [Section 1.7.2, "Attribute Mappings for Provisioning"](#).
- You must not remove the process form fields (attributes) that are used during SoD validation of entitlement provisioning operations. These fields are listed in [Section 1.7.2, "Attribute Mappings for Provisioning"](#).
- The connector supports both direct provisioning and request-based provisioning. To enable request-based provisioning, there are resource object forms corresponding to all the process forms.

Note: As mentioned earlier in the guide, if you enable request-based provisioning, then direct provisioning is automatically disabled.

As part of the procedure described in this section, you must modify only the process form or both the process form and object form. If the attribute is to be added only on the process form, then ensure that the attribute is populated

automatically during provisioning operations either by a pre-populate adapter or by a default value for the attribute.

4.2 Adding or Removing Attributes for Reconciliation

This section discusses the following topics:

- [Section 4.2.1, "Adding New Attributes for Reconciliation"](#)
- [Section 4.2.2, "Removing Attributes Used for Reconciliation"](#)

4.2.1 Adding New Attributes for Reconciliation

By default, the attributes listed in [Section 1.6.2, "Target System Columns Used in Reconciliation"](#) are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

To add a new attribute for reconciliation:

See Also: *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Open the properties file in a text editor, and add the column from the query corresponding to the connector that you are using.

See Also:

[Section 1.6.1, "Reconciliation Queries"](#)

[Section 4.1.2, "Guidelines for Configuring Queries Used in Reconciliation"](#)

[Section 4.1.3, "Guidelines Common to Configuring Both Types of Queries"](#)

2. Save the changes to the file.
3. Log in to the Design Console.
4. In the resource object definition, add the reconciliation field corresponding to the attribute as follows:
 - a. Expand the **Resource Management** folder, and then double-click **Resource Objects**.
 - b. Search for and open the resource object corresponding to the connector that you are using:
 - Resource object for the User Management connector:
eBusiness Suite User
 - Resource object for the User Management with HR Foundation connector:
eBusiness Suite User HR Foundation
 - Resource object for the User Management with TCA Foundation connector:
eBusiness Suite User TCA Foundation

- c. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box. The following screenshot shows this page:

- d. Specify a value for the field name.
 - e. From the **Field Type** list, select a data type for the field. In addition, if you want to designate the attribute as a mandatory attribute, then select the check box.
 - f. Click the Save icon, and then close the dialog box.
 - g. If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.
 - h. Click the Save icon.
5. Add an entry for the attribute in the lookup definition for reconciliation attribute mapping as follows:
 - a. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - b. Search for and open the lookup definition for the connector that you are using:
 - For User Management: Lookup.EBS.UM.UserRecon
 - For User Management with HR Foundation: Lookup.EBS.UM.UserHRMSRecon
 - For User Management with TCA Foundation: Lookup.EBS.UM.UserTCARecon
 - c. To add a row, click **Add**.
 - d. In the **Code Key** column, enter the name that you have set for the attribute in the resource object.
 - e. In the **Decode** column, enter the name of the column name in the query. If you have set an alias for the column in the query, then enter the alias in the Decode column.
 - f. Click the Save icon.
 6. Add the attribute as a field on the process form as follows:
 - a. Expand the **Development Tools** folder, and then double-click **Form Designer**.
 - b. Search for and open the process form for the connector that you are using:
See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process forms for each connector.
 - c. Click **Create New Version** to create a version of the process form. Then, enter a version name and click the Save icon.
 - d. Click **Add**. The following screenshot shows this page:

- e. Specify the properties of the attribute according to your requirement.
- f. Click the Save icon.
- g. Click **Make Version Active** to activate the new version of the process form.
7. Create a reconciliation field mapping in the process definition as follows:
 - a. Expand the **Process Management** folder, and then double-click **Process Definition**.
 - b. Search for and open the process definition for the connector that you are using:
 - For the User Management connector: eBusiness Suite User
 - For the User Management with HR Foundation connector: eBusiness Suite User HRMS
 - For the User Management with TCA Foundation connector: eBusiness Suite User TCA
 - c. On the Reconciliation Field Mapping tab, click Add Field Map. The following screenshot shows this page:

- d. From the Field name list in the Add Reconciliation Field Mapping dialog box, select the name that you have assigned to the attribute created in the resource object.
 - e. Double-click the Process Data Field, a new pop-up will appear. The entries in the pop-up correspond to the process form fields.
 - f. Select the corresponding newly added field from the pop-up.
 - g. If the field mapping is a key field for matching the process data, check the key Field for Reconciliation matching check box.
 - h. Click the Save icon.
8. Add the attribute for provisioning. See [Section 4.3, "Adding or Removing Attribute Mappings for Provisioning"](#) for detailed information about the procedure.

4.2.2 Removing Attributes Used for Reconciliation

By default, the attributes listed in [Section 1.6.2, "Target System Columns Used in Reconciliation"](#) are mapped for reconciliation between Oracle Identity Manager and the target system. From that list of attributes, you must ensure that mappings for the following attributes are not modified or removed:

User Management connector

- Person ID
- User ID
- User name
- Effective Date From
- Effective Date To

User Management with HR Foundation connector

Attributes of the FND_USER record:

- User ID
- User name
- Effective Date From
- Effective Date To

Attributes of the HR Foundation record:

- Employee Number
- First Name
- Last Name
- Gender
- Person Type ID
- Business Group ID
- Hire Date
- Person ID

User Management with TCA Foundation connector

Attributes of the FND_USER record:

- User ID
- User name
- Effective Date From
- Effective Date To

Attributes of the TCA Foundation record:

- First Name
- Last Name
- Party ID

To remove an attribute from the list of attributes for reconciliation:

See Also: *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Open the properties file in a text editor, and remove the column from the query corresponding to the connector that you are using. Then, save and close the file.

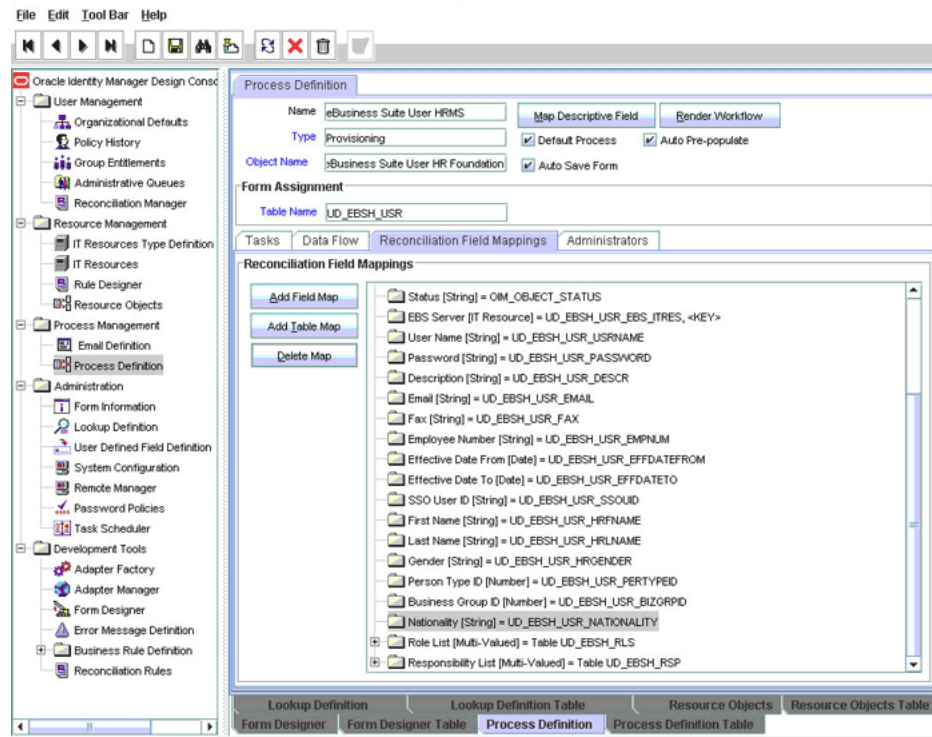
See Also:

[Section 1.6.1, "Reconciliation Queries"](#)

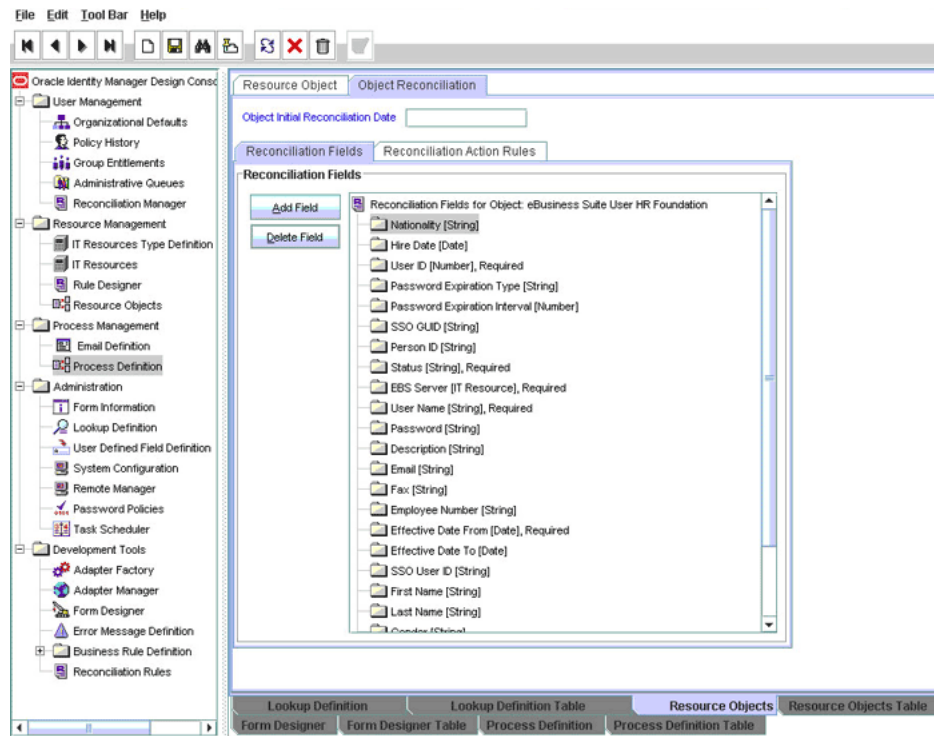
[Section 4.1.2, "Guidelines for Configuring Queries Used in Reconciliation"](#)

[Section 4.1.3, "Guidelines Common to Configuring Both Types of Queries"](#)

2. Save the file.
3. Log in to the Design Console.
4. Remove the reconciliation field mapping in the process definition as follows:
 - a. Expand the **Process Management** folder, and then double-click **Process Definition**.
 - b. Search for and open the process definition for the connector that you are using:
 See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
 - c. On the Reconciliation Field Mapping tab, select the mapping that you want to remove and then click **Delete Map**. The following screenshot shows this page:

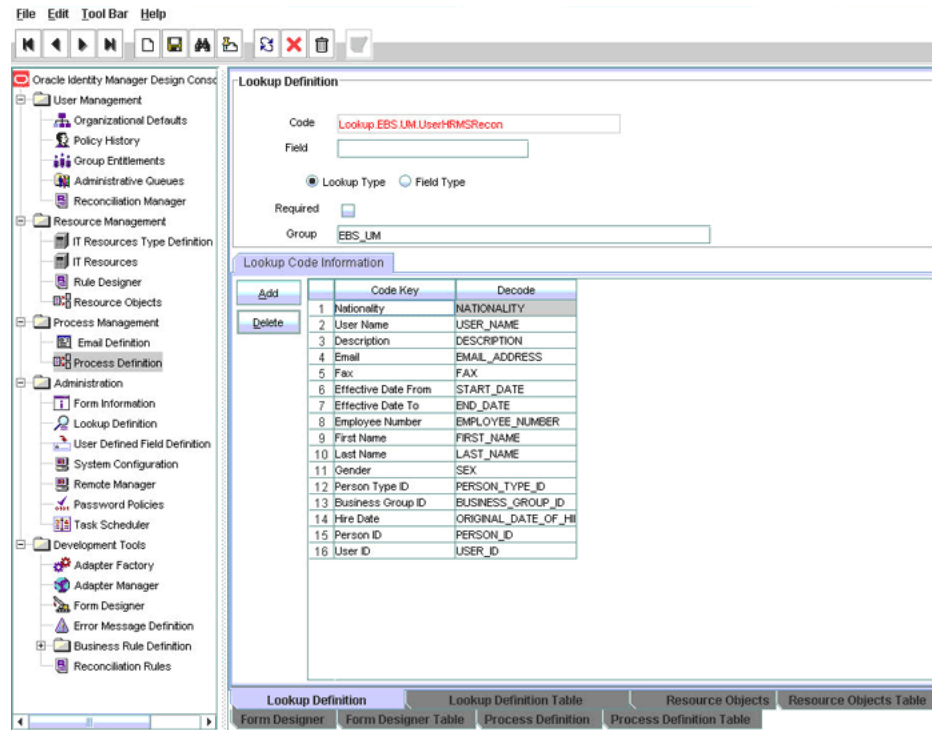


- d. Click the Save icon.
5. In the resource object definition, remove the reconciliation field corresponding to the attribute as follows:
 - a. Expand the **Resource Management** folder, and then double-click **Resource Objects**.
 - b. Search for and open the resource object corresponding to the connector that you are using:
 - Resource object for the User Management connector:
eBusiness Suite User
 - Resource object for the User Management with HR Foundation connector:
eBusiness Suite User HR Foundation
 - Resource object for the User Management with TCA Foundation connector:
eBusiness Suite User TCA Foundation
 - c. On the Object Reconciliation tab, select the attribute that you want to remove and then click **Delete Field**. The following screenshot shows this page:



- d. Click the Save icon, and then close the dialog box.
 - e. If you are using Oracle Identity Manager releases 11.1.x and 11.1.2.x, then click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.
 - f. Click the Save icon.
6. Remove the entry for the attribute in the lookup definition for reconciliation attribute mapping as follows:
 - a. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - b. Search for and open the lookup definition for the connector that you are using:
 - For User Management: Lookup.EBS.UM.UserRecon
 - For User Management with HR Foundation: Lookup.EBS.UM.UserHRMSRecon
 - For User Management with TCA Foundation: Lookup.EBS.UM.UserTCARecon

The following screenshot shows this page for the User Management connector:



- c. Select the row for the attribute that you want to remove, and then click **Delete**.
 - d. Click the Save icon.
7. Remove the attribute from the process form as follows:
 - a. Expand the **Development Tools** folder, and then double-click **Form Designer**.
 - b. Search for and open the process form for the connector that you are using:
See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
 - c. Click **Create New Version** to create a version of the process form. Then, enter a version name and click the Save icon.
 - d. Select the field that you want to remove, and then click **Delete**.

- e. Click the Save icon.
 - f. Click **Make Version Active** to activate the new version of the process form.
8. Remove the attribute from the list used for provisioning. See [Section 4.2.2, "Removing Attributes Used for Reconciliation"](#) for detailed information about the procedure.

4.3 Adding or Removing Attribute Mappings for Provisioning

By default, the attributes listed in [Section 1.7.2, "Attribute Mappings for Provisioning"](#) are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can add new attributes for provisioning.

Note: Attributes marked as mandatory in [Section 1.7.2, "Attribute Mappings for Provisioning"](#) cannot be modified or removed.

You cannot add, modify, or remove child form attributes for provisioning.

The connector uses custom stored procedures during User Create and User Update operations. These stored procedures are used to validate and transform data that is sent to the target system APIs. Wrapper packages are used to hold the custom stored procedures. [Table 1–10, "Provisioning Functions"](#) lists these wrapper packages.

Attributes used for provisioning are defined as parameters of both the custom and the target system stored procedures. If you add or remove an attribute (parameter) from a custom stored procedure, then you must make the same change in the target system stored procedure. This guideline forms the basis of one of the steps that you perform while adding or removing attributes for provisioning.

The original packages on the target system are part of the APPS user's schema. If you use the APPS user for connector operations, then the wrapper packages become part of

the APPS user's schema at the end of the connector deployment procedure. If you use a different user account for connector operations, then the wrapper packages are part of that user's schema. You use this information to locate the wrapper package to be modified while adding or removing attributes for provisioning.

The rest of this section describes the following procedures:

- [Section 4.3.1, "Adding New Attributes for Provisioning"](#)
- [Section 4.3.2, "Removing Attributes for Provisioning"](#)

4.3.1 Adding New Attributes for Provisioning

To add a new attribute for provisioning:

1. Add the attribute as a field on the process form or object form as follows:

Note: Proceed to the next step if you have already added the field to the process form while performing the procedure described in [Section 4.2.1, "Adding New Attributes for Reconciliation"](#).

- a. Expand **Development Tools**, and then double-click **Form Designer**.
- b. Search for and open the process form for the connector that you are using:
See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
- c. Click **Create New Version** to create a version of the form. Then, enter a version name and click the Save icon.
- d. Click **Add**. The following screenshot shows this page:

Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Apply
UD_EBSH_USR_PASSWORD	String	30	Password	PasswordField		3	
UD_EBSH_USR_DESCR	String	240	Description	TextField		4	
UD_EBSH_USR_EMAIL	String	240	Email	TextField		5	
UD_EBSH_USR_FAX	String	80	Fax	TextField		6	
UD_EBSH_USR_EMPNUM	String	30	Employee Number	TextField		12	
UD_EBSH_USR_EFFDATEFROM	Date		Effective Date From	DateFieldDlg		9	
UD_EBSH_USR_EFFDATETO	Date		Effective Date To	DateFieldDlg		10	
UD_EBSH_USR_SSUID	String	256	SSO User ID	TextField		11	
UD_EBSH_USR_PERTYPEID	long		Person Type ID	TextField		16	
UD_EBSH_USR_BIZGRPID	long		Business Group ID	TextField		17	
UD_EBSH_USR_SODCHECKSTATUS	String	50	SODCheckStatus	DOField	SODCheckNotInitiate	22	
UD_EBSH_USR_SODCHECKTRACKINGID	String	50	SODCheckTrackingID	DOField		23	
UD_EBSH_USR_SODCHECKRESULT	String	4000	SODCheckResult	DOField		24	
UD_EBSH_USR_SODCHECKVIOLATION	String	4000	SODCheckViolation	DOField		25	
UD_EBSH_USR_SODCHECKTIMESTAMP	String	50	SODCheckTimestamp	DOField		26	
UD_EBSH_USR_NATIONALITY	String	30	Nationality	TextField			

- e. Specify the properties of the attribute according to your requirement.
- f. Click the Save icon.

- g. Click **Make Version Active** to activate the new version of the process form.
2. To add the attribute as a parameter in the custom stored procedure:
 - a. Determine the name of the wrapper package that holds the custom stored procedure in which you must add the attribute. See [Section 1–10, "Provisioning Functions"](#) for a listing of the wrapper packages.
 - b. Add the parameter in the custom stored procedure.
 You can use a PL/SQL editor to open and edit the custom stored procedure. Alternatively, you can edit the custom stored procedure in the wrapper script provided on the connector installation package. To modify the stored procedure by using this script:
See Also: [Section 2.1.2.2, "Compiling Custom Wrapper Packages"](#) for information about the script
 - i. Open the package (.pck file) in a text editor.
 - ii. Add the parameter in the appropriate stored procedure.
 - iii. Save and close the file.
 - iv. Compile the package. See [Section 2.1.2.2, "Compiling Custom Wrapper Packages"](#) for information.
3. Modify the configurations lookup definition as follows:

Signatures of the custom stored procedures are stored in the following lookup definitions:

- For the User Management connector: Lookup.EBS.UM.Configuration
- For the User Management with HR Foundation connector: Lookup.EBS.UMHRMS.Configuration
- For the User Management with TCA Foundation connector: Lookup.EBS.UMTCA.Configuration

Depending on the stored procedure in which you add the parameter, you must make the required change in the corresponding lookup definition as follows:

- a. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
- b. Search for and open one of the following lookup definitions:
 - Lookup.EBS.UM.Configuration
 - Lookup.EBS.UMTCA.Configuration
 - Lookup.EBS.UMHRMS.Configuration
- c. Search for the entry containing the stored procedure signature that you modified earlier.
- d. In the Decode column, add a question mark (?) to the list of question marks.

Note: Each question mark in the signature value of the Decode column stands for a parameter of the stored procedure.

- e. Click the Save icon.

4. Add an entry in the lookup definition for provisioning attribute mappings as follows:

Note: Perform this step only if you are using FND user attributes as extended attributes.

- a. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
 - b. Search for and open the lookup definition for the connector that you are using:
 For the User Management connector: Lookup.EBS.UM.UserProvisioning
 For the User Management with HR Foundation connector:
 Lookup.EBS.UM.UserHRMSProvisioning
 For the User Management with TCA Foundation connector:
 Lookup.EBS.UM.UserTCAProvisioning
 - c. To add a row, click **Add**.
 - d. In the **Code Key** column, enter the field name (column name) for the attribute on the process form. See Step 1 for information about this field name.
 - e. In the **Decode** column, enter the stored procedure argument metadata.
 - f. Click the Save icon.
5. If you are using Employee record fields as extended attributes, then:
 - Add an entry in the Lookup.EBS.UM.CreateEmployee and Lookup.EBS.UM.UpdateEmployee lookup definitions as follows:
 - a. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
 - b. Search for and open the **Lookup.EBS.UM.CreateEmployee** lookup definition.
 - c. To add a row, click **Add**.
 - d. In the **Code Key** column, enter the process form field name added in Step 1.
 - e. In the **Decode** column, enter information about the corresponding argument in the stored procedure used for HRMS person record provisioning.
 - f. Click the Save icon.
 - g. Repeat steps 5.b through 5.f with the following difference:
 While performing step 5.b, search for and open the **Lookup.EBS.UM.UpdateEmployee** lookup definition, instead of Lookup.EBS.UM.CreateEmployee.
 - Add an entry in the Lookup.EBS.UMHRMS.EmployeeInfoMapping lookup definition as follows:
 - a. In the **Code Key** column, enter the name of the process form column for information about the HR Foundation person record.
 - b. In the **Decode** column, enter the name of the column used for fetching the person record data from the target system database.

- Modify the `Lookup.EBS.UMHRMS.Configuration` lookup definition as follows:
 - a. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
 - b. Search for and open the `Lookup.EBS.UMHRMS.Configuration` lookup definition.
 - c. Search for the `GET_EMPLOYEE_DATA_QUERY` code key entry.
 - d. In the **Decode** column, modify the SELECT statement to include the newly added attribute (in Step 1).
 - e. Click the Save icon.
- 6. If you are using person party record fields as extended attributes, then add an entry in the `Lookup.EBS.UM.PartyProvisioning` and `Lookup.EBS.UM.UpdateParty` lookup definitions as follows:
 - a. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
 - b. Search for and open the `Lookup.EBS.UM.PartyProvisioning` lookup definition.
 - c. To add a row, click **Add**.
 - d. In the **Code Key** column, enter the process form field name added in Step 1.
 - e. In the **Decode** column, enter information about the corresponding argument in the stored procedure used for HRMS person record provisioning.
 - f. Click the Save icon.
 - g. Repeat steps 6.b through 6.f with the following difference:
While performing step 6.b, search for and open the `Lookup.EBS.UM.UpdateParty` lookup definition, instead of `Lookup.EBS.UM.PartyProvisioning`.
- 7. Add the attribute as a reconciliation field in the resource object:
 - a. On the Design Console, expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the resource object for the connector that you are using.
See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process forms for each connector.
 - c. Click **Add Field**.
 - d. Enter the field name and field type
 - e. If you want make this a mandatory field for reconciliation, then select the Required check box.
 - f. Click the Save icon.
- 8. To enable updates of the attribute, add an update process task in the process definition as follows:

Note: Ensure that the stored procedure in which you add the attribute (parameter) must be able to post updates of this attribute to the target system database.

To add an update process task:

- a. On the Design Console, expand **Process Management**, and then double-click **Process Definition**.

- b. Search for and open the process definition for the connector that you are using:

For the User Management connector: eBusiness Suite User

For the User Management with HR Foundation connector: eBusiness Suite User HRMS

For the User Management with TCA Foundation connector: eBusiness Suite User TCA

- c. On the Tasks tab, click **Add**.
- d. On the General tab of the dialog box that is displayed, enter a name and description for the task. The following screenshot shows this page:

Note: The name must be in the *PROCESS_FORM_FIELD_NAME* Updated format.

- e. Click the Save icon.
- f. On the Integration tab, attach the adapter. Depending upon the category of the user record adapter for adapter mapping to which the attribute is being added, use one of the following adapters:

If the new attribute belongs to the FND_USER, then integrate with the adpEBSUPDATEUSER adapter.

If the new attribute belongs to the HRMS Person record, then integrate it with the adpEBSUPDATEEMPLOYEE adapter.

If the new attribute belongs to the TCA Party record, then integrate it with the adpEBSUPDATEPARTY adapter.

Note: Do not use the adapter used for Username Updated task

- g. Click the Save icon.
- h. On the Response tab, add appropriate responses.
For sample responses, see an existing process tasks such as the Password Updated process task.
- i. Click the Save icon.
- j. If you added the attribute in both the resource object and the process form, then go to the Data Flow tab and perform the instructions up to Step r.
- k. Click **Add Field Map**.
- l. Select the name of the field, from the second select box, for the object form field that you added.
- m. Select the name of the corresponding field, from the third select box, for the process form field that you added.
- n. Click the Save icon.

- o. On the Reconciliation Field Mapping tab, click **Add Field Map**.
 - p. In the dialog box that is displayed, select one from the Field name drop-down box; this field name corresponds to the attribute name in Resource Object.
 - q. Double-click the Process Data Field, a new pop-up will appear. The entries in the pop-up correspond to the process form fields.
 - r. Select the corresponding newly added field from the pop-up.
 - s. If the field mapping is a key field for matching the process data, then check the key Field for Reconciliation matching check box.
 - t. Click the Save icon, and then close the dialog box.
9. Adding the attribute for reconciliation.

When you add an attribute on the process form, you must also enable reconciliation of values for that attribute from the target system. See [Section 4.2.1, "Adding New Attributes for Reconciliation"](#) for more information.

Note: ■ Perform steps 10 and 11 only if you want to perform request-based provisioning.

10. Update the request dataset.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

- a. In a text editor, open the XML file located in the *OIM_HOME/DataSet/file* directory for editing.
- b. Add the `AttributeReference` element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

For example, while performing Step 1 of this procedure, if you added City as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "City"
attr-ref = "City"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

In this `AttributeReference` element:

- For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if `UD_EBSH_USR_CITY` is the value in the Name column of the process form, then you must specify `CITY` as the value of the name attribute in the `AttributeReference` element.

- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 1.

- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 1.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 1.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 1.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing Step 1, if you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

11. Run the PurgeCache utility to clear content related to request datasets from the server cache.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

12. Import into MDS, the request dataset definitions in XML format.

See the ["Importing Request Datasets into MDS"](#) section for detailed information about the procedure.

Note: This step is only required for release 11.1.2 and request datasets are not required for it.

13. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See [Section 2.3.3.2.2, "Creating a New UI Form"](#) and [Section 2.3.3.2.6, "Updating an Existing Application Instance with a New Form"](#) for the procedures.

4.3.2 Removing Attributes for Provisioning

By default, the attributes listed in [Section 1.7.2, "Attribute Mappings for Provisioning"](#) are mapped for provisioning between Oracle Identity Manager and the target system. From that list of attributes, you must ensure that mappings for the following attributes are not modified or removed:

User Management connector

- Person ID
- User ID
- User name
- Effective Date From
- Effective Date To

User Management with HR Foundation connector

Attributes of the FND_USER record:

- User ID
- User name

- Effective Date From
- Effective Date To

Attributes of the HR Foundation record:

- Employee Number
- First Name
- Last Name
- Gender
- Person Type ID
- Business Group ID
- Hire Date
- Person ID

User Management with TCA Foundation connector

Attributes of the FND_USER record:

- User ID
- User name
- Effective Date From
- Effective Date To

Attributes of the TCA Foundation record:

- First Name
- Last Name
- Party ID

All three connectors support direct provisioning and request-based provisioning. There are resource object forms corresponding to all the process forms. During request-based provisioning, if the end user is not allowed to enter data for the attribute (field) that you want to remove, then only the process form must be modified. If the end user is allowed to enter data for the attribute, then the attribute must be removed from both the resource object form and the process form.

To remove the attribute (field) from the process form or resource object form:

Note: If the attribute is to be removed only from the process form, then you must also remove any pre-populate adapter that is associated with the attribute.

To remove an attribute for provisioning:

1. Remove the attribute as a field on the process form or object form as follows:

Note: Directly proceed to the next step if you have already added the field to the process form while performing the procedure described in [Section 4.2.2, "Removing Attributes Used for Reconciliation"](#).

- a. Expand **Development Tools**, and then double-click **Form Designer**.

- b. Search for and open the process form for the connector that you are using:
See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.
 - c. Click **Create New Version** to create a version of the form. Then, enter a version name and click the Save icon.
 - d. Select the attribute to be deleted, and then click **Delete**.
 - e. Click the Save icon.
 - f. Click **Make Version Active** to activate the new version of the process form.
2. To remove the attribute (parameter) from the custom stored procedure:
 - a. Determine the name of the wrapper package that holds the custom stored procedure in which you must add the attribute. See [Section 1–10, "Provisioning Functions"](#) for a listing of the wrapper packages.
 - b. Remove the parameter from the custom stored procedure.

You can use a PL/SQL editor to open and edit the custom stored procedure. Alternatively, you can edit the custom stored procedure in the wrapper script provided on the connector installation package. To modify the stored procedure by using this script:

See Also: [Section 2.1.2.2, "Compiling Custom Wrapper Packages"](#) for information about the script

 - i. Open the package (.pck file) in a text editor.
 - ii. Add the parameter in the appropriate stored procedure.
 - iii. Save and close the file.
 - iv. Compile the package. See [Section 2.1.2.2, "Compiling Custom Wrapper Packages"](#) for information.
3. Modify the configurations lookup definition as follows:

Signatures of the custom stored procedures are stored in the following lookup definitions:

 - For the User Management connector: Lookup.EBS.UM.Configuration
 - For the User Management with HR Foundation connector: Lookup.EBS.UMHRMS.Configuration
 - For the User Management with TCA Foundation connector: Lookup.EBS.UMTCA.Configuration

Depending on the stored procedure in which you add the parameter, you must make the required change in the corresponding lookup definition as follows:

 - a. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
 - b. Search for and open one of the following lookup definitions:
 - Lookup.EBS.UM.Configuration
 - Lookup.EBS.UMTCA.Configuration
 - Lookup.EBS.UMHRMS.Configuration

- c. Search for the entry containing the stored procedure signature that you modified earlier.
- d. In the Decode column, remove a question mark (?) from the list of question marks. The following screenshot shows this page:

Note: Each question mark in the signature value of the Decode column stands for a parameter of the stored procedure.

- e. Click the Save icon.
4. Remove the entry from the lookup definition for provisioning attribute mappings as follows:
 - a. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
 - b. Search for and open the lookup definition for the connector that you are using:
 For the User Management connector: Lookup.EBS.UM.UserProvisioning
 For the User Management with HR Foundation connector:
 Lookup.EBS.UM.UserHRMSProvisioning
 For the User Management with TCA Foundation connector:
 Lookup.EBS.UM.UserTCAProvisioning
 - c. To remove the row corresponding to the attribute that you want to remove, select the row and then click **Delete**.
 - d. Click the Save icon
 5. If you are removing attributes specific to Employee record fields, then:
 - a. Remove the entry for the attribute from the Lookup.EBS.UM.CreateEmployee, Lookup.EBS.UM.UpdateEmployee, and Lookup.EBS.UMHRMS.EmployeeInfoMapping lookup definitions.
 - b. Modify the Lookup.EBS.UMHRMS.Configuration lookup definition by removing the attribute from the SELECT statement of the **GET_EMPLOYEE_DATA_QUERY** code key entry.
 6. If you are removing attributes specific to person party record fields, then remove the entry for the attribute from the Lookup.EBS.UM.PartyProvisioning and Lookup.EBS.UM.UpdateParty lookup definitions.
 7. Remove the attribute (reconciliation field) from the resource object:
 - a. On the Design Console, expand **Resource Management**, and then double-click **Resource Objects**.
 - b. Search for and open the resource object for the connector that you are using.
 See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process forms for each connector.
 - c. Select the field that you want to remove, and then click **Delete Field**.
 - d. Click the Save icon.
 8. From the appropriate provisioning process definition, delete the process task corresponding to the attribute that you want to delete as follows:

Note: Ensure that the stored procedure in which you add the attribute (parameter) is able to post updates of this attribute to the target system database.

- a. On the Design Console, expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the process definition for the connector that you are using:
 For the User Management connector: eBusiness Suite User
 For the User Management with HR Foundation connector: eBusiness Suite User HRMS
 For the User Management with TCA Foundation connector: eBusiness Suite User TCA
 - c. On the Tasks tab, select the process task to be deleted and then click **Delete**.
 - d. Click the Save icon.
 - e. If the fields must be deleted from both the process form and the resource object form, then:
 Select the mapping to be deleted.
 Click Delete Field Map.
 Click the Save icon.
 - f. If there is more than one data flow mapping to be deleted, repeat the preceding step.
 - g. On the Reconciliation Field Mapping page, select the mapping to be deleted.
 - h. Click Delete Field Map.
 - i. If there are multiple mappings to be removed, then repeat the preceding two steps.
 - j. Click the Save icon.
9. Remove the attribute for reconciliation as follows:
 See [Section 4.2.2, "Removing Attributes Used for Reconciliation"](#) for more information.

Note: ■Perform steps 10 and 11 only if you want to perform request-based provisioning.

10. Update the request dataset.
 When you remove an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:
 - a. In a text editor, open the XML file located in the *OIM_HOME/DataSet/file* directory for editing.
 - b. Remove the AttributeReference element corresponding to the attribute removed from the process form while performing Step 1. If you remove more

than one attribute from the process form, then repeat this step for each attribute that you remove.

For example, while performing Step 1 of this procedure, if you remove the City attribute from the process form, then remove the following line:

```
<AttributeReference
name = "City"
attr-ref = "City"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

- c. Save and close the XML file.
11. Run the PurgeCache utility to clear content related to request datasets from the server cache.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

12. Import into MDS, the request dataset definitions in XML format.

See the ["Importing Request Datasets into MDS"](#) section for detailed information about the procedure.

4.4 Adding Filter Parameters in a Reconciliation Query

You can add a parameter in the WHERE clause of a reconciliation query and specify a value for the parameter in the reconciliation scheduled task. For example, you can add a parameter in the WHERE clause of the UM_USER_RECON query so that it returns records of users whose user name is the one that you specify in the scheduled task.

To add a parameter in a reconciliation query:

Note: Before you modify a query in the properties file, you must run the query by using any standard database client to ensure that the query produces the required results when run against the target system database.

1. Modify the query as follows:
 - a. Open the properties file in a text editor.
 - b. Add the parameter condition in the WHERE clause of the query that you want to modify. Use the :PARAMETER_NAME format to represent the parameter for which a value is provided in the scheduled task.

Note:

The parameter name must begin with the colon (:) as a prefix. In addition, there must be no space between the colon and parameter name and within the parameter name.

You can add multiple parameters in a single query.

In the following example, the condition highlighted in bold has been added to the WHERE clause of the UM_USER_RECON query:

```
WHERE ((LAST_UPDATE_DATE - TO_DATE('01011970','ddmmyyyy')) *24*60*60*1000)
> :lastExecutionTime) \
AND UPPER(user_name)=UPPER(:userName) \
```

Note: The UPPER function has been used in this example because the target system stores the user names in uppercase letters.

- c. Save and close the properties file.
2. Configure the Lookup.EBS.UM.QueryFilters lookup definition as follows:
 - a. Log in to the Design Console.
 - b. Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - c. Search for and open the appropriate lookup definition:
 - Lookup.EBS.UM.QueryFilter
 - Lookup.EBS.UMHRMS.QueryFilter
 - Lookup.EBS.UMTCA.QueryFilter
 - d. To add a row, click **Add**.
 - e. In the **Code Key** column, enter the variable name that you specified in the properties file. Do not include the colon (:) character. For example, enter `username` in the Code Key column.
 - f. In the **Decode** column, enter the value that you want to assign to the parameter for subsequent reconciliation runs. Use one of the following formats to specify a value:
 - `value|STRING`
Sample value: `jdoe|STRING`

Note: For the USER NAME example, you can enter the preceding sample value.

- `value|DATE|DATE_FORMAT`
Sample value: `24-Mar-09|DATE|DD-Mon-YY`
- `value|NUMBER`
Sample value: `33|NUMBER`

- g. Click the Save icon.

When you next run the query that you have modified, the condition that you add is applied as an additional filter during reconciliation.

4.5 Modifying Field Lengths on the Process Form

You might want to modify the lengths of fields (attributes) on the process form. For example, if you use the Japanese locale, then you might want to increase the lengths of process form fields to accommodate multibyte data from the target system.

If you want to modify the length of field on the process form, then:

1. Log in to the Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the process form.

See [Section 4.9, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of process forms for each connector. The following screenshot shows this page:

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Apply
1	UD_EBSH_USR_NATIONALITY	String	15	Nationality	TextField		27	
2	UD_EBSH_USR_HIREDATE	Date		Hire Date	DateFieldDlg		18	
3	UD_EBSH_USR_PSWD_EXP_TYPE	String	30	Password Expiration	LookupField		7	
4	UD_EBSH_USR_PERSONID	long		Person ID	DOField		21	
5	UD_EBSH_USR_HRLNAME	String	150	Last Name	TextField		14	
6	UD_EBSH_USR_HRGENDER	String	10	Gender	LookupField		15	
7	UD_EBSH_USR_HRFNAME	String	150	First Name	TextField		13	
8	UD_EBSH_USR_PSWD_EXP_INTVL	long		Password Expiration	TextField		8	
9	UD_EBSH_USR_USERID	long		User ID	DOField		19	
10	UD_EBSH_USR_SSOIDENT	String	256	SSO GUID	DOField		20	
11	UD_EBSH_USR_EBS_ITRES	long		EBS Server	ITResourceLoo		1	
12	UD_EBSH_USR_USRNAME	String	100	User Name	TextField		2	
13	UD_EBSH_USR_PASSWORD	String	30	Password	PasswordField		3	
14	UD_EBSH_USR_DESCR	String	240	Description	TextField		4	
15	UD_EBSH_USR_EMAIL	String	240	Email	TextField		5	

4. Modify the length of the required field.
5. Click the Save icon.

4.6 Configuring Validation of Data During Reconciliation

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the Email attribute to ensure that it does not contain the number sign (#).

Note: This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

The validation class must implement the `oracle.iam.connectors.common.validate.Validator` interface and the `validate` method.

The following sample validation class checks if the value in the Email attribute contains the number sign (#):

```
package oracle.iam.connectors.common.validate;
import java.util.HashMap;
public class TestValidator implements Validator {
    public boolean validate(HashMap hmUserDetails,
        HashMap hmEntitlementDetails, String field) {
        /*
         * You must write code to validate attributes. Parent
         * data values can be fetched by using hmUserDetails.get(field)
         * For child data values, loop through the
         * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
         * Depending on the outcome of the validation operation,
         * the code must return true or false.
         */
        /*
         * In this sample code, the value "false" is returned if the field
         * contains the number sign (#). Otherwise, the value "true" is
         * returned.
         */
        boolean valid=true;
        String sEmail=(String) hmUserDetails.get(field);
        for(int i=0;i<sEmail.length();i++){
            if (sEmail.charAt(i) == '#'){
                valid=false;
                break;
            }
        }
        return valid;
    }
}
```

2. Create a JAR file to hold the Java class.
3. If you are using Oracle Identity Manager release 9.1.0.x, then copy the JAR file into the `OIM_HOME/xellerate/ScheduleTask` directory:

See Also: The Java documents shipped with the connector for more information about this interface

4. If you are using Oracle Identity Manager release 11g, then use UploadJars utility to upload the JAR file into the database.
5. Log in to the Design Console.
6. Search for and open the **Lookup.EBS.UM.Validation** lookup definition. If it does not exist, create one.
7. In the **Code Key** column, enter the resource object attribute name. In the **Decode** column, enter the class name that is implementing the validation logic.

For example, if you want to perform validation of the Email attribute, then you must enter the following values in the Code Key and Decode columns:

- Code Key: Email

- Decode: oracle.iam.connectors.common.validate.TestValidator

Here, the Code Key specifies the name of the resource object attribute that you want to validate and Decode is the complete package name of the Implementation class.

8. Save the changes to the lookup definition.
9. To enable validation in the scheduled task for your database, set the value of the Use Validation For Reconciliation entry to yes, and then save your changes.

Note: Follow the similar procedure for HRMS and TCA connectors with the lookup names Lookup.EBS.UMHRMS.Validation and Lookup.EBS.UMTCA.Validation.

4.7 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled single-valued account data according to your requirements. For example, you can use email to create a different value for the Email field in Oracle Identity Manager.

Note: This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure transformation of single-valued account data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class.

The transformation class must implement the oracle.iam.connectors.common.transform.Transformation interface and the transform method.

The following sample transformation class creates a value for the Email attribute by using values fetched from the Email of the target system:

```
package oracle.iam.connectors.common.transform;
import java.util.HashMap;
public class TestTransformer implements Transformation {
    /*
        Description:Abstract method for transforming the attributes
        param hmUserDetails<String,Object>
        HashMap containing parent data details
        param hmEntitlementDetails <String,Object>
        HashMap containing child data details
    */
    public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails,String sField) {
        /*
            * You must write code to transform the attributes.
            * Parent data attribute values can be fetched by using
            * hmUserDetails.get("Field Name").
            * To fetch child data values, loop through the
            * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
            * Return the transformed attribute.
        */
        String sEmail= "trans" + (String)hmUserDetails.get(sField);
```

```
        return sEmail;
    }
```

2. Create a JAR file to hold the Java class.
3. If you are using Oracle Identity Manager release 9.1.0.x, then copy the JAR file into the following *OIM_HOME/xellerate/ScheduleTask* directory.

See Also: The Java documents shipped with the connector for more information about this interface

4. If you are using Oracle Identity Manager release 11g, then use UploadJars utility to upload the JAR file into the database.
5. Log in to the Design Console.
6. Search for and open the **Lookup.EBS.UM.Transformation** lookup definition. If it does not exist, create one.
7. In the **Code Key** column, enter the resource object attribute name. In the **Decode** column, enter the class name that is implementing the validation logic.

For example, if you want to perform validation of the Email attribute, then you must enter the following values in the Code Key and Decode columns:

- Code Key: Email
- Decode: oracle.iam.connectors.common.transform.TestTransformer

Here, the Code Key specifies the name of the resource object attribute that you want to validate and Decode is the complete package name of the Implementation class.

8. Save the changes to the lookup definition.
9. To enable transformation in the scheduled task for your database, set the value of the Use Transformation For Reconciliation entry to yes, and then save your changes.

Note: Follow the similar procedure for HRMS and TCA connectors with the lookup names Lookup.EBS.UMHRMS.Transformation and Lookup.EBS.UMTCA.Transformation.

4.8 Configuring Validation of Data During Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the Email attribute to ensure that it does not contain the number sign (#).

Note: This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

The validation class must implement the `oracle.iam.connectors.common.validate.Validator` interface and the `validate` method.

The following sample validation class checks if the value in the Email attribute contains the number sign (#):

```
package oracle.iam.connectors.common.validate;
import java.util.HashMap;
public class TestValidator implements Validator {
    public boolean validate(HashMap hmUserDetails,
        HashMap hmEntitlementDetails, String field) {
        /*
        * You must write code to validate attributes. Parent
        * data values can be fetched by using hmUserDetails.get(field)
        * For child data values, loop through the
        * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
        * Depending on the outcome of the validation operation,
        * the code must return true or false.
        */
        /*
        * In this sample code, the value "false" is returned if the field
        * contains the number sign (#). Otherwise, the value "true" is
        * returned.
        */
        boolean valid=true;
        String sEmail=(String) hmUserDetails.get(field);
        for(int i=0;i<sEmail.length();i++){
            if (sEmail.charAt(i) == '#'){
                valid=false;
                break;
            }
        }
        return valid;
    }
}
```

2. Create a JAR file to hold the Java class.
3. If you are using Oracle Identity Manager release 9.1.0.x, then copy the JAR file into the `OIM_HOME/xellerate/ScheduleTask` directory:

See Also: The Java documents shipped with the connector for more information about this interface

4. If you are using Oracle Identity Manager release 11g, then use UploadJars utility to upload the JAR file into the database.
5. Log in to the Design Console.
6. Search for and open the **Lookup.EBS.UM.Prov.Validation** lookup definition. If it does not exist, create one.
7. In the **Code Key** column, enter the resource object attribute name. In the **Decode** column, enter the class name that is implementing the validation logic.

For example, if you want to perform validation of the Email attribute, then you must enter the following values in the Code Key and Decode columns:

- Code Key: UD_EBS_USER_EMAIL
- Decode: oracle.iam.connectors.common.validate.TestValidator

Here, the Code Key specifies the name of the resource object attribute that you want to validate and Decode is the complete package name of the Implementation class.

8. Save the changes to the lookup definition.

9. To enable validation, set the value of the Use Validation For Provisioning entry to yes in the lookup definition Lookup.EBS.UM.Configuration and then save the changes.

Note: Follow the similar procedure for HRMS and TCA connectors with the lookup names Lookup.EBS.UMHRMS.Prov.Validation, Lookup.EBS.UMTCA.Prov.Validation, Lookup.EBS.UMHRMS.Configuration, and Lookup.EBS.UMTCA.Configuration.

4.9 Configuring the Connector for Multiple Installations of the Target System

You may want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must configure the connector for each installation of the target system. To do so, create copies of the connector objects listed in the following table:

See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

Table 4–1 Connector Objects

Connector Object	User Management	User Management with HR Foundation	User Management with TCA Foundation
Resource Objects			
	eBusiness Suite User	eBusiness Suite User HR Foundation	eBusiness Suite User TCA Foundation
	eBusiness Suite User Responsibility	eBusiness Suite User HR Foundation Responsibility	eBusiness Suite User TCA Foundation Responsibility
	eBusiness Suite User Role	eBusiness Suite User HR Foundation Role	eBusiness Suite User TCA Foundation Role
Process Definitions			
	eBusiness Suite User	eBusiness Suite User HRMS	eBusiness Suite User TCA
	eBusiness Suite User Request	eBusiness Suite User HRMS Req	eBusiness Suite User TCA Req
	EBS User Responsibility	EBS UM HRMS Responsibility	EBS UM TCA Responsibility
	EBS User Responsibility Req	EBS UM HRMS Responsibility Req	EBS UM TCA Responsibility Req
	EBS User Role	EBS UM HRMS Role	EBS UM TCA Role
	EBS User Role Request	EBS UM HRMS Role Req	EBS UM TCA Role Request
Process and Object Forms			
	UD_EBS_UO	UD_EBSH_UO	UD_EBST_UO

Table 4–1 (Cont.) Connector Objects

Connector Object	User Management	User Management with HR Foundation	User Management with TCA Foundation
	UD_EBS_RSO	UD_EBSH_RSO	UD_EBST_RSO
	UD_EBS_RLO	UD_EBSH_RLO	UD_EBST_RLO
	UD_EBS_USER	UD_EBSH_USR	UD_EBST_USR
	UD_EBS_RESP	UD_EBSH_RSP	UD_EBST_RSP
	UD_EBS_RLS	UD_EBSH_RLS	UD_EBST_RLS
	UD_EBS_RLPO	UD_EBH_RLPO	UD_EBT_RLPO
	UD_EBS_RLCO	UD_EBH_RLCO	UD_EBT_RLCO
	UD_EBS_RLPP	UD_EBH_RLPP	UD_EBT_RLPP
	UD_EBS_RLCP	UD_EBH_RLCP	UD_EBT_RLCP
	UD_EBS_RSPO	UD_EBH_RSPO	UD_EBT_RSPO
	UD_EBS_RSCO	UD_EBH_RSCO	UD_EBT_RSCO
	UD_EBS_RSPP	UD_EBH_RSPP	UD_EBT_RSPP
	UD_EBS_RSCP	UD_EBH_RSCP	UD_EBT_RSCP
Process Task Type Adapters			
	EBS Create User	EBS Create User HRMS	EBS Create User TCA
	EBS Update Employee	EBS Update Party	
Lookup Definitions			
	Lookup.EBS.UM.UserProvisioning	Lookup.EBS.UM.UserHRMSProvisioning	Lookup.EBS.UM.UserTCAProvisioning
	Lookup.EBS.UM.UserRecon	Lookup.EBS.UM.UserHRMSRecon	Lookup.EBS.UM.UserTCAREcon
	Lookup.EBS.UM.Configuration	Lookup.EBS.UMHRMS.Configuration	Lookup.EBS.UMTCA.Configuration
	Lookup.EBS.Roles.Mapping	Lookup.EBS.UM.CreateEmployee	Lookup.EBS.UM.PartyProvisioning
	Lookup.EBS.Responsibility.Mapping	Lookup.EBS.UM.UpdateEmployee	Lookup.EBS.UM.UpdateParty
	Lookup.EBS.UM.QueryFilters	Lookup.EBS.UMHRMS.EmployeeInfoMapping	Lookup.EBS.UserTCAResponsibility.Mapping
		Lookup.EBS.HRMSRole.Mapping	Lookup.EBS.UserTCARoles.Mapping
		Lookup.EBS.HRMSResponsibility.Mapping	Lookup.EBS.UMTCA.QueryFilters
		Lookup.EBS.UMHRMS.QueryFilters	
Scheduled Tasks			

Table 4–1 (Cont.) Connector Objects

Connector Object	User Management	User Management with HR Foundation	User Management with TCA Foundation
	eBusiness UM Target Resource User Reconciliation	eBusiness UM Target Resource User-HRMS Reconciliation	eBusiness UM Target Resource User-TCA Reconciliation
IT Resources			
	EBS-APPS12	EBSHF-APPS12	EBSTCAF-APPS12

Apply the following guidelines while creating copies of the connector objects:

- In copies of the forms (both process and object forms), the last segment of the form name corresponding to each form must be maintained. In other words, the names of the form copies must end in the same string as the original forms.
For example, the copy of the UD_EBS_USER form must be in the format UD_NAME_USER. In this format, the last part of the form name (_USER) is retained.
- In copies of child forms, the names of forms fields in the copy of the child form must end in the same string as the names of fields in the original form.
For example, the copy of the UD_EBS_RESP_APP_NAME field must be in the format UD_NAME_RESP_APP_NAME.
- While creating copies of the adapters listed in the preceding table, the literal values used for Process Form field names, resource object names, and lookup field names in the adapters must be modified.
- While creating copies of the process tasks in each of the process definition, the required changes must be made in the literal values that are passed to the process form fields.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

When you configure the scheduled task for reconciliation, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

4.10 Customizing the Connector to Handle Timezone Differences

If Oracle Identity Manager and the target system are running in different timezones, then fields storing date values must be converted from the Oracle Identity Manager timezone to the timezone of the target system. This must be done using custom wrapper packages that are shipped with connector.

The following example shows the procedure that must be followed while handling the employee hire date field, when Oracle Identity Manager and the target system are running in two different timezones:

1. Open the OIM_EMPLOYEE_WRAPPER.pck file in a text editor.
2. Edit the **create_emp_api** stored procedure by ensuring that the hire date which is passed to hr_employee_api.create_employee() is in the timezone of the target system than the timezone of Oracle Identity Manager. In other words, convert p_hire_date value from the Oracle Identity Manager timezone value to the target system timezone value.

3. Declare the `l_hire` local variable by adding the following entry to the "Declare cursors and local variables" section:

```
l_hire_date per_all_people_f.original_date_of_hire%type;
```

4. Initialize the `l_hire` local variable with appropriate `TIMEZONE_DIFF_HOURS` as follows:

- If the timezone of Oracle Identity Manager is ahead of the timezone of the target system, then add the following entry:

```
l_hire_date:= trunc(p_hire_date-TIMEZONE_DIFF_HOURS/24)
```

In this entry, replace `TIMEZONE_DIFF_HOURS` with the difference in the number of hours between the timezone of Oracle Identity Manager and the target system.

- If the timezone of the target system is ahead of the timezone of Oracle Identity Manager, then add the following entry:

```
l_hire_date:= trunc(p_hire_date+TIMEZONE_DIFF_HOURS/24)
```

In this entry, replace `TIMEZONE_DIFF_HOURS` with the difference in the number of hours between the timezone of Oracle Identity Manager and the target system.

For example:

```
l_hire_date:= trunc(p_hire_date-12.5/24);
```

In this example, Oracle Identity Manager is in a timezone that is 12 hours and 30 minutes ahead of the timezone of the target system. Therefore, the timezone difference has been mentioned as "-12.5".

Note: The conversion in the preceding example is a sample. You can customize it according to the requirements in your production environment.

5. Pass the local variable `l_hire` date value to `hr_employee_api.create_employee()` API by replacing `p_hire_date` with `l_hire_date`. The following is a code snippet that highlights the change:

Start of API

```
hr_employee_api.create_employee
(p_hire_date=> l_hire_date
```

6. Save and close the `OIM_EMPLOYEE_WRAPPER.pck` file.
7. Import the `OIM_EMPLOYEE_WRAPPER.pck` file into the target system database for the changes to take effect.

Note:

- Perform similar steps for any date fields used in the connector by changing appropriate wrapper package and modifying the configuration lookup definition to use the custom wrapper package, for the changes to take effect.
 - After performing this procedure, values in the date fields in the process form still hold values in the Oracle Identity Manager timezone. Therefore, perform a target reconciliation run to set the values in the date fields to values in the target system timezone.
-
-

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- [Section 5.1, "Running Test Cases"](#)
- [Section 5.2, "Troubleshooting"](#)

5.1 Running Test Cases

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

The testing utility is located in the /test directory of the installation media.

To use the testing utility:

1. Open one of the following files:
 - For Oracle Identity Manager release 9.1.0.x:
`OIM_HOME/xellerate/XLintegrations/EBSUM/config/config_um_prov.properties`
 - For Oracle Identity Manager releases 11.1.x and 11.1.2.x:
`OIM_HOME/server/XLintegrations/EBSUM/config/config_um_prov.properties`
2. Specify values for the attributes in this file. These attributes are described in the following table.

Attribute	Description	Sample Value
MODE	Specifies the mode to run the testing utility Note: For this release of the connector, only the FILE mode is supported.	FILE
PROPERTIES_FILE_NAME	Specifies the name of the properties file that contains data for the testing utility	config_um_prov_fileOption.properties
ACTION	Specifies the provisioning action to be performed by the testing utility	The required action can be CONNECT,CREATE_USER, UPDATE_USER, DISABLE_USER, ENABLE_USER, ADD_RESPONSIBILITY, or REMOVE_RESPONSIBILITY.

3. Open one of the following files:

- For Oracle Identity Manager release 9.1.0.x:
OIM_HOME/xellerate/XLIntegrations/EBSUM/config/config_um_prov_fileOption.properties
 - For Oracle Identity Manager releases 11.1.x and 11.1.2.x:
OIM_HOME/server/XLIntegrations/EBSUM/config/config_um_prov_fileOption.properties
4. Specify values for the following parameters listed in the file:

Parameter	Description
ITR.CONNECTION_RETRIES	Enter the number of consecutive attempts to be made to establish a connection with the target system. Sample value: 3
ITR.RETRY_INTERVAL	Enter the interval in milliseconds between consecutive attempts to establish a connection with the target system. Sample value: 120000
ITR.ADMIN_ID	Use Login ID of the Oracle E-Business User Management server administrator Sample value: apps
ITR.ADMIN_PASSWORD	Password of the Oracle E-Business User Management server administrator Sample value: passw0rd1
ITR.STATEMENT_TIMEOUT	Enter the time in milliseconds within which a query run on the target system is expected to return results. If the results of a query are not returned within the specified time, then it is assumed that the connection with the target system has failed. The connector then attempts to reestablish a connection with the target system. Sample value: 120000
ITR.CONNECTION_TIMEOUT	Enter the time in milliseconds within which the target system is expected to respond to a connection attempt. For a particular connection attempt, if the target system does not respond within the time interval specified by the Connection Timeout parameter, then it is assumed that the connection attempt has failed. Sample value: 120000
ITR.EBSCONTEXT_USER_ID	This parameter is used only by the Oracle E-Business User Management connector. Sample value: 0
ITR.EBSCONTEXT_APPLICATIONNAME	This parameter is used only by the Oracle E-Business User Management connector. Sample value: 0
ITR.EBSCONTEXT_RESPONSIBILITY_NAME	This parameter is used only by the Oracle E-Business User Management connector. Sample value: 0
ITR.JDBC_URL	Specify the JDBC URL for the target system database. Sample value: jdbc:oracle:thin:@172.21.176.18:1521:vis
ITR.CONNECTION_PROPERTIES	Specify the connection properties for the target system database.
ITR.IS_SSL_ENABLED	To configure SSL to secure communication between Oracle Identity Manager and the target system. Sample value: No
UD_EBS_USER_USERNAME	User Login ID Sample value: ORATEST

Parameter	Description
UD_EBS_USER_PASSWORD	Password of the user Sample value: passw0rd1
UD_EBS_USER_PASSWORD_EXPIRATION_TYPE	Password Expiration type of the user Sample value: Days, Accesses, None
UD_EBS_USER_PASSWORD_EXPIRATION_INTERVAL	Password Expiration value of the user This value depends on the value assigned to the Password expiration Type attribute.
UD_EBS_USER_DESCRIPTION	Description of the user Sample value: Test description
UD_EBS_USER_EMAIL	E-mail address of the user Sample value: test@example.com
UD_EBS_USER_FAX	Fax number of the user Sample value: 657895421
UD_EBS_USER_EFFECTIVE_DATEFROM	Start date of the user Sample value: 2009-03-11
UD_EBS_USER_EFFECTIVE_DATETO	End date of the user Sample value: 2009-04-12
UD_EBS_USER_USER_ID	User ID of the user Sample value: 1051274
UPDATE_FIELDNAME	Name of the process form field to be updated Sample value: UD_EBS_USER_PASSWORD
APPLICATION_NAME	Application short name Sample value: 1~160
RESPONSIBILITY_NAME	Responsibility name Sample value: 1~160~20456
RESP_START_DATE	Start date of the responsibility Sample value: 2006-11-11
RESP_END_DATE	End date of the responsibility Sample value: 2006-11-11
SECURITY_GROUP_NAME	Security group name Sample value: 1~1

5. Run the testing utility file.

Note: Before running the testing utility, in Oracle Identity Manager 11g, extract EBSUM.jar file for MANIFEST.MF file and set Class-Path to correct path of jars, include Jdbc driver jar file and repackage EBSUM.jar with these settings.

- On Microsoft Windows, run the following file:
 - For Oracle Identity Manager release 9.1.0.x:
`OIM_HOME\xellerate\XLIIntegrations\EBSUM\scripts\OracleEBiz.bat`

- For Oracle Identity Manager releases 11.1.x and 11.1.2.x:
`OIM_HOME\server\XLIntegrations\EBSUM\scripts\OracleEBiz.bat`
 - On UNIX, run the following file:
 - For Oracle Identity Manager release 9.1.0.x:
`OIM_HOME/xellerate/XLIntegrations/EBSUM/scripts/OracleEBiz.sh`
 - For Oracle Identity Manager releases 11.1.x and 11.1.2.x:
`OIM_HOME/server/XLIntegrations/EBSUM/scripts/OracleEBiz.sh`
6. If the script runs without any error, then verify that the required provisioning action has been carried out on the target system.

5.2 Troubleshooting

The following table lists solutions to some commonly encountered errors associated with the connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with the Oracle E-Business User Management server.	<ul style="list-style-type: none"> ■ Ensure that the Oracle E-Business User Management server is running. ■ Check if the user exists in Oracle E-Business User Management. ■ Ensure that Oracle Identity Manager is running. ■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that the IP address, administrator ID, and administrator password are correct.
The Operation Failed message is displayed on the Oracle Identity Manager Administrative and User Console	<ul style="list-style-type: none"> ■ Ensure that the values for the attributes do not contain delimiter characters (white space). ■ Ensure that the attribute values do not exceed the specified length.
One of the following error messages is thrown when Oracle Identity Manager tries to exchange data with the target system: table or view does not exist insufficient privileges	<p>This error message is thrown because the target system account for connector operations does not have the required privileges. See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for information about creating this account and assigning the required privileges to it.</p>
Reinstallation of the connector is unsuccessful.	<p>Perform the following steps to resolve the issue:</p> <ol style="list-style-type: none"> 1. In a text editor, open the <code>OIM_HOME/ConnectorDefaultDirectory/ORCL_EBS_UM_RELEASE_NU_MBER/xml/Oracle-eBusiness Suite-HRMS-Main-ConnectorConfig.xml</code> for editing. 2. Search for all resource forms and remove the <Form name> entries to prevent them from being reimported. For example, search for and remove the entry: <code><Form name = "UD_EBSX_XXXX" subtype = "Resource Form"></code> 3. Save and close the file. 4. Retry installing the connector.

Known Issues

The following are known issues associated with this release of the connector:

Oracle Identity Manager Issues

This section discusses the following issues associated with Oracle Identity Manager release 11.1.2.x:

- **Issue:** Responsibility entitlement provisioning does not allow to select security group field value and considers DEFAULT security group.

OIM release 11.1.2.x considers only one child form field as an entitlement for entitlement provisioning functionality. Due to this, you cannot provision responsibility with security group while provisioning responsibility entitlement.

Workaround:

1. Do entitlement provisioning of responsibility which considers **DEFAULT** security group.
2. Edit account.
3. Select suitable security group.
4. Update the account.

- **Issue:** Lookup Query feature in 11.1.2.x does not work and not supported.

Workaround:

1. Create new version for the child forms (ex: UD_EBS_RESP) that you are using.
2. Add property "Lookup Code" as property name and corresponding lookup as property value for each column names

(For example, Application Name, Responsibility Name, Security Group Name and Role Name).

Property value:

- Lookup.EBS.Application for Application Name.
 - Lookup.EBS.UMX.Roles for Role name.
 - Lookup.EBS.Responsibility for Responsibility Name.
 - Lookup.EBS.SecurityGroup for Security Group Name.
3. Make version active.
 4. Create UI form.

Special Characters Supported by Oracle E-Business Suite 11.5.10

[Table A-1](#) lists special characters that supported by Oracle E-Business Suite 11.5.10. You can use these characters in combination with letters (alphabets) and numerals while specifying a password.

Note:

These characters are not supported by Oracle E-Business Suite 12.0.1 through 12.0.6.

See *Oracle Identity Manager Globalization Guide* for information about special characters that are supported by Oracle Identity Manager.

Table A-1 Special Characters Supported by Oracle E-Business Suite 11.5.10

Name of the Character	Character
asterisk	*
backslash	\
colon	:
comma	,
double quotation mark	"
left parenthesis	(
right parenthesis)
left angle bracket	<
right angle bracket	>
plus sign	+
semicolon	;
slash	/
tilde	~

Index

A

Administrative and User Console, 2-51, 5-4
architecture, 1-3

C

certified components, 1-1
certified languages, 1-3
clearing server cache, 2-33
components, certified, 1-1
configuring connector, 3-1
connector architecture, 1-3
connector configuration, 3-1
connector features, 1-4
connector files and directories
 description, 2-1
connector testing, 5-1
connector version number, determining, 2-4

D

data encryption and integrity, 2-20
Data Transformation, 4-29
defining
 IT resources, 2-43
determining version number of connector, 2-4

E

enabling logging, 2-35
errors, 5-4

F

files and directories of the connector
 See connector files and directories

G

globalization features, 1-3

I

installing connector, 2-14
issues, 6-1
IT resources

defining, 2-43
parameters, 2-43

L

limitations, 6-1
logging enabling, 2-35
lookup field synchronization, 1-27, 3-1, 3-7
lookup fields, 1-27, 3-1, 3-7
Lookup.EBS.UM.ProvValidation, 4-28, 4-31
Lookup.EBS.UM.Transformation, 4-30

M

multilanguage support, 1-3

O

Oracle Database, 2-20
Oracle Identity Manager Administrative and User
 Console, 2-51, 5-4

P

parameters of IT resources, 2-43
problems, 5-4
Provisioning, 1-20
 Data Validation, 4-30
provisioning
 direct provisioning, 3-20
 identity fields, 1-23
 provisioning triggered by policy changes, 3-18
 request-based provisioning, 3-18

R

Reconciliation, 1-13
 Data Validation, 4-27
reconciliation action rule
 target resource reconciliation, 1-19
reconciliation rule
 target resource reconciliation, 1-18
reconciliation scheduled tasks, 3-11

S

scheduled tasks

- defining, 3-13
 - reconciliation, 3-11
- server cache, clearing, 2-33
- stages of connector deployment
 - installation, 2-10
 - postinstallation, 2-14
 - preinstallation, 2-1
- supported
 - releases of Oracle Identity Manager, 1-2
 - target systems, 1-2

T

- target resource reconciliation, 1-1
 - adding new fields, 4-5, 4-8
 - reconciliation action rule, 1-19
 - reconciliation action rules, 1-19
 - reconciliation rule, 1-18
- target system user account, 2-6
- target system, multiple installations, 4-32
- target systems
 - supported, 1-2
- temporary tables, 1-14
- test cases, 5-1
- testing the connector, 5-1
- testing utility, 5-1
- transformation, 4-29
- Transformation of Data During User Reconciliation, 4-29
- troubleshooting, 5-4

V

- validation, 4-27, 4-30
- Validation of Data During Provisioning, 4-30
- Validation of Data During Reconciliation, 4-27
- version number of connector, determining, 2-4