

Oracle® Identity Manager

Connector Guide for Oracle E-Business User Management

Release 9.1.0

E11203-03

July 2009

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on 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. 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.

Contents

Preface	ix
Audience	ix
Documentation Accessibility	ix
Related Documents	x
Documentation Updates	x
Conventions	x
 What's New in Oracle Identity Manager Connector for Oracle E-Business User Management?	xi
Software Updates	xi
Documentation-Specific Updates.....	xiv
 1 About the Connector	
1.1 Certified Components	1-1
1.2 Certified Languages.....	1-2
1.3 Connector Architecture.....	1-3
1.4 Features of the Connector	1-3
1.4.1 Oracle E-Business User Management Connectors.....	1-3
1.4.1.1 User Management	1-4
1.4.1.2 User Management with HR Foundation.....	1-5
1.4.1.3 User Management with TCA Foundation	1-6
1.4.1.4 Similarities Between the Three Connectors	1-6
1.4.1.5 Differences Between the Connectors	1-7
1.4.2 Management of Entitlements	1-8
1.4.3 SoD Validation of Entitlement Provisioning	1-9
1.4.4 Support for an SSO-Enabled Target System Installation	1-9
1.4.5 Reconciliation of Effective-Dated Events	1-10
1.4.6 Account Status Reconciliation and Provisioning	1-10
1.4.7 Configurable Reconciliation Queries	1-11
1.4.8 Account Password Management.....	1-11
1.4.9 Support for Full and Incremental Reconciliation.....	1-11
1.4.10 Support for Limited (Filtered) Reconciliation	1-11
1.4.11 Support for Batched Reconciliation	1-11
1.4.12 Connection Pooling	1-12
1.5 Reconciliation Process	1-12

1.5.1	Reconciliation Queries	1-13
1.5.2	Target System Columns Used in Reconciliation	1-14
1.5.3	Reconciliation Rule	1-17
1.5.4	Reconciliation Action Rules for Target Resource Reconciliation.....	1-18
1.6	Provisioning Process.....	1-18
1.6.1	Request-Based Provisioning of Entitlements.....	1-20
1.6.2	Attribute Mappings for Provisioning	1-21
1.6.3	Provisioning Functions	1-23
1.7	Lookup Definitions Used During Connector Operations.....	1-24
1.7.1	Lookup Definitions That Are Common to All Three Connectors	1-25
1.7.2	Lookup Definitions That Are Specific to the User Management Connector	1-27
1.7.3	Lookup Definitions That Are Specific to the User Management with HR Foundation Connector 1-28	
1.7.4	Lookup Definitions That Are Specific to the User Management with TCA Foundation Connector 1-30	
1.8	Roadmap for Deploying and Using the Connector	1-32

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	2-3
2.1.1.3	Using External Code Files	2-3
2.1.2	Preinstallation on the Target System	2-4
2.1.2.1	Creating a Target System User Account for Connector Operations.....	2-4
2.1.2.2	Compiling Custom Wrapper Packages	2-6
2.1.2.3	Setting the Employee Number Creation Mode.....	2-7
2.2	Installation	2-7
2.2.1	Running the Connector Installer	2-8
2.2.2	Copying Files to the Oracle Identity Manager Host Computer.....	2-11
2.3	Postinstallation	2-11
2.3.1	Configuring SoD	2-11
2.3.1.1	Configuring the Oracle Applications Access Controls Governor to Act As the SoD Engine 2-12	
2.3.1.2	Specify a Value for the TopologyName IT Resource Parameter	2-12
2.3.1.3	Disabling and Enabling SoD	2-12
2.3.2	Configuring Secure Communication Between the Target System and Oracle Identity Manager 2-16	
2.3.2.1	Configuring Data Encryption and Integrity in Oracle Database.....	2-16
2.3.2.2	Configuring SSL Communication in Oracle Database.....	2-16
2.3.3	Postinstallation on Oracle Identity Manager	2-17
2.3.3.1	Enabling Request-Based Provisioning of Entitlements.....	2-18
2.3.3.2	Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server 2-20	
2.3.3.3	Clearing Content Related to Connector Resource Bundles from the Server Cache ... 2-28	
2.3.3.4	Enabling Logging	2-29
2.3.3.4.1	Enabling Logging on IBM WebSphere Application Server	2-30

2.3.3.4.2	Enabling Logging on JBoss Application Server	2-30
2.3.3.4.3	Enabling Logging on Oracle Application Server	2-31
2.3.3.4.4	Enabling Logging on Oracle WebLogic Server	2-31
2.3.3.5	Determining Values for the JDBC URL and Connection Properties Parameters.....	2-31
2.3.3.5.1	Supported JDBC URL Formats.....	2-31
2.3.3.5.2	Only Data Encryption and Integrity Is Configured	2-32
2.3.3.5.3	Only SSL Communication Is Configured	2-33
2.3.3.5.4	Both Data Encryption and Integrity and SSL Communication Are Configured .	2-34
2.3.3.6	Configuring the IT Resource.....	2-35

3 Using the Connector

3.1	Setting Up Lookup Definitions in Oracle Identity Manager	3-1
3.1.1	Setting Up the Lookup.EBS.UM.Configurations Lookup Definition.....	3-2
3.1.2	Setting Up the Lookup.EBS.UMHRMS.Configurations Lookup Definition.....	3-2
3.1.3	Setting Up the Lookup.EBS.UMTCA.Configurations Lookup Definition	3-3
3.2	Scheduled Task for Lookup Field Synchronization.....	3-3
3.3	Configuring Reconciliation.....	3-4
3.3.1	Reconciliation Time Stamp	3-4
3.3.2	Batched Reconciliation	3-5
3.3.3	Configuring Limited Reconciliation	3-5
3.3.4	Reconciliation Scheduled Tasks.....	3-7
3.4	Configuring Scheduled Tasks	3-9
3.5	Attributes for Which You Can Specify Values During New Resource and Entitlement Provisioning 3-11	
3.5.1	Resource Provisioning Using the User Management Connector	3-11
3.5.2	Resource Provisioning Using the User Management with TCA Foundation Connector .	3-11
3.5.3	Resource Provisioning Using the User Management with HR Foundation Connector....	3-12
3.5.4	Entitlement Provisioning Using All Three Connectors.....	3-12
3.6	Provisioning Operations Performed in an SoD-Enabled Environment.....	3-12
3.6.1	Overview of the Provisioning Process in an SoD-Enabled Environment	3-13
3.6.2	Direct Provisioning in an SoD-Enabled Environment	3-14
3.6.3	Request-Based Provisioning in an SoD-Enabled Environment	3-25

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.....	4-1
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	4-4
4.2.1	Adding New Attributes for Reconciliation.....	4-4
4.2.2	Removing Attributes Used for Reconciliation.....	4-7
4.3	Adding or Removing Attribute Mappings for Provisioning.....	4-12

4.3.1	Adding New Attributes for Provisioning	4-13
4.3.2	Removing Attributes for Provisioning	4-17
4.4	Adding Filter Parameters in a Reconciliation Query.....	4-21
4.5	Modifying Field Lengths on the Process Form.....	4-22
4.6	Configuring the Connector for Multiple Installations of the Target System	4-23

5 Testing and Troubleshooting

5.1	Running Test Cases.....	5-1
5.2	Troubleshooting	5-3

6 Known Issues

A Special Characters Supported by Oracle E-Business Suite 11.5.10

Index

List of Tables

1-1	Certified Components	1-1
1-2	Differences Between the Connectors.....	1-8
1-3	Attribute Mappings for Reconciliation in the User Management Connector.....	1-15
1-4	Attribute Mappings for Reconciliation in the User Management with HR Foundation Connector 1-15	
1-5	Attribute Mappings for Reconciliation in the User Management with TCA Foundation Connector 1-16	
1-6	Relationship Between Process Form Fields for Responsibilities and Target System Data Fields 1-16	
1-7	Relationship Between Process Form Fields for Roles and Target System Data Fields.	1-17
1-8	Action Rules for Target Resource Reconciliation.....	1-18
1-9	Attribute Mappings for Provisioning	1-21
1-10	Provisioning Functions	1-23
1-11	Lookup Definitions Common to All Three Connectors	1-26
1-12	Lookup Definitions Specific to the User Management Connector	1-28
1-13	Lookup Definitions Specific to the User Management with HR Foundation Connector	1-29
1-14	Lookup Definitions Synchronized with the Target System.....	1-31
2-1	Files and Directories on the Installation Media.....	2-1
2-2	Files to Be Copied to the Oracle Identity Manager Host Computer	2-11
2-3	Certificate Store Locations	2-17
2-4	Queries for Lookup Field Synchronization.....	2-21
2-5	IT Resource Parameters.....	2-37
3-1	Attributes of the eBusiness UM Lookup Definition Reconciliation Scheduled Task	3-3
3-2	Attributes of the eBusiness UM Target Resource User Reconciliation Scheduled Task .	3-7
4-1	Connector Objects	4-23
A-1	Special Characters Supported by Oracle E-Business Suite 11.5.10	A-1

List of Figures

1-1	Architecture of the Connector	1-3
1-2	Architecture of the Connector with Configured to Work with an SSO Solution	1-10

Preface

This guide provides information about Oracle Identity Manager Connector for Oracle E-Business User Management.

Audience

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at <http://www.fcc.gov/cgb/consumerfacts/trs.html>, and a list of phone numbers is available at <http://www.fcc.gov/cgb/dro/trsphonebk.html>.

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.

See Also: The earlier release of this guide for information about updates that were new for that release

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 updates made in release 9.1.0 of the connector:

- [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 target system versions:

Oracle E-Business Suite 11.5.10, 12.0.1 through 12.0.6 running on Oracle Real Application Clusters 10g and 11g

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 1.4.1, "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 1.4.3, "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 1.4.4, "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 1.7, "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 1.4.5, "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 1.4.6, "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 1.5.1, "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 4.6, "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 1.4.12, "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 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 1.8, "Roadmap for Deploying and Using the Connector"](#) for detailed information about the organization of content in this guide.

- In the ["Certified Components"](#) section, 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, "Certified Languages"](#)
- [Section 1.3, "Connector Architecture"](#)
- [Section 1.4, "Features of the Connector"](#)
- [Section 1.5, "Reconciliation Process"](#)
- [Section 1.6, "Provisioning Process"](#)
- [Section 1.7, "Lookup Definitions Used During Connector Operations"](#)
- [Section 1.8, "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	Oracle Identity Manager release 9.1.0.2 or later

Table 1–1 (Cont.) Certified Components

Component	Requirement
Target system	<p>Oracle E-Business Suite 11.5.10, 12.0.x</p> <p>These applications may run on Oracle Database 10g or Oracle Database 11g, as either single database or 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 Oracle Applications Access Controls Governor release 8.2.1 along with the latest patch set.</p> <p>Note: Contact Oracle Support for information about the patch set for release 8.2.1. See Section 1.4.3, "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
External code	<ul style="list-style-type: none"> ■ If Oracle Identity Manager is using Microsoft SQL Server, then the JDBC class library (classes12.jar or ojdbc14.jar) is the required external code file. See Section 2.1.1.3, "Using External Code Files" for more information. ■ If the target system is SSO-enabled, then you must also deploy the connector for the LDAP system used by the SSO system. See Section 1.4.4, "Support for an SSO-Enabled Target System Installation" for more information.

1.2 Certified Languages

The connector supports the following languages:

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

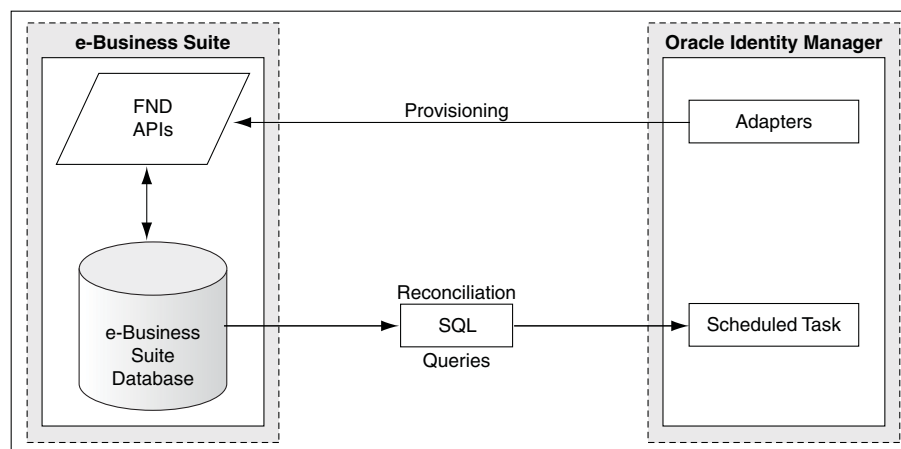
See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

1.3 Connector Architecture

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 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



1.4 Features of the Connector

The following are features of the connector:

- [Section 1.4.1, "Oracle E-Business User Management Connectors"](#)
- [Section 1.4.2, "Management of Entitlements"](#)
- [Section 1.4.3, "SoD Validation of Entitlement Provisioning"](#)
- [Section 1.4.4, "Support for an SSO-Enabled Target System Installation"](#)
- [Section 1.4.5, "Reconciliation of Effective-Dated Events"](#)
- [Section 1.4.6, "Account Status Reconciliation and Provisioning"](#)
- [Section 1.4.7, "Configurable Reconciliation Queries"](#)
- [Section 1.4.8, "Account Password Management"](#)
- [Section 1.4.9, "Support for Full and Incremental Reconciliation"](#)
- [Section 1.4.10, "Support for Limited \(Filtered\) Reconciliation"](#)
- [Section 1.4.11, "Support for Batched Reconciliation"](#)
- [Section 1.4.12, "Connection Pooling"](#)

1.4.1 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 1.4.1.1, "User Management"](#)
- [Section 1.4.1.2, "User Management with HR Foundation"](#)
- [Section 1.4.1.3, "User Management with TCA Foundation"](#)

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

- [Section 1.4.1.4, "Similarities Between the Three Connectors"](#)
- [Section 1.4.1.5, "Differences Between the Connectors"](#)

1.4.1.1 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.

1.4.1.2 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 party record is created. Next, the link between the FND_USER record and party record is established. The connector does not check for an existing party 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 must not use the connector for an Oracle E-Business HRMS installation that your organization uses to manage employee records. In other words, this connector is not compatible for use with a fully deployed 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.

1.4.1.3 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.

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.

1.4.1.4 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.

1.4.1.5 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.

1.4.2 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.

1.4.3 SoD Validation of Entitlement Provisioning

From this release onward, the connector supports the SoD feature introduced in Oracle Identity Manager release 9.1.0.2. The following are the focal points of this software update:

- The SoD Invocation Library (SIL) is bundled with Oracle Identity Manager release 9.1.0.2. 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

1.4.4 Support for an SSO-Enabled Target System Installation

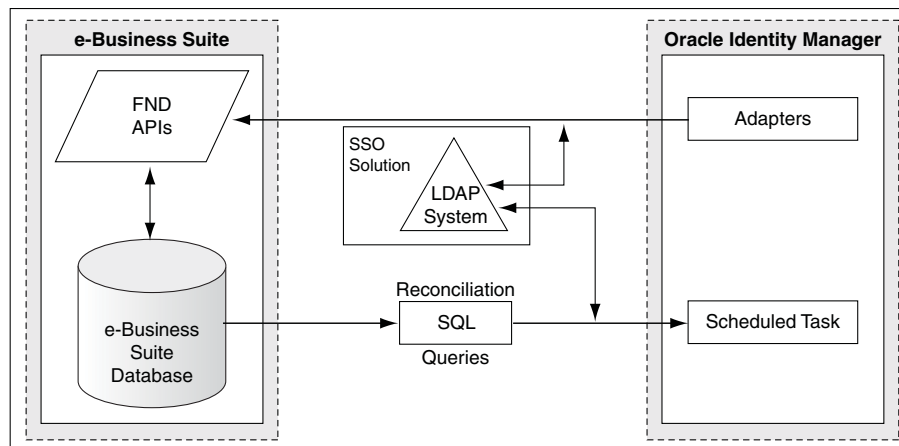
Note: This feature is available in all three connectors.

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



1.4.5 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.

1.4.6 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.

1.4.7 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 1.5.1, "Reconciliation Queries"](#) for information about the reconciliation queries.

1.4.8 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.

1.4.9 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.

1.4.10 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.

1.4.11 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.

1.4.12 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.

1.5 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 1.5.3, "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 1.5.1, "Reconciliation Queries"](#)
- [Section 1.5.2, "Target System Columns Used in Reconciliation"](#)
- [Section 1.5.3, "Reconciliation Rule"](#)
- [Section 1.5.4, "Reconciliation Action Rules for Target Resource Reconciliation"](#)

1.5.1 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.

1.5.2 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
Effective Start Date	START_DATE	Start date of the responsibility assignment
Effective End Date	END_DATE	End date of the responsibility assignment

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: <i>IT_RESOURCE_KEY~APPLICATION_ID</i> 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: <i>IT_RESOURCE_KEY~APPLICATION_ID~ROLE_ID</i> 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

1.5.3 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.

1.5.4 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.

1.6 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 1.6.1, "Request-Based Provisioning of Entitlements"](#)
- [Section 1.6.2, "Attribute Mappings for Provisioning"](#)
- [Section 1.6.3, "Provisioning Functions"](#)

1.6.1 Request-Based Provisioning of Entitlements

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.

1.6.2 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	Password Expiration Type	All	
This is a lookup field.			

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

Process Form Attribute	Target System Attribute	Connector	Mandatory?
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	
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 <code>USER_GUID</code> column of the <code>FND_USER</code> 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	

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

Process Form Attribute	Target System Attribute	Connector	Mandatory?
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	<i>IT_RESOURCE_KEY~APPLICATION_ID</i>	All	
Responsibility Name	<i>IT_RESOURCE_KEY~APPLICATION_ID~RESPONSIBILITY_ID</i>	All	Yes
Effective Start Date	Effective Dates From	All	
Effective End Date	Effective Dates To	All	
Roles Child Form Fields (for all three connectors)			
Application Name	<i>IT_RESOURCE_KEY~APPLICATION_ID</i>	All	
Role Name	<i>IT_RESOURCE_KEY~APPLICATION_ID~ROLE_ID</i>	All	Yes
Start Date	Start Date	All	
Expiration Date	Expiration Date	All	

1.6.3 Provisioning Functions

[Table 1–10](#) lists provisioning functions and the corresponding adapters.

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

Table 1–10 (Cont.) Provisioning Functions

Provisioning Function	Adapter	Stored Procedure in Wrapper Package
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
Update Responsibility	EBS Update 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
Update Role	EBS Update Role	WF_LOCAL_SYNCH_PKG.PropagateUserRole
Remove Role	EBS Revoke Role	WF_LOCAL_SYNCH_PKG.PropagateUserRole
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
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
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

1.7 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 1.7.1, "Lookup Definitions That Are Common to All Three Connectors"](#)
- [Section 1.7.2, "Lookup Definitions That Are Specific to the User Management Connector"](#)
- [Section 1.7.3, "Lookup Definitions That Are Specific to the User Management with HR Foundation Connector"](#)
- [Section 1.7.4, "Lookup Definitions That Are Specific to the User Management with TCA Foundation Connector"](#)

1.7.1 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.Applicatio n	<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>

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>	<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.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>	<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.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>	<p>This lookup definition is preconfigured. You must not modify this lookup definition.</p>

1.7.2 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,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.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.Configurations	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.

1.7.3 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.UserH RMSProvisioning	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.UserH RMSRecon	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.Create Employee	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,vva rchar2, 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.Updat eEmployee	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,vva rchar2, IN OUT	You must not modify this lookup definition.
Lookup.EBS.HRMSRes ponsibility.Mapping Note: This lookup definition is used for request-based responsibility provisioning.	Name of the process form column for the responsibility attributes in the eBusiness Suite User HR Foundation Responsibility resource object	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 Note: This lookup definition is used for request-based role provisioning.	Name of the process form column for the role attributes in the eBusiness Suite User HR Foundation Role resource object	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. Configurations	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.

1.7.4 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.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.
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.Q ueryFilters	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.C onfigurations	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 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"](#)

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, "Using External Code Files"](#)

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 Oracle_EBS_User-Management-CI.xml Oracle_EBS_User-HRMS-Management-CI.xml Oracle_EBS_User-TCA-Management-CI.xml	This directory contains the configuration files that are used by the Connector Installer during installation of each connector.
lib/EBSUM.jar	This JAR file contains the class files that are used during reconciliation and provisioning operations.

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

File in the Installation Media Directory	Description
lib/EBSCCommon.jar	This JAR file contains utility classes that support provisioning and reconciliation operations.
lib/Common.jar	This JAR file contains classes that are used by all release 9.1.0 connectors.
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 into the following directories:</p> <p><i>OIM_HOME/xellerate/connectorResources</i></p> <p>Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.</p>
scripts/OIM.bat scripts/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/OIM_FND_GLOBAL.pck	This is the customized apps.fnd_global package.
scripts/OIM_FND_USER_PKG.pck	This is the customized apps.fnd_user package.
scripts/OIM_EMPLOYEE_WRAPPER.pck	This is a customized wrapper package for creating and updating employee records.
scripts/OIM_TCA_WRAPPER.pck	This is a customized wrapper package for creating and updating party records.
scripts/OimUser.sql scripts/OimUserGrants.sql scripts/OimUserSynonyms.sql	<p>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.</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/WL_LOCAL_SYNCH_PKG.pck	This is the customized version of the apps.wf_local_synch package. It is used for role management.
test/config/config_um_prov.properties	<p>This properties file contains data that is used by the testing utility.</p> <p>See Section 5.1, "Running Test Cases" for more information.</p>
test/config/config_um_prov_fileOption.properties	<p>This properties file contains data that is used by the testing utility.</p> <p>See Section 5.1, "Running Test Cases" for more information.</p>
test/config/log.properties	This file contains properties that you use to enable log4j logging.
test/scripts/OracleEbiz.bat test/scripts/OracleEbiz.sh	This file is used to run the testing utility.
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.

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

File in the Installation Media Directory	Description
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.

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.
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 Using External Code Files

If Oracle Identity Manager is using Microsoft SQL Server, then:

1. Copy the JDBC class library (`classes12.jar` or `ojdbc14.jar`) file from the Oracle home directory on the target system host computer. For example, if the target system is using Oracle9i Database, then you can copy the file from the `ORACLE_HOME/ora92/jdbc/lib` directory.
2. Paste the file into the `OIM_HOME/xellerate/ThirdParty` directory.
3. Add `OIM_HOME/xellerate/ext/ojdbc14.jar` in the classpath of the application server.

If your Oracle Identity Manager installation is running on Oracle WebLogic Server, then:

- a. Open the following file in a text editor:
`ORACLE_HOME/user_projects/domains/DOMAIN_NAME/bin/startWebLogic.sh` (or `startWebLogic.cmd`) file
- b. Search for the following line in the file:
On Microsoft Windows:

```
set SAVE_JAVA_OPTIONS=%JAVA_OPTIONS%
```


On UNIX:

```
SAVE_JAVA_OPTIONS="${JAVA_OPTIONS}"
```
- c. Add the following line immediately after the line given in the preceding step:

Note: Replace *FULL_PATH_TO_ojdbc14.jar* with the full path to the *ojdbc14.jar* file.

On Microsoft Windows:

```
set CLASSPATH=FULL_PATH_TO_ojdbc14.jar;%CLASSPATH%
```

On UNIX:

```
CLASSPATH=FULL_PATH_TO_ojdbc14.jar:$CLASSPATH  
export CLASSPATH
```

- d. Save and close the file.

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 Client installed on the computer on which you perform the procedure described in this section. The Oracle Client release must be the same as the database release. In addition, if Oracle Client is not installed on the database host computer, then the *tnsnames.ora* file on the Oracle 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. Copy the scripts directory from the installation media to a temporary directory on either the target system server or to a computer on which the Oracle Database client has been installed.
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 APPS User
Enter the password of the APPS User that can grant the required privileges to 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 to the account:

Note: The OimUserGrants.sql file contains commands to grant these permissions.

```

SELECT, UPDATE ON APPS.FND_USER
SELECT, UPDATE ON APPS.HZ_PARTIES
SELECT, UPDATE ON APPS.HZ_PERSON_PROFILES
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
EXECUTE ON APPS.FND_USER_PKG
EXECUTE ON APPS.OIM_FND_USER_PKG
EXECUTE ON APPS.FND_GLOBAL
EXECUTE ON APPS.OIM_FND_GLOBAL
EXECUTE ON APPS.HR_EMPLOYEE_API
EXECUTE ON APPS.HR_PERSON_API
EXECUTE ON APPS.WF_LOCAL_SYNCH.PROPAGATEUSERROLE
EXECUTE ON APPS.OIM_EMPLOYEE_WRAPPER
EXECUTE ON APPS.OIM_EMPLOYEE_WRAPPER_PKG
EXECUTE ON APPS.OIM_TCA_WRAPPER
EXECUTE ON APPS.OIM_TCA_WRAPPER_PKG
EXECUTE ON APPS.FND_OID_USERS
CREATE SESSION
CREATE SYNONYM
```

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

If you plan to use the APPS account for reconciliation and provisioning 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 by using the account that you create as described in [Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"](#).
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>/OimUserSynonyms.sql
```

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. Direct provisioning is automatically disabled when you enable request-based provisioning. See [Section 2.3.3.1, "Enabling Request-Based Provisioning of Entitlements"](#) 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 into the following directory:
OIM_HOME/xellerate/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 *Oracle Identity Manager Administrative and User Console Guide*.
3. Click **Deployment Management**, and then click **Install 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.
OIM_HOME/xellerate/ConnectorDefaultDirectory

You can select one of the following options:

- For the User Management connector:
Oracle EBS User Management 9.1.0.0
- For the User Management with HR Foundation connector:
Oracle EBS HR Foundation User Management 9.1.0.0
- For the User Management with TCA Foundation connector:
Oracle EBS TCA Foundation User Management 9.1.0.0

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:

Alternative Directory:

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.

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

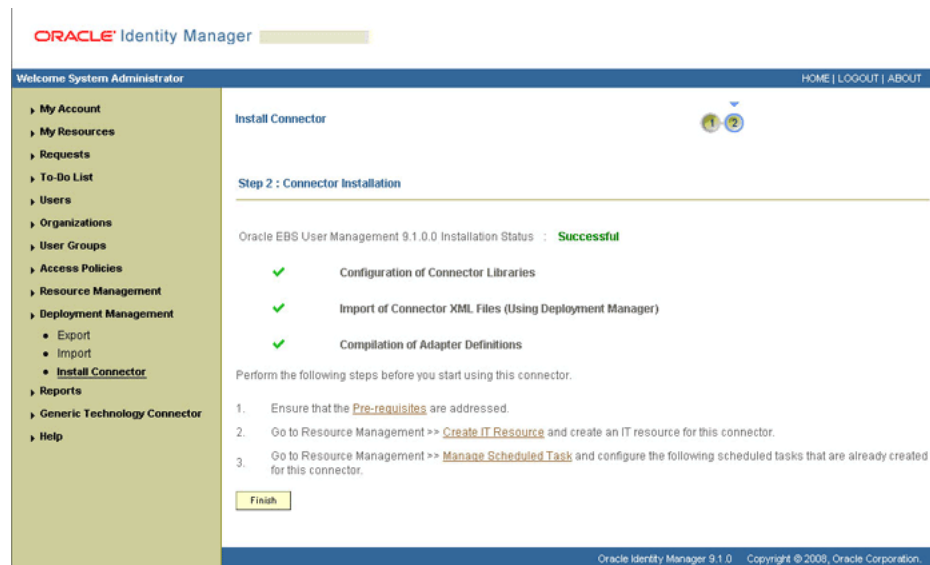
The following tasks are performed in sequence:

- 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:



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 `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 clustered environment, 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](#).

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 Host Computer
Files in the config directory	<i>OIM_HOME</i> /xellerate/XLintegrations/EBSUM/config Note: You must create the EBSUM/config directory.
Files in the test/config directory	<i>OIM_HOME</i> /xellerate/XLintegrations/EBSUM/config
Files in the test/scripts directory	<i>OIM_HOME</i> /xellerate/XLintegrations/EBSUM/scripts Note: You must create the EBSUM/scripts directory.

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"](#)

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, "Specify 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

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 Release 9.1.0.2* for information about this procedure.

2.3.1.2 Specify 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. See the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in *Oracle Identity Manager Tools Reference for Release 9.1.0.2* for information about this element.

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

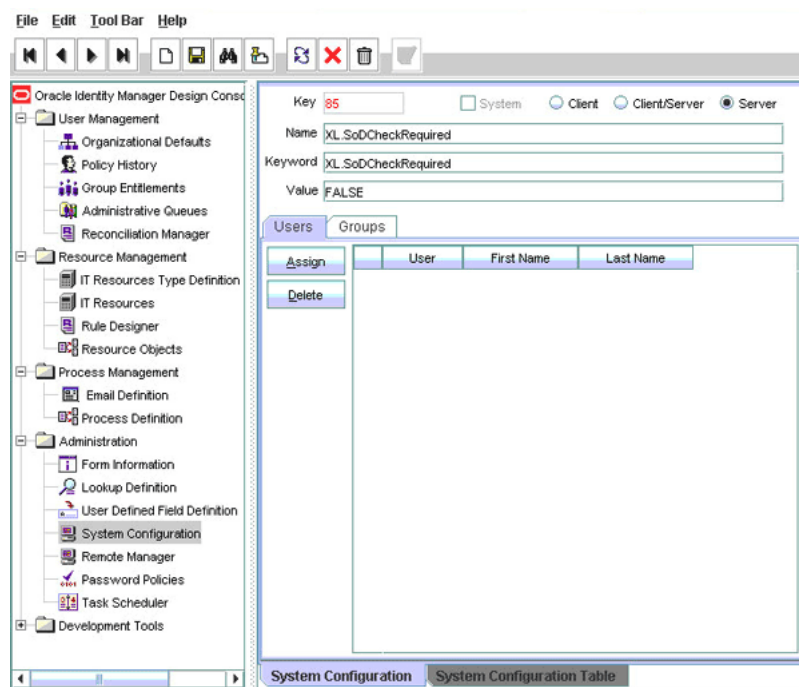
2.3.1.3 Disabling and Enabling SoD

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 the Design Console.
2. Set the XL.SoDCheckRequired system property to FALSE as follows:
 - a. Expand Administration, and 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.
- e. If you are going to perform the procedure described in [Section 2.3.3.1, "Enabling Request-Based Provisioning of Entitlements"](#), then for all approval process definitions, the human approval tasks must be made unconditional 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 4.6, "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 Oracle Identity Manager Design Console. The 'General' tab is selected, showing the task name 'Manager Approval' and description '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'.

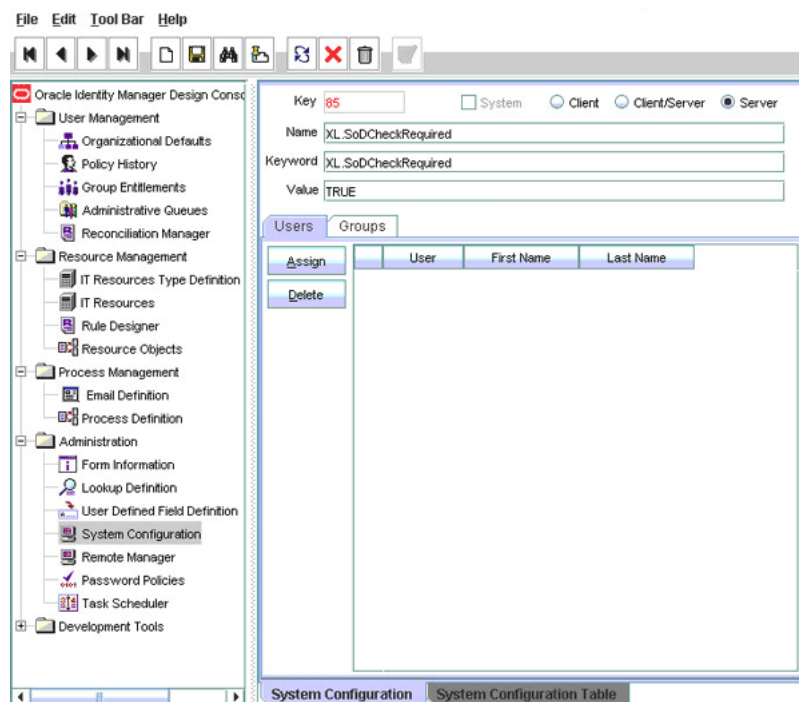
- Save the changes to the process definition.

3. Restart Oracle Identity Manager.

To enable SoD:

Note: If you are enabling SoD for the first time, then see *Oracle Identity Manager Readme for Release 9.1.0.2* for detailed information.

1. Log in to the Design Console.
2. Expand Administration, and double-click System Configuration.
3. Set the XL.SoDCheckRequired system property to TRUE as follows:
 - a. Search for and open the XL.SoDCheckRequired system property.
 - b. Set the value of the system property to TRUE. The following screenshot shows this page:



- c. Click the Save icon.
4. Search for and open the XL.SIL.Home.Dir system property. Verify that the value of this system property is set to the full path and name of the *SIL_HOME* directory.
5. If you are going to perform the procedure described in [Section 2.3.3.1, "Enabling Request-Based Provisioning of Entitlements"](#), 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 4.6, "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.
6. 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: For a clustered configuration, 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/tcs055071Node0/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, "Enabling Request-Based Provisioning of Entitlements"](#)
- [Section 2.3.3.2, "Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server"](#)
- [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"](#)

2.3.3.1 Enabling Request-Based Provisioning of Entitlements

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.

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.

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.

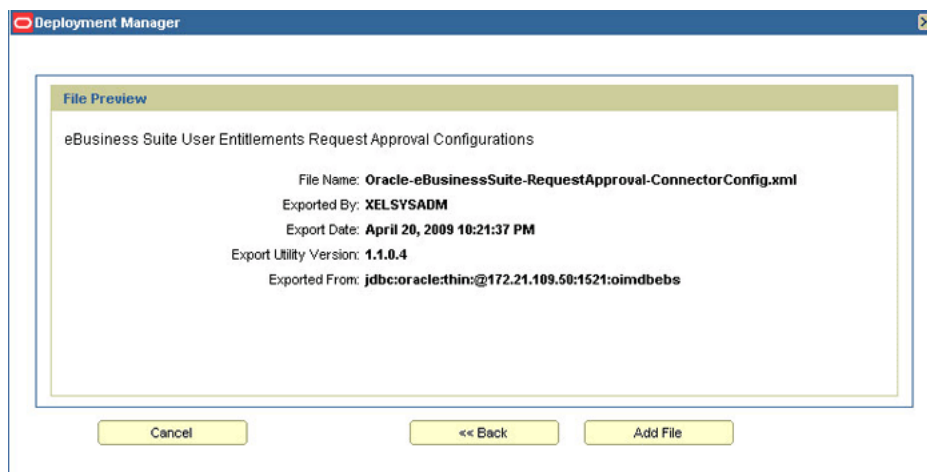
To enable request-based provisioning of entitlements:

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

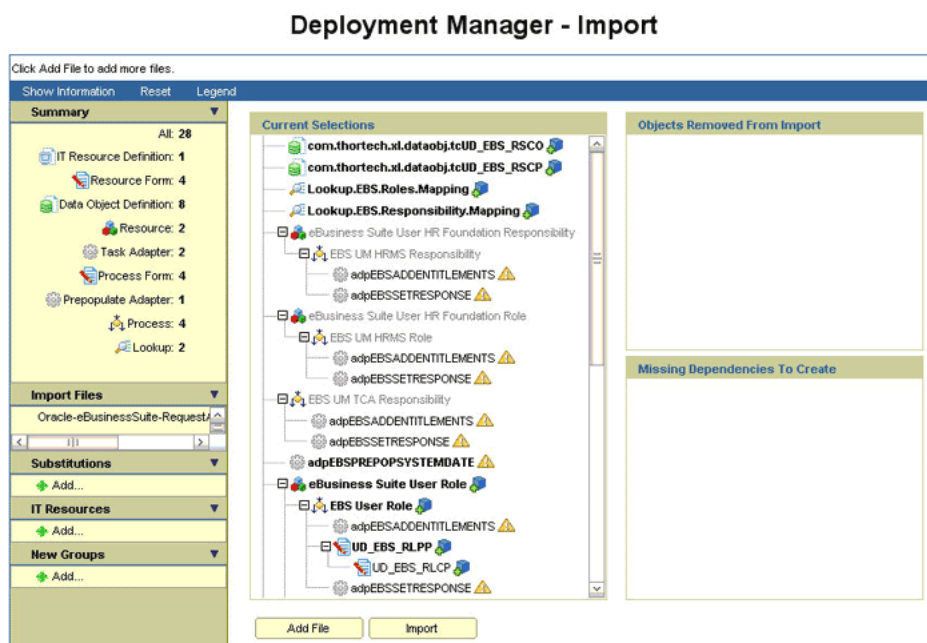
- For the User Management with TCA Foundation connector:
Oracle-eBusinessSuite-TCA-RequestApproval-ConnectorConfig.xml

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:



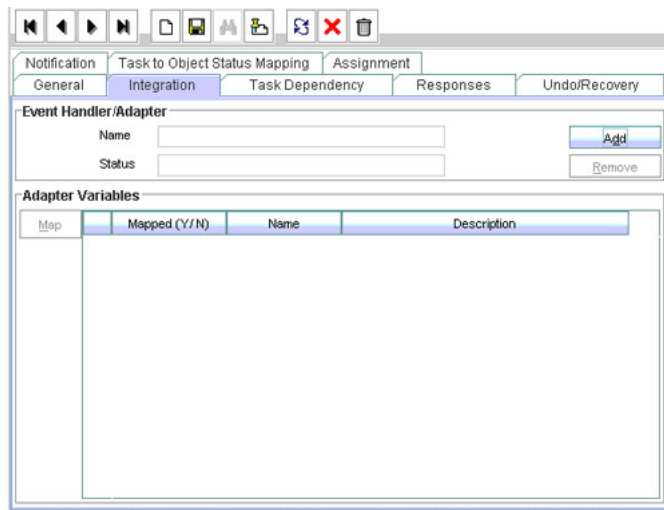
8. Click **Import**.

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.

2.3.3.2 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 4.6, "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

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_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
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_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_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_EBS_RESP_APP_NAME\$' + '~' , 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

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_RLCO_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_EBS_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_EBS_RLCO_APP_NAME\$' '~',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
UD_EBS_RLCP_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_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_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_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_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_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

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

Field Name	Oracle Database Version of the Query	Microsoft SQL Server Version of the Query
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
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_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

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_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)
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_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_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_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_EBST_RSP_APP_NAMES\$' + '~' , lkv_encoded)>0
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_RO LE_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

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_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
UD_EBT_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_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_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_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_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_EBT_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_EBT_RSCP_APP_NAME\$' + '~' , lkv_encoded)>0

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

Note: In a clustered environment, you must perform this procedure on each node of the cluster.

While you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the `OIM_HOME/xellerate/connectorResources` directory. Whenever you add a new resource bundle in 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, change to the `OIM_HOME/xellerate/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:

```
OIM_HOME/xellerate/bin/BATCH_FILE_NAME
```

2. Enter one of the following commands:

- 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 the content category that you must delete from the server cache.

See Also: The following file for information about content categories:

```
OIM_HOME/xellerate/config/xlconfig.xml
```

2.3.3.4 Enabling Logging

Note: In a clustered environment, you must perform this procedure on each node of the cluster.

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 may 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. Perform the procedure given in one of the following sections:

- [Section 2.3.3.4.1, "Enabling Logging on IBM WebSphere Application Server"](#)
- [Section 2.3.3.4.2, "Enabling Logging on JBoss Application Server"](#)
- [Section 2.3.3.4.3, "Enabling Logging on Oracle Application Server"](#)
- [Section 2.3.3.4.4, "Enabling Logging on Oracle WebLogic Server"](#)

2.3.3.4.1 Enabling Logging on IBM WebSphere Application Server To enable logging:

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

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

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

For example:

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

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

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

2.3.3.4.2 Enabling Logging on 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`

2.3.3.4.3 Enabling Logging on Oracle Application Server To enable logging:

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

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

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

For example:

```
log4j.logger.ADAPTER.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

2.3.3.4.4 Enabling Logging on Oracle WebLogic Server To enable logging:

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

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

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

For example:

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

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

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=
srvce1)))
```

- 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:srvce1
```

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

JDBC URL format:

```
jdbc:oracle:thin:@//HOST_NAME.DOMAIN:PORT_NUMBER/ORACLE_DATAB
ASE_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=myho
st) (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.trustStore
Type=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. Expand **Resource Management**.
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter EBS-APPS12 and then click **Search**.
5. Click the edit icon for the IT resource. The following screenshot shows this page:

Oracle Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

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

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

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

Oracle Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

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"/>

7. Specify values for the parameters of the IT resource. [Table 2–5](#) 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 2–5 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 2–5 (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>
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	This is the name of the IT resource created for the LDAP-based system.
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: <code>orclGUID</code></p> <p>For Microsoft Active Directory: <code>objectGUID</code></p> <p>For Sun Java System Directory: <code>nsUniqueID</code></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 <code>USER_GUID</code> 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: <code>uid</code></p> <p>For Microsoft Active Directory: <code>sAMAccountName</code></p> <p>For Sun Java System Directory: <code>uid</code></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>
TopologyName	<p>If you have installed the OAACG SIL provider, then enter the value of the Topology element in the <code>SILConfig.xml</code> file. See the SoD documentation for more information.</p> <p>Default value: <i>None</i></p>

Table 2–5 (Cont.) IT Resource Parameters

Parameter	Description
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.Configurations</code> For the User Management with HR Foundation connector: <code>Lookup.EBS.UMHRMS.Configurations</code> For the User Management with TCA Foundation connector: <code>Lookup.EBS.UMTCA.Configurations</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>
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>

Table 2–5 (Cont.) IT Resource Parameters

Parameter	Description
Pool preference	Preferred connection pooling implementation Value: <code>Default</code> Note: Do not change this value of this parameter.
Connection pooling supported	Enter <code>true</code> if you want to enable connection pooling for this target system installation. Otherwise, enter <code>false</code> . Default value: <code>false</code>
Target supports only one connection	Indicates whether the target system can support one or more connections at a time Value: <code>false</code> Note: Do not change the value of this parameter.
ResourceConnection class definition	Implementation of the ResourceConnection class Value: <code>oracle.iam.connectors.ebs.common.vo.EBSResourceConnectionImpl</code> Note: Do not change the value of this parameter.
Native connection pool class definition	Wrapper to the native pool mechanism that implements the GenericPool Note: Do not specify a value for this parameter.
Pool excluded fields	Comma-separated list of IT parameters whose change must not trigger a refresh of the connector pool Value: <code>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</code> Note: 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. You must restart Oracle Identity Manager for changes that you make to this parameter to take effect.

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

Additional Configuration Step for Connection Pooling

If Oracle Identity Manager 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.

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"](#)

3.1 Setting Up Lookup Definitions in Oracle Identity Manager

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 3.1.1, "Setting Up the Lookup.EBS.UM.Configurations Lookup Definition"](#)
- [Section 3.1.2, "Setting Up the Lookup.EBS.UMHRMS.Configurations Lookup Definition"](#)

- [Section 3.1.3, "Setting Up the Lookup.EBS.UMTCA.Configurations Lookup Definition"](#)

3.1.1 Setting Up the Lookup.EBS.UM.Configurations Lookup Definition

If you are using the User Management connector, then provide a Decode value for the following entry of the Lookup.EBS.UM.Configurations 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 1.4.12, "Connection Pooling"](#) for more information about this feature.

3.1.2 Setting Up the Lookup.EBS.UMHRMS.Configurations 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.Configurations 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 1.4.12, "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. You can enter values for these fields on the Administrative and User Console while performing direct provisioning. 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.Configurations 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.

3.1.3 Setting Up the Lookup.EBS.UMTCA.Configurations 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.Configurations 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 1.4.12, "Connection Pooling"](#) for more information about this feature.

3.2 Scheduled Task for Lookup Field Synchronization

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 4.6, "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 3–1](#) describes the attributes of this scheduled task.

Table 3–1 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

Table 3–1 (Cont.) Attributes of the eBusiness UM Lookup Definition Reconciliation Scheduled Task

Attribute	Description
Lookup Definition Name	<p>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:</p> <ul style="list-style-type: none"> Lookup.EBS.Application Lookup.EBS.Responsibility Lookup.EBS.UMX.Roles
Task Name	<p>This attribute holds the name of the scheduled task.</p> <p>Value: <code>eBusiness UM Lookup Definition Reconciliation</code></p> <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 scheduled task as the value of the attribute in that scheduled task.</p>
Mode	<p>Default value: <code>Update</code></p> <p>Note: You must not change the default value.</p>

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.

See *Oracle Identity Manager Globalization Guide* for information about special characters that are supported by 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',
'DDMYYYY')) *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 3–2 describes the attributes of these scheduled tasks.

Note:

- 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 4.6, "Configuring the Connector for Multiple Installations of the Target System"](#) for more information about creating copies of connector objects.
-

Table 3–2 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>

Table 3–2 (Cont.) Attributes of the eBusiness UM Target Resource User Reconciliation Scheduled Task

Attribute	Description
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>
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: <code>EBS-APPS12</code></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: <code>eBusiness UM Target Resource User Reconciliation</code> Value for the User Management with HR Foundation connector: <code>eBusiness UM Target Resource User-HRMS Reconciliation</code> Value for the User Management with TCA Foundation connector: <code>eBusiness UM Target Resource User-TCA Reconciliation</code> <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: <code>eBusiness Suite User</code> Value for the User Management with HR Foundation connector: <code>eBusiness Suite User HR Foundation</code> Value for the User Management with TCA Foundation connector: <code>eBusiness Suite User TCA Foundation</code> <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: <code>Lookup.EBS.UM.QueryFilters</code> Value for the User Management with HR Foundation connector: <code>Lookup.EBS.UMHRMS.QueryFilters</code> Value for the User Management with TCA Foundation connector: <code>Lookup.EBS.UMTCA.QueryFilters</code> <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. Expand **Resource Management**.
3. Click **Manage Scheduled Task**.
4. 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 Now
eBusiness UM Target Resource User Reconciliation	Inactive	ONCE	n/a	n/a	n/a	[Edit Icon]	Enable	Disabled	[Run Now Icon]

First | Previous | Next | Last

5. In the search results table, click the edit icon in the Edit column for the scheduled task. The following screenshot shows the Scheduled Task Details page:

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 [Clear]

Status: ☐ Enabled ☒ Disabled

Schedule

Max Retries: 2

Next Start: May 18, 2009 4:21:00

Frequency: ☒ Once ☐ Every [] Minutes

Last Start: n/a

Last Stop: n/a

6. On the Edit Scheduled Task Details page, you can modify the following details of the scheduled task by clicking **Edit**:

- **Status:** Specify whether or not 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.

When you click Edit, the Edit Scheduled Task page is displayed.

- After modifying the values for the scheduled task details listed in the previous step, click **Continue**.
- Specify values for the attributes of the scheduled task. To do so, select each attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for the attributes that you want to change. You must specify values for attributes whose default value is the "Enter a value" string.
 - 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.
-

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 displays 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 main area shows a table of attributes for a scheduled task. The table has three columns: 'Attribute Name', 'Attribute Value', and 'Delete'. The attributes listed are: Batch Size (1000), IT Resource Name (EBS-APPS12), Last Execution Time (0), Query Filter Lookup Definition (Lookup EBS UM QueryFilters), Query Name (UM_USER_RECON), Query Properties File, Recon Lookup Definition (Lookup EBS UM UserRecon), Resource Object Name (eBusiness Suite User), Target Date Format (MMdd/yyyy hh:mm:ss), and Task Name (eBusiness UM Target Resource User Reconciliation). Below the table, there are input fields for 'Attribute' and 'With', and buttons for 'Add' and 'Update'.

Attribute Name	Attribute Value	Delete
Batch Size	1000	
IT Resource Name	EBS-APPS12	
Last Execution Time	0	
Query Filter Lookup Definition	Lookup EBS UM QueryFilters	
Query Name	UM_USER_RECON	
Query Properties File		
Recon Lookup Definition	Lookup EBS UM UserRecon	
Resource Object Name	eBusiness Suite User	
Target Date Format	MMdd/yyyy hh:mm:ss	
Task Name	eBusiness UM Target Resource User Reconciliation	

Below the table, there are input fields for 'Attribute' and 'With', and buttons for 'Add' and 'Update'.

- Click **Save Changes** to commit all the changes to the database.

Note: If you want to stop a scheduled task while it is running, then use the Stop Execution feature of the Design Console. See the "The Task Scheduler Form" section in *Oracle Identity Manager Design Console Guide* for information about this feature.

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

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.

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:

Note: Request-based provisioning is disabled when you perform this procedure.

1. Open the resource object.
2. To detach the object form from the resource object, remove the name of the field from the Table Name field.
3. Deselect the **Self Request Allowed** check box.
4. Click the Save icon.
5. Open the process definition of provisioning type.
6. Deselect the **Auto Save** check box.
7. On the Data Flow tab, delete all mappings that are displayed.
8. Click the Save icon.

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

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. From the Users menu, select **Manage** if you want to provision a target system account to an existing OIM User.
3. If you select Create, 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:

4. If you select Manage, then search for the OIM User and select the link for the user from the list of users displayed in the search results.
5. 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.

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

- 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
- Help

User Detail
This is information about the user.

You can view additional details about this user: Select...

User ID	ROGER	User Disabled	<input type="checkbox"/>
First Name	Roger	User Locked	<input type="checkbox"/>
Middle Name		Start Date	
Last Name	Doe	End Date	
Status	Active	Provisioning Date	
Organization	Xellerate Users	Provisioned Date	May 15, 2009
User Type	End-User	Deprovisioning Date	
Employee Type	Full-Time Employee	Deprovisioned Date	
Manager ID		Change Password at next login	<input checked="" type="checkbox"/>
Email			

[Edit](#) [Disable](#) [Unlock](#) [Delete](#) [Change Password](#)

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

6. On the Resource Profile page, click **Provision New Resource**. The following screenshot shows the Resource Profile page.

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

- 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
- Help

Resources Not Found
There are no resources for this user

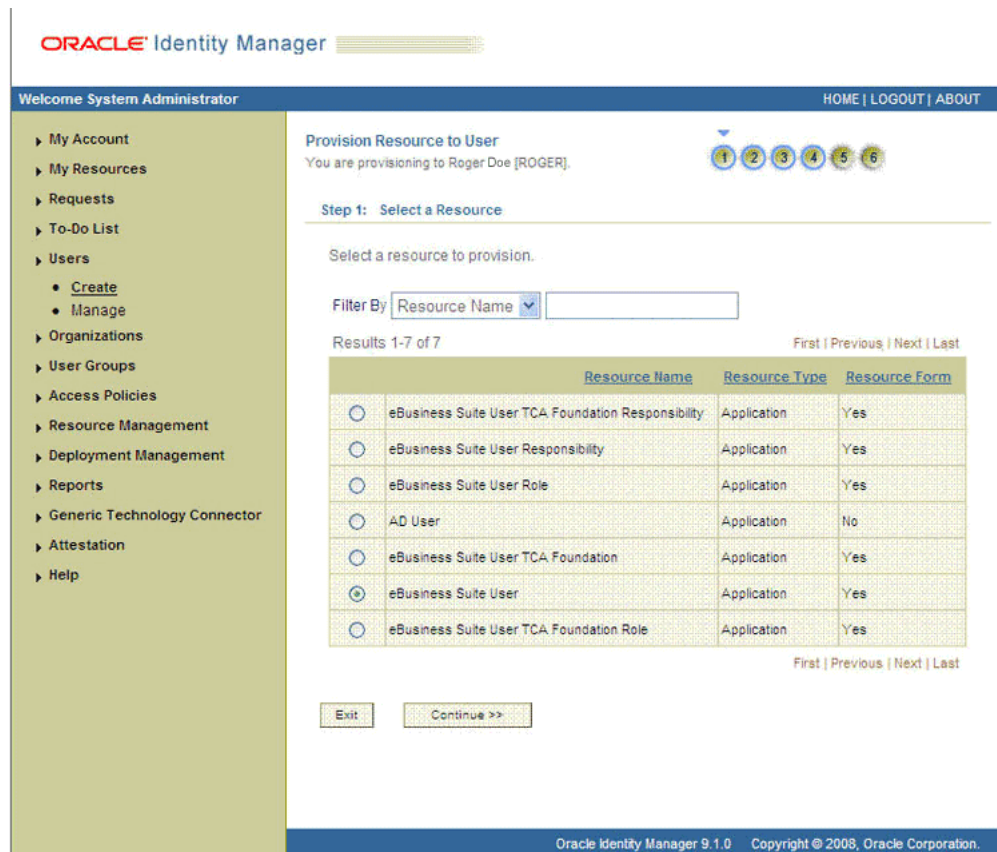
[User Detail](#) >> [Resource Profile](#)

User Name : [ROGER](#)
First Name : Roger
Last Name : Doe

[Provision New Resource](#)

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

7. 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.



ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

Provision Resource to User
You are provisioning to Roger Doe [ROGER].

Step 1: Select a Resource

Select a resource to provision.

Filter By: Resource Name

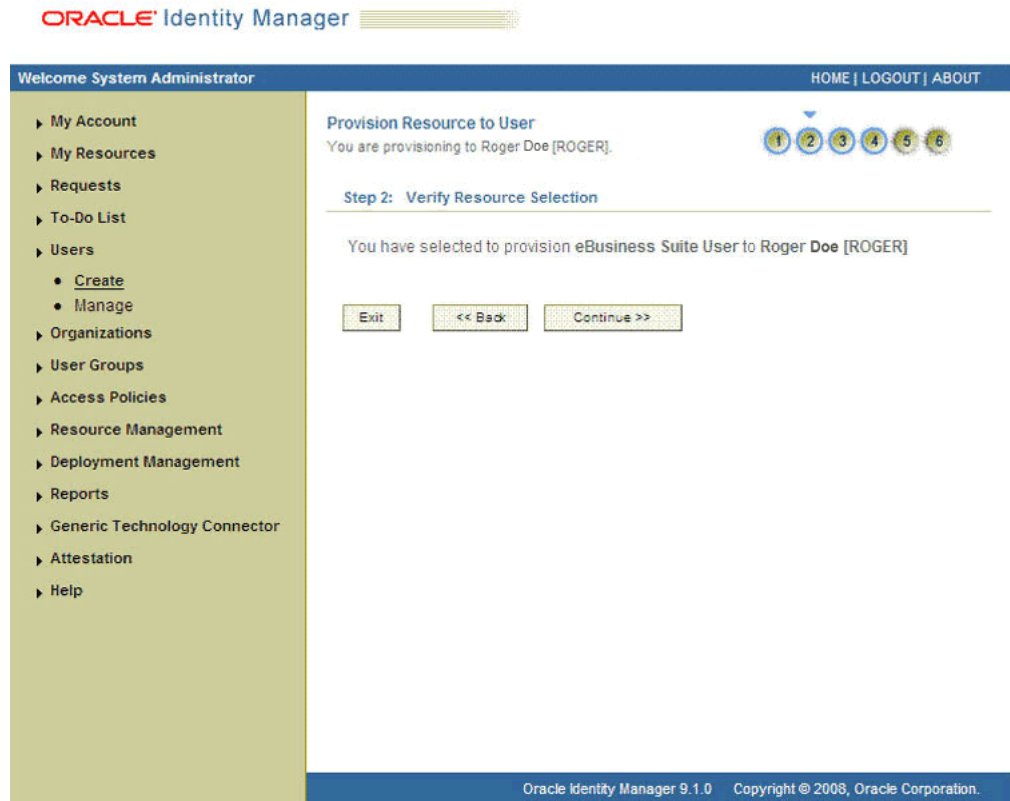
Results 1-7 of 7 First | Previous | Next | Last

	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

First | Previous | Next | Last

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

8. On the Step 2: Verify Resource Selection page, click **Continue**. The following screenshot shows the Step 2: Verify Resource Selection page.



9. 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.

ORACLE Identity Manager

Welcome System Administrator

HOME | LOGOUT | ABOUT

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 >>

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

10. On the Step 3: Provide Process Data page for responsibility data, specify the application name, responsibility name, and effective start date 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:

ORACLE Identity Manager

Welcome System Administrator

HOME | LOGOUT | ABOUT

Provision Resource to User
You are provisioning to Roger Doe [ROGER]

Step 3: Provide Resource Data

eBusiness Suite Responsibilities

Prepopulate

* Indicates required field

Application Name

Responsibility Name *

Effective Start Date

Add

Application Name	Responsibility Name	Effective Start Date	Remove
IEX	Collections Manager		<input type="checkbox"/>
IEX	Collections Agent		<input type="checkbox"/>
IEX	Collections Leasing Agent		<input type="checkbox"/>

Remove

Exit << Back Continue >>

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

11. 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:

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

- 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
- Help

Provision Resource to User
You are provisioning to Roger Doe [ROGER].

Step 3: Provide Resource Data

eBusiness Suite User Role Grants

* Indicates required field

Application Name

Role Name

Start Date

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

- 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.

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

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
Help

Provision Resource to User
You are provisioning to Roger Doe [ROGER]

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-APPS12
Description	
Email	
Fax	
S50 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 >>](#)

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

13. The "Provisioning has been initiated" message is displayed. 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:

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

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
Help

User Detail >> Resource Profile

User Name : [ROGER](#)
First Name : Roger
Last Name : Doe

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

Resource Name	Status	Description	Request ID	Resource Form	Process Form	Enable	Disable	Revoke
eBusiness Suite User	Provisioned	ROGER		View	View Edit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

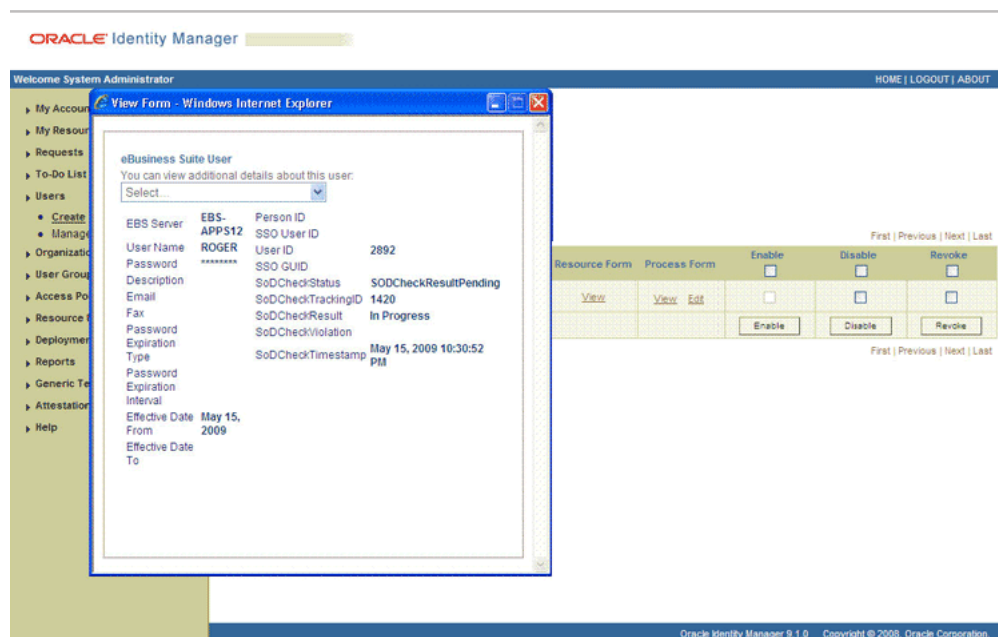
[Enable](#) [Disable](#) [Revoke](#)

[Provision New Resource](#)

First | Previous | Next | Last

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

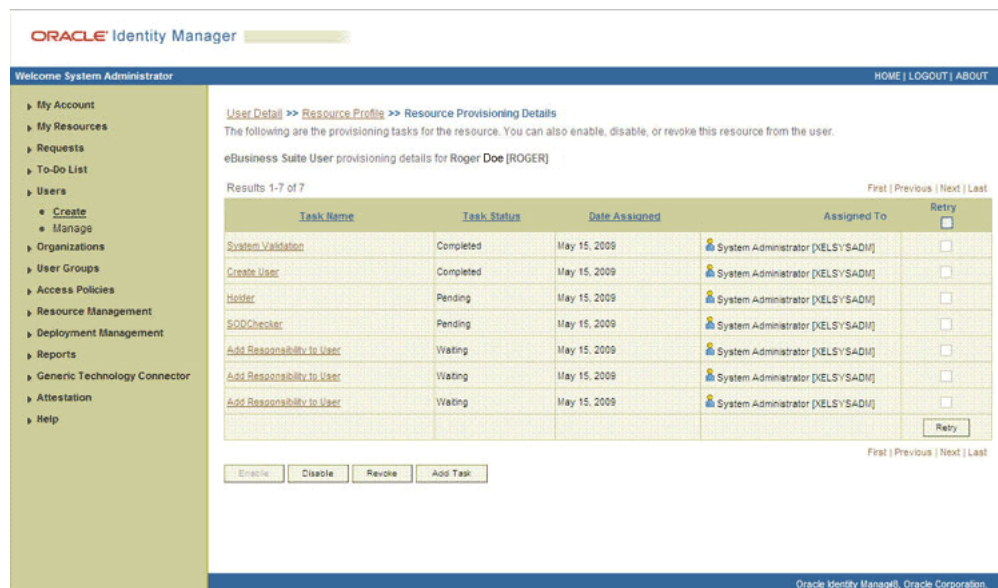
14. If you click the View link in the Process Form column, then the process form is displayed. The following screenshot shows this page:



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.

15. If you click the resource, then the Resource Provisioning Details page is displayed. The following screenshot shows this page:



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.

16. After the Get SOD Check Results Provisioning scheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. If you click the View link in the Process Form column, then the process form is displayed. The following screenshot shows this page:

The screenshot shows the Oracle Identity Manager interface. A 'View Form' window is open, displaying details for a user named 'eBusiness Suite User'. The form includes fields for 'Person ID', 'SSO User ID', 'User ID', 'SSO GUID', 'Description', 'Email', 'Fax', 'Password', 'Expiration', 'Type', 'Password', 'Expiration', 'Interval', 'Effective Date From', 'Effective Date To', 'SoDCheckStatus', 'SoDCheckTrackingID', 'SoDCheckResult', 'Policy Name', 'Responsibilities', 'Conflicting Duties', 'Collections Manager', 'Collections', 'Leasing Agent', 'Collections Agent', 'Collections', and 'SoDCheckTimestamp'.

Request ID	Resource Form	Process Form	Enable	Disable	Revoke
	View	View Edit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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:

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

[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 [XELSY\$ADM]	<input type="checkbox"/>
Create User	Completed	May 15, 2009	System Administrator [XELSY\$ADM]	<input type="checkbox"/>
SODChecker	Completed	May 15, 2009	System Administrator [XELSY\$ADM]	<input type="checkbox"/>
Holder	Canceled	May 15, 2009	System Administrator [XELSY\$ADM]	<input type="checkbox"/>
Add Responsibility to User	Canceled	May 15, 2009	System Administrator [XELSY\$ADM]	<input type="checkbox"/>
Add Responsibility to User	Canceled	May 15, 2009	System Administrator [XELSY\$ADM]	<input type="checkbox"/>
Add Responsibility to User	Canceled	May 15, 2009	System Administrator [XELSY\$ADM]	<input type="checkbox"/>

First | Previous | Next | Last

[Enable](#) [Disable](#) [Revoke](#) [Add Task](#)

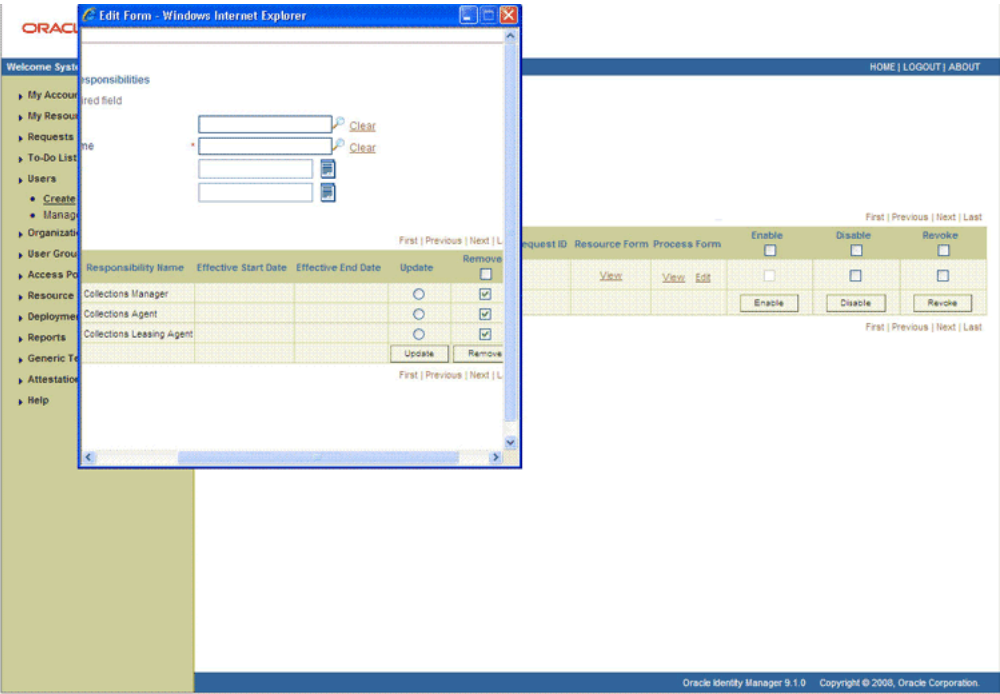
Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

In this screenshot, the status of the Add User Role tasks is Canceled because the request failed the SoD validation process.

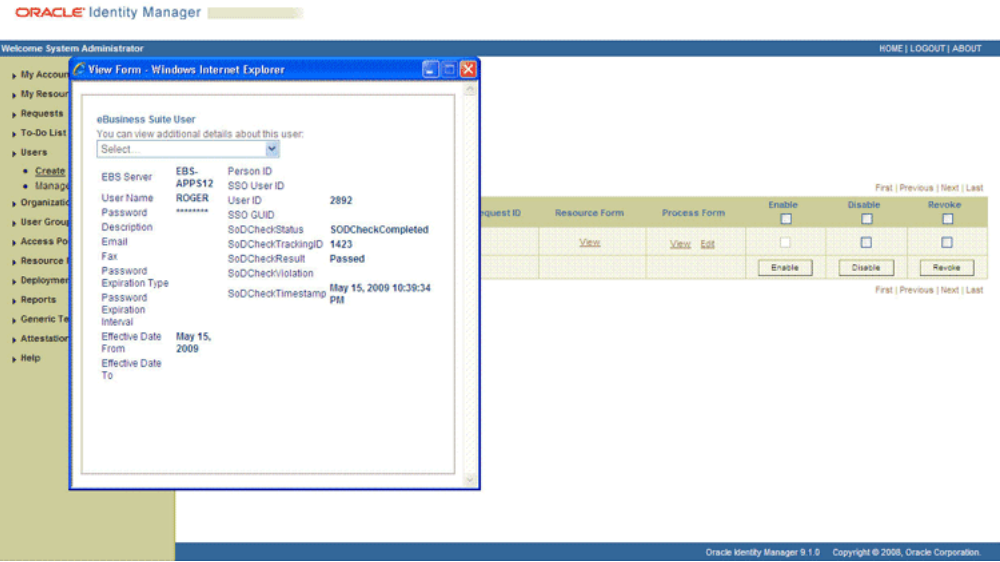
17. As the administrator assigning a resource to a user, you can either end the process when a violation is detected or modify the assignment data and then resend it. To modify the assignment data, first click the **Edit** link in the Process Form column on the Resource Profile page.
18. In the Edit 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:



- 19. Rerun the Get SOD Check Results Provisioning scheduled task to initiate the SoD validation process.
- 20. After the Get SOD Check Results Provisioningscheduled task is run, the results of the SoD validation process are brought to Oracle Identity Manager. If you click the View link in the Process Form column, then the process form is displayed. The following screenshot shows this page:



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:

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

[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

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

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.

End-User's Role in Request-Based Provisioning

The following are types of request-based provisioning:

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.

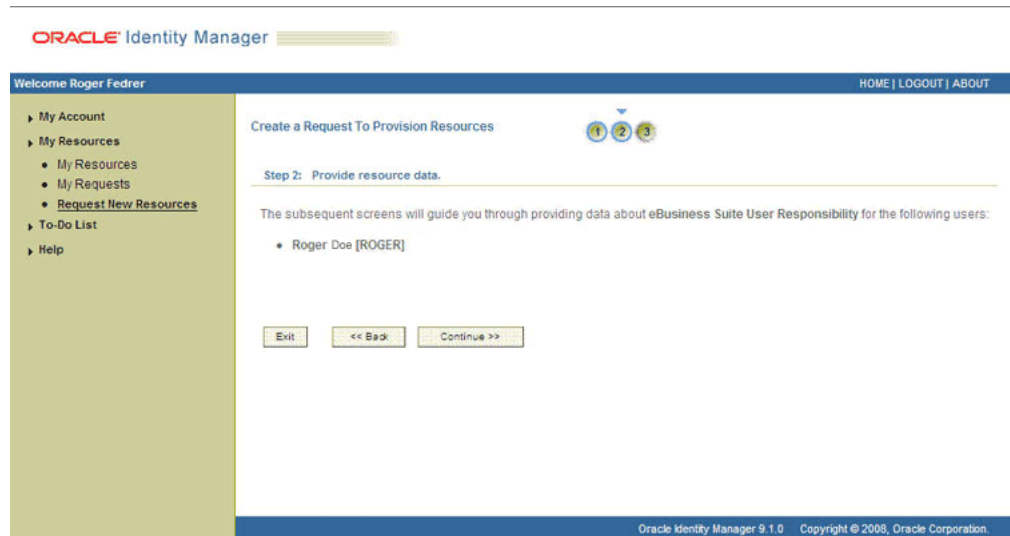
1. Log in to the Administrative and User Console.
2. Expand **My Resources**, and then click **Request New Resources**.
3. On the Step 1: Provide resources page, use the Add button to select one of the following:
 - eBusiness Suite User, if you want to create a request for a target system account
 - 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:



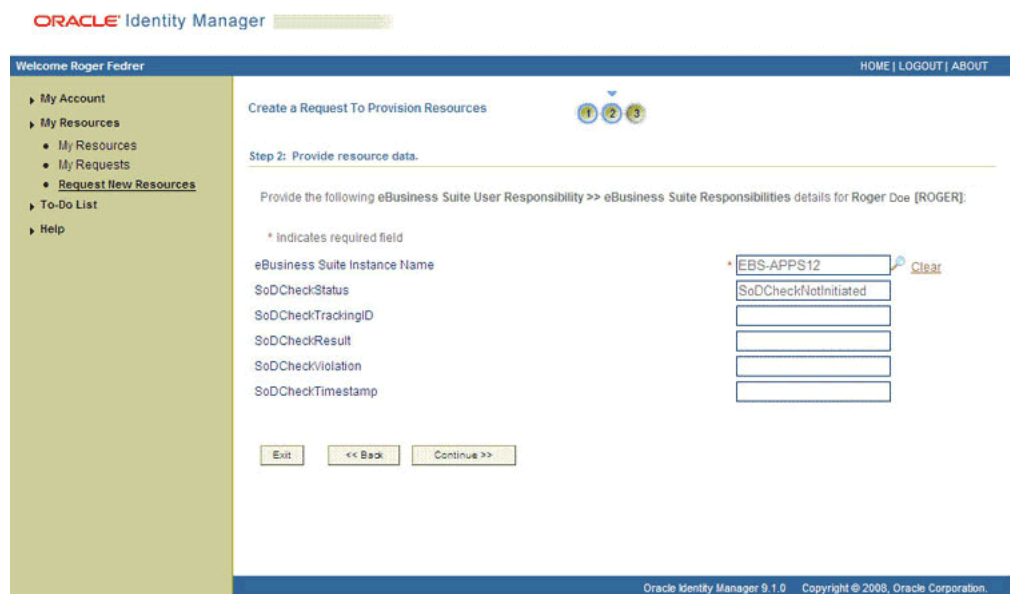
4. On the Step 2: Provide resource data page, click Continue.

The following screenshot shows this page:



- 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:



- On the third Step 2: Provide resource data page, to add the responsibility data, specify the application name, responsibility 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 [Calendar](#)

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="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

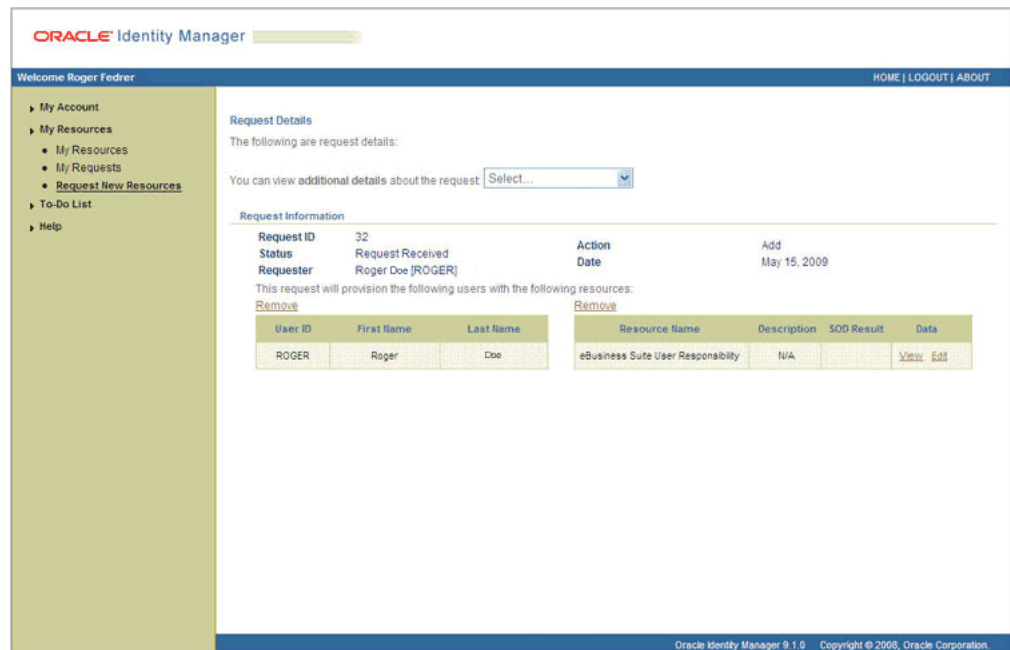
No comments have been added to this request. [Click here to add a comment.](#)

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:



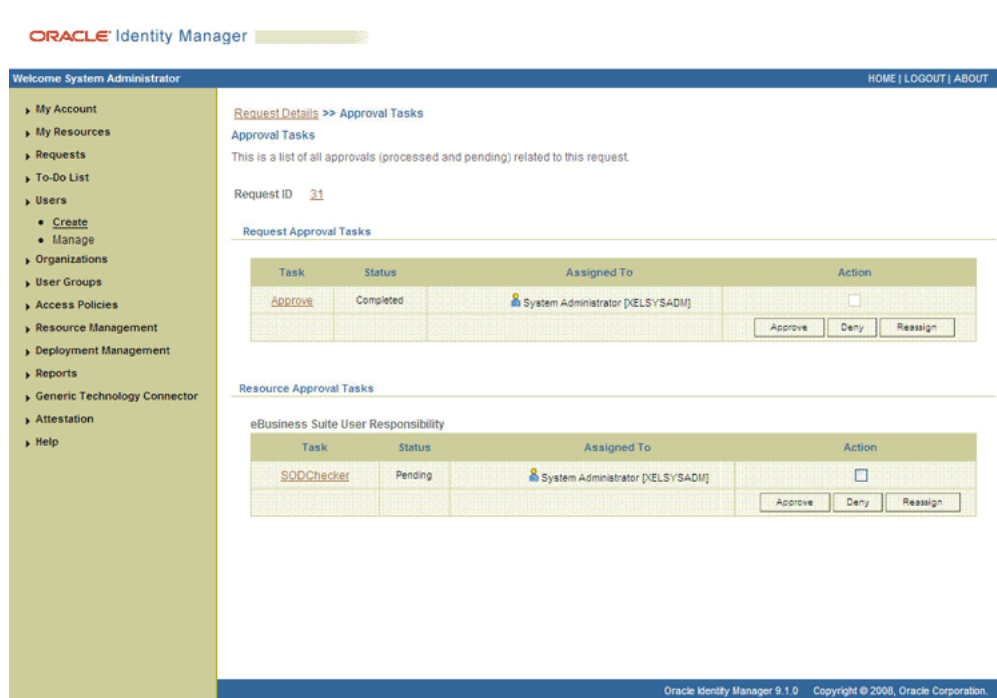
9. If you click the request ID, then the Request Details page is displayed. The following screenshot shows this page:



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.

10. 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.

11. To initiate SoD validation of pending entitlement requests, the approver must run the Get SOD Check Results Approval scheduled task.
12. 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.

The following screenshot shows the Approvals Task page after the request passes the SoD validation process.

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.

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

Request Details
The following are request details:

You can view additional details about the request: Select...

Request Information

Request ID	31	Request Received	Action	Add
Status	Request Received	Requester	Date	May 15, 2009
Requester	Roger Doe (ROGER)	This request will provision the following users with the following resources:		

[Remove](#)

User ID	First Name	Last Name	Resource Name	Description	SOD Result	Data
ROGER	Roger	Doe	eBusiness Suite User Responsibility	NA		View Edit

Pending Standard Approval Tasks
[Request More Information](#)

Task	Assigned To	Status	Approve/Deny
Approve	System Administrator (KLSYSADIV)	Pending	<input type="checkbox"/>

[Approve](#) [Deny](#) [Reassign](#)

[Back To Pending Approvals](#)

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

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.

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:

Edit Form - Windows Internet Explorer

eBusiness Suite Responsibilities

* Indicates required field

Application Name [Clear](#)

Responsibility Name [Clear](#)

Effective Start Date [Clear](#)

[Add](#)

Results 1-1 of 1

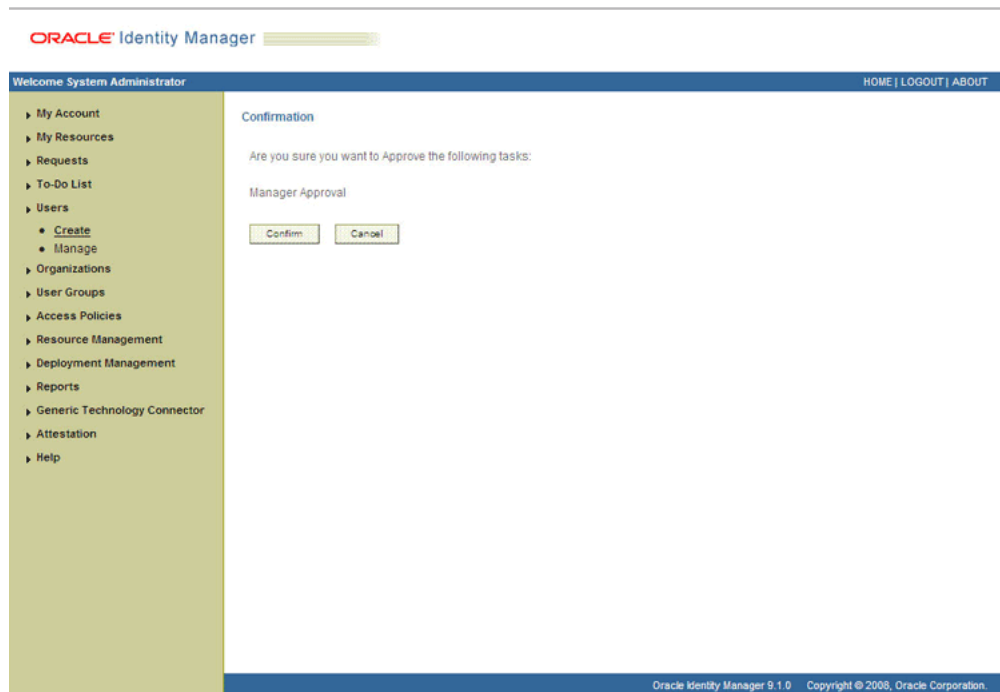
Application Name	Responsibility Name	Effective Start Date	Update	Remove
EX	Collectons Agent HTML		<input type="button" value="Update"/>	<input type="checkbox"/>

[First](#) [Previous](#) [Next](#) [Last](#)

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

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:



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 the Connector for Multiple Installations of the Target System"](#)

4.1 Guidelines on Extending the Functionality of the Connector

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 1.6.2, "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 1.6.2, "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 1.5.2, "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.

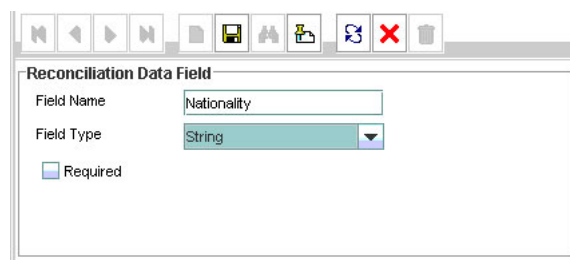
See Also:

[Section 1.5.1, "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.
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:

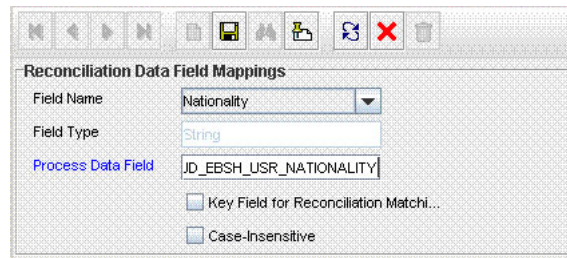
- For User Management: Lookup.EBS.UM.UserRecon
 - For User Management with HR Foundation: Lookup.EBS.UM.UserHRMSRecon
 - For User Management with TCA Foundation: Lookup.EBS.UM.UserTCARecon
- c. To add a row, click **Add**.
 - d. In the **Code Key** column, enter the name that you have set for the attribute 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 4.6, "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:

The screenshot shows the Oracle Identity Manager Design Console with the 'Form Designer' window open. The window displays the 'Form Information' tab for the form 'UD_EBSH_USR'. The 'Form Type' is set to 'Process'. The 'Version Information' section shows the 'Latest Version' as 0 and the 'Active Version' as 0. The 'Operations' section shows the 'Current Version' as 0. The 'Properties' tab is selected, showing a table of fields for the form. The table has columns: Name, Variant Type, Length, Field Label, Field Type, Default Value, Order, and Apply. The table lists 27 fields, including UD_EBSH_USR_PASSWORD, UD_EBSH_USR_DESCR, UD_EBSH_USR_EMAIL, UD_EBSH_USR_FAX, UD_EBSH_USR_EMPNUM, UD_EBSH_USR_EFFDATEFROM, UD_EBSH_USR_EFFDATETO, UD_EBSH_USR_SSOID, UD_EBSH_USR_PERTYPEID, UD_EBSH_USR_BIZORPID, UD_EBSH_USR_SODCHECKSTATUS, UD_EBSH_USR_SODCHECKTRACKINGID, UD_EBSH_USR_SODCHECKRESULT, UD_EBSH_USR_SODCHECKVIOLATION, UD_EBSH_USR_SODCHECKTIMESTAMP, and UD_EBSH_USR_NATIONALITY.

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	30	Effective Date From	DateField		9	
UD_EBSH_USR_EFFDATETO	Date	30	Effective Date To	DateField		10	
UD_EBSH_USR_SSOID	String	256	SSO User ID	TextField		11	
UD_EBSH_USR_PERTYPEID	long		Person Type ID	TextField		16	
UD_EBSH_USR_BIZORPID	long		Business Group ID	TextField		17	
UD_EBSH_USR_SODCHECKSTATUS	long	50	SoDCheckStatus	SoDField	SODCheckNotInitiate	22	
UD_EBSH_USR_SODCHECKTRACKINGID	String	50	SoDCheckTrackingID	SoDField		23	
UD_EBSH_USR_SODCHECKRESULT	String	4000	SoDCheckResult	SoDField		24	
UD_EBSH_USR_SODCHECKVIOLATION	String	4000	SoDCheckViolation	SoDField		25	
UD_EBSH_USR_SODCHECKTIMESTAMP	String	50	SoDCheckTimestamp	SoDField		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.
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 1.5.2, "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 1.5.1, "Reconciliation Queries"](#)

[Section 4.1.2, "Guidelines for Configuring Queries Used in Reconciliation"](#)

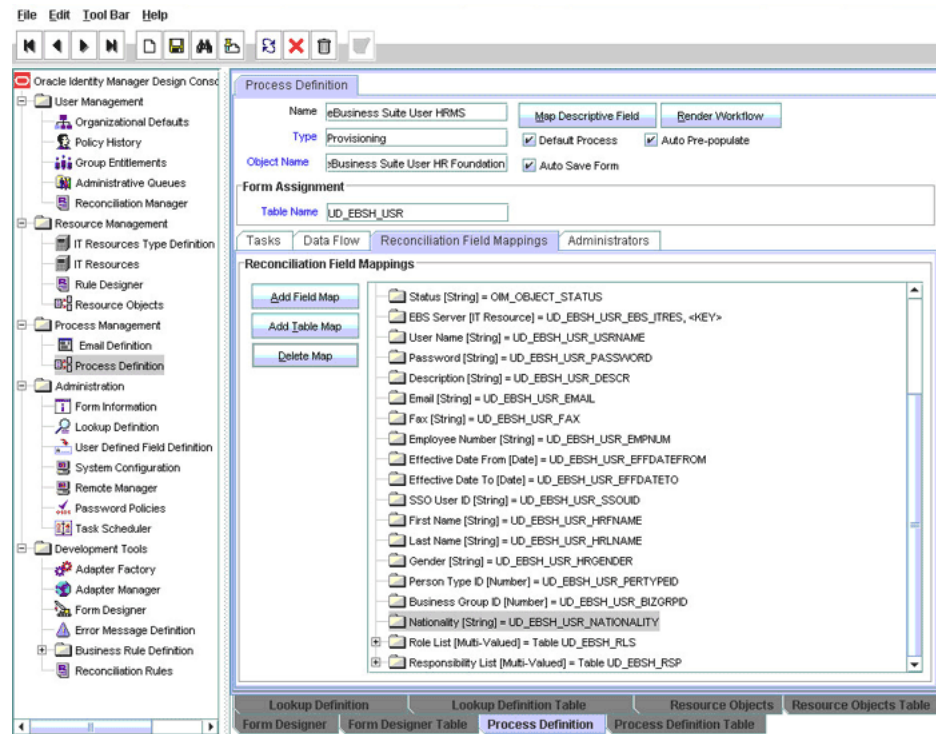
[Section 4.1.3, "Guidelines Common to Configuring Both Types of Queries"](#)

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:

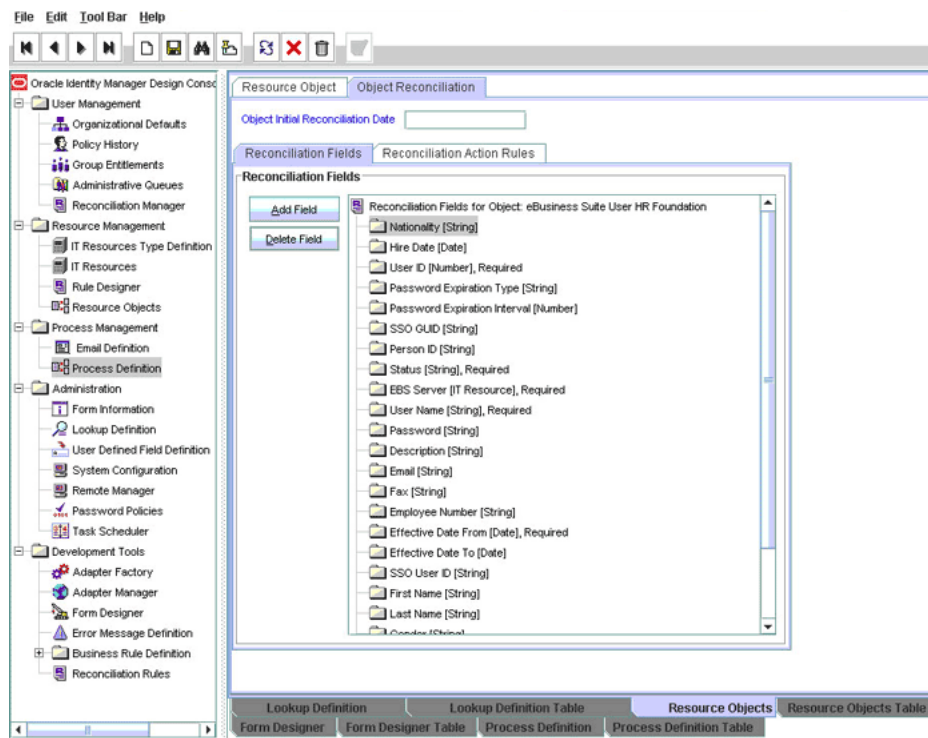
See [Section 4.6, "Configuring the Connector for Multiple Installations of the Target System"](#) for a listing of the process definitions for each connector.

- 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.
6. Remove the entry for the attribute in the lookup definition for reconciliation attribute mapping as follows:
- Expand the **Administration** folder, and then double-click **Lookup Definition**.
 - 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:

Oracle Identity Manager Design Console

File Edit Tool Bar Help

Lookup Definition

Code: Lookup.EBS_UM.UserHRMSRecon

Field:

Lookup Type: ☒ Lookup Type ☐ Field Type

Required: ☐

Group: EBS_UM

Lookup Code Information

	Code Key	Decode
1	Nationality	NATIONALITY
2	User Name	USER_NAME
3	Description	DESCRIPTION
4	Email	EMAIL_ADDRESS
5	Fax	FAX
6	Effective Date From	START_DATE
7	Effective Date To	END_DATE
8	Employee Number	EMPLOYEE_NUMBER
9	First Name	FIRST_NAME
10	Last Name	LAST_NAME
11	Gender	SEX
12	Person Type ID	PERSON_TYPE_ID
13	Business Group ID	BUSINESS_GROUP_ID
14	Hire Date	ORIGINAL_DATE_OF_HI
15	Person ID	PERSON_ID
16	User ID	USER_ID

Lookup Definition Lookup Definition Table Resource Objects Resource Objects Table

Form Designer Form Designer Table Process Definition Process Definition Table

- 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 4.6, "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**.

The screenshot shows the Oracle Identity Manager Design Console Form Designer. The left pane shows a tree view with categories like User Management, Resource Management, Process Management, and Administration. The main pane is titled 'Form Designer' and contains sections for Table Information, Version Information, and Operations. Below these is a table with columns for Name, Variant Type, Length, Field Label, Field Type, Default Value, Order, and Application. The table lists various attributes for the 'UD_EBSH_USR' form, including password, description, email, fax, employee number, effective dates, SSO User ID, Person Type ID, Business Group ID, SoD check status, SoD check tracking ID, SoD check result, SoD check violation, SoD check timestamp, and Nationality.

Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application
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_SSOUID	String	256	SSO User ID	TextField		11	
UD_EBSH_USR_PERTYPEID	long		Person Type ID	TextField		16	
UD_EBSH_USR_BIZORPID	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. 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 1.6.2, "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 1.6.2, "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: Directly proceed to the next step if you have already added the field to the process form while performing the procedure described in [Section 4.2.1, "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 4.6, "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:

- e. Specify the properties of the attribute according to your requirement.
- f. Click the Save icon.

- Note:** Each question mark in the signature value of the Decode column stands for a parameter of the stored procedure.

4. Add an entry in 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 add a row, click **Add**. The following screenshot shows this page:
 - 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. 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 4.6, "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.
6. 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.
- 7. 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.

4.3.2 Removing Attributes for Provisioning

By default, the attributes listed in [Section 1.6.2, "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. Add 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 4.6, "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.Configurations
- For the User Management with HR Foundation connector: Lookup.EBS.UMTCA.Configurations
- For the User Management with TCA Foundation connector: Lookup.EBS.UMHRMS.Configurations

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.Configurations
 - Lookup.EBS.UMTCA.Configurations
 - Lookup.EBS.UMHRMS.Configurations
- 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. 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 4.6, "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.
6. 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.
7. Remove the attribute for reconciliation as follows:
See [Section 4.2.2, "Removing Attributes Used for Reconciliation"](#) for more information.

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 4.6, "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:

4. Modify the length of the required field.
5. Click the Save icon.

4.6 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

Table 4–1 (Cont.) Connector Objects

Connector Object	User Management	User Management with HR Foundation	User Management with TCA Foundation
	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
	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.Configurations	Lookup.EBS.UMHRMS.Configurations	Lookup.EBS.UMTCA.Configurations
	Lookup.EBS.Roles.Mapping	Lookup.EBS.UM.CreateEmployee	Lookup.EBS.UM.PartyProvisioning

Table 4–1 (Cont.) Connector Objects

Connector Object	User Management	User Management with HR Foundation	User Management with TCA Foundation
	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			
	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.

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.

To use the testing utility:

1. Open the following file:

OIM_HOME/xellerate/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 the following file:

OIM_HOME/xellerate/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
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.

Parameter	Description
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: OFA
RESPONSIBILITY_NAME	Responsibility name Sample value: @Engineering
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

5. Run the testing utility file.
 - For Microsoft Windows, run the following file:
OIM_HOME\xellerate\XLIIntegrations\EBSUM\scripts\OracleEBiz.bat
 - For UNIX, run the following file:
OIM_HOME/xellerate/XLIIntegrations/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	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.

Known Issues

The following are known issues associated with this release of the connector:

- **Bug 7207232**

Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

See [Section 4.5, "Modifying Field Lengths on the Process Form"](#) for information about working around this issue.

- **Bug 8504052**

The Test Connectivity option does not work for the IT resource that you create to hold information about the SoD engine.

- **Bug 8513985**

The "Lookup properties not configured correctly" message might be displayed on the Administrative and User Console even when lookup field values are correctly displayed. You can ignore this message.

- **Bug 8501508**

During SoD-enabled provisioning, the connector does not provision entitlements if a conflict is encountered. When this occurs, you must revoke the conflicting entitlement and retry the entitlement provisioning operation. An error is thrown if you try to update the conflicting entitlement.

- **Bug 8535215**

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.

- **Bug 8534970**

During reconciliation, the "java.sql.SQLException: ORA-01858" error is thrown if a date literal is included in the reconciliation query without specifying a format for the date literal. To avoid this problem, 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').`

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

additional files, 1-2
Administrative and User Console, 2-18, 5-4
architecture, 1-3

C

certified components, 1-1
certified languages, 1-2
clearing server cache, 2-28
components, certified, 1-1
configuring connector, 3-1
connector architecture, 1-3
connector configuration, 3-1
connector features, 1-3
connector files and directories
 description, 2-1
connector testing, 5-1
connector version number, determining, 2-3

D

data encryption and integrity, 2-16
defining
 IT resources, 2-35
determining version number of connector, 2-3

E

enabling logging, 2-29
errors, 5-3
external code files, 1-2, 2-3

F

files
 additional, 1-2
 external code, 1-2
 See also XML files
files and directories of the connector
 See connector files and directories

G

globalization features, 1-2

I

installing connector, 2-11
issues, 6-1
IT resources
 defining, 2-35
 parameters, 2-35

L

limitations, 6-1
logging enabling, 2-29
lookup field synchronization, 1-24, 3-1, 3-3
lookup fields, 1-24, 3-1, 3-3

M

multilanguage support, 1-2

O

Oracle Database, 2-16
Oracle Identity Manager Administrative and User
 Console, 2-18, 5-4

P

parameters of IT resources, 2-35
problems, 5-3
Provisioning, 1-18
provisioning
 direct provisioning, 3-14
 identity fields, 1-21
 provisioning triggered by policy changes, 3-13
 request-based provisioning, 3-13

R

Reconciliation, 1-12
reconciliation action rule
 target resource reconciliation, 1-18
reconciliation rule
 target resource reconciliation, 1-17
reconciliation scheduled tasks, 3-7

S

- scheduled tasks
 - defining, 3-9
 - reconciliation, 3-7
- server cache, clearing, 2-28
- SoD, xii
- stages of connector deployment
 - installation, 2-7
 - postinstallation, 2-11
 - preinstallation, 2-1
- supported
 - releases of Oracle Identity Manager, 1-1
 - target systems, 1-2

T

- target resource reconciliation, 1-1
 - adding new fields, 4-4, 4-7
 - reconciliation action rule, 1-18
 - reconciliation action rules, 1-18
 - reconciliation rule, 1-17
- target system user account, 2-4
- target system, multiple installations, 4-23
- target systems
 - supported, 1-2
- temporary tables, 1-13
- test cases, 5-1
- testing the connector, 5-1
- testing utility, 5-1
- troubleshooting, 5-3

V

- version number of connector, determining, 2-3