Oracle® Identity Manager

Connector Guide for Oracle E-Business Employee Reconciliation

Release 9.1.0

E11202-03

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for Oracle E-Business Employee Reconciliation, Release 9.1.0

E11202-03

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

2 Deploying the Connector

3 Using the Connector

List of Figures

List of Tables

Preface

This guide provides information about Oracle Identity Manager Connector for Oracle E-Business Employee Reconciliation.

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	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 Employee Reconciliation?

This chapter provides an overview of the updates made to the software and documentation for release 9.1.0 of the Oracle E-Business Employee Reconciliation connector.

> **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 software updates:

- Software Updates in Release 9.1.0

Software Updates in Release 9.1.0

The following are software updates in release 9.1.0:

- Dedicated Support for Trusted Source Reconciliation
- Support for New Target System Versions and Configurations
- Support for Configurable Reconciliation Queries (Configurable Attribute Mappings)
- Support for Effective-Dated Lifecycle Events
- Support for Multiple Person Types
- Support for Creating Copies of Connector Objects
- Support for Target System Account with Minimum Permissions for Connector Operations

- Support for Connection Pooling
- Support for the Multiple Trusted Source Reconciliation Feature of Oracle Identity Manager
- Support for SSL Communication Between the Target System and Oracle Identity Manager

Dedicated Support for Trusted Source Reconciliation

The connector provides all the features required to integrate Oracle E-Business HRMS as a trusted source of identity data. The connector can also be configured for use in scenarios in which Oracle E-Business HRMS is one of the trusted sources in the operating environment of the organization.

Note: If you want to manage Oracle E-Business Suite as a target resource of Oracle Identity Manager, then use the Oracle E-Business User Management connector.

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 10*g* and 11*g*

The Section 1.1, "Certified Components" section provides information about these and other certified software components that you can use with the connector.

Support for Configurable Reconciliation Queries (Configurable Attribute Mappings)

Reconciliation involves running a SQL query on the target system database to fetch the required person records to Oracle Identity Manager. From this release onward, you can modify the predefined SQL queries that are shipped in the connector deployment package. You can also create and use your own SQL queries for reconciliation. This feature can also be used to extend the default set of attribute mappings for reconciliation.

See the following sections for more information:

- Section 1.5.1, "Reconciliation Queries"
- Section 4.5, "Configuring Reconciliation Queries"

Support for Effective-Dated Lifecycle Events

Oracle E-Business HRMS allows effective-dating of lifecycle events. For example, a change in an employee's designation can be scheduled for the end of the current quarter. The connector can detect and respond to such effective-dated lifecycle events.

See Section 1.3, "Connector Architecture" for more information.

Support for Multiple Person Types

An organization can use Oracle E-Business HRMS to store different types of person records. Examples of person types include employees, part-time workers, contingent workers, and contractors. The connector can distinguish between records of different person types. In addition, you can add to or modify the predefined set of supported person types.

See the following sections for more information:

- Section 1.5.4.2, "Lookup.EBS.HRMS.PersonTypes Lookup Definition"
- Section 4.5, "Configuring 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" sections for more information.

Support for Target System Account with Minimum Permissions for Connector Operations

You can create and use an Oracle E-Business HRMS user account 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. This approach was resource-intensive. 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 1.4.9, "Connection Pooling" 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.

Support for SSL Communication Between the Target System and Oracle Identity Manager

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

See Section 2.3.4, "Configuring Secure Communication Between the Target System and Oracle Identity Manager" for more information.

Documentation-Specific Updates

The following are documentation-specific updates in release 9.1.0:

- Major changes have been made in the structure of guide for this release. The objective of these changes is to synchronize the guide with the software updates and to improve the usability of information provided by the guide.

  See Section 1.6, "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.

1

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 HRMS as an authoritative (trusted) source of identity data for Oracle Identity Manager.

In the identity reconciliation (trusted source) configuration of the connector, person records are created and modified only on Oracle E-Business HRMS and information about these users is reconciled into Oracle Identity Manager.

> **Note:** At some places in this guide, Oracle E-Business HRMS has been referred to as the **target system.**

This chapter is divided the following sections:

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 **Note:** This release of the connector leverages features, such as reconciliation of future-dated user lifecycle events, introduced in Oracle Identity Manager release 9.1.0.2.
Target system	Oracle E-Business Suite 11.5.10, 12.0.x These applications may run on Oracle Database 10*g* or Oracle Database 11*g*, as either single databse or RAC implementation. **Note:** Communication between Oracle Identity Manager and the target system can be in SSL or non-SSL mode.

1.2 Certified Languages

The connector supports the following languages:

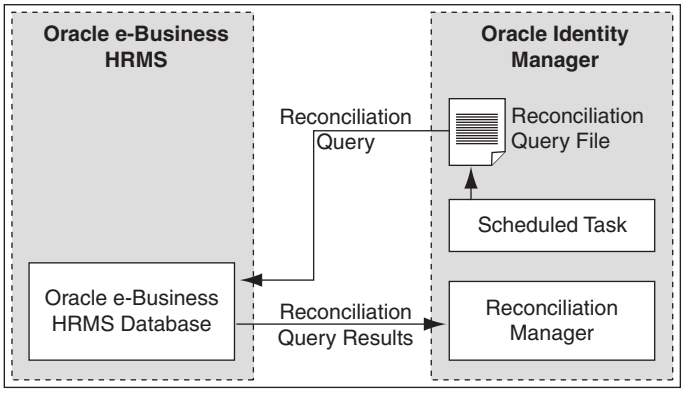
- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

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

1.3 Connector Architecture

Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector



The connector is configured to perform identity (trusted source) reconciliation with the target system. In this form of reconciliation, identity data is fetched to Oracle Identity Manager and this data is used to create or update OIM Users.

The following is an overview of the steps involved in trusted source 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 eBusiness HRMS Trusted Reconciliation scheduled task, you specify the name of the properties file and the query that you want to run.

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.

   The Section 3.2.6, "Configuring the Reconciliation Scheduled Tasks" section provides information about the scheduled task.

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. Person records on the target system that meet the query criteria are fetched into Oracle Identity Manager.

6. Each person record fetched from the target system is compared with existing OIM User records. The reconciliation rule is applied during the comparison process. See Section 1.5.3, "Reconciliation Rules for Trusted Source Reconciliation" for information about the 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 person record and an OIM User, then the OIM User is updated with changes made to the person record.
   - If no match is found, then the target system person record is used to create an OIM User.

Oracle E-Business HRMS allows effective-dating of some employee lifecycle events. For example, a person's hire date can be set to a future date. This effective date is stored in the EFFECTIVE_START_DATE column of the target system database table. Similarly, events such as a person's resignation and last day with the organization can be set in advance. The date for an event of this type is stored in the EFFECTIVE_END_DATE column. For a particular future-dated change, when the current date equals the date stored in the EFFECTIVE_START_DATE or EFFECTIVE_END_DATE column, the appropriate change is made in the person's record on the target system.

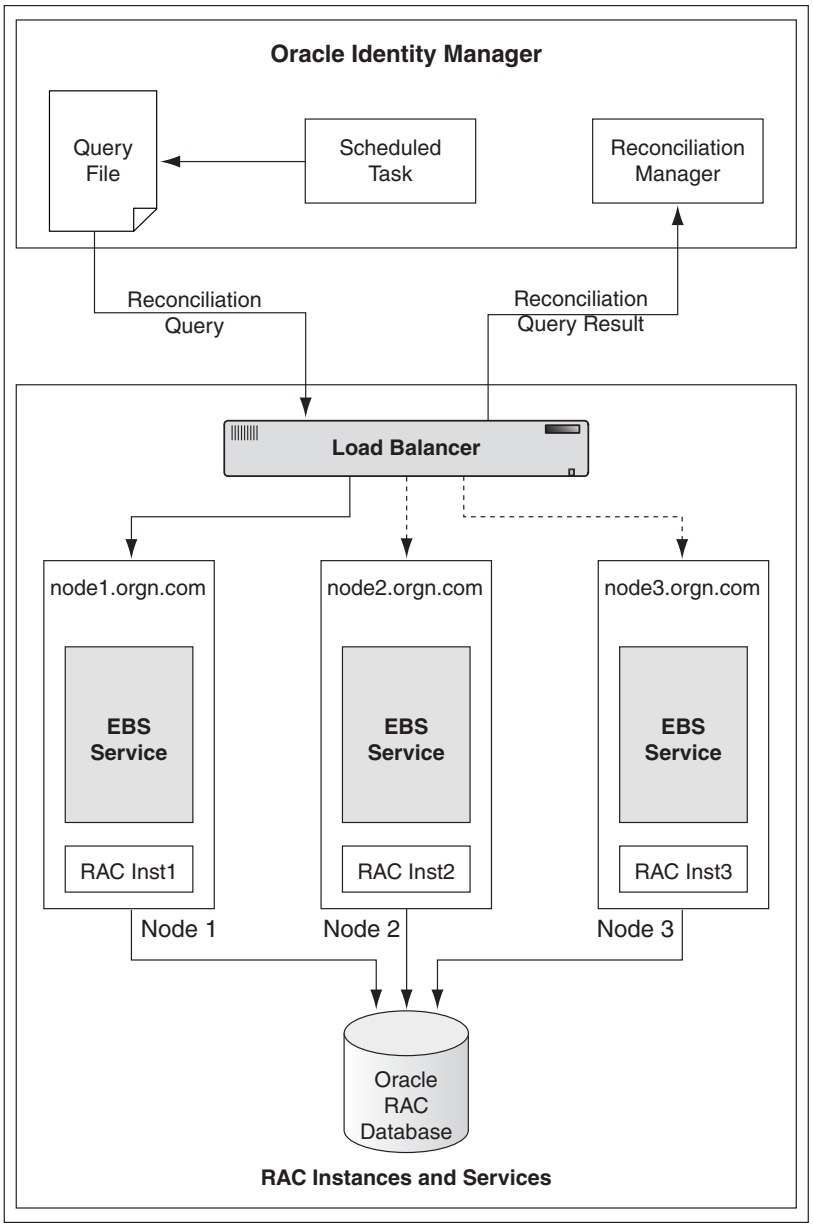
The connector can detect and respond to these effective-dated lifecycle events.

When you run the predefined query to reconcile all person records, only records with current-dated changes are fetched into Oracle Identity Manager. When you run the predefined query to reconcile future hires, only records with future-dated Start Date values are fetched into Oracle Identity Manager.

Note: In Oracle Identity Manager release 9.1.0.2, reconciliation events created out of future-dated hire events are set to the Event Deferred state. The Process Deferred Recon Events scheduled task is used to process events that are in this state. For each event in the Event Deferred state, the scheduled task compares the Start Provisioning date of the event with the system date. If the Start Provisioning date is less than or equals the system date, then the event is forwarded to the Reconciliation Manager in Oracle Identity Manager.

Figure 1–2 shows the architecture of the connector integrating Oracle Identity Manager with an Oracle RAC installation.

Figure 1–2 Architecture of Integration with an Oracle RAC Installation



As shown in this figure, the load balancer acts as the interface for reconciliation queries sent by the scheduled task. During each reconciliation run, the query is sent to one of the Oracle RAC nodes and the query results are sent through the load balancer to Oracle Identity Manager.

1.4 Features of the Connector

The following are features of the connector:

- Section 1.4.1, "Dedicated Support for Trusted Source Reconciliation"
- Section 1.4.2, "Predefined Reconciliation Queries"
- Section 1.4.3, "Custom Reconciliation Queries"
- Section 1.4.4, "Reconciliation of Effective-Dated Events"

1.4.1 Dedicated Support for Trusted Source Reconciliation

You can use the connector to integrate Oracle E-Business HRMS as a trusted source of Oracle Identity Manager. In other words, the target system is the authoritative source of identity data for Oracle Identity Manager. This identity data is used to create or update OIM Users. The connector can also be configured for use in scenarios in which Oracle E-Business HRMS is one of the trusted sources in the operating environment of the organization.

The connector cannot be used to set up Oracle E-Business HRMS as a target resource. In other words, the connector does not support provisioning operations and target resource reconciliation with Oracle E-Business HRMS. This is because person records maintained in Oracle E-Business HRMS are not accounts that users can use to log in to the system and perform business-related work.

1.4.2 Predefined Reconciliation Queries

The connector is shipped with predefined queries that enable you to reconcile data for the following types of lifecycle events on the target system:

- A person's record is added or modified.
- A person's department is changed.
- A person's record is created, but the hire date is set to a future date. This is an effective-dated hire.
- A person's services are terminated.
- A person's record is deleted.

While configuring the reconciliation scheduled task, you can specify the query that you want to run on the target system.

Note: Oracle E-Business HRMS allows you to configure (customize) the changes that must be applied to a person record in response to the promotion event. Therefore, the connector does not provide a predefined query for this lifecycle event. If required, you can create a reconciliation query to fetch promotion events into Oracle Identity Manager. The procedure to create custom reconciliation queries is explained later.

See Section 1.5.1, "Reconciliation Queries" for more information.

1.4.3 Custom Reconciliation Queries

You can modify and use any of the predefined queries. In addition, you can create your own reconciliation queries.

See the following sections for more information:

- Section 1.5.1, "Reconciliation Queries"
- Section 4.5, "Configuring Reconciliation Queries"

1.4.4 Reconciliation of Effective-Dated Events

The target system allows you to set a future or effective date for certain lifecycle events. The connector can detect and respond to these events. For example, suppose you schedule John's employment with your organization to begin 2 months from the current date. When you configure the scheduled task to reconcile future hires, the query fetches John's record because his hire date is set to a future date. However, if you configure the scheduled task to reconcile newly added or modified records, John's newly created record will be ignored because it is effective dated.

See Section 1.3, "Connector Architecture" for more information.

1.4.5 Support for Multiple Person Types

An organization can use Oracle E-Business HRMS to store different types of person records. Examples of person types include employees, part-time workers, contingent workers, and contractors. The connector can distinguish between records of different person types. In addition, you can add to or modify the predefined set of supported person types.

See the following sections for more information:

- Section 1.5.4.2, "Lookup.EBS.HRMS.PersonTypes Lookup Definition"
- Section 4.5, "Configuring Reconciliation Queries"

1.4.6 Full and Incremental Reconciliation

In full reconciliation, all person records are fetched from the target system to Oracle Identity Manager. In incremental reconciliation, only person 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 3.1, "Performing First-Time (Full) Reconciliation" for more information.

1.4.7 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 3.2.5, "Configuring Limited Reconciliation" for more information.

1.4.8 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 3.2.1, "Batched Reconciliation" for more information.

1.4.9 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target system. 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.

The configuration properties of the connection pool are part of the IT resource definition. See Section 2.3.3, "Setting Up Connection Pooling" for information about using the connection pool.

1.4.10 Support for SSL Communication Between the Target System and Oracle Identity Manager

You can configure SSL to secure communication between Oracle Identity Manager and the target system.

See Section 2.3.4, "Configuring Secure Communication Between the Target System and Oracle Identity Manager" for more information.

1.5 Connector Objects Used During Reconciliation

This section discusses the following topics:

- Section 1.5.1, "Reconciliation Queries"
- Section 1.5.2, "Target System Fields Used in Reconciliation"
- Section 1.5.3, "Reconciliation Rules for Trusted Source Reconciliation"
- Section 1.5.4, "Lookup Definitions Used During 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 ebsERQuery.properties file.

Note: Depending on your requirements, you can modify existing queries or add your own query in the ebsERQuery.properties or a different properties file. The Section 4.5, "Configuring Reconciliation Queries" section provides more information.

Columns in the SELECT clause of each predefined query are from the PER_ALL_PEOPLE_F table of the target system. Column aliases in the SELECT clause

are mapped to Oracle Identity Manager process form fields by the Lookup.EBS.HRMS.Recon lookup definition.

> **See Also:** Section 1.5.4.1, "Lookup.EBS.HRMS.Recon Lookup Definition"

Most of 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. Except for the query to reconcile deleted user records, the predefined queries apply some variation of the following criteria to extract records for reconciliation from the target system:

> **Note:** You can specify a value for the Last Execution Time attribute. See Section 3.2.3, "Reconciliation Time Stamp" for more information.

- The date in the LAST_UPDATE_DATE column of the PER_ALL_PEOPLE_F table must be greater than the date part of the time stamp stored in the Last Execution Time scheduled task attribute.
- The CURRENT_EMPLOYEE_FLAG column must be set to `y`.
- The date of the host computer on which the target system database is running must be between dates stored in the EFFECTIVE_START_DATE and EFFECTIVE_START_DATE columns.

The queries in the predefined properties file support the following modes of reconciliation:

- Section 1.5.1.1, "Reconciliation of New and Modified Person Records"
- Section 1.5.1.2, "Reconciliation of Persons Whose Department Has Changed"
- Section 1.5.1.3, "Reconciliation of Future Hires"
- Section 1.5.1.4, "Reconciliation of Terminated Persons"
- Section 1.5.1.5, "Reconciliation of Deleted Person Records"
- Section 1.5.1.6, "Reconciliation of All Person Records"

1.5.1.1 Reconciliation of New and Modified Person Records

The ReconcileCurrentPersons query is used to reconcile all person records that have been added or modified after the time stamp stored in the Last Execution Time attribute.

The following is a sample scenario in which the ReconcileCurrentPersons query can be used:

Drew, Maria, and Richard joined the organization on 21-March. Person records for these individuals were created in Oracle E-Business HRMS on the same day. Theresa's last name was updated on the same day. These newly added and modified person records are fetched into Oracle Identity Manager during the next run of the ReconcileCurrentPersons query.

The ReconcileCurrentPersons query uses data stored in the following target system tables:

PER_ALL_PEOPLE_F

PER_PERSON_TYPES

PER_PERSON_TYPE_USAGES_F

PER_ALL_ASSIGNMENTS_F

PER_ALL_PEOPLE_F

PER_JOBS

PER_GRADES

HR_ALL_ORGANIZATION_UNITS

1.5.1.2 Reconciliation of Persons Whose Department Has Changed

The ChangedDepartments query is used to reconcile records of persons whose department has changed within the date range that you specify in the query. In addition to the three criteria listed earlier, this query accepts a date range for the department change. Only users whose departments were changed within the specified date range are reconciled.

The following is a sample scenario in which the ChangedDepartments query can be used:

After the merger of the West Coast Sales and Support teams, some members of both teams were assigned to other teams. This change in teams took place over a period of 3 weeks. When you run the ChangedDepartments query, you can specify a start date and end date to reconcile the modified records of individuals who moved to new teams.

The ChangedDepartments query uses data stored in the following target system tables:

PER_ALL_PEOPLE_F PAPF

PER_ALL_ASSIGNMENTS_F N_PAAF

PER_ALL_ASSIGNMENTS_F O_PAAF

PER_PERSON_TYPES PPT

PER_PERSON_TYPE_USAGES_F PPU

PER_ALL_PEOPLE_F SUP

PER_JOBS

PER_GRADES

1.5.1.3 Reconciliation of Future Hires

The FutureHires query is used to reconcile records of future hires. For these persons, the date in the DATE_START column is greater than the current date. When this query is run, the following criterion is applied along with the first two criteria mentioned earlier:

The date of the host computer on which the target system database is running is less than the date stored in the EFFECTIVE_START_DATE column.

The following is a sample scenario in which the FutureHires query can be used:

Anson has been hired for a project that is scheduled to start in June. Anson's appointment letter states that he must join the company on 25-May, which is 10 weeks away from the current date. In the person record that is created for Anson, the DATE_START column is set to 25-May. Anson's record cannot be fetched by the ReconcileCurrentPersons query because the record is effective (future) dated. When

you run the FutureHires query, Anson's record meets the query criteria and the record is fetched into Oracle Identity Manager.

Note: The FutureHires query is used in conjunction with the Last Execution Time scheduled task attribute.

The FutureHires query uses data stored in the following target system tables:

PER_ALL_PEOPLE_FPAPF

PER_PERIODS_OF_SERVICE PPS

PER_PERSON_TYPES PPT

PER_PERSON_TYPE_USAGES_F

PER_ALL_ASSIGNMENTS_F

PER_ALL_PEOPLE_F

PER_JOBS

PER_GRADES

HR_ALL_ORGANIZATION_UNITS

1.5.1.4 Reconciliation of Terminated Persons

For a person whose services have been terminated, the date in the End Date column is less than or equals the current date.

The TerminatedPersons query is used to reconcile records of persons whose services have been terminated. In these records, the DATE_END column value is less than or equals the current date. When the record of a terminated person is reconciled, the status of the corresponding OIM User is set to `Disabled`.

The following is a sample scenario in which the TerminatedPersons query can be used:

Patrick has resigned and his last date with the company is 25-Aug. When the TerminatedPersons query is run on 31-Aug, the OIM User identity for Patrick is set to the `Disabled` state.

Note: The TerminatedPersons query is used in conjunction with the Last Execution Time scheduled task attribute.

The TerminatedPersons query uses data stored in the following target system tables:

PER_ALL_PEOPLE_F

PER_PERIODS_OF_SERVICE

PER_PERSON_TYPES

PER_PERSON_TYPE_USAGES_F

PER_ALL_ASSIGNMENTS_F

PER_JOBS

PER_GRADES

1.5.1.5 Reconciliation of Deleted Person Records

The DeletedPersons query is used to reconcile deletion of person records. In this mode of reconciliation, Person ID values of all target system records are fetched and compared with the Person ID values of existing OIM User records. If a match is not found for a particular OIM User, then the status of that OIM User is set to `Deleted`.

Caution: You must not modify this query. If you add a WHERE clause to this query, then only a subset of the actual set of person IDs is brought to Oracle Identity Manager for comparison. OIM Users whose user IDs do not match any of these person IDs are deleted from Oracle Identity Manager.

The following is a sample scenario in which the DeletedPersons query can be used:

The company maintains a policy of retaining for 2 years records of individuals who have left the company. Martin's record was deleted 2 years after he left the company. During the next run of the DeletedPersons query, the reconciliation module detects that there is no person record in the target system corresponding to the Martin's OIM User identity, which is currently in the `Disabled` state. Now, the status of Martin's OIM User identity is set to `Deleted`.

The DeletedPersons query uses data stored in the PER_ALL_PEOPLE_F target system table.

1.5.1.6 Reconciliation of All Person Records

The ReconcileAllPersons query is used to reconcile all person records that are reconciled individually by each of the other queries:

Note: Deleted person records are brought into Oracle Identity Manager only when you run the DeletedPersons query.

- New and modified person records
- Records of persons whose department has changed
- Records created for future hires
- Terminated person records

1.5.2 Target System Fields Used in Reconciliation

During trusted source reconciliation, values of the target system fields listed in Table 1–2 are fetched into Oracle Identity Manager. These fields are columns of the PER_ALL_PEOPLE_F table.

Table 1–2 Reconciled Target System Fields

Oracle E-Business HRMS Attribute	OIM User Form Field	Description
PERSON_ID	User ID	Unique ID of a person record in the PER_ALL_PEOPLE_F table
PERSON_ID	Person ID	Unique ID of a person record
FIRST_NAME	First Name	First name

Table 1–2 (Cont.) Reconciled Target System Fields

Oracle E-Business HRMS Attribute	OIM User Form Field	Description
LAST_NAME	Last Name	Last name
EFFECTIVE_START_DATE	Start Date	Start date for the account on the target system
EFFECTIVE_END_DATE	End Date	End date for the account on the target system
EMAIL_ADDRESS	Email	E-mail address
EMPLOYEE_NUMBER	Employee Number	Employee number
BUSINESS_GROUP_ID	Business Group ID	Unique ID for the business division in an organization
SUPERVISOR_ID	Supervisor ID	Unique ID of the person's supervisor
SUPERVISOR_NAME	Supervisor Name	Name of the person's supervisor
JOB	Job	Job code of the person
GRADE	Grade	Grade of the person

1.5.3 Reconciliation Rules for Trusted Source Reconciliation

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

The following is the process matching rule:

Rule name: eBusiness Employee Recon Rule

Rule element: Person ID Equals Person ID

In this rule:

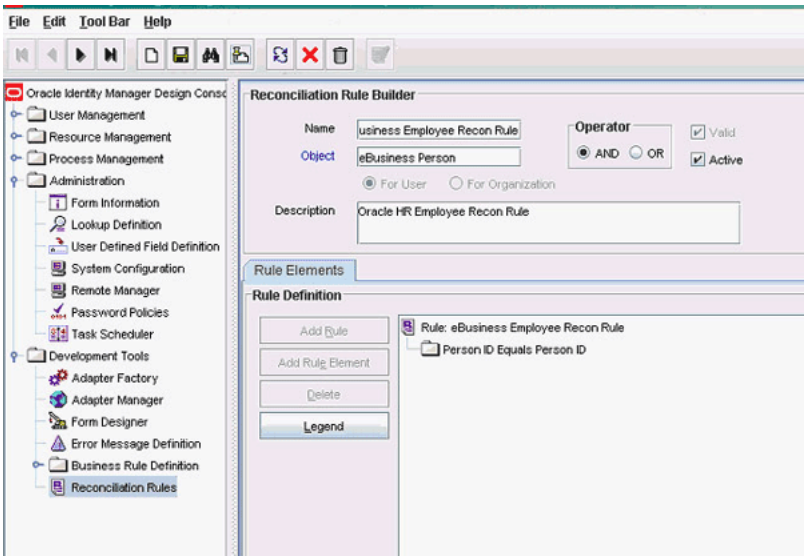
- The Person ID field on the left of "Equals" is the field on the OIM User form.
- The Person ID field on the right of "Equals" is the target system field.

After you deploy the connector, you can view the reconciliation rule for trusted source 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 **eBusiness Employee Recon Rule**. Figure 1–3 shows the reconciliation rule for trusted source reconciliation.

Figure 1–3 Reconciliation Rule



1.5.4 Lookup Definitions Used During Reconciliation

The following lookup definitions are created in Oracle Identity Manager when you deploy the connector:

- Section 1.5.4.1, "Lookup.EBS.HRMS.Recon Lookup Definition"
- Section 1.5.4.2, "Lookup.EBS.HRMS.PersonTypes Lookup Definition"
- Section 1.5.4.3, "Lookup.EBS.HRMS.DeleteRecon Lookup Definition"
- Section 1.5.4.4, "Lookup.EBS.HRMS.QueryFilters Lookup Definition"
- Section 1.5.4.5, "Lookup.EBS.ER.Configurations Lookup Definition"

1.5.4.1 Lookup.EBS.HRMS.Recon Lookup Definition

The Lookup.EBS.HRMS.Recon lookup definition holds information about target system to process form field mappings. The Code Key column of this lookup definition holds OIM User form field names. The Decode column holds aliases for target system database columns that are in the SELECT clause of the reconciliation query. See Section 4.5, "Configuring Reconciliation Queries" for more information about reconciliation queries.

Table 1–3 describes entries in the Lookup.EBS.HRMS.Recon lookup definition.

> **Note:** If required, you can add entries in this lookup definition. The Section 4.1, "Adding New Attributes for Reconciliation" section provides more information.

Table 1–3 Entries in the Lookup.EBS.HRMS.Recon Lookup Definition

Code Key	Decode
Person ID	PERSON_ID1
User ID	PERSON_ID2
First Name	FIRST_NAME

Table 1–3 (Cont.) Entries in the Lookup.EBS.HRMS.Recon Lookup Definition

Code Key	Decode
Last Name	LAST_NAME
Email Address	EMAIL_ADDRESS
Effective Start Date	EFFECTIVE_START_DATE
Employee Number	EMPLOYEE_NUMBER
Effective End Date	EFFECTIVE_END_DATE
Employee Type	USER_PERSON_TYPE
Business Group ID	BUSINESS_GROUP_ID
Supervisor ID	SUPERVISOR_ID
Supervisor Name	SUPERVISOR_NAME
Job	JOB
Grade	GRADE

1.5.4.2 Lookup.EBS.HRMS.PersonTypes Lookup Definition

The Lookup.EBS.HRMS.PersonTypes lookup definition maps user (person) types defined in the target system and Oracle Identity Manager. The Code Key column holds USER_PERSON_TYPE values of the target system, and the Decode column holds USR_EMP_TYPE values of Oracle Identity Manager.

If required, you can add entries in this lookup definition. For example, if University Student is one of the person types in your operating environment and if you have added the Intern user type in Oracle Identity Manager, then you can add an entry that maps University Student to Intern.

Note: If you add or modify entries in this lookup definition, then you must make the same change in the reconciliation queries. See Section 4.5, "Configuring Reconciliation Queries" for more information.

Table 1–4 shows the default entries in the lookup definition.

Table 1–4 Entries in the Lookup.EBS.HRMS.PersonTypes Lookup Definition

Code Key	Decode
Employee	Full-Time
Contingent Employee	Part-Time
Contractor	Consultant

1.5.4.3 Lookup.EBS.HRMS.DeleteRecon Lookup Definition

The Lookup.EBS.HRMS.DeleteRecon lookup definition maps the Person ID field of the OIM User form and the PERSON_ID field of the target system. This lookup definition is used during reconciliation of deleted person records.

Caution: You must not modify this lookup definition. If you modify this lookup definition, then reconciliation of deleted employee records will not work.

See Also: For information about reconciliation of deleted person records, see the following sections:

- Section 4.5, "Configuring Reconciliation Queries"
- Section 3.2.6.1.2, "Scheduled Task for Reconciliation of Deleted Employees"

1.5.4.4 Lookup.EBS.HRMS.QueryFilters Lookup Definition

The Lookup.EBS.HRMS.QueryFilters lookup definition contains reconciliation filter parameters that you specify. These filter parameters are automatically appended to the WHERE clause of the query that you select for reconciliation.

See Section 3.2.4, "Setting the Business Group ID and Date Range for Reconciliation" for information about the predefined entries in this lookup definition.

You can add multiple filter parameters in the lookup definition. See Section 3.2.5, "Configuring Limited Reconciliation" for the procedure.

1.5.4.5 Lookup.EBS.ER.Configurations Lookup Definition

You use this lookup definition to specify whether or not you want to use the connection pooling feature introduced in Oracle Identity Manager release 9.1.0.2.

The Lookup.EBS.ER.Configurations lookup definition contains the following entry:

Code Key: `USE_CONNECTION_POOLING`

Decode: You can specify either `Yes` or `No`.

This lookup definition is used in conjunction with the parameters of the IT resource that hold connection pooling information.

See Section 2.3.3, "Setting Up Connection Pooling" for more information.

1.6 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" provides information about configuring reconciliation.
- 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, "Troubleshooting" describes the procedure to test the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2

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"

2.1.1.1 Files and Directories On the Installation Media

Table 2–1 describes the contents of the connector deployment directory.

Table 2–1 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
config/ebsERQuery.properties	This file contains the SQL queries that are used during reconciliation. See Section 4.5, "Configuring Reconciliation Queries" for more information.
configuration/Oracle_Employee_Reconciliation-CI.xml	This XML file contains configuration information that is used during connector installation.
lib/EBSER.jar	This JAR file contains the class files that are required for reconciliation. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/ScheduleTask

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

File in the Installation Media Directory	Description
lib/EBSCommon.jar	This JAR file contains the class files that are used by both this connector and the Oracle E-Business User Management connector. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/JavaTasks
lib/Common.jar	This JAR file contains classes that are used by all release 9.1.0 connectors. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/JavaTasks
Files in the resources directory	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 directory: *OIM_HOME*/xellerate/connectorResources **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.
scripts/OimUserSynonyms.sql	This file contains commands to create synonyms for the Oracle Identity Manager wrapper and various tables used in the target system schema for reconciliation. This file is used when you perform the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations".
scripts/OimUserGrants.sql	The file contains commands to provide the required grants to the target system account that is used for connector operations. This file is used when you perform the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations".
scripts/OimUser.sql	The file contains commands to create and configure the target system account that is used for connector operations. This file is used when you perform the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations".

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

File in the Installation Media Directory	Description
scripts/OIM.sh scripts/OIM.bat	The script contains commands to call the SQL files in the scripts directory. This script is used when you perform the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations".
scripts/OIM_FND_GLOBAL.pck scripts/OIM_FND_USER_PKG.pck	These files contain the code that is called when you create the target system user account. These files are used when you perform the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations".
xml/Oracle-eBusinessSuite_ER-ConnectorConfig.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Resource object ■ Scheduled task for trusted source reconciliation

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/ScheduleTask 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.

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the following procedure:

2.1.2.1 Creating a Target System User Account for Connector Operations

Note: You must have DBA privileges to be able 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 reconciliation operations. You provide the credentials of this user account while performing the procedure described in the Section 2.3.6, "Configuring the IT Resource" section.

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 to enter 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 password

     Enter the password of the DBA account whose login you enter earlier.
   - Details of the target system account that you want to create

     Enter a user name and 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.

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 ON APPS.PER_ALL_PEOPLE_F

SELECT ON APPS.PER_ADDRESSES

SELECT ON APPS.PER_ALL_ASSIGNMENTS_F

SELECT ON APPS.HR_LOCATIONS_ALL

SELECT ON APPS.HR_ALL_ORGANIZATION_UNITS

SELECT ON APPS.PER_PERIODS_OF_SERVICE

SELECT ON APPS.PER_PERSON_TYPE_USAGES_F

SELECT ON APPS.PER_JOBS

SELECT ON APPS.PER_GRADES

CREATE SESSION

CREATE SYNONYM

CREATE TABLE

DROP ANY TABLE

At the end of the operation, a log file (OIM_APPS_USER.log) is created in the scripts directory. Verify that there are no error messages in the log file. If no error messages are recorded in the log file, then the account has been created successfully.

2.2 Installation

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.

Installing the connector involves performing the following procedures:

- 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

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. From the Connector List list, select **Oracle EBS Employee Reconciliation 9.1.0**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

   The following screenshot shows the Administrative and User Console page on which you select the connector for installation:

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 **Oracle EBS Employee Reconciliation 9.1.0**.

5. Click **Load**.

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

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

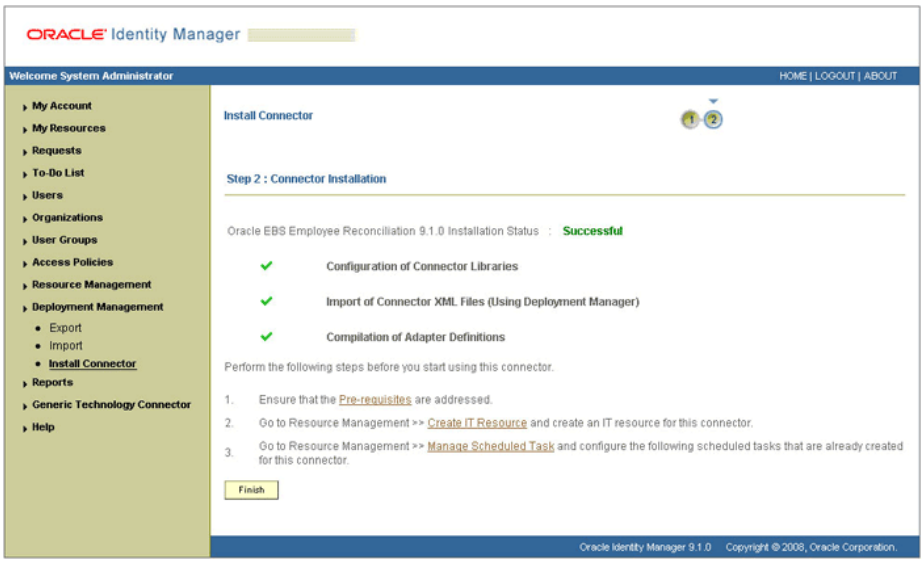
   b. Import of the connector configuration XML file (by using the Deployment Manager).

   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, as shown in the following screenshot:



In addition, a list of the 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 2.3.1, "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 in Section 2.3.6, "Configuring the IT Resource".

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 in Section 3.2.6, "Configuring the Reconciliation Scheduled Tasks".

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, perform the following steps:

1. If your Oracle Identity Manager installation is running on JBoss Application Server, then:
   - Copy the ojdbc14.jar file from the *OIM_HOME*/xellerate/ext directory into the *JBOSS_HOME*/server/default/lib directory.
   - Add the following in the classpath of the application server:

     JBOSS_HOME/server/default/lib/ojdbc14.jar
2. 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 add the ojdbc14.jar file in the classpath as follows:

   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.
3. Create the *OIM_HOME*/xellerate/XLintegrations/EBSER/config directory.
4. Copy all files from the config directory on the installation media into the *OIM_HOME*/xellerate/XLintegrations/EBSER/config directory.

2.3 Postinstallation

Postinstallation procedures are described in the following sections:

- Section 2.3.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.2, "Enabling Logging"

- Section 2.3.3, "Setting Up Connection Pooling"
- Section 2.3.4, "Configuring Secure Communication Between the Target System and Oracle Identity Manager"
- Section 2.3.5, "Determining Values for the JDBC URL and Connection Properties Parameters"
- Section 2.3.6, "Configuring the IT Resource"

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

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

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 *OIM_HOME*/config/xlconfig.xml file for information about content categories.

2.3.2 Enabling Logging

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

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

  This level enables logging of information about fine-grained events that are useful for debugging.

- `INFO`

  This level enables logging of messages that highlight the progress of the application at a coarse-grained level.

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

  This level enables logging of information about error events that 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. Depending on the application server that you use, perform the procedure given in one of the following sections:

- Section 2.3.2.1, "Enabling Logging on IBM WebSphere Application Server and Oracle WebLogic Server"
- Section 2.3.2.2, "Enabling Logging on JBoss Application Server"
- Section 2.3.2.3, "Enabling Logging on Oracle Application Server"

2.3.2.1 Enabling Logging on IBM WebSphere Application Server and Oracle WebLogic Server

To enable logging on IBM WebSphere Application Server or Oracle WebLogic Server:

1. Make the following changes in the *OIM_HOME*/config/log.properties:
   - Search for the following line:

     ```
     log4j.rootLogger=WARN,stdout
     ```

   - Make this line a comment and uncomment the line preceding this line.

– Locate the following lines, and then uncomment them by removing the number sign (#) at the start of the lines:

```
#log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
#log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
```

Note: You can change the default date format given in the preceding line.

```
#log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
#log4j.appender.logfile.MaxBackupIndex=20
#log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
#log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
```

2. In the following line, replace c:/oracle/xellerate/logs/xel.log with the name and the location of the file to which the logs listed in the preceding step must be written:

```
log4j.appender.logfile.File=c:/oracle/xellerate/logs/xel.log
```

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

```
log4j.logger.OIMCP.EBSER=LOG_LEVEL
```

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

   For example:

   log4j.logger.OIMCP.EBSER=DEBUG

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

DIRECTORY_PATH/xel.log

2.3.2.2 Enabling Logging on JBoss Application Server

To enable logging on JBoss Application Server:

1. In the *JBOSS_HOME*/server/default/conf/jboss-log4j.xml file, locate or add the following lines:

```
<category name="OIMCP.EBSER">
   <priority value="LOG_LEVEL"/>
</category>
```

2. In the second XML code line of each set, replace *LOG_LEVEL* with the log level that you want to set. For example:

```
<category name="OIMCP.EBSER">
   <priority value="DEBUG"/>
</category>
```

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

JBOSS_HOME/server/default/log/server.log

2.3.2.3 Enabling Logging on Oracle Application Server

To enable logging on Oracle Application Server:

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

```
log4j.logger.OIMCP.EBSER=LOG_LEVEL
```

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

   For example:

   ```
   log4j.logger.OIMCP.EBSER=DEBUG
   ```

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

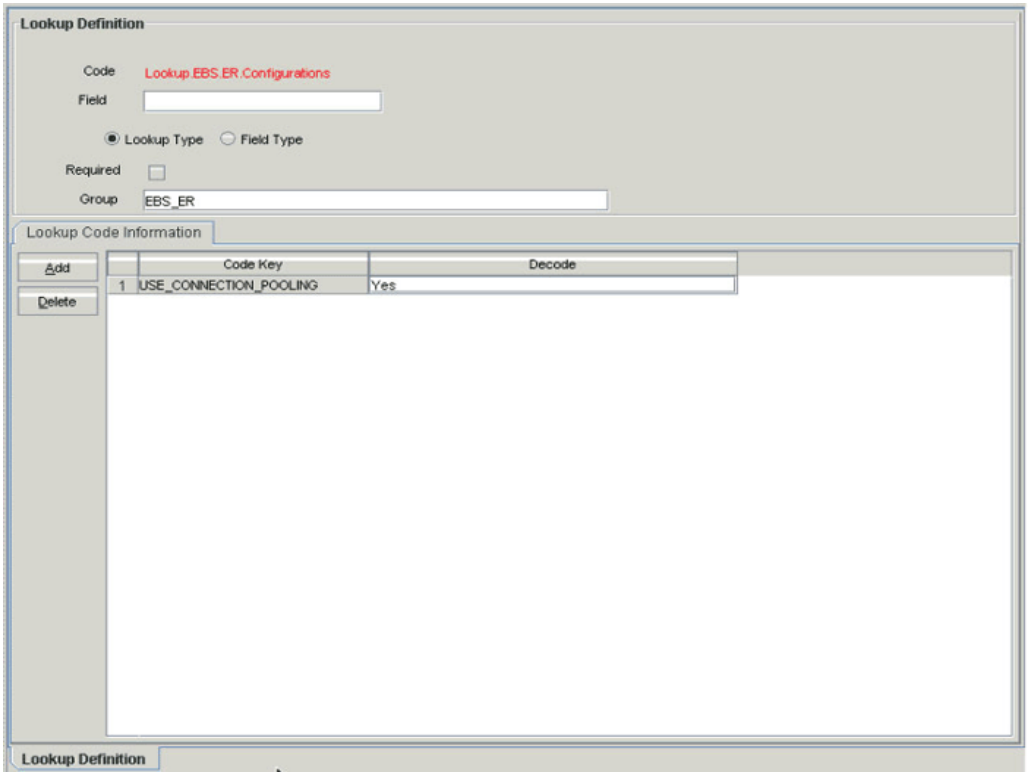
ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log

2.3.3 Setting Up Connection Pooling

If you want to use the connection pooling feature, then:

1. Configure the Lookup.EBS.ER.Configurations 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.ER.Configurations** lookup definition.
   d. In the Decode column for the USE_CONNECTION_POOLING Code Key, enter `Yes`.

      The following screenshot shows the Lookup.EBS.ER.Configurations lookup definition:



   e. Click the Save icon.

2. Specify values for the IT resource parameters that are related to connection pooling. The procedure to configure the IT resource is described later in this guide.

3. If Oracle Identity Manager is running on Oracle Application Server, then edit the opmn.xml file as follows:

   a. Open the following file in a text editor:

      OAS_HOME/opmn/conf/opmn.xml

   b. Search for the following block of lines:

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

      Replace *ADMIN_SERVER* with the name of the Oracle Application Server instance.

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

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

   d. Save and close the file.

   e. Restart the server.

2.3.4 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 2.3.4.1, "Configuring Data Encryption and Integrity in Oracle Database"
- Section 2.3.4.2, "Configuring SSL Communication in Oracle Database"

2.3.4.1 Configuring Data Encryption and Integrity in Oracle Database

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

2.3.4.2 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 2–2. 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 2–2 Certificate Store Locations

Application Server	Certificate Store Location
Oracle WebLogic Server	■ If you are using Oracle jrockit_R27.3.1-jdk, then copy the certificate into the following directory: *JROCKIT_HOME*/jre/lib/security ■ If you are using the default Oracle WebLogic Server JDK, then copy the certificate into the following directory: *WEBLOGIC_HOME*/java/jre/lib/security/cacerts
IBM WebSphere Application Server	■ For a nonclustered configuration of any supported IBM WebSphere Application Server release, import the certificate into the following certificate store: *WEBSPHERE_HOME*/java/jre/lib/security/cacerts ■ For IBM WebSphere Application Server 6.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/Web_Sphere/profiles/*SERVER_NAME*/config/cells/*CELL_NAME*/nodes/*NODE_NAME*/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 `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/etc/DummyServerTrustFile.jks
JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts

2.3.5 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 the Section 2.3.6, "Configuring the IT Resource" section.

The values that you specify for the JDBC URL and Connection Properties parameters depend on the security measures that you have implemented. This section contains the following topics:

- Section 2.3.5.1, "Supported JDBC URL Formats"

- Section 2.3.5.2, "Only Data Encryption and Integrity Is Configured"
- Section 2.3.5.3, "Only SSL Communication Is Configured"
- Section 2.3.5.4, "Both Data Encryption and Integrity and SSL Communication Are Configured"

2.3.5.1 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_DATABASE_SERVICE_NAME*

  Sample value:

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

2.3.5.2 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=(3DES1
68),oracle.net.crypto_checksum_client=REQUESTED,oracle.net.crypto_checksum_type
s_client=(MD5)
```

2.3.5.3 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 description, `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.

2.3.5.4 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 the Section 2.3.5.2, "Only Data Encryption and Integrity Is Configured" and Section 2.3.5.3, "Only SSL Communication Is Configured" sections. 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 the Section 2.3.5.2, "Only Data Encryption and Integrity Is Configured" and Section 2.3.5.3, "Only SSL Communication Is Configured" sections. For example:

  ```
  oracle.net.encryption_client=REQUIRED,oracle.net.encryption_types_client=(3DES1
  68),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.

2.3.6 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:

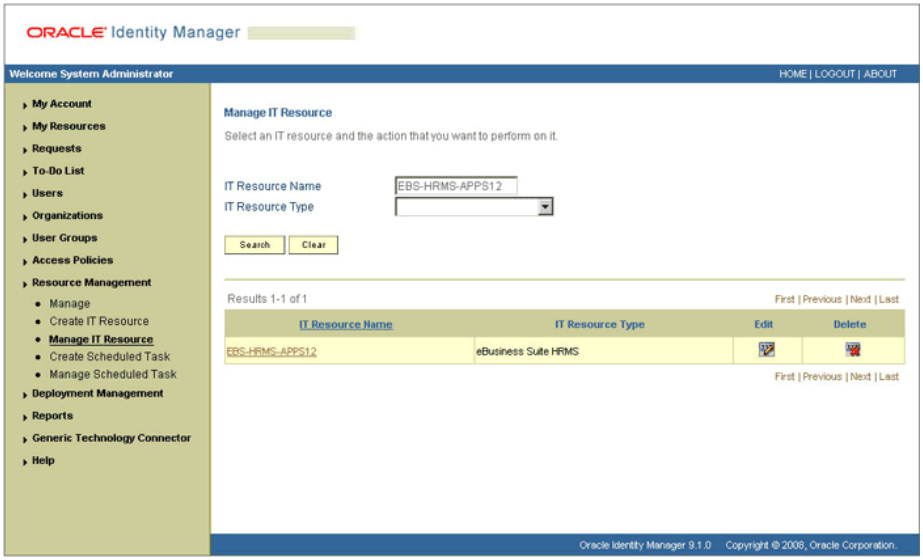
The EBS-HRMS-APPS12 IT resource is an instance of the eBusiness Suite HRMS IT resource type. If you do not want to use this IT resource, then you must create a different IT resource of the eBusiness Suite HRMS IT resource type.

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.

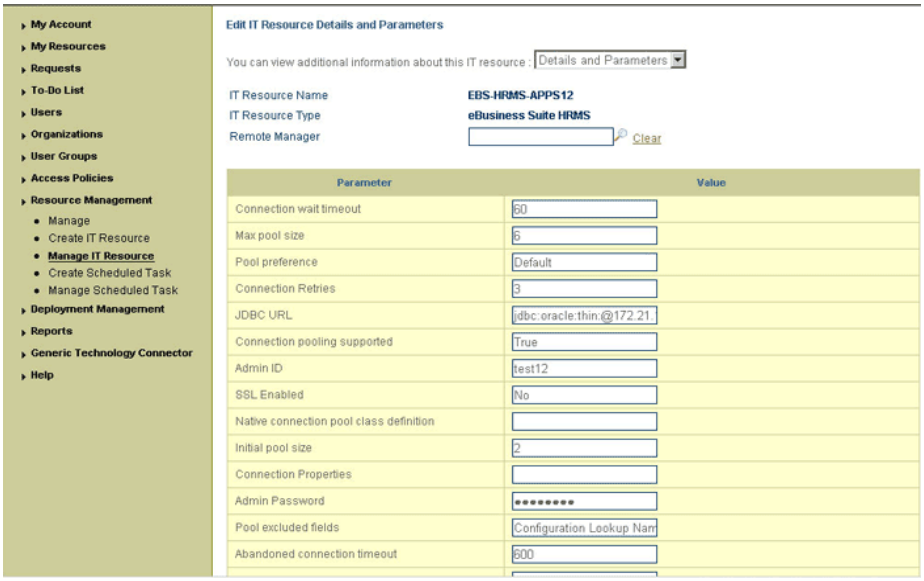
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `EBS-HRMS-APPS12` and then click **Search**.
5. Click the edit icon for the IT resource.

   The following screenshot shows the Administrative and User Console page on which you click the edit icon:



6. From the list at the top of the page, select **Details and Parameters** and then click **Edit**.

   The following screenshot shows the Administrative and User Console page on which you set values for the IT resource parameters:



7. Specify values for the parameters of the IT resource. Table 2–3 describes each parameter.

Table 2–3 IT Resource Parameters

Parameter	Description
Admin ID	Enter the user name of the target system account to be used for connector operations. You create this account by performing the procedure described in the Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" section. Default value: `apps`
Admin Password	Enter the password of the target system account specified by the Admin ID parameter.
Connection Properties	Specify the connection properties for the target system database. See Section 2.3.5, "Determining Values for the JDBC URL and Connection Properties Parameters" for detailed information.
Connection Retries	Enter the number of consecutive attempts to be made at establishing a connection with the target system. Default value: 3
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. Default value: 1200
JDBC URL	Specify the JDBC URL for the target system database. See Section 2.3.5, "Determining Values for the JDBC URL and Connection Properties Parameters" for detailed information.
Retry Interval	Enter the interval in milliseconds between consecutive attempts at establishing a connection with `the` target system. Default value: 10000
SID Name	Enter the SID of the target system database.
SSL Enabled	Enter `yes` if you plan to configure SSL to secure communication between Oracle Identity Manager and the target system. Otherwise, enter `no`. Default value: `no`
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. Default value: `1200`
Configuration Lookup Name	This parameter holds the name of the lookup definition that contains configuration information. Default value: `Lookup.EBS.ER.Configurations` **Note:** You must not change the value of this parameter. However, if you create a copy of all the connector objects, then you can specify the unique name of the copy of this lookup definition as the value of the Configuration Lookup Name parameter in the copy of the IT resource.
Connection Pooling Parameters	

Table 2–3 (Cont.) IT Resource Parameters

Parameter	Description
Abandoned connection timeout	Time (in seconds) after which a connection must be automatically closed if it is not returned to the pool **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). Default value: `600`
Connection wait timeout	Maximum time (in seconds) for which the connector must wait for a connection to be available Default value: `60`
Inactive connection timeout	Time (in seconds) of inactivity after which a connection must be dropped and replaced by a new connection in the pool Default value: `600`
Initial pool size	Number of connections that must be established when the connection pool is initialized The pool is initialized when it receives the first connection request from a connector. Default value: `1` Sample value: `3`
Max pool size	Maximum number of connections that must be established in the pool at any point of time This number includes the connections that have been borrowed from the pool. Default value: 100 Sample value: `30`
Min pool size	Minimum number of connections that must be in the pool at any point of time This number includes the connections that have been borrowed from the pool. Default value: `5`
Validate connection on borrow	Specifies whether or not a connection must be validated before it is lent by the pool The value can be `true` or `false`. It is recommended that you set the value to `true`. Default value: `true`
Timeout check interval	Time interval (in seconds) at which the timeouts specified by the other parameters must be checked Default value: `30`
Pool preference	Preferred connection pooling implementation Value: `Default` **Note:** Do not change this value of this parameter.
Connection pooling supported	Enter `true` if you want to enable connection pooling for this target system installation. Otherwise, enter `false`. Default value: `true`
Target supports only one connection	Indicates whether the target system can support one or more connections at a time Value: `false` **Note:** Do not change the value of this parameter.

Table 2–3 (Cont.) IT Resource Parameters

Parameter	Description
ResourceConnection class definition	Implementation of the ResourceConnection class Default value: `oracle.iam.connectors.ebs.common.vo.EBSResourceConnectionImpl` **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 shouldn't trigger a refresh of the connector pool Default value: `Configuration Lookup Name,Statement Timeout` **Note:** You must not change the value of this parameter.

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

3

Using the Connector

This chapter describes the following procedures:

- Section 3.1, "Performing First-Time (Full) Reconciliation" provides instructions on configuring the reconciliation scheduled task for fetching all person records from the target system to Oracle Identity Manager.
- Section 3.2, "Configuring Reconciliation" provides detailed information about the various options that you can apply while configuring reconciliation.

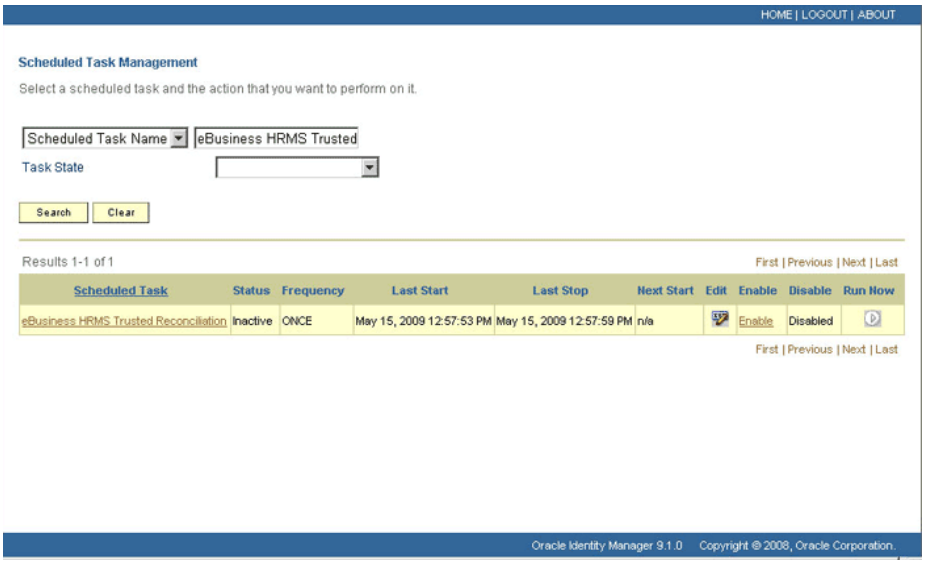
3.1 Performing First-Time (Full) Reconciliation

After you deploy the connector, you must run first-time reconciliation to fetch all existing target system records into Oracle Identity Manager. The first-time reconciliation run is a full reconciliation run. At the start of this reconciliation run, the Last Execution Time scheduled task attribute is populated with the time stamp. For subsequent runs, the scheduled task automatically switches to incremental reconciliation because the Last Execution Time attribute contains a non-zero value.

Note: At any time after first-time reconciliation, you can switch from incremental to full reconciliation by setting the Last Execution Time attribute to `0` and specifying a non-zero value for the Batch Size scheduled task attribute.

The following are the steps involved in this procedure:

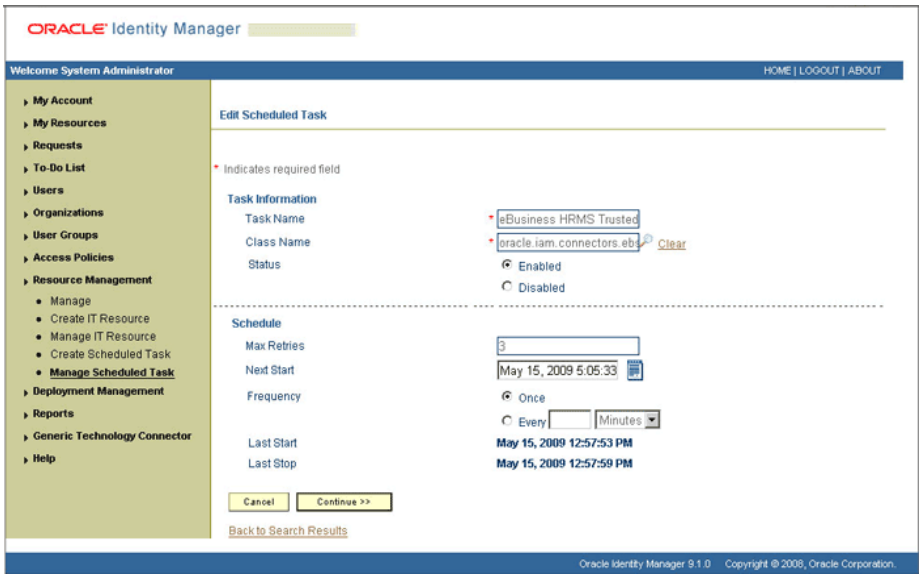
1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage Scheduled Task**.
4. On the Scheduled Task Management page, enter the name of the scheduled task (`eBusiness HRMS Trusted Reconciliation`) as the search criteria and then click **Search**.
5. In the search results table, click the edit icon in the Edit column for the scheduled task. The following screenshot shows the Scheduled Task Management page on which you click the edit icon:



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

   - **Status:** Select **Enabled**.
   - **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:** Specify the date and time at which you want to run reconciliation.
   - **Frequency:** Select **Once**.

   When you click Edit, the Edit Scheduled Task page is displayed. The following screenshot shows this page:



7. After modifying the values for the scheduled task details listed in the previous step, click **Continue**.

8. 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**. Table 3–1 describes the values that you must specify.

Table 3–1 Attribute Values for First-Time Reconciliation

Attribute	Description
Task Name	Accept the default value (`eBusiness HRMS Trusted Reconciliation`).
IT Resource Name	Enter the name that you specify for the IT resource while performing the procedure described in the Section 2.3.6, "Configuring the IT Resource" section. Default value: `EBS-HRMS-APPS12`
Last Execution Time	Accept the default value (`0`).
Resource Object	Accept the default value (`eBusiness Person`).
User Type	Enter the user type that must be assigned to OIM Users created during reconciliation. Default value: `End-User`
Organization	Enter the name of the Oracle Identity Manager organization in which OIM Users must be created or modified during reconciliation. Default value: `Xellerate Users`
Batch Size	Accept the default value (`1000`).
Query Properties File	Enter the full path and name of the properties file in which the reconciliation query that you want to run is stored. Sample value: *`DIRECTORY_PATH`*`/ebsERQuery.properties` In this value, *`DIRECTORY_PATH`* is the path of the directory on the target system host computer in which this file is stored. See Section 4.5, "Configuring Reconciliation Queries" for information about this file.
Query Name	Enter the name of the reconciliation query that you want to run. Sample value: `ReconcileCurrentPersons` **Note:** You must run either the ReconcileCurrentPersons query or your version of this query. None of the remaining predefined queries can be used for first-time reconciliation.
Person Type Look Up Definition	Accept the default value (`Lookup.EBS.HRMS.PersonTypes`).
Recon Lookup Definition	Accept the default value (`Lookup.EBS.HRMS.Recon`).
Query Filter Lookup Definition	This attribute holds the name of the lookup definition that contains information about reconciliation filter parameters. Default value: `Lookup.EBS.HRMS.QueryFilters` **Note:** 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. You must not change the value of this attribute. However, if you create a copy of all the connector objects, then you can specify the unique name of the copy of this lookup definition as the value of the Query Filter Lookup Definition attribute in the copy of the scheduled task.
Target Date Format	Enter the format of date values stored in the target system database. Default value: `MM/dd/yyyy hh:mm:ss`

The following screenshot shows the Attributes page. The attributes of the scheduled task that you select for modification are displayed on this page.

9. In the Lookup.EBS.HRMS.QueryFilters lookup definition, specify the business group ID of the person records that you want to reconcile:
   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.HRMS.QueryFilters** lookup definition.
   d. In the **Decode** column for the businessGroupID Code Key, add the business group ID in the following format:

      BUSINESS_GROUP_ID|NUMBER

      For example: 202|NUMBER

   e. In the Decode column for the following Code Keys, enter the date range that you want to be applied during reconciliation:

      – **fromDate**

        Enter the start date of the date range that you want to apply for reconciliation of newly created and modified records.

        The format is as follows:

        FROM_DATE|Date|*FORMAT*

        For example: 12-May-2009|Date|DD-Mon-YYYY

      – **toDate**

        Enter the end date of the date range that you want to apply for reconciliation of newly created and modified records.

        The format is as follows:

        TO_DATE|Date|*FORMAT*

        For example: 16-May-2009|Date|DD-Mon-YYYY

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

11. After each run of the scheduled task, repeat Steps 1 through 10 for each person type whose records you want to reconcile into Oracle Identity Manager. Each time you perform the procedure, change the value of the User Type scheduled task attribute to the person type for which you are running reconciliation.

3.2 Configuring Reconciliation

Configuring reconciliation involves configuring the scheduled task that initiates reconciliation.

The following sections discuss some of the attributes of the scheduled task:

- Section 3.2.1, "Batched Reconciliation"
- Section 3.2.2, "Reconciliation Query"
- Section 3.2.3, "Reconciliation Time Stamp"

The following section describes the procedure additional options to configure reconciliation:

- Section 3.2.4, "Setting the Business Group ID and Date Range for Reconciliation"
- Section 3.2.5, "Configuring Limited Reconciliation"

The following section describes the procedure to configure the scheduled tasks:

- Section 3.2.6, "Configuring the Reconciliation Scheduled Tasks"

3.2.1 Batched Reconciliation

Note: This section describes the Batch Size attribute of the scheduled task.

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 values for the Batch Size reconciliation scheduled task attribute. You use this attribute to specify the number of records that must be included in each batch. The default value is 1000.

Note: If you want to configure full reconciliation, then you must specify a non-zero value for the Batch Size attribute.

Suppose you specify `20` as the value of the Batch Size attribute. If 314 person records were created or modified after the last reconciliation run, then these records are reconciled in batches of 20 records. The last batch contains 14 records.

3.2.2 Reconciliation Query

Note: This section describes the Query Name attribute of the scheduled task.

The following are the predefined reconciliation queries in the ebsERQuery.properties file:

- ReconcileAllPersons
- ReconcileCurrentPersons
- ChangedDepartments
- FutureHires
- TerminatedPersons
- DeletedPersons

See Section 1.5.1, "Reconciliation Queries" for information about these queries. As mentioned in the Section 4.5, "Configuring Reconciliation Queries" section, you can use one of the predefined queries, a modified predefined query, or your own query.

While configuring the scheduled task, you specify the name of the query as the value of the Query Name attribute.

3.2.3 Reconciliation Time Stamp

Note: 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 query, if you want to perform full reconciliation, then set the value of the attribute to 0.
- If you want to specify a time stamp, then first run the following query to convert the time stamp into the required format:

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

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

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

  The query returns the following value:

```
1228435200000
```

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

- The Last Execution Time attribute is updated during each reconciliation run, regardless of the reconciliation query that you specify. For example, when you run the ReconcileCurrentPersons query, the Last Execution Time attribute is set to the time stamp at which the run begins. If you next run the FutureHires query, then the time stamp currently stored in the Last Execution Time attribute is used to determine the subset of future hires' records that must be fetched for reconciliation.

  To reuse the time stamp for a particular mode of reconciliation, you must note down the value of the Last Execution Time attribute, set the value of the attribute to `0`, and then perform the rest of the procedure to configure the scheduled task. For example, if you are switching from the ReconcileCurrentPersons query to the FutureHires query, first note down the value of the Last Execution Time attribute and then perform the rest of the procedure.

3.2.4 Setting the Business Group ID and Date Range for Reconciliation

In the Lookup.EBS.HRMS.QueryFilters lookup definition, specify the business group ID of the person records that you want to reconcile:

1. Log in to the Design Console.
2. Expand the **Administration** folder, and then double-click **Lookup Definition**.
3. Search for and open the **Lookup.EBS.HRMS.QueryFilters** lookup definition.
4. In the **Decode** column for the businessGroupID Code Key, add the business group ID in the following format:

   BUSINESS_GROUP_ID|NUMBER

   For example: 202|NUMBER
5. In the Decode column for the following Code Keys, enter the date range that you want to be applied during reconciliation:
   - **fromDate**

     Enter the start date of the date range that you want to apply for reconciliation of newly created and modified records.

     The format is as follows:

     FROM_DATE|Date|*FORMAT*

     For example: 12-May-2009|Date|DD-Mon-YYYY
   - **toDate**

     Enter the end date of the date range that you want to apply for reconciliation of newly created and modified records.

     The format is as follows:

     TO_DATE|Date|*FORMAT*

     For example: 16-May-2009|Date|DD-Mon-YYYY

3.2.5 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 Lookup.EBS.HRMS.QueryFilters lookup definition. For example, you can add a parameter in the WHERE clause of the ReconcileCurrentPersons query so that it returns records of persons whose last name is the one that you specify in the lookup definition.

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 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.

      In the following snippet of the ReconcileCurrentPersons query, the variable condition highlighted in bold has been added:

```
AND(TRUNC(SYSDATE) BETWEEN SUP.EFFECTIVE_START_DATE(+) AND
SUP.EFFECTIVE_END_DATE(+)) \
AND LAST_NAME=:lastname \
AND ( (ROUND((PAPF.LAST_UPDATE_DATE -TO_DATE('01011970', 'DDMMYYYY')) *1440
*60 *1000) > :lastExecutionTime) \
OR (ROUND((PAAF.LAST_UPDATE_DATE -TO_DATE('01011970', 'DDMMYYYY')) *1440
*60 *1000) > :lastExecutionTime) ) \
ORDER BY PAPF.PERSON_ID
```

   c. Save and close the file.
2. Configure the Lookup.EBS.HRMS.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.HRMS.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 `lastname` 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: Doe|STRING

Note: For the LAST NAME example, you can enter the preceding sample value.

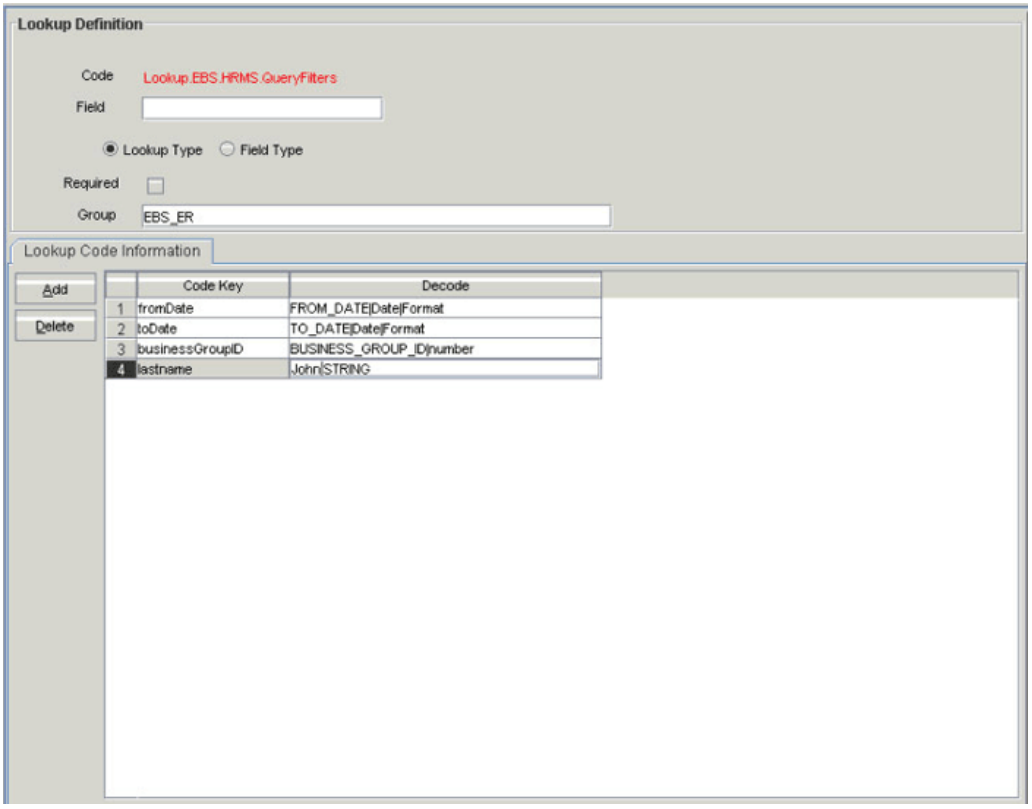
– *value*|DATE|*DATE_FORMAT*

Sample value: 4-Dec-08|DATE|DD-Mon-YY

– *value*|NUMBER

Sample value: 33|NUMBER

The following screenshot shows the Lookup.EBS.HRMS.QueryFilters lookup definition:



g. Click the Save icon.

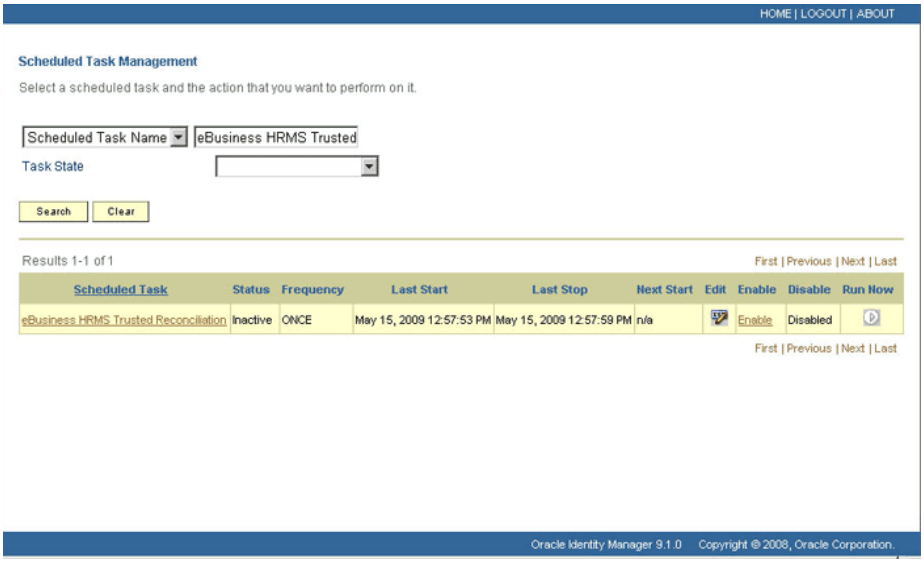
When you next run the query that you have modified, the condition that you add is applied as an additional filter during reconciliation.

3.2.6 Configuring the Reconciliation Scheduled Tasks

When you run the Connector Installer, the scheduled tasks for reconciliation are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

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 (`eBusiness HRMS Trusted Reconciliation`) as the search criteria and then click **Search**.

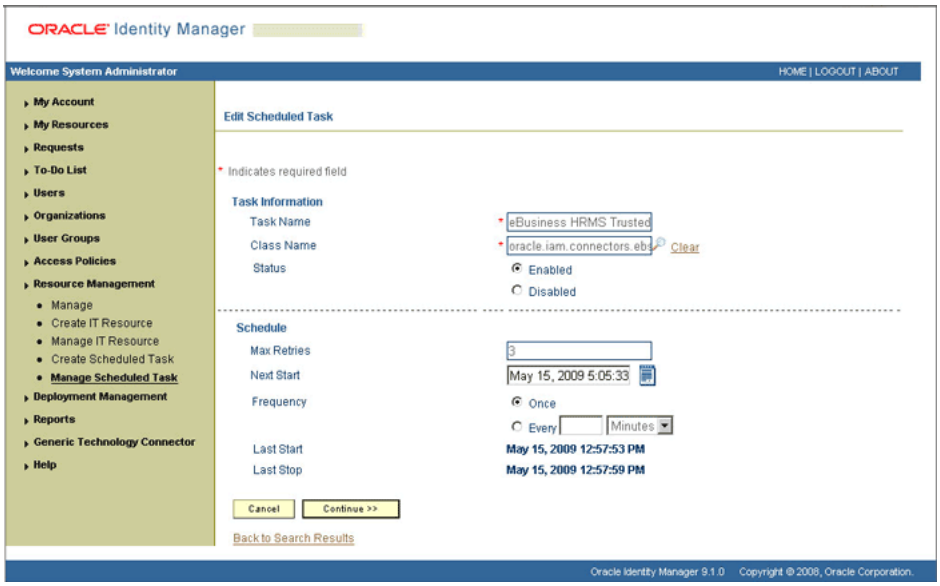
   The following screenshot shows the Scheduled Task Management page:



5. In the search results table, click the edit icon in the Edit column for the scheduled task.
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 1.
   - **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. The following screenshot shows this page:

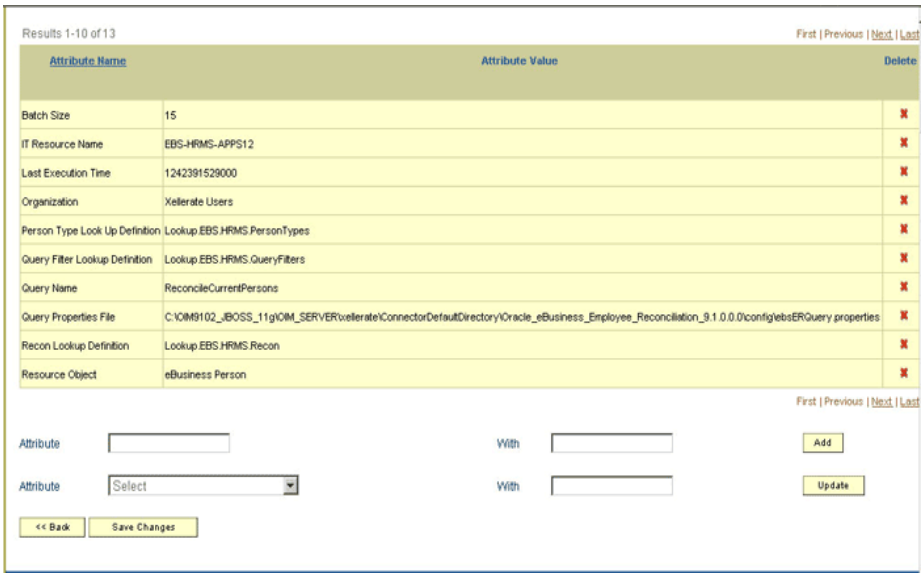


7. After modifying the values for the scheduled task details listed in the previous step, click **Continue**.
8. Specify values for the attributes of the scheduled task. To do so, select each attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for the attributes that you want to change.
- 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.



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

3.2.6.1 Attributes of the Scheduled Tasks

The following sections provide information about the attributes of the scheduled tasks for this connector:

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.
- See *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes.

- Section 3.2.6.1.1, "Scheduled Task for Reconciliation of All Employees"
- Section 3.2.6.1.2, "Scheduled Task for Reconciliation of Deleted Employees"

3.2.6.1.1 Scheduled Task for Reconciliation of All Employees

Table 3–2 describes the attributes of the scheduled task for reconciliation of all persons.

Table 3–2 Attributes of Scheduled Task for Reconciliation of All Employees

Attribute	Description
Task Name	This attribute holds the name of the scheduled task. Value: `eBusiness HRMS Trusted Reconciliation` **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that new scheduled task as the value of the Task Name attribute in that scheduled task.
IT Resource Name	Enter the name that you specify for the IT resource while performing the procedure described in the Section 2.3.6, "Configuring the IT Resource" section. Default value: `EBS-HRMS-APPS12`
Last Execution Time	This attribute holds the time stamp at which the last reconciliation run started. Default value: `0` See Section 3.2.3, "Reconciliation Time Stamp" for information about setting a value for the Last Execution Time attribute.
Resource Object	This attribute holds the name of the resource object. Value: `eBusiness Person` **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.
User Type	Enter the person type for which reconciliation is to be run. You can enter any one of the values in the Decode column of the Lookup.EBS.HRMS.PersonTypes lookup definition. See Section 1.5.4.2, "Lookup.EBS.HRMS.PersonTypes Lookup Definition" for more information. Default value: `End-User`
Organization	Enter the name of the Oracle Identity Manager organization in which OIM Users must be created or modified during reconciliation. Default value: `Xellerate Users`
Batch Size	Enter the number of records that must be included in each batch fetched from the target system. Default value: `1000`
Query Properties File	Enter the full path and name of the properties file in which the reconciliation query that you want to run is stored. Default value: *OIM_HOME*/xellerate/XLIntegrations/EBSER/config/ebsERQuery.properties In this value, *DIRECTORY_PATH* is the path of the directory on the target system host computer in which this file is stored. See Section 4.5, "Configuring Reconciliation Queries" for information about this file.
Query Name	Enter the name of the reconciliation query that you want to run. See Section 4.5, "Configuring Reconciliation Queries" for information about specifying a value for this attribute. Sample value: `ReconcileCurrentPersons`
Person Type Look Up Definition	This attribute holds the name of the lookup definition that maps person types defined on the target system with person types defined in Oracle Identity Manager. Value: `Lookup.EBS.HRMS.PersonTypes` **Note:** Do not change the default value.

Table 3–2 (Cont.) Attributes of Scheduled Task for Reconciliation of All Employees

Attribute	Description
Recon Lookup Definition	This attribute holds the name of the lookup definition which holds information about target system to process form field mappings. Value: `Lookup.EBS.HRMS.Recon` **Note:** Do not change the default value.
Query Filter Lookup Definition	This attribute holds the name of the lookup definition that contains information about reconciliation filter parameters. Default value: `Lookup.EBS.HRMS.QueryFilters` **Note:** 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. You must not change the value of this attribute. However, if you create a copy of all the connector objects, then you can specify the unique name of the copy of this lookup definition as the value of the Query Filter Lookup Definition attribute in the copy of the scheduled task.
Target Date Format	Enter the format of date values stored in the target system database. Default value: `MM/dd/yyyy hh:mm:ss`

3.2.6.1.2 Scheduled Task for Reconciliation of Deleted Employees

Table 3–2 describes the attributes of the scheduled task for reconciliation of deleted persons.

Table 3–3 Attributes of Scheduled Task for Reconciliation of Deleted Employees

Attribute	Description
Task Name	This attribute holds the name of the scheduled task. Value: `eBusiness HRMS Delete Reconciliation` **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that new scheduled task as the value of the Task Name attribute in that scheduled task.
Delete Recon Lookup Definition	Enter the name of the of the lookup definition that stores the mapping between the Person ID field of the OIM User form and the PERSON_ID field of the target system. Value: `Lookup.EBS.HRMS.DeleteRecon` **Note:** Do not change the default value.
IT Resource Name	Enter the name that you specify for the IT resource while performing the procedure described in the Section 2.3.6, "Configuring the IT Resource" section. Default value: `EBS-HRMS-APPS12`
Resource Object	This attribute holds the name of the of the resource object. Value: `eBusiness Person` **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.

Table 3–3 (Cont.) Attributes of Scheduled Task for Reconciliation of Deleted Employees

Attribute	Description
Query Properties File	Enter the full path and name of the properties file in which the reconciliation query that you want to run is stored. Sample value: *OIM_HOME*/xellerate/XLIntegrations/EBSER/config In this value, *DIRECTORY_PATH* is the path of the directory on the target system host computer in which this file is stored. See Section 4.5, "Configuring Reconciliation Queries" for information about this file.
Query Name	This attribute holds the name of the query for reconciliation of deleted person records. Value: `DeletedPersons` **Note:** Do not change the default value.

4

Extending the Functionality of the Connector

After you deploy the connector, you might need to configure it to meet your business requirements. The following are procedures that you can perform to extend the functionality of the connector:

- Table 1–2, " Reconciled Target System Fields" lists the target system fields whose values are fetched into Oracle Identity Manager. Check if this set of fields meets your requirements. See Section 4.1, "Adding New Attributes for Reconciliation" if there are additional target system fields that you want include in this set.
- The Section 1.5.4.1, "Lookup.EBS.HRMS.Recon Lookup Definition" section lists the predefined attribute mappings. See Section 4.2, "Modifying the Names of Predefined Attributes Mapped for Reconciliation" if you want to modify the names of any of these attributes.
- The Section 1.5.4.1, "Lookup.EBS.HRMS.Recon Lookup Definition" section lists the predefined attribute mappings. You can remove some of these attribute mappings. See Section 4.3, "Deleting Predefined Attributes Mapped for Reconciliation" if you want to perform this procedure.
- See Section 4.4, "Modifying Field Lengths on the OIM User Form" if the lengths of fields on the OIM User form do not match the lengths of target system fields.
- Predefined reconciliation queries are stored in the *OIM_HOME*/xellerate/ScheduleTask/ebsERQuery.properties file. Open this file in a text editor, and check if the predefined queries meet your requirements. See Section 4.5, "Configuring Reconciliation Queries" if you want to modify a predefined query or create your own query.
- In a particular reconciliation query, the connector allows you to specify the value of a WHERE clause parameter as the value of a scheduled task attribute. For example, you can add a parameter in the WHERE clause of the ReconcileCurrentPersons query so that it returns records of persons whose last name is the one that you specify in the scheduled task. See Section 3.2.5, "Configuring Limited Reconciliation" if you want to use this feature of the connector.
- See Section 4.7, "Configuring the Connector for Multiple Trusted Source Reconciliation" if Oracle E-Business HRMS is only one of multiple trusted sources that you want to configure for Oracle Identity Manager.

4.1 Adding New Attributes for Reconciliation

Note:

In this section, the term "attributes" refers to the identity data fields that store user data.

This section describes an optional procedure. Perform this procedure only if you want to add new attributes for reconciliation.

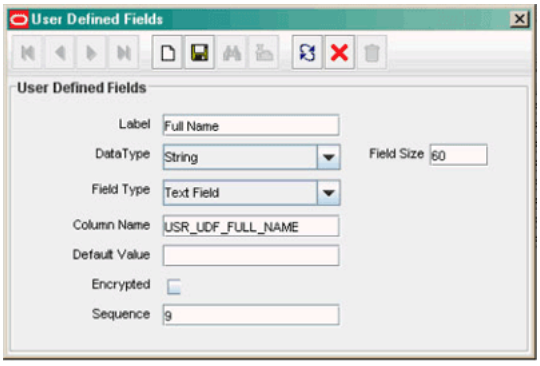
By default, the attributes listed in Table 1–2 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation as follows:

Note: A sample scenario in which you add the Full Name field for reconciliation has been used to illustrate the procedure.

1. Log in to the Design Console.
2. Create a UDF for the field that you want to add as follows:
   a. Expand **Administration**, and then double-click **User Defined Field Definition**.
   b. Search for and open the **USR** table.
   c. Click **Add**.
   d. In the User Defined Fields dialog box, enter the following values:
      – **Label**: Enter a label for the field. For example, enter `Full Name`.
      – **DataType**: Select a data type for the field. For example, select `String`.
      – **Field Size**: Enter a length for the field. For example, enter `20`.
      – **Column Name**: Enter a column name for the field. For example, enter `FULL_NAME`.

        Oracle Identity Manager automatically appends `USR_UDF_` to the column name that you specify. So, for example, if you specify `FULL_NAME` as the column name, then the actual column name is changed to `USR_UDF_FULL_NAME`.

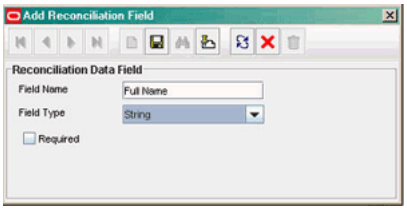
        The following screenshot shows the User Defined Fields dialog box:



   e. Click the Save icon.

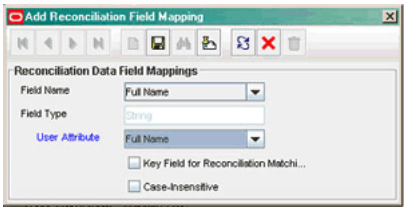
3. Add a reconciliation field in the resource object as follows:
   a. Expand **Resource Management**, and double-click **Resource Objects**.
   b. Search for and open the **eBusiness Person** resource object.
   c. On the Reconciliation Fields subtab of the Object Reconciliation tab, click **Add**.
   d. In the Add Reconciliation Field dialog box:
      – In the **Field Name** field, enter a name for the reconciliation field.
      – From the **Field Type** list, select the data type of the field.
      – Click the Save icon, and then close the dialog box.

      The following screenshot shows the Add Reconciliation Field dialog box:



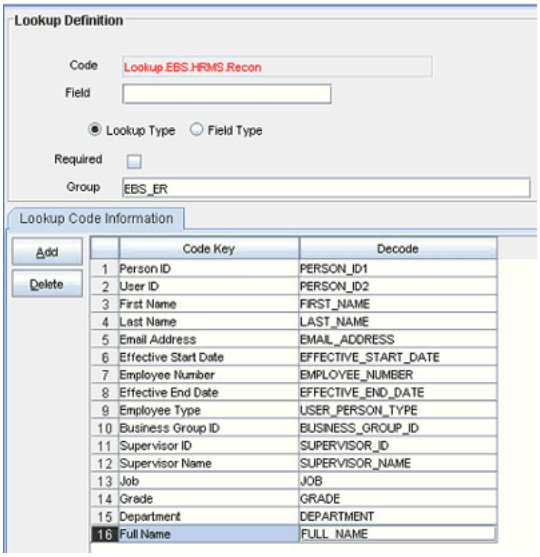
   e. Click the Save icon.
4. In the process definition, create a reconciliation field mapping as follows:
   a. Expand **Process Management**, and double-click **Process Definition**.
   b. Search for and open the **eBusiness HRMS Person** process definition.
   c. On the Reconciliation Field Mappings tab, click **Add Field Map**.
   d. In the Add Reconciliation Field Mapping dialog box:
      – From the Field Name list, select **Full Name**.
      – From the User Attribute list, select **FULL_NAME**.
      – Click the Save icon, and then close the dialog box.

      The following screenshot shows the Add Reconciliation Field Mapping dialog box:



   e. Click the Save icon.
5. In the lookup definition that holds attribute mappings for reconciliation, add an entry as follows:
   a. Expand **Administration**, and double-click **Lookup Definition**.
   b. Search for and open the **Lookup.EBS.HRMS.Recon** lookup definition.
   c. Click **Add**.
   d. In the **Code Key** column, enter (for example) `Full Name`.
   e. In the **Decode** column, enter (for example) `FULL_NAME`.

The following screenshot shows the Lookup.EBS.HRMS.Recon lookup definition:



6. Add a column in the SELECT clause of reconciliation queries that you use from the properties file:

   a. Open the properties file in a text editor. This file is in the following directory:

      OIM_HOME/xellerate/XLIntegration/EBSER/config

   b. Add the column name in the SELECT clause of each query in the properties file.

      Caution: This does not apply to the query to reconcile deleted users. Do not make changes in that query.

   c. Save and close the file.

4.2 Modifying the Names of Predefined Attributes Mapped for Reconciliation

Note:

In this section, the term "attributes" refers to the identity data fields that store user data.

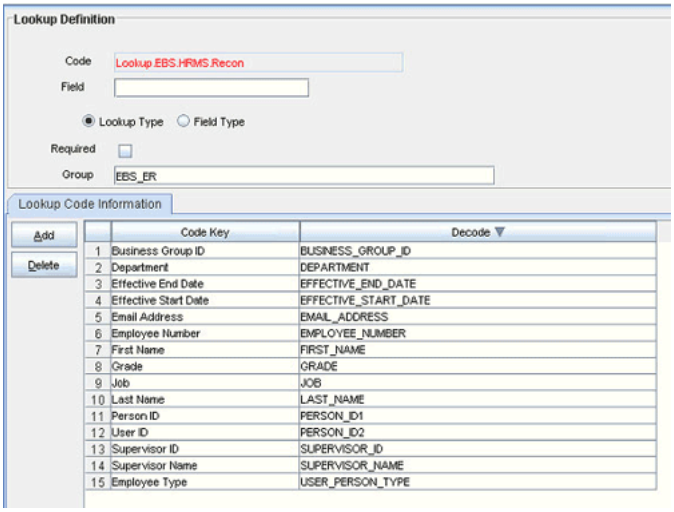
This section describes an optional procedure. Perform this procedure only if you want to modify the name of a predefined attribute mapped for reconciliation.

You can modify the names of the predefined target system attributes that are mapped for reconciliation. For example, you can change the FIRST_NAME attribute to FName. See Section 1.5.4.1, "Lookup.EBS.HRMS.Recon Lookup Definition" for more information about predefined attribute mappings.

To modify the name of a predefined attribute mapped for reconciliation:

1. Modify the name of the attribute in the Decode column of the Lookup.EBS.HRMS.Recon lookup definition as follows:
   a. Expand **Administration**, and double-click **Lookup Definition**.
   b. Search for and open the **Lookup.EBS.HRMS.Recon** lookup definition.
   c. In the Decode column, modify the entry for the attribute.

      The following screenshot shows Lookup.EBS.HRMS.Recon lookup definition:



   d. Click the Save icon.
2. In all the reconciliation queries in the properties file, change the column name for the attribute.

   Note: The column name must be the same as the name of the attribute in the Decode column of the Lookup.EBS.HRMS.Recon lookup definition.

   a. Open the properties file in a text editor.
   b. Change the name of the column in the SELECT clause of each query in the properties file.
   c. Save and close the file.

4.3 Deleting Predefined Attributes Mapped for Reconciliation

Note:

In this section, the term "attributes" refers to the identity data fields that store user data.

This section describes an optional procedure. Perform this procedure only if you want to delete any of the predefined attribute mappings.

The Section 1.5.4.1, "Lookup.EBS.HRMS.Recon Lookup Definition" section shows the predefined attribute mappings for reconciliation. Of the attributes listed in the table, you can remove the following attributes:

- PERSON_ID1
- EMPLOYEE_NUMBER
- BUSINESS_GROUP_ID
- SUPERVISOR_ID
- SUPERVISOR_NAME
- JOB
- GRADE

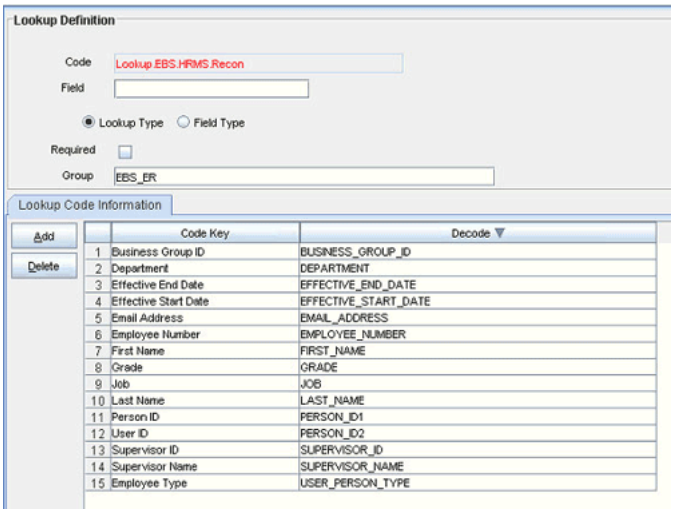
To remove the mapping for any one of these attributes:

1. In all the reconciliation queries in the properties file, remove the column from the SELECT clause as follows:
   a. Open the properties file in a text editor.
   b. Remove the column name in the SELECT clause of each query in the properties file.

      Caution: This does not apply to the query to reconcile deleted users. Do not make changes in that query.

   c. Save and close the file.
2. Log in to the Design Console.
3. In the lookup definition that holds attribute mappings for reconciliation, remove the entry for the attribute as follows:
   a. Expand **Administration**, and double-click **Lookup Definition**.
   b. Search for and open the **Lookup.EBS.HRMS.Recon** lookup definition.
   c. Select the row corresponding to the entry that you want to remove.

      The following screenshot shows Lookup.EBS.HRMS.Recon lookup definition:

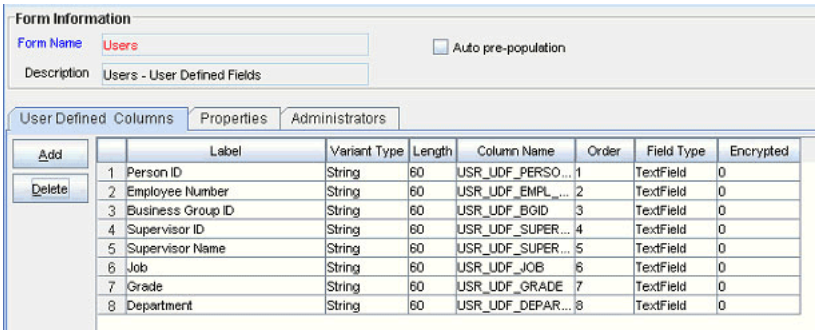


   d. Click **Delete**, and then click the Save icon.
4. Remove the attribute from the OIM User form as follows:

a. Expand **Administration**, and double-click **User Defined Field Definition**.

b. Search for and open the **Users** form.

The following screenshot shows Users form:



c. Delete the row corresponding to the attribute that you want to remove.

d. Click the Save icon.

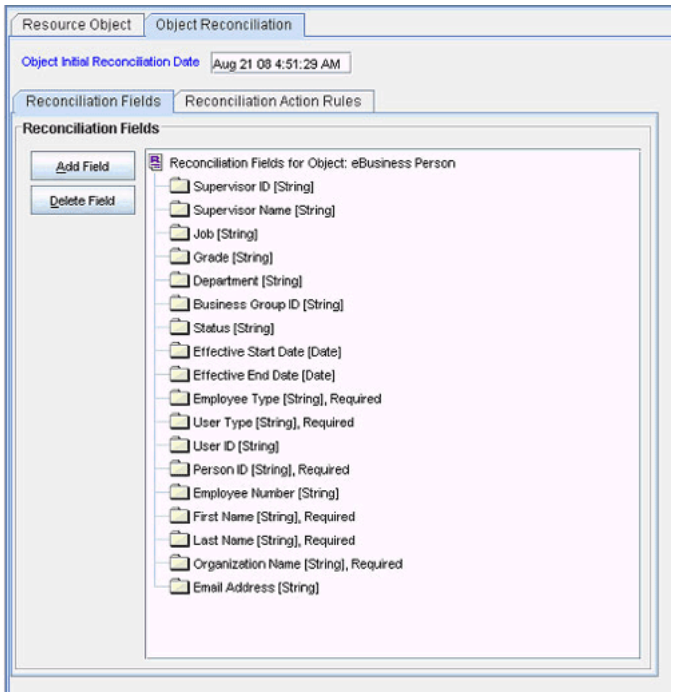
5. Delete the field from the eBusiness Person resource object as follows:

a. Expand **Resource Management**, and double-click **Resource Objects**.

b. Search for and open the **eBusiness Person** resource object.

c. On the Reconciliation Fields subtab of the Object Reconciliation tab, select the field that you want to delete and then click **Delete**.

The following screenshot shows the reconciliation fields:



d. Click the Save icon.

6. Remove the reconciliation field mapping from the eBusiness HRMS Person process definition as follows:

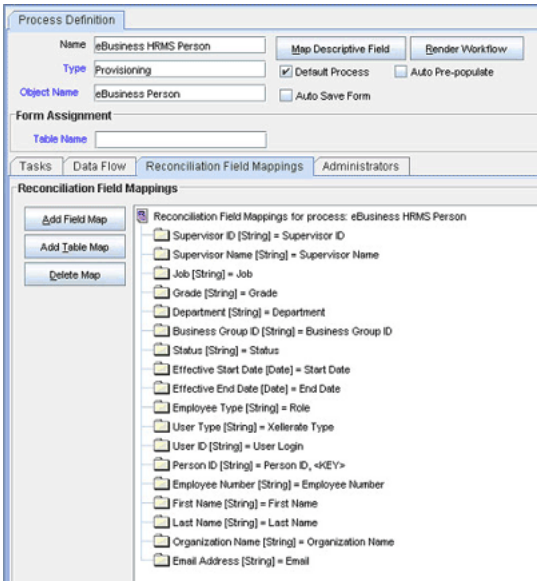
a. Expand **Process Management**.

b. Double-click **Process Definition**.

c. Search for and open the **eBusiness HRMS Person** process definition.

d. On the Reconciliation Field Mappings tab, click the entry for the field that you want to remove and then click **Remove Field Map**.

The following screenshot shows the reconciliation field mappings:



e. Click the Save icon.

4.4 Modifying Field Lengths on the OIM User Form

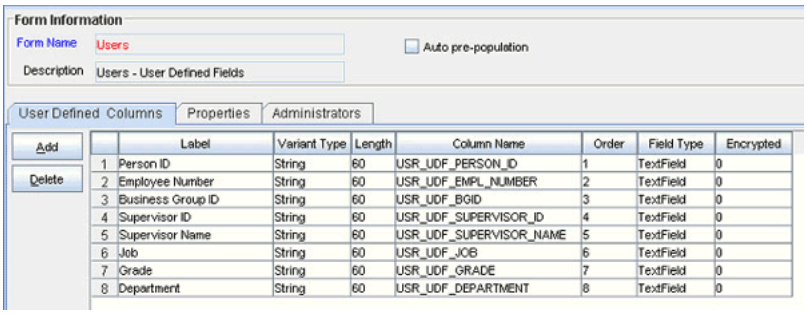
Note: This section describes an optional procedure. Perform this procedure only if you want to modify field lengths on the OIM User form.

You might want to modify the lengths of fields (attributes) on the OIM User form. For example, if you use the Japanese locale, then you might want to increase the lengths of OIM User form fields to accommodate multibyte data from the target system.

If you want to modify the length of field on the OIM User form, then:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **User Defined Field Definition**.
3. Search for and open the **Users** form.
4. Modify the length of the required field.

The following screenshot shows the Users form:



	Label	Variant Type	Length	Column Name	Order	Field Type	Encrypted
1	Person ID	String	60	USR_UDF_PERSON_ID	1	TextField	0
2	Employee Number	String	60	USR_UDF_EMPL_NUMBER	2	TextField	0
3	Business Group ID	String	60	USR_UDF_BGID	3	TextField	0
4	Supervisor ID	String	60	USR_UDF_SUPERVISOR_ID	4	TextField	0
5	Supervisor Name	String	60	USR_UDF_SUPERVISOR_NAME	5	TextField	0
6	Job	String	60	USR_UDF_JOB	6	TextField	0
7	Grade	String	60	USR_UDF_GRADE	7	TextField	0
8	Department	String	60	USR_UDF_DEPARTMENT	8	TextField	0

5. Click the Save icon.

4.5 Configuring Reconciliation Queries

Note: This section describes an optional procedure. Perform this procedure only if you want to modify one of the predefined reconciliation queries or create your own query.

You can modify existing queries in the properties file. In addition, you can add your own queries in the file. The query whose name you specify as the value of the Query Name scheduled task attribute is applied during reconciliation.

To modify an existing query or to add a query in the properties file:

Caution: You must not modify the DeletedPersons query. If you add a WHERE clause to this query, then only a subset of the actual set of person IDs is brought to Oracle Identity Manager for comparison. OIM Users whose user IDs do not match any of these person IDs are deleted from Oracle Identity Manager.

1. Open the properties file in a text editor. If you are creating your own properties file, then ensure that the extension is .properties. You can place this properties file in any directory on the target system host computer.
2. Apply the following guidelines while modifying or adding a query:

Note: 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.

- Query Name

  Do not include spaces in the query name.

  Ensure that the query name is not the same as the name of any other query in the properties file.

- SELECT clause

  Add or modify the column list in the SELECT clause. Note that changes that you make in the SELECT clause must be duplicated in the Lookup.EBS.HRMS.Recon lookup definition and, if required, on the process

form. See Section 4.1, "Adding New Attributes for Reconciliation" for more information.

If you are adding columns from tables other than those listed in the OimUserGrants.sql file, then add the required entries in the OimUserGrants.sql file and the OimUserSynonyms.sql file. See Section 2.1.2.1, "Creating a Target System User Account for Connector Operations" for information about the existing permissions in these files.

Apply the following format if you want to add an entry in the OimUserGrants.sql script:

```
PROMPT GRANT SELECT ON SCHEMA_NAME.TABLE_NAME TO &USERNAME;
GRANT SELECT ON SCHEMA_NAME.TABLE_NAME TO &USERNAME;
```

Apply the following format if you want to add an entry in the OimUserSynonyms.sql script:

```
PROMPT CREATE SYNONYM TABLE_NAME FOR SCHEMA_NAME.TABLE_NAME;
CREATE SYNONYM TABLE_NAME FOR SCHEMA_NAME.TABLE_NAME;
```

- WHERE clause

  Ensure that the following conditions are included in the WHERE clause of the query:

  Note: The remaining conditions in the WHERE clause of all the predefined queries are optional. Retain these conditions only if you want them to be applied during reconciliation.

  * PPT.USER_PERSON_TYPE_IN('Employee','Contractor','Contingent Employee')

    The person types listed in this condition must be the same as the ones listed in the Lookup.EBS.HRMS.PersonTypes lookup definition. See Section 1.5.4.2, "Lookup.EBS.HRMS.PersonTypes Lookup Definition" for more information about this lookup definition.

  * (ROUND((PAPF.LAST_UPDATE_DATE – TO_DATE('01011970','DDMMYYYY')) *1440 *60 *1000) > :lastExecutionTime)

    This condition is used to determine if a target system record was added or updated after the time stamp stored in the Last Execution Time scheduled task attribute.

  * If you are adding a column from a table other than the tables listed in the OimUserGrants.sql file and if that table contains a column in which time-stamp information is stored, then add the following condition:

    (ROUND((*TABLE_ALIAS.TIME_STAMP_COLUMN_NAME* – TO_DATE('01011970','DDMMYYYY')) *1440 *60 *1000) > :lastExecution-Time)

  The following is a sample extension to the WHERE clause:

  ```
  AND HAOU.NAME IN ('Sales', 'Operations') \
  ```

  This sample condition is used to restrict user records fetched to the ones who belong to the Sales or Operations departments. HAOU is the alias for the HR_ALL_ORGANIZATION_UNITS table.

- Comments

  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 file for an example.

- Line breaks

  If you want to introduce line breaks in the query (to improve readability), then add a backslash (\) at the end of each line.

- SQL keywords

  You must ensure that the query does not contain any clause or keyword that modifies or can be used to modify data in the database. An error message is written to the log file if the following keywords are encountered:

  – ALTER
  – CREATE
  – DELETE
  – DROP
  – EXECUTE
  – INSERT
  – UPDATE

3. Save and close the properties file.

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 create a copy of the connector for each installation 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 following connector objects:

See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

- Resource object
- IT resource
- Lookup definitions:
  – Lookup.EBS.ER.Configurations

  - Lookup.EBS.HRMS.DeleteRecon
  - Lookup.EBS.HRMS.PersonTypes
  - Lookup.EBS.HRMS.QueryFilters
  - Lookup.EBS.HRMS.Recon
- Scheduled tasks
  - eBusiness HRMS Trusted Reconciliation
  - eBusiness HRMS Delete Reconciliation

4.7 Configuring the Connector for Multiple Trusted Source Reconciliation

Note:

This connector supports multiple trusted source reconciliation.

This section describes an optional procedure. Perform this procedure only if you want to configure the connector for multiple trusted source reconciliation.

The following are examples of scenarios in which there is more than one trusted source for person data in an organization:

- One of the target systems is a trusted source for data about persons. The second target system is a trusted source for data about contractors. The third target system is a trusted source for data about interns.
- One target system holds the data of some of the identity fields that constitute an OIM User. Two other systems hold data for the remaining identity fields. In other words, to create an OIM User, data from all three systems would need to be reconciled.

If the operating environment of your organization is similar to that described in either one of these scenarios, then this connector enables you to use the target system as one of the trusted sources of person data in your organization.

See *Oracle Identity Manager Design Console Guide* for detailed information about multiple trusted source reconciliation.

5

Troubleshooting

Table 5–1 lists errors and exceptions that you might encounter while working with the connector. Solutions to these issues are also provided in the table.

Table 5–1 Troubleshooting Errors Encountered During Connector Operations

Error	Solution
ORA-00942: table or view does not exist.	This exception is encountered when an invalid table name is included in the reconciliation query. If this exception occurs, first check the query and then verify that the table exists in the target system database.
ORA-00904: "PAPF"."PERSON_I": invalid identifier.	This exception is encountered when an invalid column name is included in the reconciliation query. If this exception occurs, first check the query and then verify that the column exists in the target system database.
java.sql.SQLException: Invalid column index	This exception is encountered if the code refers to a column that is not present in the reconciliation query. If this exception occurs, then: ■ Check the columns in the reconciliation query. ■ Verify that the query name mentioned as the value of the Query Name attribute of the scheduled task is correct. See Section 3.2.6.1, "Attributes of the Scheduled Tasks" for more information. ■ Verify that all the columns in the reconciliation query are correctly mapped in the lookup definition used for reconciliation. See Section 1.5.4, "Lookup Definitions Used During Reconciliation" for more information.
ORA-01031: insufficient privileges	This exception is encountered if the target system account used for connector operations does not have the permissions required to connect to the target system tables. If this exception occurs, then: Ensure that the target system account has the permissions required to connect to all the tables listed in the reconciliation query. To do this, check the GRANT statements in the OimUserGrants.sql and OimUserSynonyms.sql files. See the following sections for more information: Section 4.5, "Configuring Reconciliation Queries" Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"
java.sql.SQLException: Attempt to set a parameter name that does not occur in the SQL: Address	This error is encountered if you specify a filter parameter in the Lookup.EBS.HRMS.QueryFilters lookup definition but do not specify the same parameter in the reconciliation query.
java.sql.SQLException: Missing IN or OUT parameter at index	This error is encountered if you specify a filter parameter in the reconciliation query but do not specify the same parameter in the Lookup.EBS.HRMS.QueryFilters lookup definition.

6

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 4.4, "Modifying Field Lengths on the OIM User Form" for information about working around this issue.

- **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.

Index

M

N

O

P

R

S

T