Oracle® Identity Governance

Configuring the Oracle E-Business HRMS Application

12c (12.2.1.3.0)

E90969-04

October 2020

ORACLE®

Oracle Identity Governance Configuring the Oracle E-Business HRMS Application, 12c (12.2.1.3.0)

E90969-04

Contents

6   Using the Oracle E-Business Suite HRMS Connectors

7   Extending the Functionality of the Oracle E-Business Suite HRMS Connectors

8   Upgrading the Oracle E-Business Suite HRMS Connectors

9   Known Issues and Workarounds for the Oracle E-Business Suite HRMS Connectors

A   Sample SQL Queries for the EBS HRMS Connector

B   Sample SQL Queries for the EBS ER Connector

C   Files and Directories in the Oracle E-Business Suite HRMS Connectors Installation Package

D   Privileges Granted to the User Account

List of Figures

List of Tables

Preface

This guide describes the connectors that are used to integrate Oracle Identity Governance with Oracle E-Business HRMS.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For information about installing and using Oracle Identity Governance 12.2.1.3.0, visit the following Oracle Help Center page:

```
https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.3/
index.html
```

For information about installing and using Oracle Identity Manager 11.1.2.3, visit the following Oracle Help Center page:

```
http://docs.oracle.com/cd/E52734_01/index.html
```

For information about Oracle Identity Governance Connectors 12.2.1.3.0 documentation, visit the following Oracle Help Center page:

```
https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/
12.2.1.3/index.html
```

For information about Oracle Identity Manager Connectors 11.1.1 documentation, visit the following Oracle Help Center page:

```
http://docs.oracle.com/cd/E22999_01/index.htm
```

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 This Guide?

These are the updates made to the software and documentation for release 12.2.1.3.0.

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector document. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on the Oracle E-Business Suite HRMS target. This helps in quicker onboarding of the applications for Oracle E-Business Suite HRMS into Oracle Identity Governance by using an intuitive UI

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific update has been made in revision "04" of this guide:

The "Target system" row of Table 1-1 has been updated to include a note about applying an Oracle Database patch. In addition, Oracle Database 19c has been added as one of the supported versions for running the target system.

The following documentation-specific update has been made in revision "03" of this guide:

Figure 3-4 has been modified.

The following documentation-specific update has been made in revision "02" of this guide:

The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance release 12*c* PS4 (12.2.1.4.0).

This is the first release of the connector. Therefore, there are no documentation-specific updates in this release.

1

About the Oracle E-Business Suite HRMS Connectors

The Oracle E-Business Suite HRMS connectors let you create and onboard Oracle E-Business Suite HRMS applications in Oracle Identity Governance.

This chapter contains the following sections:

- Introduction to the Oracle E-Business Suite HRMS Connectors
- Certified Components
- Certified Languages
- Usage Recommendation
- Supported Connector Operations
- Connector Architecture
- About Reconciliation Queries and Provisioning Procedures
- Supported Connector Features Matrix
- Connector Features

> **✎ Note:**
>
> In this guide, **Oracle E-Business Suite HRMS connectors** refers to both the connectors for Oracle EBS Employee Reconciliation (for an Authoritative application) and Oracle EBS HRMS connector (for a Target application).

1.1 Introduction to the Oracle E-Business Suite HRMS Connectors

You can manage HRMS records by using the Oracle E-Business Suite HRMS connectors.

Oracle Identity Governance is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premises or on the Cloud. Oracle Identity Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications.

> **Note:**
>
> In this guide, the connector that is deployed using the **Applications** option on the **Manage** tab of Identity Self Service is referred to as an **AOB application**. The connector that is deployed using the **Manage Connector** option in Oracle Identity System Administration is referred to as a **CI-based connector** (Connector Installer-based connector).

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Oracle Identity Self Service. This capability lets business users to onboard applications with minimum details and effort. The connector installation package includes a collection of predefined templates (XML files) that contain all the information required for provisioning and reconciling data from a given application or target system. These templates also include basic connectivity and configuration details specific to your target system. The connector uses information from these predefined templates allowing you to onboard your applications quickly and easily using only a single and simplified UI.

Application onboarding is the process of registering or associating an application with Oracle Identity Governance and making that application available for provisioning and reconciliation of user information.

You can use the Oracle E-Business Suite HRMS connectors to create and onboard Target applications and Authoritative applications in Oracle Identity Governance. The connector bundle provides two separate versions (XML files) of the connector for this purpose. The following sections provide information about these connectors:

- About the Oracle EBS Employee Reconciliation Connector
- About the Oracle EBS HRMS Connector

1.1.1 About the Oracle EBS Employee Reconciliation Connector

You use the Oracle EBS Employee Reconciliation Connector to create and onboard Authoritative applications in Oracle Identity Governance. In other words, the target system is the authoritative source of identity data for Oracle Identity Governance.

This identity data is used to create or update OIG Users.

> **Note:**
>
> In this guide, Oracle EBS Employee Reconciliation Connector is referred to as the **EBS ER connector**.

The EBS ER connector can also be configured for use in scenarios in which EBS ER connector is one of the trusted sources in the operating environment of the organization.

You use the EBS ER connector to reconcile all the person types that are supported by the Oracle E-Business Suite HRMS store. The PER_ALL_PEOPLE_F table represents the Oracle E-Business Suite HRMS store. You can also use this connector to reconcile new, modified, terminated, and deleted person type records.

The following are the person types (HRMS or Person record) supported by the Oracle E-Business Suite HR store:

- Employee
- Contingent workers/ Part-time workers
- Contractors

1.1.2 About the Oracle EBS HRMS Connector

You use the Oracle EBS HRMS connector to provision and reconcile HRMS person records (PER_ALL_PEOPLE_F records) to and from Oracle E-Business Suite HRMS. In other words, you use this connector to create PER_ALL_PEOPLE_F records for OIG Users and grant assignments and addresses to these accounts.

You can also reconcile newly created and modified PER_ALL_PEOPLE_F records from the target system.

> ✎ **Note:**
>
> In this guide, the Oracle EBS HRMS Connector for an authoritative application is referred to as the **EBS HRMS connector**.

The object class used for HR management is `__PERSON__`. When you provision an account, an HRMS person record is created and stored in the PER_ALL_PEOPLE_F table. It can be of the following types:

- Employee
- Contingent workers/ Part-time workers
- Contractors

1.2 Certified Components

These are the software components and their versions required for installing and using the connector.

Table 1-1   Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases: • Oracle Identity Governance 12c (12.2.1.4.0) • Oracle Identity Governance 12c (12.2.1.3.0)	You can use one of the following releases: • Oracle Identity Governance 12c (12.2.1.4.0) • Oracle Identity Governance 12c (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) and any later BP in this release track **Note:**You must download and apply the patch 21687999 from My Oracle Support. You will not be able to add child data if you do not apply the patch.
Target system	The target system can be any one of the following: • Oracle E-Business Suite 12.1.1 through 12.1.3 • Oracle E-Business Suite 12.2.*x* These applications may run on Oracle Database 10*g,* 11*g*, 12c, or 19c as either single database or Oracle RAC implementation. **Note:** • If your target system is running on Oracle Database release 19.*x*, then download and apply the Oracle Database patch 31142749 from My Oracle Support. Applying this patch ensures that provisioning operations work fine. • Communication between Oracle Identity Governance and the target system can be in SSL or non-SSL mode.	The target system can be any one of the following: • Oracle E-Business Suite 12.1.1 through 12.1.3 • Oracle E-Business Suite 12.2.*x* These applications may run on Oracle Database 10*g,* 11*g*, 12c, or 19c as either single database or Oracle RAC implementation. **Note:** • If your target system is running on Oracle Database release 19.*x*, then download and apply the Oracle Database patch 31142749 from My Oracle Support. Applying this patch ensures that provisioning operations work fine. • Communication between Oracle Identity Governance and the target system can be in SSL or non-SSL mode.
Connector server	11.1.2.1.0 and later	11.1.2.1.0 and later
Connector Server JDK	JDK 1.6 or later	JDK 1.6 or later

1.3 Certified Languages

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- French (Canadian)
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.4 Usage Recommendation

These are the recommendations for the EBS HRMS connector versions that you can deploy and use depending on the Oracle Identity Governance or Oracle Identity Manager version that you are using.

- If you are using Oracle Identity Governance 12c (12.2.1.3.0) or later, then use the latest 12.2.1.*x* version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.

- If you are using Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) and any later BP in this release track, then you must use the latest 11.1.1.*x* version of this connector. If you want to use the 12.2.1.*x* version of this connector with Oracle Identity Manager release 11.1.2.3.0 and any later BP, then you can install and use the it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0.

> **✎ Note:**
>
> If you are using the latest 12.2.1.*x* version of the EBS HRMS connector in the CI-based mode, then see *Oracle Identity Manager Connector Guide for Oracle E-Business HRMS*, Release 11.1.1 for complete details on connector deployment, usage, and customization.

- If you are using an Oracle Identity Manager release that is earlier than Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), then you must use the 9.1.*x* version of this connector.

1.5 Supported Connector Operations

These are the list of operations that the connector supports for your target system.

Table 1-2   Supported Connector Operations

Operation	Supported?
User Management	
Create Person	Yes
Update Person	Yes
Delete Person	Yes
Enable Person	No
Disable Person	No
Entitlement Grant Management	
Add Address	Yes
Update Address	Yes
Delete Address	Yes
Add Assignment	Yes
Update Assignment	Yes

Table 1-2   (Cont.) Supported Connector Operations

Operation	Supported?
Delete Assignment	Yes

1.6 Connector Architecture

The Oracle E-Business Suite HRMS Connectors are implemented using the Integrated Common Framework (ICF) component.

The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Governance connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped along with Oracle Identity Governance. Therefore, you need not configure or modify the ICF.

During connector operations, Oracle Identity Governance interacts with a layer called Glue. Glue is specific for each of the applications and uses ICF API to invoke operations on the Identity Connector (IC). The connector then calls the target system APIs to perform operations on the resource.

As discussed in one of the earlier sections, there are two versions of the Oracle E-Business HRMS connector as follows:

- **EBS HRMS Connector**

  The basic function of this connector is to enable management of employee data on Oracle E-Business Suite HRMS through Oracle Identity Governance. You can create and manage employee records for OIG Users through provisioning. In addition, data related to newly created and modified employee records can be reconciled (using scheduled tasks) and linked with existing OIG Users and provisioned resources.

  Figure 1-1 shows the architecture of the EBS HRMS connector.

Figure 1-1   Connector Architecture of the EBS HRMS Connector
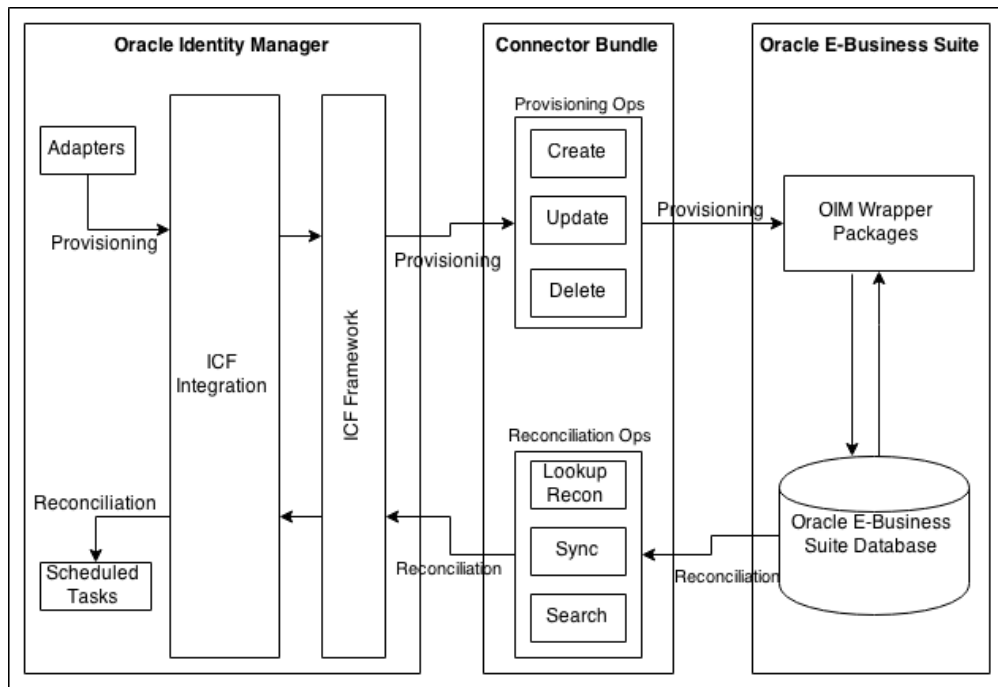
- **EBS ER Connector**

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

   Figure 1-1 shows the architecture of the EBS ER connector.

Figure 1-2   Connector Architecture of the EBS ER Connector
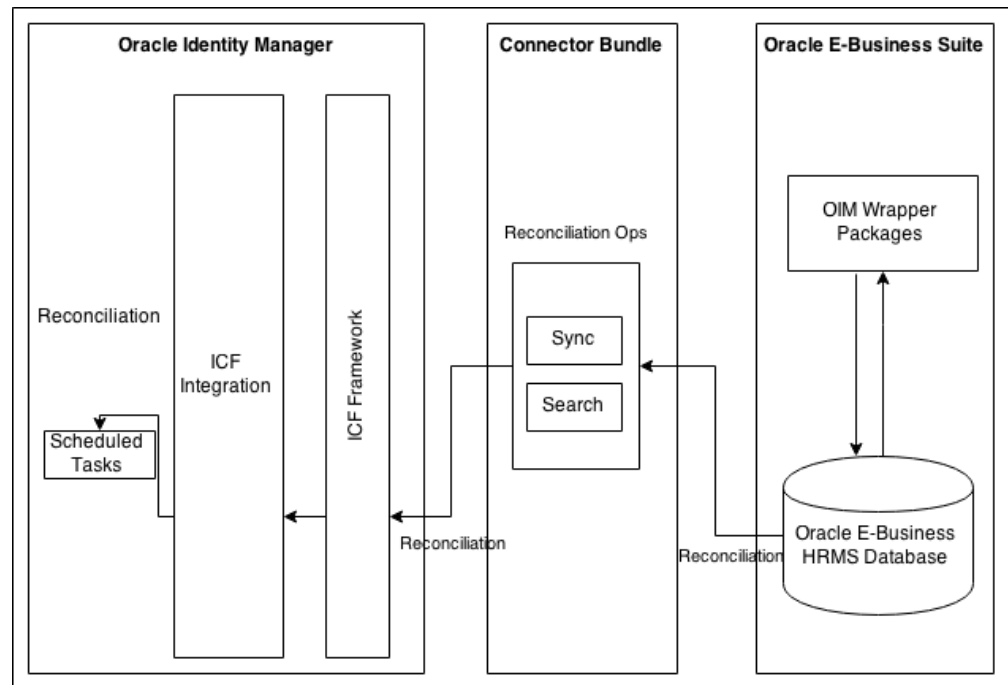
1.7 About Reconciliation Queries and Provisioning Procedures

Reconciliation queries and provisioning procedures help in performing reconciliation and provisioning operations more efficiently.

The following sections provide information about reconciliation queries and provisioning procedures:

- About Reconciliation Queries for the EBS HRMS Connector
- About Reconciliation Queries for the EBS HRMS ER Connector
- About Provisioning Procedures for the EBS HRMS Connector

1.7.1 About Reconciliation Queries for the EBS HRMS Connector

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

A SQL query is used to fetch target system records during reconciliation. All predefined SQL queries that are required to perform reconciliation are stored in the search.properties file. The search.properties file is a common file for all EBS Suite connectors. In other words, the search.properties file contains the queries for the EBS UM, HRMS Target, and HRMS Trusted connectors.

When you run a scheduled job, the connector locates the corresponding SQL query in the search.properties file and then runs it on the target system database.

Target system records that meet the query criteria are returned to Oracle Identity Governance.

Depending on your requirements, you can modify existing queries or add your own query in the search.properties. This is discussed later in this guide.

Information in the search.properties file is virtually divided into two parts. The first part lists entries containing the SQL query names in the following format:

OBJ_CLASS.OP_NAME.MODE=QUERY_NAME

In this format:

- *OBJ_CLASS* is the name of the object class on which the reconciliation operation is to be performed.

- *OP_NAME* is the type of reconciliation operation to be performed. A reconciliation operation can be a search op, sync op, or lookup op.

- *MODE* is the name of the mode in which the connector is expected to perform reconciliation. For example, trusted. Note that this value is optional.

- *QUERY_NAME* is the name of the SQL query that is to be run on the target system database.

The second part lists the SQL query names and the corresponding SQL queries.

The following are the entries corresponding to the HRMS Target connector in the search.properties file:

- __PERSON__.search=TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUE RY

  This query is used to reconcile all newly created and modified HRMS person records from the target system. The reconciliation operation that is performed is search based.

- __PERSON__.sync=TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUER Y

  This query is used to reconcile all newly created and modified HRMS person records from the target system. The reconciliation operation that is performed is sync based.

- __PERSON__.sync.terminate=HRMS_TERMINATED_EMPLOYEE_RECON_QU ERY

  The HRMS_TERMINATED_EMPLOYEE_RECON_QUERY query is used to reconcile records of persons whose services have been terminated. When the connector fetches the records of such persons, the accounts of the corresponding users in Oracle Identity Governance are revoked.

- __JOBS__.lookup=LOOKUP_JOBS_QUERY

  This query is used to synchronize values in the PER_JOBS table of the target system with the Lookup.EBSHRMS.Jobs lookup definition in Oracle Identity Governance.

- __GRADES__.lookup=LOOKUP_GRADES_QUERY

  This query is used to synchronize values in the PER_GRADES table of the target system with the Lookup.EBSHRMS.Grades lookup definition in Oracle Identity Governance.

- __ORGANIZATION__.lookup=LOOKUP_ORGANIZATION_QUERY

    This query is used to synchronize values in the HR_ALL_ORGANIZATION_UNITS table of the target system with the Lookup.EBSHRMS.Organization lookup definition in Oracle Identity Governance.

- __PERSONTYPE__.lookup=LOOKUP_PERSONTYPE_QUERY

    This query is used to synchronize values in the PER_PERSON_TYPES and HR_ALL_ORGANIZATION_UNITS tables of the target system with the Lookup.EBSHRMS.PersonType lookup definition in Oracle Identity Governance.

1.7.2 About Reconciliation Queries for the EBS HRMS ER Connector

The EBS HRMS ER connector is configured to perform trusted source reconciliation with the target system. The target system is used as the trusted source and users are directly created and modified on it. During reconciliation, the EBS HRMS ER connector fetches data (using scheduled jobs) about these target system users into Oracle Identity Governance. This data is used to create or update the corresponding OIM Users.

A SQL query is used to fetch target system records during reconciliation. All predefined SQL queries that are required to perform reconciliation are stored in the search.properties file. The search.properties file is a common file for all EBS Suite connectors. In other words, the search.properties file contains the queries for the EBS UM, HRMS Target, and HRMS Trusted connectors.

When you run a scheduled job, the connector locates the corresponding SQL query in the search.properties file and then runs it on the target system database. Target system records that meet the query criteria are returned to Oracle Identity Governance.

Depending on your requirements, you can modify existing queries or add your own query in the search.properties. This is discussed later in this guide.

Information in the search.properties file is virtually divided into two parts. The first part lists entries containing the SQL query names in the following format:

OBJ_CLASS.OP_NAME.MODE=QUERY_NAME

In this format:

- *OBJ_CLASS* is the name of the object class on which the reconciliation operation is to be performed.

- *OP_NAME* is the type of reconciliation operation to be performed. A reconciliation operation can be a search op, sync op, or lookup op.

- *MODE* is the name of the mode in which the connector is expected to perform reconciliation. For example, trusted. Note that this value is optional.

- *QUERY_NAME* is the name of the SQL query that is to be run on the target system database.

The second part lists the SQL query names and the corresponding SQL queries.

The following are the entries corresponding to the HRMS Target connector in the search.properties file:

- __PERSON__.search.trusted=HRMS_CURRENT_EMPLOYEE_RECON_QUERY

The HRMS_CURRENT_EMPLOYEE_RECON_QUERY query is used to reconcile all employee records that are currently active from the target system. The reconciliation operation that is performed is search based.

- __PERSON__.search.future_trusted=HRMS_CURRENT_FUTURE_EMPLOYEE_RECON_QUERY

  The HRMS_CURRENT_FUTURE_EMPLOYEE_RECON_QUERY query is used to reconcile all future-dated employee records from the target system. The reconciliation operation that is performed is search based.

- __PERSON__.sync.trusted=HRMS_CURRENT_EMPLOYEE_RECON_QUERY

  The HRMS_CURRENT_EMPLOYEE_RECON_QUERY query is used to reconcile all employee records that are currently active from the target system. The reconciliation operation that is performed is sync based.

- __PERSON__.sync.future_trusted=HRMS_CURRENT_FUTURE_EMPLOYEE_RECON_QUERY

  The HRMS_CURRENT_FUTURE_EMPLOYEE_RECON_QUERY query is used to reconcile all future-dated employee records from the target system.The reconciliation operation that is performed is sync based.

1.7.3 About Provisioning Procedures for the EBS HRMS Connector

Provisioning involves management of person accounts in the target system. When you allocate (or provision) an Oracle E-Business HRMS resource to an OIM User, the operation results in the creation of a person record on Oracle E-Business HRMS for that user. Similarly, when you update the resource on Oracle Identity Governance, the same update is made to the person record on the target system.

The connector uses stored procedures for performing provisioning operations. These stored procedures are available in the wrapper packages of the target system. Information about all stored procedures used for performing provisioning operations are defined in the Procedures.properties file. The same file contains stored procedures information for both the HRMS Target and User Management connectors.

When you perform a provisioning operation, the connector locates the corresponding stored procedure in the Procedures.properties file and the runs it on the target system to complete the provisioning operation.

Depending on your requirements, you can modify existing stored procedures or add your own stored procedures to the Procedures.properties file. This is discussed later in the guide.

The first property in the Procedures.properties file, DB.PACKAGES, lists all the wrapper packages that are used during connector operations. The subsequent entries in this file are in the following format:

OBJ_NAME.OP_NAME=WRAPPER_PCKG.STORED_PROC

In this format:

- OBJ_NAME is the name of the object on which the provisioning operation must be performed.
- OP_NAME is the type of provisioning operation to be performed. A provisioning operation can be a create, update, delete, or terminate.
- WRAPPER_PCKG is the name of the wrapper package.

- *STORED_PROC* is the name of the stored procedure in the wrapper package that is to be run to on the target system to complete the provisioning operation.

The following are the entries corresponding to the HRMS Target connector in the Procedures.properties file:

- **Entries corresponding to the __PERSON__ object:**

  - __PERSON__.create=OIM_EMPLOYEE_WRAPPER.CREATE_PERSON_API

    In this entry, the CREATE_PERSON_API stored procedure of the OIM_EMPLOYEE_WRAPPER wrapper package is used for performing the Create provisioning operation against the __PERSON__ object.

  - __PERSON__.update=OIM_EMPLOYEE_WRAPPER.UPDATE_PERSON_API

    In this entry, the UPDATE_PERSON_API stored procedure of the OIM_EMPLOYEE_WRAPPER wrapper package is used for performing the Update provisioning operation against the __PERSON__ object.

  - __PERSON__.delete=OIM_EMPLOYEE_WRAPPER.DELETE_PERSON_API

    In this entry, the DELETE_PERSON_API stored procedure of the OIM_EMPLOYEE_WRAPPER wrapper package is used for performing the Delete provisioning operation against the __PERSON__ object.

  - __PERSON__.terminate=OIM_EMPLOYEE_WRAPPER.TERMINATE_PERSON_API

    In this entry, the TERMINATE_PERSON_API stored procedure of the OIM_EMPLOYEE_WRAPPER wrapper package is used for performing the Terminate services provisioning operation against the __PERSON__ object.

- **Entries corresponding to child objects:**

  - __ADDRESS__.add=OIM_EMPLOYEE_ADDRESS_WRAPPER.CREATE_PERSON_ADDRESS_API

    In this entry, the CREATE_PERSON_ADDRESS_API stored procedure of the OIM_EMPLOYEE_WRAPPER wrapper package is used for adding address for the __PERSON__ object.

  - __ADDRESS__.remove=OIM_EMPLOYEE_ADDRESS_WRAPPER.DELETE_PERSON_ADDRESS_API

    In this entry, the DELETE_PERSON_ADDRESS_API stored procedure of the OIM_EMPLOYEE_WRAPPER wrapper package is used for removing the address for the __PERSON__ object.

  - __ASSIGNMENT__.add=OIM_EMPLOYEE_WRAPPER.CREATE_PERSON_ASSIGNMENT_API

    In this entry, the CREATE_PERSON_ASSIGNMENT_API stored procedure of the OIM_EMPLOYEE_WRAPPER wrapper package is used for adding assignments for person records.

  - __ASSIGNMENT__.remove=OIM_EMPLOYEE_WRAPPER.DELETE_PERSON_ASSIGNMENT_API

    In this entry, the DELETE_PERSON_ASSIGNMENT_API stored procedure of the OIM_EMPLOYEE_WRAPPER wrapper package is used for removing assignments from person records.

ORACLE®

- – __ASSIGNMENT__.update=OIM_EMPLOYEE_WRAPPER.UPDATE_PERSO
  N_ASSIGNMENT_API

  In this entry, the UPDATE_PERSON_ASSIGNMENT_API stored procedure
  of the OIM_EMPLOYEE_WRAPPER wrapper package is used for updating
  assignments for person records.

- – __ADDRESS__.update=OIM_EMPLOYEE_ADDRESS_WRAPPER.UPDATE_
  PERSON_ADDRESS_API

  In this entry, the UPDATE_PERSON_ADDRESS_API stored procedure of
  the OIM_EMPLOYEE_WRAPPER wrapper package is used for updating the
  address of a person records.

1.8 Supported Connector Features Matrix

Provides the list of features supported by the AOB application and CI-based
connector.

Table 1-3   Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Trusted Source and Target Resource Reconciliation	Yes	Yes
Configurable Reconciliation Queries and Stored Procedures	Yes	Yes
Full and incremental reconciliation	Yes	Yes
Batched reconciliation	No	Yes
Limited reconciliation	Yes	Yes
Connection pooling	Yes	Yes
SSL communication	Yes	Yes

1.9 Connector Features

The features of the connector include full reconciliation, batched reconciliation, limited
reconciliation, connection pooling, SSL communication, and so on.

The following are the features of the connector:

- • Support for Trusted Source and Target Resource Reconciliation
- • Configurable Reconciliation Queries and Stored Procedures
- • Full and Incremental Reconciliation
- • Batched Reconciliation
- • Limited (Filtered) Reconciliation
- • Connection Pooling
- • Support for SSL Communication Between the Target System and Oracle Identity
  Governance

1.9.1 Support for Trusted Source and Target Resource Reconciliation

There are two versions of the connectors available to provide support for trusted source (authoritative application) and target resource (Target application) reconciliation.

You can use the EBS ER connector to integrate Oracle E-Business HRMS as a trusted source of Oracle Identity Governance. In this mode, the connector reconciles all the person types that are supported by the Oracle E-Business Suite HRMS store.

In the target resource mode, you can use the EBS HRMS connector to create a Target application to provision and reconcile the HRMS/Person records from the Oracle E-Business Suite HRMS store.

1.9.2 Configurable Reconciliation Queries and Stored Procedures

The connector bundle JAR file contains predefined SQL queries and stored procedures for performing reconciliation and provisioning operations, which you can modify to suit your requirements.

Reconciliation involves running a SQL query on the target system database to fetch the required Person records to Oracle Identity Governance. Predefined SQL queries are stored in the search.properties file in the connector bundle JAR package. You can modify these SQL queries or add your own SQL queries for reconciliation.

Similarly, provisioning involves running stored procedures on the target system database to create or update the required Person records. Information about the stored procedures related to performing provisioning operations are stored in the Procedures.properties file in the connector bundle JAR. You can modify these stored procedures or add your own stored procedures for provisioning.

See the following sections for more information about these SQL queries and stored procedures:

- About Reconciliation Queries for the EBS HRMS Connector
- About Reconciliation Queries for the EBS HRMS ER Connector
- About Provisioning Procedures for the EBS HRMS Connector

1.9.3 Full and Incremental Reconciliation

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

You can switch from incremental to full reconciliation at any time after you deploy the connector. See section Performing Full and Incremental Reconciliation for more information on performing full and incremental reconciliation runs.

1.9.4 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 Performing Batched Reconciliation for more information on performing batched reconciliation.

1.9.5 Limited (Filtered) Reconciliation

To limit or filter the records that are fetched into Oracle Identity Governance during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

See section Performing Limited Reconciliation for more information on performing limited reconciliation.

1.9.6 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Governance connectors can use these connections to communicate with target systems.

At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each set of basic configuration parameters that you provide while creating an application. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

For more information about the parameters that you can configure for connection pooling, see Advanced Setting Parameters for the EBS HRMS Connector and Advanced Setting Parameters for the EBS ER Connector.

1.9.7 Support for SSL Communication Between the Target System and Oracle Identity Governance

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

See Configuring Secure Communication Between the Target System and Oracle Identity Governance for information about configuring secure communication.

2

Creating an Application By Using the Oracle E-Business Suite HRMS Connectors

Learn about onboarding applications using the connector and the prerequisites for doing so.

- Process Flow for Creating an Application By Using the Connector
- Prerequisites for Creating an Application By Using Connector
- Creating an Application By Using the Connector

2.1 Process Flow for Creating an Application By Using the Connector

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Identity Self Service.

Figure 2-1 is a flowchart depicting high-level steps for creating an application in Oracle Identity Governance by using the connector installation package.

Figure 2-1   Overall Flow of the Process for Creating an Application By Using the Connector
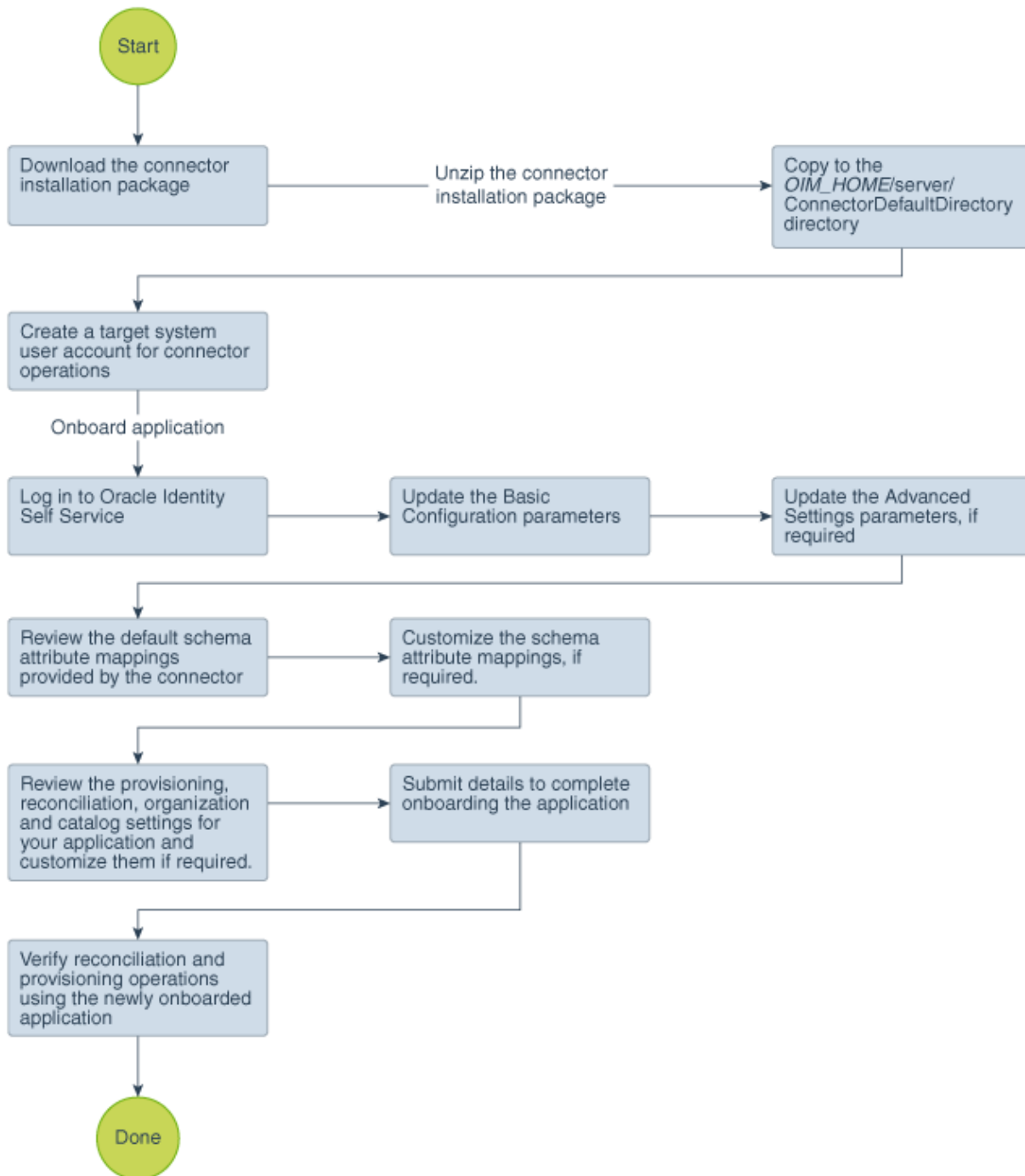
2.2 Prerequisites for Creating an Application By Using Connector

Learn about the tasks that you must complete before you create the application.

- Downloading the Connector Installation Package
- Creating a Target System User Account for Connector Operations

2.2.1 Downloading the Connector Installation Package

You can obtain the installation package for your connector on the Oracle Technology Network (OTN) website.

To download the connector installation package:

1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html.

2. Click **OTN License Agreement** and read the license agreement.

3. Select the **Accept License Agreement** option.

   You must accept the license agreement before you can download the installation package.

4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.

5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*

6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

2.2.2 Creating a Target System User Account for Connector Operations

Oracle Identity Governance requires a target system user account to access the target system during reconciliation and provisioning operations. Depending on the target system you are using, you can create the user in your target system and assign specific permissions and roles to the user.

You provide the credentials of this user account as part of Basic Configuration Parameters for the EBS HRMS Connector or Basic Configuration Parameters for the EBS ER Connector while creating an application.

> **✏ Note:**
>
> Target system documentation for detailed information about creating the user

To create a target system user account for connector operations:

1. From the installation media, copy the scripts directory to a temporary directory on either the target system host computer or a computer on which the Oracle Database Client has been installed. If you are installing in the same host computer where the connector directory is present, then skip this step and proceed to the next.

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. Change to the directory containing the scripts directory and depending on the host platform, run either the Run_HRMS_DBScripts.sh or Run_HRMS_DBScripts.bat file. These files are present in the scripts directory of the installation media.

4. When you run the script, you are prompted for the following information:

   - `Enter the ORACLE_HOME`

     Set a value for the ORACLE_HOME environment variable. 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.

   - `Would you like to create new user for connector operations [y/n]`

     Enter `y` or `n` to specify whether you want to create a new user for connector operations.

     This connects you the SQL*Plus client.

   - `Are you running this script with EBS target 12.1.x [y/n]`

     Enter `y` if you are using Oracle E-Business Suite release 12.1.1 through 12.1.3. When you do so, version compatible scripts will run on your target system.

     Enter `n` if you are using Oracle E-Business Suite 12.2.x and later versions.

   - `Enter password`

     Enter the password for the Oracle database login. If you entered `n` at the earlier prompt to create a new user for connector operations, then the Type and Package are created, and then the connection to the database is disconnected. If you entered y, then the Type and Package are created, and then the connection to the database remains.

   - `Enter password`

     Enter the password of the dba user.

   - `Enter New database Username to be created`

     Enter a user name for the target system account that you want to create.

   - `Enter the New user password`

     Enter a password for the target system account that you want to create.

This installs all wrappers packages under the APPS schema, creates the new target system account, and then grants all the required privileges on the tables and packages.

- `Connecting with newly created database user`

  Enter the connection string or service name that you provided earlier.

  The user account for connector operations is created. The privileges granted to this user account are listed in Privileges Granted to the User Account.

- `Enter the hostname for network acl [Input will be ignored If DB version is earlier than 11g]`

  Enter the name of the computer hosting network acl in the following format:

  `*.DOMAIN_NAME.com`

  This prompt is received only if you entered `y` at one of the earlier prompts to create a new user for connector operations.

2.3 Creating an Application By Using the Connector

You can onboard an application into Oracle Identity Governance from the connector package by creating a target application. To do so, you must log in to Identity Self Service and then choose the **Applications** box on the **Manage** tab.

The following is the high-level procedure to create an application by using the connector:

> **Note:**
>
> For detailed information on each of the steps in this procedure, see Creating Applications of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1. Create an application in Identity Self Service. The high-level steps are as follows:

   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.

   b. Ensure that the **Connector Package** option is selected when creating an application.

   c. Update the basic configuration parameters to include connectivity-related information.

   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.

   e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.

   f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.

g. Review the details of the application and click **Finish** to submit the application details.

The application is created in Oracle Identity Governance.

h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.

If you click **Yes**, then the default form is automatically created and is attached with the newly created application. The default form is created with the same name as the application. The default form cannot be modified later. Therefore, if you want to customize it, click **No** to manually create a new form and attach it with your application.

2. Verify reconciliation and provisioning operations on the newly created application.

> **See Also:**
>
> - Configuring the Oracle EBS HRMS Connector for a Target Application and Configuring the Oracle EBS Employee Reconciliation Connector for an Authoritative Application for details on basic configuration and advanced settings parameters, default user account attribute mappings, default correlation rules, and reconciliation jobs that are predefined for this connector
>
> - Configuring Oracle Identity Governance for details on creating a new form and associating it with your application, if you chose not to create the default form.

3

Configuring the Oracle EBS HRMS Connector for a Target Application

While creating a Target application, you must configure the connection-related parameters that the connector uses to connect Oracle Identity Governance with your target system and perform connector operations. In addition, you can view and edit attribute mappings between the process form fields in Oracle Identity Governance and target system columns, predefined correlation rules, situations and responses, and reconciliation jobs.

- Basic Configuration Parameters for the EBS HRMS Connector
- Advanced Setting Parameters for the EBS HRMS Connector
- Attribute Mapping for the EBS HRMS Connector
- Correlation Rules for the EBS HRMS Connector
- Reconciliation Jobs for the EBS HRMS Connector

3.1 Basic Configuration Parameters for the EBS HRMS Connector

These are the connection-related parameters that Oracle Identity Governance requires to connect to the EBS HRMS connector. These parameters are applicable for target applications only.

Table 3-1   Parameters in the Basic Configuration Section for EBS HRMS

Parameter	Mandatory?	Description
Connection URL	Yes	Enter the database connection string using the `host:post:sid` syntax format.
		Default value: `jdbc:oracle:thin:@%h:%p:%d`
		See Determining Values for the JDBC URL and Connection Properties Parameters for more information about the supported JDBC URL formats and the value that you need to enter depending on the security measures that you have implemented.

Table 3-1   (Cont.) Parameters in the Basic Configuration Section for EBS HRMS

Parameter	Mandatory?	Description
User	Yes	Enter the user name of the target system account created while performing the Prerequisites for Creating an Application By Using Connector procedure. This user is used for various connector operations.
Password	Yes	Enter the password for the user name of the target system account to be used for connector operations.
Connector Server Name	No	If you are using a Connector Server, then enter the name of its IT resource.
Batch Size	No	Enter the number of records that the connector must include in each batch that it fetches from the target system during reconciliation. **Default value:** 1000
Context Application ID	No	Enter the ID of the application to which the user belongs. **Default value:** 0
Context Responsibility ID	No	Enter the responsibility assigned to the user in whose context the connector operations are performed on the target system. **Default value:** 0
Context User ID	No	Enter the user ID of the user in whose context the connector operations are performed on the target system. **Default value:** 0
Database	No	Enter the name of the target system database against which connector operations must be performed.

Table 3-1   (Cont.) Parameters in the Basic Configuration Section for EBS HRMS

Parameter	Mandatory?	Description
Delete Person	No	Specifies whether the employee record must be completely deleted from the target system. There is no hard delete of employee records in the target system. In other words, when you delete an employee record, the employee record is just set to terminated, but the record is not completely deleted from the target system.
		If you set the value of this parameter to `true`, then the employee record is completely deleted from the target system.
		If you set the value of this parameter to `false`, then the employee record is not deleted from the target system, but its status is just set to `terminated`.
Host	No	Enter the host name where the database is running.
Port	No	Enter the port number at which the target system database is listening.

3.2 Advanced Setting Parameters for the EBS HRMS Connector

These are the configuration-related entries that the connector uses during reconciliation and provisioning operations.

Table 3-2   Advanced Setting Parameters for the EBS HRMS Connector

Parameter	Mandatory?	Description
Connector Name	Yes	This parameter holds the name of the connector class. **Value:** `org.identityconnectors. ebs.EBSConnector`

Table 3-2 (Cont.) Advanced Setting Parameters for the EBS HRMS Connector

Parameter	Mandatory?	Description
Bundle Name	Yes	This parameter holds the name of the connector bundle package. **Value:** `org.identityconnectors.ebs`
Bundle Version	Yes	This parameter hods the version of the connector bundle class. **Value:** `12.3.0`
Pool Max Idle	No	Enter the maximum number of idle objects in a pool. **Default value:** `10`
Pool Max Size	No	Enter the maximum number of connections that the pool can create. **Default value:** `10`
Pool Max Wait	No	Enter the maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. **Default value:** `150000`
Pool Min Evict Idle Time	No	Enter the minimum time, in milliseconds, the connector must wait before evicting an idle object. **Default value:** `120000`
Pool Min Idle	No	Enter the minimum number of idle objects in a pool. **Default value:** `1`
FilterDateAttributes	No	Enter the target system date attribute that the connector must use for filtering user records. If you want to enter more than one date attribute, then ensure to include them as a comma-separated list. **Default value:** `HIRE_DATE`
FilterDateAttributeFormat	No	Enter the format of the attribute specified as the value of the FilterDateAttributes parameter. **Default value:** `dd-MMM-yyyy`

3.3 Attribute Mapping for the EBS HRMS Connector

The Schema page for a target application displays the default schema (provided by the connector) that maps Oracle Identity Governance attributes to target system columns. The connector uses these mappings during reconciliation and provisioning operations.

Oracle EBS HRMS User Account Attributes

Table 3-3 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Oracle EBS HRMS columns. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3   Oracle EBS HRMS User Account Schema Attributes

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Employee Number	EMPLOYEE_NUMBER	String	No	Yes	Yes	No	No
First Name	FIRST_NAME	String	Yes	Yes	Yes	No	No
Last Name	LAST_NAME	String	Yes	Yes	Yes	No	No
Gender	SEX	String	Yes	Yes	Yes	No	No
Business Group Id	BUSINESS_GROUP_ID	String	Yes	Yes	Yes	No	No
Person Type	PERSON_TYPE_ID	String	No	Yes	Yes	No	No
Email	EMAIL_ADDRESS	String	No	Yes	Yes	No	No
Nationality	NATIONALITY	String	No	Yes	Yes	No	No
National Identifier	NATIONAL_IDENTIFIER	String	No	Yes	Yes	No	No
Date Of Birth	DATE_OF_BIRTH	Date	No	Yes	Yes	No	No
Person Id	__UID__	String	No	Yes	Yes	Yes	No

Table 3-3   (Cont.) Oracle EBS HRMS User Account Schema Attributes

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property ?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Hire Date	HIRE_DATE	Date	No	Yes	Yes	No	No
Title	TITLE	String	No	Yes	Yes	No	No
Status	__ENABLE__	String	No	No	Yes	No	No
Marital Status	MARITAL_STATUS	String	No	Yes	No	No	No

Figure 3-1 shows the default User account attribute mappings.

Figure 3-1   Default Attribute Mappings for Oracle EBS HRMS User Account

Address Entitlement Attributes

Table 3-4 lists the address-specific attribute mappings between the process form fields in Oracle Identity Governance and Oracle EBS HRMS columns. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4   Default Attribute Mappings for an Address Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Address Id	__ADDRESS__~__ADDRESS__~ADDRESS_ID	String	No	Yes	Yes	No
Country	__ADDRESS__~__ADDRESS__~COUNTRY	String	Yes	Yes	No	No
Address1	__ADDRESS__~__ADDRESS__~ADDRESS_LINE1	String	Yes	Yes	No	No
Address2	__ADDRESS__~__ADDRESS__~ADDRESS_LINE2	String	No	Yes	No	No
Address3	__ADDRESS__~__ADDRESS__~ADDRESS_LINE3	String	No	Yes	No	No
City	__ADDRESS__~__ADDRESS__~TOWN_OR_CITY	String	Yes	Yes	No	No
Postal Code	__ADDRESS__~__ADDRESS__~POSTAL_CODE	Int	No	Yes	No	No

Table 3-4   (Cont.) Default Attribute Mappings for an Address Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive ?
Region	__ADDRES S__~__AD DRESS__~ REGION_1	String	No	Yes	No	No
Region2	__ADDRES S__~__AD DRESS__~ REGION_2	String	No	Yes	No	No
Region3	__ADDRES S__~__AD DRESS__~ REGION_3	String	No	Yes	No	No
Style	__ADDRES S__~__AD DRESS__~ STYLE	String	Yes	Yes	No	No
Start Date	__ADDRES S__~__AD DRESS__~ DATE_FRO M	Date	Yes	Yes	No	No
End Date	__ADDRES S__~__AD DRESS__~ DATE_TO	Date	No	Yes	No	No
Address Type	__ADDRES S__~__AD DRESS__~ ADDRESS_ TYPE	String	No	Yes	No	No
Primary Flag	__ADDRES S__~__AD DRESS__~ PRIMARY_ FLAG	String	Yes	Yes	No	No

Figure 3-2 shows the address entitlement mappings.

Figure 3-2   Default Attribute Mappings for an Address Entitlement

Assignment Entitlement Attributes

Table 3-5 lists the assignment-specific attribute mappings between the process form fields in Oracle Identity Governance and Oracle EBS HRMS columns. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5   Default Attribute Mappings for an Assignment Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Assignment Id	__ASSIGN MENT__~_ _ASSIGNM ENT__~AS SIGNMENT _ID	String	No	Yes	Yes	No
Organizatio n Id	__ASSIGN MENT__~_ _ASSIGNM ENT__~OR GANIZATIO N_ID	String	Yes	Yes	No	No
Grade Id	__ASSIGN MENT__~_ _ASSIGNM ENT__~GR ADE_ID	String	No	Yes	No	No
Job Id	__ASSIGN MENT__~_ _ASSIGNM ENT__~JO B_ID	String	Yes	Yes	No	No
Supervisor Id	__ASSIGN MENT__~_ _ASSIGNM ENT__~SU PERVISOR _ID	Int	No	Yes	No	No
Change Reason	__ASSIGN MENT__~_ _ASSIGNM ENT__~CH ANGE_REA SON	String	No	Yes	No	No
Effective Date	__ASSIGN MENT__~_ _ASSIGNM ENT__~AS G_EFFECTI VE_START _DATE	String	Yes	Yes	No	No

Figure 3-3 shows the assignment entitlement mappings.

Figure 3-3   Default Attribute Mappings for an Assignment Entitlement

3.4 Correlation Rules for the EBS HRMS Connector

When you create a Target application, the connector uses correlation rules to determine the identity to which Oracle Identity Governance must assign a resource.

Predefined Identity Correlation Rules

By default, the EBS HRMS connector provides a simple correlation rule when you create a Target application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

Table 3-6 lists the default simple correlation rule for Oracle EBS HRMS that are connected using the OR operator. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6   Predefined Identity Correlation Rules for Oracle EBS HRMS

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__UID__	Equals	EBS Person ID	No
__UID__	Equals	User Login	No

In this identity rule:

• __UID__ is a single-valued attribute on the target system that identifies the user account.

• EBS Person ID and User Login are fields on the OIG User form.

Figure 3-4 shows the simple correlation rule for the EBS HRMS connector.

Figure 3-4   Simple Correlation Rules for the EBS HRMS Connector

The application is already setup with default attributes. You can review and customize them as per your need.

◢ Preview Settings

Provisioning   Reconciliation   Organization   Catalog

Below are pre-defined rules that have been set for you.

◢ Identity Correlation Rule

Choose Type of Correlation Rule

◉ Simple Correlation Rule   ◯ Complex Correlation Rule

➕ Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
__UID__ ▾	Equals ▾	EBS Person ID 🔍	☐	✖
__UID__ ▾	Equals ▾	User Login 🔍	☐	✖

Rule Operator

| OR ▾ |

Predefined Situations and Responses

The EBS HRMS connector provides a default set of situations and responses when you create a Target application. These situations and responses specify the action that Oracle Identity Governance must take based on the result of a reconciliation event.

Table 3-7 lists the default situations and responses for the EBS HRMS Connector. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-7   Predefined Situations and Responses for the EBS HRMS Connector

Situation	Response
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 3-5 shows the situations and responses for Oracle E-Business HRMS that the connector provides by default.

Figure 3-5   Predefined Situations and Responses for the EBS HRMS Connector
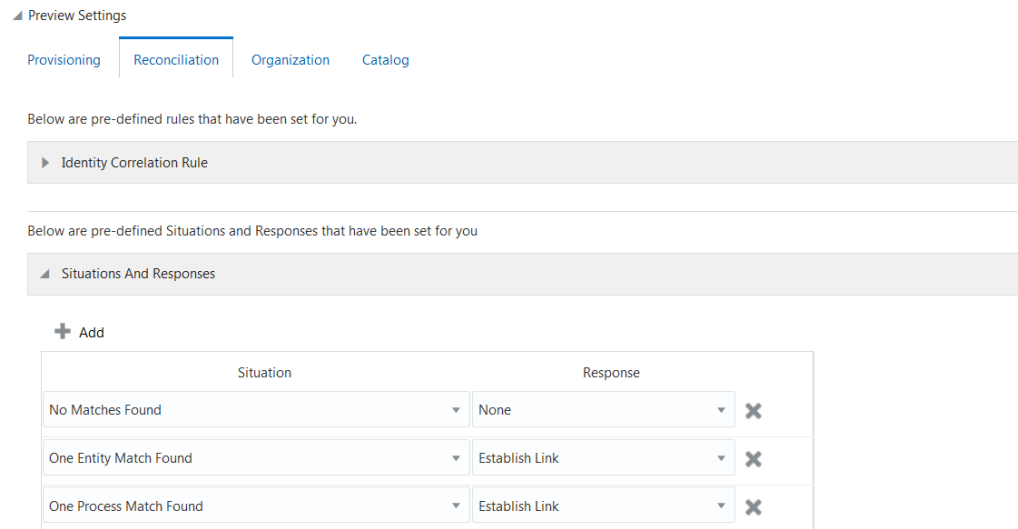
3.5 Reconciliation Jobs for the EBS HRMS Connector

These are the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application for your target system.

You can either use these predefined jobs or edit them to meet your requirements. Alternatively, you can create custom reconciliation jobs. For information about editing these predefined jobs or creating new ones, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Full Reconciliation Job

The Oracle EBS HRMS Target User Reconciliation job is used for reconciliation of person records.

Table 3-8   Parameters of the Oracle EBS HRMS Target User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application.
	Do not modify this value.

Table 3-8   (Cont.) Parameters of the Oracle EBS HRMS Target User Reconciliation Job

Parameter	Description
Filter	Enter the expression for filtering person records that the connector must reconcile.
	Sample value: `equalTo('__UID__','10533')`
	For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Developing and Customizing Applications for Oracle Identity Governance*.
Incremental Recon Attribute	Enter the name of the target system column that holds the timestamp at which the person record was modified.
	Sample value: `PERSON_UPDATED_DATE`
Object Type	Type of object you want to reconcile.
	Default value: `__PERSON__`
Latest Token	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The Latest Token parameter is used for internal purposes. By default, this value is empty.
	Note: Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute.
	Sample value: `1432623600000`
Scheduled Task Name	Name of the scheduled job used for reconciliation.
	Note: For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter.

Incremental Reconciliation Job

The Oracle EBS HRMS Target Incremental User Reconciliation job is used for performing incremental reconciliation.

Table 3-9   Oracle EBS HRMS Target Incremental User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application.
	Do not modify this value.

Table 3-9   (Cont.) Oracle EBS HRMS Target Incremental User Reconciliation Job

Parameter	Description
Sync Token	This parameter must be left blank when you run incremental reconciliation for the first time. This ensures that the connector fetches data about all records from the target system into Oracle Identity Governance.
	After the first reconciliation run, the connector automatically enters a value for this parameter in an XML serialized format. From the next reconciliation run onward, the connector fetches only data about records that are modified since the last reconciliation run into Oracle Identity Governance.
	Sample value: `<Long>1433010600000</Long>`
Object Type	Type of object you want to reconcile.
	Default value: `__PERSON__`
Scheduled Task Name	Name of the scheduled job.
	Note: For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.

Delete User Reconciliation Job

The Oracle EBS HRMS Target User Delete Reconciliation job is used to reconcile data about deleted person records in the target system. During a reconciliation run, for each deleted user account on the target system, the corresponding resource is revoked for the corresponding OIG User.

Table 3-10   Oracle EBS HRMS Target User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application.
	Do not modify this value.
Filter	Enter the expression for filtering deleted person records that the connector must reconcile.
	Sample value: `equalTo('__UID__','10533')`
	For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Developing and Customizing Applications for Oracle Identity Governance*.

Table 3-10   (Cont.) Oracle EBS HRMS Target User Delete Reconciliation Job

Parameter	Description
Object Type	Type of object you want to reconcile. **Default value:** __PERSON__

Reconciliation Jobs for Entitlements

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Job Id lookup field to select a job ID to be assigned from the list of job IDs in the lookup field. When you create the application, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Governance. The reconciliation jobs for entitlements are used for copying additions or changes made to the target system lookup fields into the corresponding lookup definitions in Oracle Identity Governance.

The following jobs are available for reconciling entitlements:

- Oracle EBS HRMS Target Jobs Lookup Reconciliation

- Oracle EBS HRMS Target Grades Lookup Reconciliation

- Oracle EBS HRMS Target Organization Lookup Reconciliation

- Oracle EBS HRMS Target Person Type Lookup Reconciliation

- Oracle EBS HRMS Target Address Type Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-11   Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.

Table 3-11   (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Lookup Name	This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which the connector must fetch values. Depending on the reconciliation job you are using, the default values are as follows: • For Oracle EBS HRMS Target Jobs Lookup Reconciliation- `Lookup.EBSHRMS.Jobs` • For Oracle EBS HRMS Target Grades Lookup Reconciliation- `Lookup.EBSHRMS.Grade` • For Oracle EBS HRMS Target Organization Lookup Reconciliation- `Lookup.EBSHRMS.Organization` • For Oracle EBS HRMS Target Person Type Lookup Reconciliation- `Lookup.EBSHRMS.PersonType` • For Oracle EBS HRMS Target Address Type Lookup Reconciliation- `Lookup.EBSHRMS.AddressType`
Object Type	Enter the type of object whose values must be synchronized. Depending on the reconciliation job you are using, the default values are as follows: • For Oracle EBS HRMS Target Jobs Lookup Reconciliation- `__JOBS__` • For Oracle EBS HRMS Target Grades Lookup Reconciliation- `__GRADES__` • For Oracle EBS HRMS Target Organization Lookup Reconciliation- `__ORGANIZATION__` • For Oracle EBS HRMS Target Person Type Lookup Reconciliation- `__PERSONTYPE__` • For Oracle EBS HRMS Target Address Type Lookup Reconciliation- `__ADDRESSTYPE__`
Code Key Attribute	Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). **Default value:** `CODE` **Note:** Do not change the value of this attribute.

Table 3-11   (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute).
	Default value: DECODE

4

Configuring the Oracle EBS Employee Reconciliation Connector for an Authoritative Application

You must configure connection-related parameters that the connector uses to connect Oracle Identity Governance with your target system and perform connector operations. In addition, you can view and edit mappings between reconciliation fields in Oracle Identity Governance and target system columns, predefined correlation rules, situations and responses, and reconciliation jobs.

- Basic Configuration Parameters for the EBS ER Connector
- Advanced Setting Parameters for the EBS ER Connector
- Attribute Mappings for the EBS ER Connector
- Correlation Rules for the EBS ER Connector
- Reconciliation Jobs for the EBS ER Connector

4.1 Basic Configuration Parameters for the EBS ER Connector

These are the connection-related parameters that Oracle Identity Governance requires to connect to your target system. These parameters are applicable for authoritative applications only.

Table 4-1   Parameters in the Basic Configuration Section for the EBS ER Connector

Parameter	Mandatory?	Description
Connection URL	Yes	Enter the database connection string using the `host:post:sid` syntax format.
		Default value: `jdbc:oracle:thin:@%h:%p:%d`
		See Determining Values for the JDBC URL and Connection Properties Parameters for more information about the supported JDBC URL formats and the value that you need to enter depending on the security measures that you have implemented.

Table 4-1   (Cont.) Parameters in the Basic Configuration Section for the EBS ER Connector

Parameter	Mandatory?	Description
User	Yes	Enter the user name of the target system account created while performing the Prerequisites for Creating an Application By Using Connector procedure. This user is used for various connector operations.
Password	Yes	Enter the password for the user name of the target system account to be used for connector operations.
Connector Server Name	No	If you are using a Connector Server, then enter the name of its IT resource.
Batch Size	No	Enter the number of records that the connector must include in each batch that it fetches from the target system during reconciliation. **Default value:** `1000`
Database	No	Enter the name of the target system database against which connector operations must be performed.
Host	No	Enter the host name or IP address where the database is running.
Include Future Hires	No	Specifies whether the connector must detect and reconcile records with future-dated Start Date values. If you set the value of this parameter to `true`, then the connector reconciles all employee records with future-dated start Date values. If you set the value of this parameter to `false`, then the connector does not reconcile employee records with future-dated Start Date values. **Default value:** `true`
Port	No	Enter the number of the port at which the target system database is listening.

4.2 Advanced Setting Parameters for the EBS ER Connector

These are the configuration-related entries that the connector uses during reconciliation and provisioning operations.

Table 4-2   Advanced Setting Parameters for the EBS ER Connector

Parameter	Mandatory?	Description
Bundle Version	Yes	This parameter hods the version of the connector bundle class. **Value:** `1.0.1116`
Connector Name	Yes	This parameter holds the name of the connector class. **Value:** `org.identityconnectors.ebs.EBSConnector`
Bundle Name	Yes	This parameter holds the name of the connector bundle package. **Value:** `org.identityconnectors.ebs`
Pool Max Idle	No	Enter the maximum number of idle objects in a pool. **Default value:** `10`
Pool Max Size	No	Enter the maximum number of connections that the pool can create. **Default value:** `10`
Pool Max Wait	No	Enter the maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. **Default value:** `150000`
Pool Min Evict Idle Time	No	Enter the minimum time, in milliseconds, the connector must wait before evicting an idle object. **Default value:** `120000`
Pool Min Idle	No	Enter the minimum number of idle objects in a pool. **Default value:** `1`

Table 4-2   (Cont.) Advanced Setting Parameters for the EBS ER Connector

Parameter	Mandatory?	Description
FilterDateAttributes	No	Enter the target system date attribute that the connector must use for filtering user records. If you want to enter more than one date attribute, then ensure to include them as a comma-separated list. **Default value:** `HIRE_DATE`
FilterDateAttributeFormat	No	Enter the format of the attribute specified as the value of the FilterDateAttributes parameter. **Default value:** `dd-MMM-yyyy`

4.3 Attribute Mappings for the EBS ER Connector

The Schema page for an Authoritative application displays the default schema (provided by the connector) that maps Oracle Identity Governance attributes to target system columns. The connector uses these mappings during reconciliation operations.

Table 4-3 lists the user-specific attribute mappings between the reconciliation fields in Oracle Identity Governance and target system columns. The table also lists the data type for a given attribute and specifies whether it is a mandatory attribute for reconciliation.

You may use the default schema that has been set for you or update and change it before continuing to the next step. You can edit the attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in Creating an Authoritative Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form that cannot be left blank during reconciliation. As there are no corresponding attributes in the target system for the Organization Name, Xellerate Type, and Role identity attributes, they have been mapped to attributes in Oracle identity Governance. In addition, the connector provides default values (as listed in the "Default Value for Identity Display Name" column of Table 4-3) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

Table 4-3   Oracle EBS HRMS Trusted User Account Schema Attributes

Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Default Value for Identity Display Name
Role	NA	String	No	Yes	Full-Time
National Identifier	NATIONAL_IDENTIFIER	String	No	Yes	NA
Business Group ID	BUSINESS_GROUP_ID	String	No	Yes	NA
First Name	FIRST_NAME	String	No	Yes	NA
PersonType	PERSON_TYPE_ID	String	No	Yes	NA
Supervisor Name	SUPERVISOR_NAME	String	No	Yes	NA
Nationality	NATIONALITY	String	No	Yes	NA
Supervisor ID	SUPERVISOR_ID	String	No	Yes	NA
Job	JOB	String	No	Yes	NA
Grade	GRADE	String	No	Yes	NA
Status	__ENABLE__	String	No	Yes	NA
Email	EMAIL_ADDRESS	String	No	Yes	NA
Xellerate Type	NA	String	No	Yes	End-User
End Date	ACTUAL_TERMINATION_DATE	Date	No	Yes	NA
User Login	__UID__	String	No	Yes	NA
Date Of Birth	DATE_OF_BIRTH	Date	No	Yes	NA
Title	TITLE	String	No	Yes	NA
Manager Login	SUPERVISOR_ID	String	No	No	NA
Start Date	HIRE_DATE	Date	No	Yes	NA
Organization Name	NA	String	No	Yes	Xellerate Users
Department	DEPARTMENT	String	No	Yes	NA
Last Name	LAST_NAME	String	No	Yes	NA
Person ID	PERSON_ID	String	No	Yes	NA
Marital Status	MARITAL_STATUS	String	No	Yes	NA

Figure 4-1 shows the default Oracle EBS HRMS Trusted User account attribute mappings.

Figure 4-1   Oracle EBS HRMS Trusted User Account Schema Attributes

4.4 Correlation Rules for the EBS ER Connector

When you create an Authoritative application, the connector uses correlation rules to determine the identity that must be reconciled into Oracle Identity Governance.

Predefined Identity Correlation Rules

By default, the EBS ER connector provides a simple correlation rule when you create a Authoritative application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

Table 4-4 lists the default simple correlation rule for an Oracle EBS HRMS Employee Reconciliation. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-4   Predefined Identity Correlation Rule for an Authoritative Application

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__UID__	Equals	User Login	No

In this identity rule:

- __UID__ is a single-valued attribute on the target system that identifies the user account.

- User Login is the field on the OIG User form.

Figure 4-2 shows the simple correlation rule for an Authoritative application.

Figure 4-2   Simple Correlation Rule for an Authoritative Application
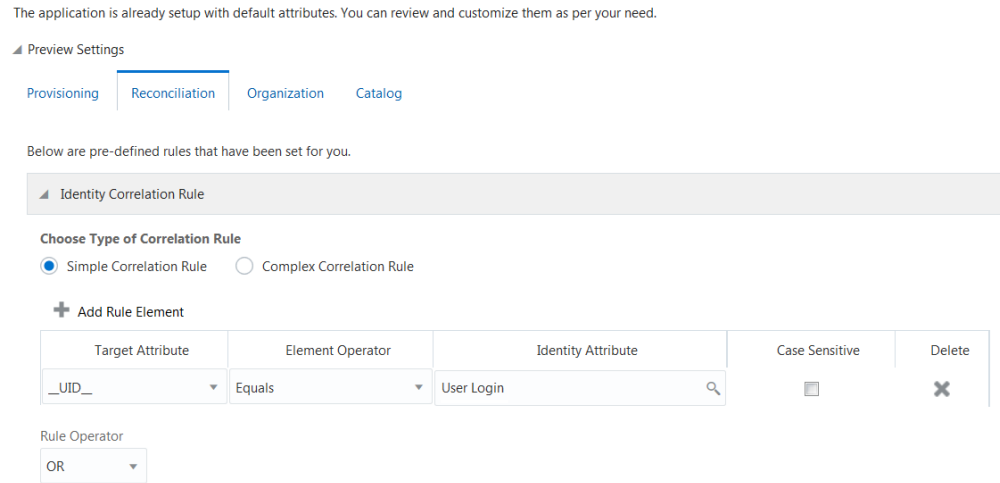
Predefined Situations and Responses

The EBS ER connector provides a default set of situations and responses when you create an Authoritative application. These situations and responses specify the action that Oracle Identity Governance must take based on the result of a reconciliation event.

Table 4-5 lists the default situations and responses for an Authoritative application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 4-5   Predefined Situations and Responses for an Authoritative Application

Situation	Response
No Matches Found	Create User
One Entity Match Found	Establish Link

Figure 4-3 shows the situations and responses for an Authoritative application that the connector provides by default.

Figure 4-3   Predefined Situations and Responses for an Authoritative Application
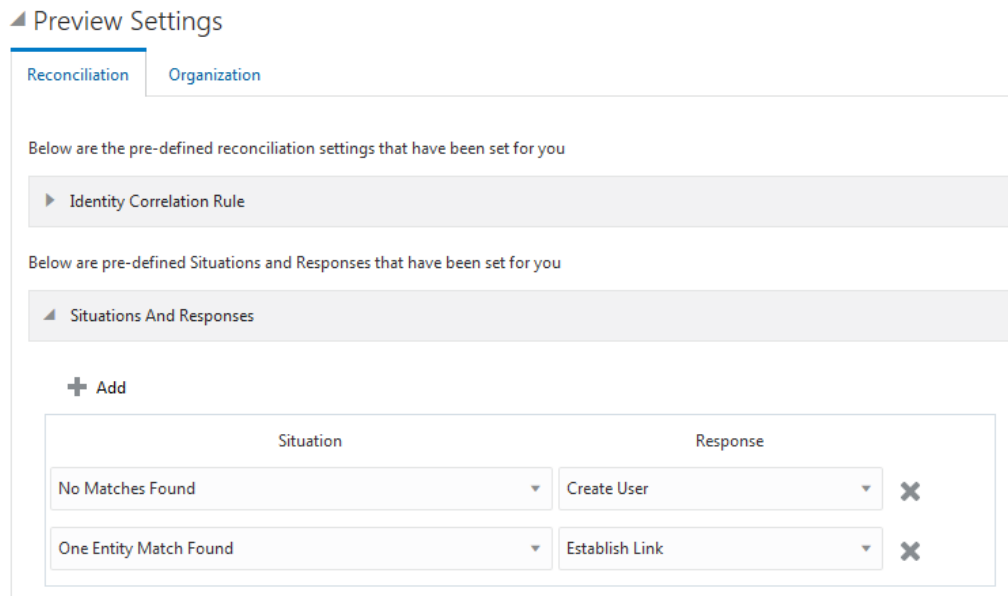
4.5 Reconciliation Jobs for the EBS ER Connector

These are the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application for your target system.

You can either use these predefined jobs or edit them to meet your requirements. Alternatively, you can create custom reconciliation jobs. For information about editing these predefined jobs or creating new ones, see Updating Reconciliation Jobs in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Full Reconciliation Job

The Oracle EBS HRMS Trusted User Reconciliation job is used to reconcile all person records for an authoritative application.

Table 4-6   Parameters of the Oracle EBS HRMS Trusted User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your authoritative application. Do not modify this value.
Filter	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: `equalTo('__UID__','10533')` For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Developing and Customizing Applications for Oracle Identity Governance*.
Incremental Recon Attribute	Enter the name of the target system attribute that holds the timestamp at which the person record was modified. **Sample value:** `PERSON_UPDATED_DATE`
Object Type	Type of object you want to reconcile. **Default value:** `__PERSON__`
Latest Token	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The Latest Token parameter is used for internal purposes. By default, this value is empty. **Note:** Do not enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute.
Scheduled Task Name	Name of the scheduled job that is used for reconciliation. **Note:** For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.

Incremental Reconciliation Job

The Oracle EBS HRMS Trusted Incremental User Reconciliation job is used for performing incremental reconciliation.

Table 4-7   Oracle EBS HRMS Trusted Incremental User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your authoritative application. Do not modify this value.
Sync Token	This attribute must be left blank when you run incremental reconciliation for the first time. This ensures that data about all records from the target system are fetched into Oracle Identity Governance. After the first reconciliation run, the connector automatically enters a value for this attribute in an XML serialized format. From the next reconciliation run onward, only data about records that are modified since the last reconciliation run ended are fetched into Oracle Identity Governance.
Object Type	Type of object you want to reconcile. Default value: __PERSON__
Scheduled Task Name	Name of the scheduled job used for reconciliation. **Note:** For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.

Delete Reconciliation Job

The Oracle EBS HRMS Trusted User Delete Reconciliation job is used to reconcile data about deleted person records in the target system. During a reconciliation run, for each deleted user account on the target system, the corresponding OIG User is deleted.

Table 4-8   Oracle EBS HRMS Trusted User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your authoritative application. Do not modify this value.

Table 4-8   (Cont.) Oracle EBS HRMS Trusted User Delete Reconciliation Job

Parameter	Description
Filter	Enter the expression for filtering deleted person records that the connector must reconcile.
	Sample value: `equalTo('__UID__','10533')`
	For information about the filters expressions that you can create and use, see ICF Filter Syntax in *Developing and Customizing Applications for Oracle Identity Governance*.
Object Type	Type of object you want to reconcile.
	Default value: `__PERSON__`
Search Type	Type of search operation to perform during reconciliation.
	Default value: `delete`
	Note: Do not modify this value.

5

Performing the Postconfiguration Tasks for the Oracle E-Business Suite HRMS Connectors

These are the tasks that you must perform after creating an application in Oracle Identity Governance.

- Configuring Oracle Identity Governance
- Harvesting Entitlements and Syncing the Catalog
- Configuring Secure Communication Between the Target System and Oracle Identity Governance
- Determining Values for the JDBC URL and Connection Properties Parameters
- Managing Logging
- Localizing Field Labels in UI Forms
- Removing the Default Validation Check for Provisioning Operations

5.1 Configuring Oracle Identity Governance

During application creation, if you did not choose to create a default form, then you must create a UI form for the application that you created by using the connector.

> ✎ **Note:**
>
> Perform the procedures described in this section only if you did not choose to create the default form during creating the application.

The following topics describe the procedures to configure Oracle Identity Governance:

- Creating and Activating a Sandbox
- Creating a New UI Form
- Publishing a Sandbox
- Updating an Existing Application Instance with a New Form

5.1.1 Creating and Activating a Sandbox

You must create and activate a sandbox to begin using the customization and form management features. You can then publish the sandbox to make the customizations available to other users.

See Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

5.1.2 Creating a New UI Form

You can use Form Designer in Oracle Identity System Administration to create and manage application instance forms.

See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

While creating the UI form, ensure that you select the resource object corresponding to the newly created application that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box.

5.1.3 Publishing a Sandbox

Before publishing a sandbox, perform this procedure as a best practice to validate all sandbox changes made till this stage as it is difficult to revert the changes after a sandbox is published.

1. In Identity System Administration, deactivate the sandbox.

2. Log out of Identity System Administration.

3. Log in to Identity Self Service using the xelsysadm user credentials and then activate the sandbox that you deactivated in Step 1.

4. In the Catalog, ensure that the application instance form for your resource appears with correct fields.

5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

5.1.4 Updating an Existing Application Instance with a New Form

For any changes that you do in the schema of your application in Identity Self Service, you must create a new UI form and update the changes in an application instance.

To update an existing application instance with a new form:

1. Create and activate a sandbox.

2. Create a new UI form for the resource.

3. Open the existing application instance.

4. In the Form field, select the new UI form that you created.

5. Save the application instance.

6. Publish the sandbox.

> **See Also:**
>
> - Creating a Sandbox and Activating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*
>
> - Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Governance*
>
> - Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*

5.2 Harvesting Entitlements and Syncing the Catalog

You can populate Entitlement schema from child process form table, and harvest addresses, assignments, application instances, and entitlements into catalog. You can also load catalog metadata.

To harvest entitlements and sync catalog:

1. If you are using the Oracle EBS HRMS connector, then run the reconciliation jobs for entitlements.

2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.

3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about this scheduled job.

> **See Also:**
>
> - Reconciliation Jobs for the EBS HRMS Connector for the list of jobs for entitlements
>
> - Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for information about the Entitlement List and Catalog Synchronization Job scheduled jobs

5.3 Configuring Secure Communication Between the Target System and Oracle Identity Governance

It is recommended that you configure SSL to secure the communication between your target system and Oracle Identity Governance.

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

- Configuring Data Encryption and Integrity
- Configuring SSL Communication

5.3.1 Configuring Data Encryption and Integrity

You can protect data against active attacks and ensure data privacy by configuring native Oracle Net Services data encryption and integrity for Oracle Advanced Security.

To configure data encryption and integrity, see Data Encryption in *Oracle Database Advanced Security Administrator's Guide* .

5.3.2 Configuring SSL Communication

You configure SSL to secure data communication between Oracle Identity Governance and the target system.

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

1. See Secure Socket Layer in *Oracle Database Advanced Security Administrator's Guide* for information about enabling SSL communication between Oracle Database and Oracle Identity Governance.

2. Export the certificate on the Oracle Database host computer.

3. Copy the certificate to Oracle Identity Governance.

4. Import the certificate into the JVM certificate store of the application server on which Oracle Identity Governance 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 5-1. This table shows the location of the certificate store for each of the supported application servers.

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

Table 5-1   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

5.4 Determining Values for the JDBC URL and Connection Properties Parameters

This section discusses the JDBC URL and Connection Properties parameters.

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

• Supported JDBC URL Formats

• Only SSL Communication Is Configured

• Both Data Encryption and Integrity and SSL Communication Are Configured

5.4.1 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

5.4.2 Only SSL Communication Is Configured

After you configure SSL communication between Oracle Identity Governance and your target system, the database URL is recorded in the tnsnames.ora file.

See Local Naming Parameters in the tnsnames.ora File in *Oracle Database Net Services Reference* for detailed information about the tnsnames.ora file.

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

Sample Format 1:

```
NET_SERVICE_NAME=
 (DESCRIPTION=
```

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

Sample Format 2:

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

Sample Format 3:

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

If you have configured only SSL communication and imported the certificate that you create on the target system host computer into the JVM certificate store of Oracle Identity Governance, then you must derive the value for the Connection URL parameter from the value of NET_SERVICE_NAME in the tnsnames.ora file. For example:

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

> **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.

5.4.3 Both Data Encryption and Integrity and SSL Communication Are Configured

If both data encryption and integrity and SSL communication are configured, then specify a value for the JDBC URL parameter in the following manner:

Enter a comma-separated combination of the values for the JDBC URL parameter described in Only SSL Communication Is Configured. For example:

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

5.5 Managing Logging

Oracle Identity Governance uses the Oracle Diagnostic Logging (ODL) logging service for recording all types of events pertaining to the connector.

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling logging

5.5.1 Understanding Log Levels

When you enable logging, Oracle Identity Governance automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations.

ODL is the principle logging service used by Oracle Identity Governance and is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Governance to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the application.

- CONFIG

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

- FINE, FINER, FINEST

These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These message types are mapped to ODL message type and level combinations as shown in Table 5-2.

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

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

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

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

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

5.5.2 Enabling logging

Perform these steps to enable logging in Oracle WebLogic Server.

1. Edit the logging.xml file as follows:

    a. Add the following blocks in the file:

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

    <logger name='ORG.IDENTITYCONNECTORS.EBS' level='[LOG_LEVEL]'
    useParentHandlers='false'>
          <handler name='ebs-handler'/>
          <handler name='console-handler'/>
       </logger>
    ```

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

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

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

```
<log_handler name='ebs-handler' level='TRACE:32'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
     <property name='logreader:' value='off'/>
     <property name='path' value='/scratch/acme1/user1/oim_Jun25.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>
</log_handlers>

<loggers>
   <logger name='ORG.IDENTITYCONNECTORS.EBS' level='TRACE:32'
useParentHandlers='false'>
     <handler name='ebs-handler'/>
     <handler name='console-handler'/>
   </logger>
```

With these sample values, when you use Oracle Identity Governance, all messages generated for this connector that are of a log level equal to or higher than the TRACE:32 level are recorded in the specified file.

2. Save and close the file.

3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

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

4. Restart the application server.

5.6 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. The resource bundles are available in the connector installation media.

To localize field label that you add in UI forms:

1. Log in to Oracle Enterprise Manager.

2. In the left pane, expand Application Deployments and then select **oracle.iam.console.identity.sysadmin.ear.**

3. In the right pane, from the Application Deployment list, select **MDS Configuration.**

4. On the MDS Configuration page, click **Export** and save the archive (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer.

5. Extract the contents of the archive, and open the following file in a text editor:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf

   > **Note:**
   >
   > You will not be able to view the BizEditorBundle.xlf unless you complete creating the application for your target system or perform any customization such as creating a UDF.

6. Edit the BizEditorBundle.xlf file in the following manner:

   a. Search for the following text:

   ```
   <file source-language="en"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   b. Replace with the following text:

   ```
   <file source-language="en" target-language="LANG_CODE"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   In this text, replace *LANG_CODE* with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

   ```
   <file source-language="en" target-language="ja"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   c. Search for the application instance code. This procedure shows a sample edit for Oracle E-Business Suite application instance. The original code is:

   ```
   <trans-unit id="$
   {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
   e']
   ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
   UD_EBS_HRMS_EMPNO__c_description']}">
   <source>Employee Number</source>
   <target/>
   </trans-unit>
   <trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.EBSHRMSForm1.entity.EBSHR
   MSForm1EO.UD_EBS_HRMS_EMPNO__c_LABEL">
   <source>Employee Number</source>
   <target/>
   ```

   d. Open the resource file (for example, EBS-HRMS.properties) from the connector package, and get the value of the attribute from the file, for example, global.udf.UD_EBS_HRMS_EMPNO=\u4567d.

   e. Replace the original code shown in Step 6.c with the following:

   ```
   <trans-unit id="$
   {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
   e']
   ```

```
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_EBS_HRMS_EMPNO__c_description']}">
<source>Employee Number</source>
<target>\u5F93\u696D\u54E1\u756A\u53F7</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.EBSHRMSForm1.entity.EBSHR
MSForm1EO.UD_EBS_HRMS_EMPNO__c_LABEL">
<source>Employee Number</source>
<target>\u5F93\u696D\u54E1\u756A\u53F7</target>
</trans-unit>
```

f. Repeat Steps 6.a through 6.d for all attributes of the process form.

g. Save the file as BizEditorBundle_*LANG_CODE*.xlf. In this file name, replace *LANG_CODE* with the code of the language to which you are localizing.

Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

> ✎ **See Also:**
>
> Deploying and Undeploying Customizations in *Developing and Customizing Applications for Oracle Identity Governance,* for more information about exporting and importing metadata files

8. Log out of and log in to Oracle Enterprise Manager.

5.7 Removing the Default Validation Check for Provisioning Operations

During a provisioning operation for child data, the connector API validates data against a combination of the Grade Id, Department Id, and Organization Id fields. If this valid combination is not found, an error is encountered and the provisioning operation fails.

If you do not want to use this strict validation, then you must remove the default validation check to perform the provisioning operation successfully. To do so:

1. Open any SQL client. For example, SQL Developer.

2. Open the body of the OIM_EMPLOYEE_WRAPPER.pck wrapper package.

3. Comment out the following lines of code by prefixing them with a double hyphen (--):

```
    IF create_person_assignment_api.grade_id IS NOT NULL THEN
        select count(*) into validcount from PER_VALID_GRADES where
business_group_id =create_person_assignment_api.organization_id
        and job_id=create_person_assignment_api.job_id and
grade_id=create_person_assignment_api.grade_id;
        if validcount = 0 then
          raise_application_error (-20001, 'Invalid combination of
organization, job and grade');
        end if;
    ELSE
        select count(*) into valid_job_count from PER_JOBS where job_id =
create_person_assignment_api.job_id;
```

```
           if valid_job_count = 0 then
               raise_application_error (-20001, 'Invalid combination of
organization, job and grade');
           end if;
      END IF;
```

4. Re-compile the wrapper package.

As an alternative to this procedure, you can edit the
scripts\OIM_EMPLOYEE_WRAPPER.pck file by commenting out the lines of code and
then running either the Run_HRMS_DBScripts.sh or Run_HRMS_DBScripts.bat file.

6

Using the Oracle E-Business Suite HRMS Connectors

You can use the Oracle E-Business Suits HRMS Connectors for performing reconciliation and provisioning operations after configuring your application to meet your requirements.

This chapter contains the following sections:

- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Performing Provisioning Operations
- Uninstalling the Connector

> **Note:**
>
> Perform sections Configuring Reconciliation Jobs and Performing Provisioning Operations if you are using the EBS HRMS connector only.

6.1 Configuring Reconciliation

You can configure the connector to specify the type of reconciliation and its schedule.

- Performing Full and Incremental Reconciliation
- Performing Limited Reconciliation
- Performing Batched Reconciliation

6.1.1 Performing Full and Incremental Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance. During incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

After you create the application, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Governance.

To perform a full reconciliation, remove (delete) any value assigned to the Latest Token and Filter parameters and run one of the following reconciliation jobs:

- For an Oracle EBS HRMS application: Oracle EBS HRMS Target User Reconciliation

- For an Oracle EBS Employee Reconciliation application: Oracle EBS HRMS Trusted User Reconciliation

To perform an incremental reconciliation run for the first time, remove (delete) any value assigned to the Sync Token parameter and run of the following reconciliation jobs:

- For an Oracle EBS HRMS application: Oracle EBS HRMS Target Incremental User Reconciliation

- For an Oracle EBS Employee Reconciliation application: Oracle EBS HRMS Trusted Incremental User Reconciliation

This ensures that the connector fetches data about all records from the target system into Oracle Identity Governance. From the next run onward, only records created or modified after the value in the Sync Token attribute are considered for reconciliation.

See Reconciliation Jobs for the EBS HRMS Connector and Reconciliation Jobs for the EBS ER Connector for information about the jobs for full and incremental reconciliation.

6.1.2 Performing Limited Reconciliation

You can perform limited reconciliation by creating filters for the reconciliation module, and reconcile records from the target system based on a specified filter criterion.

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 can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a Filter parameter (a reconciliation job parameter) that allows you to use any of the Oracle EBS HRMS User resource attributes to filter the target system records.

When you specify a value for the Filter parameter, the connector reconciles only the target system records that match the filter criterion into Oracle Identity Governance. If you do not specify a value for the Filter parameter, then the connector reconciles all the records in the target system into Oracle Identity Governance.

You specify a value for the Filter attribute while configuring the user reconciliation scheduled job.

The following is an example of a filter for a search where you want to filter only those accounts whose first name is "John":

```
equalTo('FIRST_NAME','JOHN')
```

For detailed information about ICF Filters, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance.*

6.1.3 Performing Batched Reconciliation

You can perform batched reconciliation to reconcile a specific number of records from the target system into Oracle Identity Governance.

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Governance. Depending on the number of records to be reconciled,

this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete. You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify a value for the Batch Size parameter of the Basic Configuration section. Use this parameter to specify the number of records that the connector must include in each batch. By default, this value is set to `1000`.

When you specify `All` as the value of this parameter, the connector fetches all the records into Oracle Identity Governance. If you specify a value other than `All`, then some of the newly added or modified user records may not get reconciled during the current reconciliation run. The following example illustrates this:

Suppose you specify the Batch Size value as `200`. Now suppose that 314 user records were created or modified after the last reconciliation run. Of these 314 records, only 200 records would be reconciled during the current reconciliation run. The remaining 114 records would be reconciled during the next reconciliation run.

6.2 Configuring Reconciliation Jobs

Configure reconciliation jobs to perform reconciliation runs that check for new information on your target system periodically and replicates the data in Oracle Identity Governance.

You can apply this procedure to configure the reconciliation jobs for users and entitlements.

To configure a reconciliation job:

1. Log in to Identity System Administration.

2. In the left pane, under System Management, click **Scheduler**.

3. Search for and open the scheduled job as follows:

    a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

    b. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. On the Job Details tab, you can modify the parameters of the scheduled task:

    • **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

    • **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

    In addition to modifying the job details, you can enable or disable a job.

5. On the **Job Details** tab, in the Parameters region, specify values for the attributes of the scheduled task.

> **Note:**
>
> 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.

6. Click **Apply** to save the changes.

> **Note:**
>
> You can use the Scheduler Status page in Identity System Administration to either start, stop, or reinitialize the scheduler.

6.3 Performing Provisioning Operations

You create a new user in Identity Self Service by using the Create User page. You provision or request for accounts on the Accounts tab of the User Details page.

To perform provisioning operations in Oracle Identity Governance:

1. Log in to Identity Self Service.

2. Create a user as follows:

   a. In Identity Self Service, click **Manage**. The Home tab displays the different Manage option. Click **Users**. The Manage Users page is displayed.

   b. From the Actions menu, select **Create**. Alternatively, you can click **Create** on the toolbar. The Create User page is displayed with input fields for user profile attributes.

   c. Enter details of the user in the Create User page.

3. On the Account tab, click **Request Accounts**.

4. In the Catalog page, search for and add to cart the application instance for the connector that you configured earlier, and then click **Checkout**.

5. Specify value for fields in the application form and then click **Ready to Submit**.

6. Click **Submit**.

> **See Also:**
>
> Creating a User in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance* for details about the fields on the Create User page

6.4 Uninstalling the Connector

Uninstalling the connector deletes all the account-related data associated with its resource objects.

If you want to uninstall the connector for any reason, then run the Uninstall Connector utility. Before you run this utility, ensure that you set values for `ObjectType` and `ObjectValues` properties in the ConnectorUninstall.properties file. For example, if you want to delete resource objects, scheduled tasks, and scheduled jobs associated with the connector, then enter `"ResourceObject"`, `"ScheduleTask"`, `"ScheduleJob"` as the value of the `ObjectType` property and a semicolon-separated list of object values corresponding to your connector (for example, `GoogleApps User; GoogleApps Group`) as the value of the `ObjectValues` property.

> **Note:**
>
> If you set values for the `ConnectorName` and `Release` properties along with the `ObjectType`and `ObjectValue` properties, then the deletion of objects listed in the `ObjectValues` property is performed by the utility and the Connector information is skipped.

For more information, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

7

Extending the Functionality of the Oracle E-Business Suite HRMS Connectors

You can extend the functionality of the connectors to address your specific business requirements.

This chapter contains the following sections:

7.1 Understanding Connector Schema Extension

By default, this connector provides a set of attribute mappings that can be used for reconciliation and provisioning operations between Oracle Identity Governance and the target system. Depending on your business requirements, you can add and map additional attributes for reconciliation and provisioning operations. You can extend the connector schema by adding new attributes to the get_schema() stored procedure in the OIM_EMPLOYEE_WRAPPER.pck wrapper package.

Extending the connector schema requires you to understand the following concepts:

- **Attribute initialization**

  The following initialization statement reserves an internal array that holds attribute definitions of the connector schema:

  ```
  attr.extend(NUM);
  ```

  Here, *NUM* defines the size of the array that is to be initialized. The size of the array must always be greater than or equal to the number of attributes defined. For example, the initialization statement `attr.extend(20);` reserves an internal array of 20 attributes for initialization.

- **Attribute definition**

  After initialization, you define the information for each attribute by adding a statement in the following format:

  attr (*ORD_NO*) := attributeinfo(*ATTR_NAME*,*ATTR_TYPE*,*CREATE_FLAG*,*UPDATE_FLAG*,*REQUIRED_FLAG*,*READ_FLAG*);

  In this format:

- *ORD_NO* is the order of the attribute in the array. This is mandatory.

- *ATTR_NAME* is the name of the child or single-valued attribute.

- *ATTR_TYPE* is the SQL datatype of the child or single-valued attribute.

- *CREATE_FLAG* is a flag to represent whether the attribute is required during a create provisioning operation.

- *UPDATE_FLAG* is a flag to represent whether the attribute can be updated.

- *REQUIRED_FLAG* is a flag to represent whether the attribute is mandatory.

- *READ_FLAG* is flag to represent whether the attribute can be read.

A value of `1` or `0` for each flag denotes True or False, respectively. For example, a value `1, 0, 1, 0` for the flags means that the attribute is a mandatory attribute and must be considered during create provisioning operations.

- **Attribute array extension**

You can increase the array size post initialization by including the following statement:

```
attr.extend;
```

Each inclusion of this statement increments the array size by 1.

7.2 Adding New Attributes to an Authoritative Application

By default, the attributes listed on the Schema page at the time of application creation are mapped for reconciliation between Oracle Identity Governance and the target system. If required, you can map additional attributes to you authoritative application for trusted source reconciliation.

The following sections describe the procedures to be performed for adding new attributes:

- Adding New Attributes on the Schema Page for an Authoritative Application
- Updating the DB Wrapper Package
- Updating the search.properties File for an Authoritative Application
- Updating the Connector Bundle

7.2.1 Adding New Attributes on the Schema Page for an Authoritative Application

While creating an Authoritative application, you can view the default attribute mappings between Oracle Identity Governance attributes and target system columns on the Schema page. If required, you can add new attributes.

To do so, see Providing Schema Information for Authoritative Application in *Performing Self Service Tasks with Oracle Identity Governance*.

7.2.2 Updating the DB Wrapper Package

You must extend the connector schema by updating the DB wrapper package to include the new attribute for your application.

1. Open any SQL client. For example, SQL Developer.

2. Open the body of the **OIM_EMPLOYEE_WRAPPER.pck** wrapper package.

3. Select the **get_schema()** stored procedure. The list of attributes defined in the stored procedure is displayed.

4. If the number of attributes defined exceeds the number of attributes initialized, then:

   a. Add the following attribute initialization statement:

      ```
      attr.extend;
      ```

   b. Enter the definition for the new attribute that you want to add in the following format:

      attr (*ORD_NO*) := attributeinfo(*ATTR_NAME*,*ATTR_TYPE*,*CREATE_FLAG*,*UPDATE_FLAG*,*REQUIRED_FLAG*,*READ_FLAG*);

      For example, if you are adding a new attribute to hold the blood type for a user account, then include the following statements:

      ```
      attr.extend;
      attr (28) := attributeinfo('BLOOD_TYPE','varchar2',1,1,0,1);
      ```

      In this example, a value of `1,1,0,1` for the flags means that the BLOOD_TYPE attribute is required during create provisioning operations, it can be updated and read.

      > ✎ **See Also:**
      >
      > Understanding Connector Schema Extension for more information about format in which you must add the new attribute definition

5. If the number of attributes defined does not exceed the number of attributes initialized then add only the definition for the new attribute. For example, `attr (28) := attributeinfo('BLOOD_TYPE','varchar2',1,1,0,1);`

6. Re-compile the wrapper package.

7.2.3 Updating the search.properties File for an Authoritative Application

You must update the search.properties to include the newly added attribute in the corresponding SQL query.

1. Extract the contents of the org.identityconnectors.ebs-12.3.0.jar file (located in the /bundle directory of the connector installation package) into a directory of your choice.

2. In a text editor, open the search.properties located in the configuration directory.

3. Search for the SQL query that must include the column name corresponding to the newly created attribute. For example, search for the HRMS_CURRENT_EMPLOYEE_RECON_QUERY query.

4. If the SQL query already contains the column name corresponding to the newly added attribute, then you can skip the rest of the steps mentioned in this section.

5. If the SQL query does not include information about the newly added column name, then modify it to include this information. For example, modify the HRMS_CURRENT_EMPLOYEE_RECON_QUERY query (search op) to include `PAPF.BLOOD_TYPE AS blood_type`. The Blood Type attribute is present in the PER_ALL_PEOPLE_F table and PAPF is the table alias.

6. Repeat Steps 3 through 5 to update the remaining SQL queries such as HRMS_CURRENT_FUTURE_EMPLOYEE_RECON_QUERY (for both search and sync ops), and HRMS_CURRENT_EMPLOYEE_RECON_QUERY (sync op), if applicable. For example, update the HRMS_CURRENT_EMPLOYEE_RECON_QUERY and HRMS_CURRENT_FUTURE_EMPLOYEE_RECON_QUERY queries with the SQL queries listed in Sample SQL Queries for the EBS ER Connector.

7. Save the changes and close the file.

8. Verify the updated queries.

7.2.4 Updating the Connector Bundle

You must update the connector bundle (org.identityconnectors.ebs-12.3.0.jar) to include all the updates made to the Schema page, DB wrapper package, and the properties file.

1. Update the connector bundle (org.identityconnectors.ebs-12.3.0.jar) by running the following command:

```
jar -cvfm org.identityconnectors.ebs-12.3.0.jar META-INF/MANIFEST.MF *
```

2. Run the Oracle Identity Governance Update JARs utility to replace the existing connector bundle with the updated connector bundle in the Oracle Identity Governance database. This utility is copied into the following location when you install Oracle Identity Governance:

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

For Microsoft Windows:

OIM_HOME/server/bin/UpdateJars.bat

For UNIX:

OIM_HOME/server/bin/UpdateJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Governance administrator, URL of the Oracle Identity Governance host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 4 as the value of the JAR type.

3. Restart Oracle Identity Governance after the connector bundle JAR is updated successfully.

7.3 Adding New Attributes to an Target Application

By default, the attributes listed on the Schema page at the time of application creation are mapped for reconciliation between Oracle Identity Governance and the target system. If required, you can map additional attributes to your Target application for target resource reconciliation and provisioning operations.

The following sections describe the procedures to be performed for adding new attributes:

- Adding New Attributes on the Schema Page for a Target Application
- Updating the DB Wrapper Package
- Updating the search.properties File
- Updating the Connector Bundle
- Updating the Procedures.properties File for a Target Application

7.3.1 Adding New Attributes on the Schema Page for a Target Application

While creating a Target application, you can view the default attribute mappings between Oracle Identity Governance attributes and target system columns on the Schema page. If required, you can add new attributes.

To do so, see Providing Schema Information for Target Application in *Performing Self Service Tasks with Oracle Identity Governance*.

7.3.2 Updating the DB Wrapper Package

You must extend the connector schema by updating the DB wrapper package to include the new attribute for your application.

1. Open any SQL client. For example, SQL Developer.

2. Open the body of the **OIM_EMPLOYEE_WRAPPER.pck** wrapper package.

3. Select the **get_schema()** stored procedure. The list of attributes defined in the stored procedure is displayed.

4. If the number of attributes defined exceeds the number of attributes initialized, then:

   a. Add the following attribute initialization statement:

   ```
   attr.extend;
   ```

b. Enter the definition for the new attribute that you want to add in the following format:

attr (*ORD_NO*) := attributeinfo(*ATTR_NAME*,*ATTR_TYPE*,*CREATE_FLAG*,*UPDATE_FLAG*,*REQUIRED_FLAG*,*READ_FLAG*);

For example, if you are adding a new attribute to hold the blood type for a user account, then include the following statements:

```
attr.extend;
attr (28) := attributeinfo('BLOOD_TYPE','varchar2',1,1,0,1);
```

In this example, a value of `1,1,0,1` for the flags means that the BLOOD_TYPE attribute is required during create provisioning operations, it can be updated and read.

> **✎ See Also:**
>
> Understanding Connector Schema Extension for more information about format in which you must add the new attribute definition

5. If the number of attributes defined does not exceed the number of attributes initialized then add only the definition for the new attribute. For example, `attr (28) := attributeinfo('BLOOD_TYPE','varchar2',1,1,0,1);`

6. Re-compile the wrapper package.

7.3.3 Updating the search.properties File

You must update the search.properties file to include the newly added attribute in the corresponding SQL query.

1. Extract the contents of the org.identityconnectors.ebs-12.3.0.jar file (located in the /bundle directory of the connector installation package) into a directory of your choice.

2. In a text editor, open the search.properties located in the configuration directory.

3. Search for the SQL query that must include the column name corresponding to the newly created attribute. For example, search for the TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUERY query.

4. If the SQL query already contains the column name corresponding to the newly added attribute, then you can skip the rest of the steps mentioned in this section.

5. If the SQL query does not include information about the newly added column name, then modify it to include this information. For example, modify the TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUERY query (search op) to include `PAPF.BLOOD_TYPE AS blood_type`. The Blood Type attribute is present in the PER_ALL_PEOPLE_F table and PAPF is the table alias.

See Sample SQL Queries for the EBS HRMS Connector for a sample query that includes the Blood Type column in the TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUERY queries.

6. Repeat Steps 3 through 5 to update the remaining SQL queries such as TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUERY (sync op) and

HRMS_TERMINATED_EMPLOYEE_RECON_QUERY, if applicable. For example, modify the TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUERY SQL query to include `PAPF.BLOOD_TYPE AS blood_type` and `person.BLOOD_TYPE` in the select query.

7. Save the changes and close the file.

8. Verify the updated queries.

7.3.4 Updating the Connector Bundle

You must update the connector bundle (org.identityconnectors.ebs-12.3.0.jar) to include all the updates made to the Schema page, DB wrapper package, and the properties file.

1. Update the connector bundle (org.identityconnectors.ebs-12.3.0.jar) by running the following command:

```
jar -cvfm org.identityconnectors.ebs-12.3.0.jar META-INF/MANIFEST.MF *
```

2. Run the Oracle Identity Governance Update JARs utility to replace the existing connector bundle with the updated connector bundle in the Oracle Identity Governance database. This utility is copied into the following location when you install Oracle Identity Governance:

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

For Microsoft Windows:

OIM_HOME/server/bin/UpdateJars.bat

For UNIX:

OIM_HOME/server/bin/UpdateJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Governance administrator, URL of the Oracle Identity Governance host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 4 as the value of the JAR type.

3. Restart Oracle Identity Governance after the connector bundle JAR is updated successfully.

7.3.5 Updating the Procedures.properties File for a Target Application

In order to support the newly added attribute during create and update provisioning operations, you must update the stored procedure that is invoked in the Procedures.properties file.

1. In a text editor, open the Procedures.properties file for editing.

2. Search for and determine the names of wrapper packages and stored procedures used for invoking the create person and update person provisioning operations. For example, **OIM_EMPLOYEE_WRAPPER.CREATE_PERSON_API** and **OIM_EMPLOYEE_WRAPPER.UPDATE_PERSON_API** are the wrapper packages and stored procedures used for the create person and update person provisioning operations.

3. Update the stored procedures determined in the earlier step as follows:

   a. Open any SQL client. For example, SQL Developer.

   b. Open the wrapper package and add the newly added attribute (for example, Blood Type) to the create person and update person stored procedures. For example, open the OIM_EMPLOYEE_WRAPPER package and add the newly added attribute to the CREATE_PERSON_API and UPDATE_PERSON_API stored procedures.

   Figure 7-1 highlights the stored procedures that must be updated in the OIM_EMPLOYEE_WRAPPER package to include the newly added attribute.

   Figure 7-1   Stored Procedures To Be Updated in OIM_EMPLOYEE_WRAPPER Package
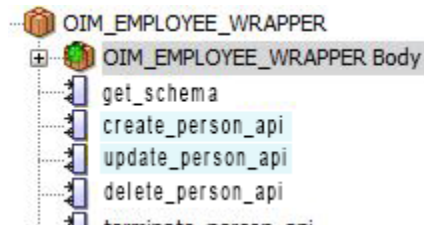
   c. Select the CREATE_PERSON_API stored procedure and update the input parameters to include the newly added attribute.

   Figure 7-2 highlights the newly added attribute in both the CREATE_PERSON_API and UPDATE_PERSON_API stored procedures.

Figure 7-2   Stored Procedures with the Newly Added Attribute

   d. Open **OIM_EMPLOYEE_WRAPPER Body** and select the **CREATE_PERSON_API** stored procedure.

   e. Update the HR_EMPLOYEE_API.create_employee API call in the procedure with the newly added attribute.

   Figure 7-3 shows the updated HR_EMPLOYEE_API.create_employee API.

Figure 7-3   HR_EMPLOYEE_API.create_employee API with the Newly Added Attribute

```
HR_EMPLOYEE_API.create_employee(p_hire_date                  => hire_date,
                                p_business_group_id          => business_group_id,
                                p_last_name                  => last_name,
                                p_first_name                 => first_name,
                                p_sex                        => sex,
                                p_person_type_id             => person_type_id,
                                p_employee_number            => employee_number,
                                p_person_id                  => person_id,
                                p_full_name                  => l_full_name,
                                p_assignment_id              => l_assignment_id,
                                p_assignment_sequence        => l_assignment_sequence,
                                p_assignment_number          => l_assignment_number,
                                p_per_object_version_number  => l_per_object_version_number,
                                p_asg_object_version_number  => l_asg_object_version_number,
                                p_per_effective_start_date   => l_effective_start_date,
                                p_per_effective_end_date     => l_effective_end_date,
                                p_per_comment_id             => l_comment_id,
                                p_name_combination_warning   => l_name_combination_warning,
                                p_assign_payroll_warning     => l_assign_payroll_warning,
                                p_orig_hire_warning          => l_orig_hire_warning,
                                p_title                      => title,
                                p_email_address              => email_address,
                                p_marital_status             => marital_status,
                                p_nationality                => nationality,
                                p_national_identifier        => national_identifier,
                                p_date_of_birth              => date_of_birth,
                                p_town_of_birth              => town_of_birth,
                                p_region_of_birth            => region_of_birth,
                                p_blood_type                    blood_type
```

f.   Update the HR_CONTINGENT_WORKER_API.create_cwk API call in the procedure with the newly added attribute.

Figure 7-4 shows the updated HR_CONTINGENT_WORKER_API.create_cwk API.

Figure 7-4   HR_CONTINGENT_WORKER_API.create_cwk API with the Newly Added Attribute

```
HR_CONTINGENT_WORKER_API.create_cwk(p_validate                  => FALSE,
                                    p_start_date                => hire_date,
                                    p_business_group_id         => business_group_id,
                                    p_last_name                 => last_name,
                                    p_first_name                => first_name,
                                    p_sex                       => sex,
                                    p_person_type_id            => person_type_id,
                                    p_npw_number                => employee_number,
                                    p_person_id                 => person_id,
                                    p_per_object_version_number => l_per_object_version_number,
                                    p_per_effective_start_date  => l_effective_start_date,
                                    p_per_effective_end_date    => l_effective_end_date,
                                    p_pdp_object_version_number => l_pdp_object_version_number,
                                    p_full_name                 => l_full_name,
                                    p_comment_id                => l_comment_id,
                                    p_assignment_id             => l_assignment_id,
                                    p_asg_object_version_number => l_asg_object_version_number,
                                    p_assignment_sequence       => l_assignment_sequence,
                                    p_assignment_number         => l_assignment_number,
                                    p_name_combination_warning  => l_name_combination_warning,
                                    p_title                     => title,
                                    p_email_address             => email_address,
                                    p_marital_status            => marital_status,
                                    p_nationality               => nationality,
                                    p_national_identifier       => national_identifier,
                                    p_date_of_birth             => date_of_birth,
                                    p_town_of_birth             => town_of_birth,
                                    p_region_of_birth           => region_of_birth,
                                    p_blood_type                => blood_type
                                    );
```

g.   Repeat Steps 3.c through 3.f to update the UPDATE_PERSON_API stored procedure to include the newly added attribute.

h.   Re-compile the wrapper package.

7.4 Adding New Multivalued Attributes to a Target Application

You can map new multivalued attributes between Oracle Identity Governance and target system for target resource reconciliation and provisioning.

By default, the attributes listed in Attribute Mapping for the EBS HRMS Connector are mapped for reconciliation and provisioning between Oracle Identity Governance and the target system. If required, you can map additional multivalued attributes to a Target application for target resource reconciliation and provisioning. See Adding New Multivalued Attributes for Reconciliation and Provisioning in *Oracle Identity Governance Configuring the Oracle E-Business Suite User Management Application*.

7.5 Configuring Transformation and Validation of Data

Configure transformation and validation of user account data by writing Groovy script logic while creating your application.

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Governance.

Similarly, you can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

To configure transformation or validation of user account data, you must write Groovy scripts while creating your application. For more information about writing Groovy script-based validation and transformation logic, see Validation and Transformation of Provisioning and Reconciliation Attributes of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

7.6 Configuring Action Scripts

You can configure **Action Scripts** by writing your own Groovy scripts while creating your application.

These scripts can be configured to run before or after the create, update, or delete an account provisioning operations. For example, you can configure a script to run before every user creation operation.

For information on adding or editing action scripts, see Updating the Provisioning Configuration in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

7.7 Configuring the Connector for Multiple Installations of the Target System

You must create copies of configurations of your base application to configure it for multiple installations of the target system.

The following example illustrates this requirement:
The London and New York offices of Example Multinational Inc. have their own installations of the target system, including independent schema for each. The company has recently installed Oracle Identity Governance, and they want to configure it to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must clone your application which copies all configurations of the base application into the cloned application. For more information about cloning applications, see Cloning Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

8

Upgrading the Oracle E-Business Suite HRMS Connectors

If you have already deployed the 11.1.1.5.0 version of this connector, then you can upgrade the connector to the current version 12.2.1.3.0.

> **✐ Note:**
>
> - The connector upgrade from version 11.1.1.5.0 to 12.2.1.3.0 is only supported in the CI-based mode.
> - Before you perform the upgrade, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
> - As a best practice, first perform the upgrade procedure in a test environment.

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

8.1 Preupgrade Steps

Preupgrade steps involve performing a reconciliation run, defining the source connector, and disabling all the scheduled tasks.

1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
2. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector. See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information.
3. If required, create the connector XML file for a clone of the source connector.
4. Disable all the scheduled jobs by stopping the scheduler service.

8.2 Upgrade Steps

This is a summary of the procedure to upgrade the connector for both staging and production environments.

Depending on the environment in which you are upgrading the connector, perform one of the following steps:

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.

- Production Environment

  Perform the upgrade procedure by using the silent mode.

See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Governance* for detailed information about the wizard and silent modes.

8.3 Postupgrade Steps

Postupgrade steps involve uploading new connector JARs, configuring the upgraded IT resource of the source connector, and restarting Oracle Identity Manager.

1. Download the latest version of this connector from Oracle Technology Network and extract its contents to any directory on the computer hosting Oracle Identity Manager.

2. Run the Upload JARs utility to post the latest version of the connector bundle JAR file (org.identityconnectors.ebs-12.3.0.jar) from the /bundle directory of the installation media to the Oracle Identity Manager database.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded (specify the JAR type as ICFBundle, option 4), and the location from which the JAR file is to be uploaded.

3. Configure the upgraded IT resource of the source connector.

4. Restart Oracle Identity Manager. Alternatively, you can purge the cache for the changes to reflect in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about the PurgeCache utility.

After upgrading the connector, you can perform either full reconciliation or incremental reconciliation. This ensures that records created or modified since the last reconciliation run (the one that you performed in Preupgrade Steps) are fetched into Oracle Identity Manager. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token attribute.

Before you perform lookup field synchronization, ensure to remove all preupgrade entries from the lookup definitions Oracle Identity Manager. After upgrade these values must be synchronized with the lookup fields in the target system.

9
Known Issues and Workarounds for the Oracle E-Business Suite HRMS Connectors

This is a known issue associated with this release of the connector.

Unable to Delete Child Data that Does Not Contain the Supervisor Id

When you delete an Assignment entitlement that does not contain the Supervisor Id, you encounter the following error:

```
The value of the attribute Supervisor Id is not of the required type
Integer.
```
Workaround

During provisioning of child data, ensure that you enter a value for the Supervisor Id attribute.

A

Sample SQL Queries for the EBS HRMS Connector

This appendix lists a sample SQL query that can be used to update queries in the search.properties file for the EBS HRMS connector (Target application).

You can use the following SQL query to update the HRMS_CURRENT_EMPLOYEE_RECON_QUERY and HRMS_CURRENT_FUTURE_EMPLOYEE_RECON_QUERY queries if you have added a new attribute, Blood Type, to your Target application (for target resource reconciliation). This newly added attribute is added as part of performing the procedure described in Updating the search.properties File.

```
TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUERY= with PERSON_RECORD as ( \
                                         SELECT PAPF.PERSON_ID AS
person_id,PAPF.FIRST_NAME AS first_name,PAPF.LAST_NAME AS
last_name,PAPF.EMAIL_ADDRESS AS email_address,PPT.USER_PERSON_TYPE
user_person_type, PAPF.EFFECTIVE_START_DATE  AS
effective_start_date,PAPF.EFFECTIVE_END_DATE  AS
effective_end_date,EMPLOYEE_NUMBER AS
employee_number,PPS.ACTUAL_TERMINATION_DATE  AS actual_termination_date,sysdate
as SYSTEM_DATE,PAPF.BUSINESS_GROUP_ID AS business_group_id,PAPF.TOWN_OF_BIRTH AS
town_of_birth,PPU.PERSON_TYPE_ID AS person_type_id,PAPF.REGION_OF_BIRTH AS
region_of_birth,PAPF.COUNTRY_OF_BIRTH AS
country_of_birth,PAPF.NATIONAL_IDENTIFIER AS national_identifier,\
                                         PAPF.TITLE AS
title,PAPF.MARITAL_STATUS AS marital_status,PAPF.SEX AS sex,PAPF.DATE_OF_BIRTH
AS date_of_birth,PAPF.NATIONALITY AS
nationality,NVL(PAPF.ORIGINAL_DATE_OF_HIRE,PAPF.START_DATE)  AS
hire_date,PAPF.LAST_UPDATE_DATE  AS person_updated_date,null AS
assignment_id,null AS asg_effective_start_date,null AS change_reason,null AS
organization_id,null AS job_id,null AS grade_id,null as supervisor_id,null AS
address_id,null AS add_effective_start_date,null AS style,null AS
address_line1,null AS address_line2,null AS address_line3,null AS country,null
AS date_from,null AS date_to,null AS postal_code,null AS region_1,null AS
region_2,null AS region_3,null AS town_or_city,null AS primary_flag,null as
address_type,PAPF.BLOOD_TYPE AS BLOOD_TYPE \
                                         FROM PER_ALL_PEOPLE_F
PAPF,PER_PERIODS_OF_SERVICE PPS,PER_PERSON_TYPES PPT ,PER_PERSON_TYPE_USAGES_F
PPU WHERE  PPT.USER_PERSON_TYPE IN('Employee','Contractor') AND
PPU.PERSON_TYPE_ID = PPT.PERSON_TYPE_ID AND PPU.PERSON_ID = PAPF.PERSON_ID AND
PAPF.PERSON_ID = PPS.PERSON_ID AND PAPF.CURRENT_EMPLOYEE_FLAG = 'Y' AND
( PPU.EFFECTIVE_START_DATE > TRUNC(SYSDATE) OR (TRUNC(SYSDATE) BETWEEN
PAPF.EFFECTIVE_START_DATE AND PAPF.EFFECTIVE_END_DATE)) AND
(PPU.EFFECTIVE_START_DATE > TRUNC(SYSDATE) OR (TRUNC(SYSDATE) BETWEEN
PPU.EFFECTIVE_START_DATE AND PPU.EFFECTIVE_END_DATE)) \
                                         union all \
                                         SELECT PAPF.PERSON_ID AS
person_id,PAPF.FIRST_NAME AS first_name,PAPF.LAST_NAME AS
last_name,PAPF.EMAIL_ADDRESS AS email_address,PPT.USER_PERSON_TYPE
user_person_type, PAPF.EFFECTIVE_START_DATE  AS
effective_start_date,PAPF.EFFECTIVE_END_DATE  AS effective_end_date,NPW_NUMBER
AS employee_number,PPS.ACTUAL_TERMINATION_DATE  AS
```

```
actual_termination_date,sysdate  as SYSTEM_DATE,PAPF.BUSINESS_GROUP_ID AS
business_group_id,PAPF.TOWN_OF_BIRTH AS town_of_birth,PPU.PERSON_TYPE_ID AS
person_type_id,PAPF.REGION_OF_BIRTH AS region_of_birth,PAPF.COUNTRY_OF_BIRTH AS
country_of_birth,PAPF.NATIONAL_IDENTIFIER AS national_identifier,\
                                        PAPF.TITLE AS
title,PAPF.MARITAL_STATUS AS marital_status,PAPF.SEX AS sex,PAPF.DATE_OF_BIRTH
AS date_of_birth,PAPF.NATIONALITY AS
nationality,NVL(PAPF.ORIGINAL_DATE_OF_HIRE,PAPF.START_DATE)  AS
hire_date,PAPF.LAST_UPDATE_DATE  AS person_updated_date,null AS
assignment_id,null AS asg_effective_start_date,null AS change_reason,null AS
organization_id,null AS job_id,null AS grade_id,null as supervisor_id,null AS
address_id,null AS add_effective_start_date,null AS style,null AS
address_line1,null AS address_line2,null AS address_line3,null AS country,null
AS date_from,null AS date_to,null AS postal_code,null AS region_1,null AS
region_2,null AS region_3,null AS town_or_city,null AS primary_flag,null as
address_type,PAPF.BLOOD_TYPE AS BLOOD_TYPE \
                                        FROM PER_ALL_PEOPLE_F
PAPF,PER_PERIODS_OF_PLACEMENT PPS,PER_PERSON_TYPES PPT ,PER_PERSON_TYPE_USAGES_F
PPU WHERE  PPT.USER_PERSON_TYPE IN('Contingent Employee','Contingent Worker')
AND    PPU.PERSON_TYPE_ID = PPT.PERSON_TYPE_ID AND PPU.PERSON_ID =
PAPF.PERSON_ID AND  PAPF.PERSON_ID = PPS.PERSON_ID AND PAPF.CURRENT_NPW_FLAG =
'Y' AND  PPU.EFFECTIVE_END_DATE > sysdate AND ( PPU.EFFECTIVE_START_DATE >
TRUNC(SYSDATE) OR (TRUNC(SYSDATE) BETWEEN PAPF.EFFECTIVE_START_DATE AND
PAPF.EFFECTIVE_END_DATE)) AND (PPU.EFFECTIVE_START_DATE > TRUNC(SYSDATE) OR
(TRUNC(SYSDATE) BETWEEN PPU.EFFECTIVE_START_DATE AND PPU.EFFECTIVE_END_DATE)) \
                                        ) select * from (  \
                                        select RESULTTABLE.*,ROW_NUMBER() OVER
(ORDER BY person_id) AS Row_Num from ( \
                                        select * from PERSON_RECORD \
                                        union all \
                                        select
person.PERSON_ID,person.FIRST_NAME,person.LAST_NAME,person.EMAIL_ADDRESS,person.U
SER_PERSON_TYPE,person.EFFECTIVE_START_DATE,person.EFFECTIVE_END_DATE ,person.EMP
LOYEE_NUMBER,person.ACTUAL_TERMINATION_DATE, \

person.SYSTEM_DATE,person.BUSINESS_GROUP_ID,person.TOWN_OF_BIRTH,person.PERSON_TY
PE_ID,person.REGION_OF_BIRTH,person.COUNTRY_OF_BIRTH,person.NATIONAL_IDENTIFIER,p
erson.TITLE,person.MARITAL_STATUS,person.SEX,person.DATE_OF_BIRTH,person.NATIONAL
ITY,person.hire_date,person.person_updated_date, \
                                        PAAF.ASSIGNMENT_ID as
assignment_id,PAAF.EFFECTIVE_START_DATE as
ASG_EFFECTIVE_START_DATE,PAAF.CHANGE_REASON,PAAF.ORGANIZATION_ID as
organization_id,PAAF.JOB_ID,PAAF.GRADE_ID as grade_id,PAAF.SUPERVISOR_ID as
supervisor_id,null AS address_id,null AS add_effective_start_date, \
                                        null AS style,null AS
address_line1,null AS address_line2,null AS address_line3,null AS country,null
AS date_from,null AS date_to,null AS postal_code,null AS region_1,null AS
region_2,null AS region_3, \
                                        null AS town_or_city,null AS
primary_flag,null as address_type, person.BLOOD_TYPE AS BLOOD_TYPE from
PERSON_RECORD person,PER_ALL_ASSIGNMENTS_F PAAF where
person.person_id=PAAF.person_id  AND    PAAF.job_id is not null AND
((PAAF.EFFECTIVE_START_DATE >= sysdate) OR (TRUNC(SYSDATE) BETWEEN
PAAF.EFFECTIVE_START_DATE AND PAAF.EFFECTIVE_END_DATE) ) \
                                        union all \
                                        select
person.PERSON_ID,person.FIRST_NAME,person.LAST_NAME,person.EMAIL_ADDRESS,person.U
SER_PERSON_TYPE,person.EFFECTIVE_START_DATE,person.EFFECTIVE_END_DATE ,person.EMP
LOYEE_NUMBER,person.ACTUAL_TERMINATION_DATE, \

person.SYSTEM_DATE,person.BUSINESS_GROUP_ID,person.TOWN_OF_BIRTH,person.PERSON_TY
```

```
PE_ID,person.REGION_OF_BIRTH,person.COUNTRY_OF_BIRTH,person.NATIONAL_IDENTIFIER,p
erson.TITLE,person.MARITAL_STATUS,person.SEX,person.DATE_OF_BIRTH,person.NATIONAL
ITY,person.hire_date,person.person_updated_date,\
                                        null as assignment_id,null as
ASG_EFFECTIVE_START_DATE,null as CHANGE_REASON,null as organization_id,null as
JOB_ID,null as grade_id,null as supervisor_id, \
                                        PA.ADDRESS_ID AS
address_id,PA.DATE_FROM AS add_effective_start_date,PA.STYLE AS style,
PA.ADDRESS_LINE1 AS address_line1, PA.ADDRESS_LINE2 AS address_line2,
PA.ADDRESS_LINE3 AS address_line3,PA.COUNTRY AS country,PA.DATE_FROM AS
date_from,PA.DATE_TO AS date_to, PA.POSTAL_CODE AS postal_code, PA.REGION_1 AS
region_1,PA.REGION_2 AS region_2, PA.REGION_3 AS region_3,PA.TOWN_OR_CITY AS
town_or_city,PA.PRIMARY_FLAG AS primary_flag,PA.ADDRESS_TYPE as
address_type,person.BLOOD_TYPE AS BLOOD_TYPE from PERSON_RECORD
person,PER_ADDRESSES PA where person.person_id= PA.person_id and ((PA.DATE_FROM
> sysdate) OR SYSDATE between  PA.DATE_FROM and nvl(PA.DATE_TO, TO_DATE('31-
DEC-4712','dd-mon-yyyy'))) \
                                        ) RESULTTABLE \
                                        --<FILTER> \
                                        ) WHERE Row_Num BETWEEN
<START_ROW_NUMBER> and <END_ROW_NUMBER>
```

B

Sample SQL Queries for the EBS ER Connector

This appendix lists a sample SQL query that can be used to update queries in the search.properties file for the EBS ER connector (Authoritative application).

You can use the following SQL query to update the HRMS_CURRENT_EMPLOYEE_RECON_QUERY and HRMS_CURRENT_FUTURE_EMPLOYEE_RECON_QUERY queries if you have added a new attribute, Blood Type, for trusted source reconciliation. This newly added attribute is added as part of performing the procedure described in Updating the search.properties File for an Authoritative Application.

```
TARGET_HRMS_CURRENT_EMPLOYEE_RECON_QUERY= with PERSON_RECORD as ( \
                                          SELECT PAPF.PERSON_ID AS
person_id,PAPF.FIRST_NAME AS first_name,PAPF.LAST_NAME AS
last_name,PAPF.EMAIL_ADDRESS AS email_address,PPT.USER_PERSON_TYPE
user_person_type, PAPF.EFFECTIVE_START_DATE  AS
effective_start_date,PAPF.EFFECTIVE_END_DATE  AS
effective_end_date,EMPLOYEE_NUMBER AS
employee_number,PPS.ACTUAL_TERMINATION_DATE  AS actual_termination_date,sysdate
as SYSTEM_DATE,PAPF.BUSINESS_GROUP_ID AS business_group_id,PAPF.TOWN_OF_BIRTH AS
town_of_birth,PPU.PERSON_TYPE_ID AS person_type_id,PAPF.REGION_OF_BIRTH AS
region_of_birth,PAPF.COUNTRY_OF_BIRTH AS
country_of_birth,PAPF.NATIONAL_IDENTIFIER AS national_identifier,\
                                          PAPF.TITLE AS
title,PAPF.MARITAL_STATUS AS marital_status,PAPF.SEX AS sex,PAPF.DATE_OF_BIRTH
AS date_of_birth,PAPF.NATIONALITY AS
nationality,NVL(PAPF.ORIGINAL_DATE_OF_HIRE,PAPF.START_DATE)  AS
hire_date,PAPF.LAST_UPDATE_DATE  AS person_updated_date,null AS
assignment_id,null AS asg_effective_start_date,null AS change_reason,null AS
organization_id,null AS job_id,null AS grade_id,null as supervisor_id,null AS
address_id,null AS add_effective_start_date,null AS style,null AS
address_line1,null AS address_line2,null AS address_line3,null AS country,null
AS date_from,null AS date_to,null AS postal_code,null AS region_1,null AS
region_2,null AS region_3,null AS town_or_city,null AS primary_flag,null as
address_type,PAPF.BLOOD_TYPE AS BLOOD_TYPE \
                                          FROM PER_ALL_PEOPLE_F
PAPF,PER_PERIODS_OF_SERVICE PPS,PER_PERSON_TYPES PPT ,PER_PERSON_TYPE_USAGES_F
PPU WHERE  PPT.USER_PERSON_TYPE IN('Employee','Contractor') AND
PPU.PERSON_TYPE_ID = PPT.PERSON_TYPE_ID AND PPU.PERSON_ID = PAPF.PERSON_ID AND
PAPF.PERSON_ID = PPS.PERSON_ID AND PAPF.CURRENT_EMPLOYEE_FLAG = 'Y' AND
( PPU.EFFECTIVE_START_DATE > TRUNC(SYSDATE) OR (TRUNC(SYSDATE) BETWEEN
PAPF.EFFECTIVE_START_DATE AND PAPF.EFFECTIVE_END_DATE)) AND
(PPU.EFFECTIVE_START_DATE > TRUNC(SYSDATE) OR (TRUNC(SYSDATE) BETWEEN
PPU.EFFECTIVE_START_DATE AND PPU.EFFECTIVE_END_DATE)) \
                                          union all \
                                          SELECT PAPF.PERSON_ID AS
person_id,PAPF.FIRST_NAME AS first_name,PAPF.LAST_NAME AS
last_name,PAPF.EMAIL_ADDRESS AS email_address,PPT.USER_PERSON_TYPE
user_person_type, PAPF.EFFECTIVE_START_DATE  AS
effective_start_date,PAPF.EFFECTIVE_END_DATE  AS effective_end_date,NPW_NUMBER
AS employee_number,PPS.ACTUAL_TERMINATION_DATE  AS
```

```
actual_termination_date,sysdate  as SYSTEM_DATE,PAPF.BUSINESS_GROUP_ID AS
business_group_id,PAPF.TOWN_OF_BIRTH AS town_of_birth,PPU.PERSON_TYPE_ID AS
person_type_id,PAPF.REGION_OF_BIRTH AS region_of_birth,PAPF.COUNTRY_OF_BIRTH AS
country_of_birth,PAPF.NATIONAL_IDENTIFIER AS national_identifier,\
                                            PAPF.TITLE AS
title,PAPF.MARITAL_STATUS AS marital_status,PAPF.SEX AS sex,PAPF.DATE_OF_BIRTH
AS date_of_birth,PAPF.NATIONALITY AS
nationality,NVL(PAPF.ORIGINAL_DATE_OF_HIRE,PAPF.START_DATE)  AS
hire_date,PAPF.LAST_UPDATE_DATE  AS person_updated_date,null AS
assignment_id,null AS asg_effective_start_date,null AS change_reason,null AS
organization_id,null AS job_id,null AS grade_id,null as supervisor_id,null AS
address_id,null AS add_effective_start_date,null AS style,null AS
address_line1,null AS address_line2,null AS address_line3,null AS country,null
AS date_from,null AS date_to,null AS postal_code,null AS region_1,null AS
region_2,null AS region_3,null AS town_or_city,null AS primary_flag,null as
address_type,PAPF.BLOOD_TYPE AS BLOOD_TYPE \
                                            FROM PER_ALL_PEOPLE_F
PAPF,PER_PERIODS_OF_PLACEMENT PPS,PER_PERSON_TYPES PPT ,PER_PERSON_TYPE_USAGES_F
PPU WHERE  PPT.USER_PERSON_TYPE IN('Contingent Employee','Contingent Worker')
AND    PPU.PERSON_TYPE_ID = PPT.PERSON_TYPE_ID AND PPU.PERSON_ID =
PAPF.PERSON_ID AND  PAPF.PERSON_ID = PPS.PERSON_ID AND PAPF.CURRENT_NPW_FLAG =
'Y' AND  PPU.EFFECTIVE_END_DATE > sysdate AND ( PPU.EFFECTIVE_START_DATE >
TRUNC(SYSDATE) OR (TRUNC(SYSDATE) BETWEEN PAPF.EFFECTIVE_START_DATE AND
PAPF.EFFECTIVE_END_DATE)) AND (PPU.EFFECTIVE_START_DATE > TRUNC(SYSDATE) OR
(TRUNC(SYSDATE) BETWEEN PPU.EFFECTIVE_START_DATE AND PPU.EFFECTIVE_END_DATE)) \
                                            ) select * from (  \
                                            select RESULTTABLE.*,ROW_NUMBER() OVER
(ORDER BY person_id) AS Row_Num from ( \
                                            select * from PERSON_RECORD \
                                            union all \
                                            select
person.PERSON_ID,person.FIRST_NAME,person.LAST_NAME,person.EMAIL_ADDRESS,person.U
SER_PERSON_TYPE,person.EFFECTIVE_START_DATE,person.EFFECTIVE_END_DATE ,person.EMP
LOYEE_NUMBER,person.ACTUAL_TERMINATION_DATE, \

person.SYSTEM_DATE,person.BUSINESS_GROUP_ID,person.TOWN_OF_BIRTH,person.PERSON_TY
PE_ID,person.REGION_OF_BIRTH,person.COUNTRY_OF_BIRTH,person.NATIONAL_IDENTIFIER,p
erson.TITLE,person.MARITAL_STATUS,person.SEX,person.DATE_OF_BIRTH,person.NATIONAL
ITY,person.hire_date,person.person_updated_date, \
                                            PAAF.ASSIGNMENT_ID as
assignment_id,PAAF.EFFECTIVE_START_DATE as
ASG_EFFECTIVE_START_DATE,PAAF.CHANGE_REASON,PAAF.ORGANIZATION_ID as
organization_id,PAAF.JOB_ID,PAAF.GRADE_ID as grade_id,PAAF.SUPERVISOR_ID as
supervisor_id,null AS address_id,null AS add_effective_start_date, \
                                            null AS style,null AS
address_line1,null AS address_line2,null AS address_line3,null AS country,null
AS date_from,null AS date_to,null AS postal_code,null AS region_1,null AS
region_2,null AS region_3, \
                                            null AS town_or_city,null AS
primary_flag,null as address_type, person.BLOOD_TYPE AS BLOOD_TYPE from
PERSON_RECORD person,PER_ALL_ASSIGNMENTS_F PAAF where
person.person_id=PAAF.person_id  AND    PAAF.job_id is not null AND
((PAAF.EFFECTIVE_START_DATE >= sysdate) OR (TRUNC(SYSDATE) BETWEEN
PAAF.EFFECTIVE_START_DATE AND PAAF.EFFECTIVE_END_DATE) ) \
                                            union all \
                                            select
person.PERSON_ID,person.FIRST_NAME,person.LAST_NAME,person.EMAIL_ADDRESS,person.U
SER_PERSON_TYPE,person.EFFECTIVE_START_DATE,person.EFFECTIVE_END_DATE ,person.EMP
LOYEE_NUMBER,person.ACTUAL_TERMINATION_DATE, \

person.SYSTEM_DATE,person.BUSINESS_GROUP_ID,person.TOWN_OF_BIRTH,person.PERSON_TY
```

```
PE_ID,person.REGION_OF_BIRTH,person.COUNTRY_OF_BIRTH,person.NATIONAL_IDENTIFIER,p
erson.TITLE,person.MARITAL_STATUS,person.SEX,person.DATE_OF_BIRTH,person.NATIONAL
ITY,person.hire_date,person.person_updated_date,\
                                        null as assignment_id,null as
ASG_EFFECTIVE_START_DATE,null as CHANGE_REASON,null as organization_id,null as
JOB_ID,null as grade_id,null as supervisor_id, \
                                        PA.ADDRESS_ID AS
address_id,PA.DATE_FROM AS add_effective_start_date,PA.STYLE AS style,
PA.ADDRESS_LINE1 AS address_line1, PA.ADDRESS_LINE2 AS address_line2,
PA.ADDRESS_LINE3 AS address_line3,PA.COUNTRY AS country,PA.DATE_FROM AS
date_from,PA.DATE_TO AS date_to, PA.POSTAL_CODE AS postal_code, PA.REGION_1 AS
region_1,PA.REGION_2 AS region_2, PA.REGION_3 AS region_3,PA.TOWN_OR_CITY AS
town_or_city,PA.PRIMARY_FLAG AS primary_flag,PA.ADDRESS_TYPE as
address_type,person.BLOOD_TYPE AS BLOOD_TYPE from PERSON_RECORD
person,PER_ADDRESSES PA where person.person_id= PA.person_id and ((PA.DATE_FROM
> sysdate) OR SYSDATE between  PA.DATE_FROM and nvl(PA.DATE_TO, TO_DATE('31-
DEC-4712','dd-mon-yyyy'))) \
                                        ) RESULTTABLE \
                                        --<FILTER> \
                                        ) WHERE Row_Num BETWEEN
<START_ROW_NUMBER> and <END_ROW_NUMBER>
```

C
Files and Directories in the Oracle E-Business Suite HRMS Connectors Installation Package

These are the components of the connector installation media that comprise the Oracle E-Business Suite HRMS Connectors.

Table C-1   Files and Directories in the Connector Installation Package

File in the Installation Package	Description
bundle/org.identityconnectors.ebs-12.3.0.jar	This JAR file contains the connector code, and properties files that hold SQL queries and stored procedures for performing reconciliation and provisioning operations, respectively.
Files in the configuration directory: • EBS-HRMS-CI.xml • EBS-HRMS-Trusted-CI.xml	These files are used for installing a CI-based connector. These XML file contain configuration information that is used during the EBS HRMS connector, and EBS Employee Reconciliation connector installation process.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the EBS HRMS and EBS Employee Reconciliation connectors. During connector deployment, these resource bundles are copied to the Oracle Identity Governance database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.
scripts/OIM_EBSHRMS_SCHEMA_PKG.pck	This package file contains the schema of the EBS HRMS connectors.
scripts/OIM_EMPLOYEE_ADDRESS_WRAPPER.pck	This package file contains procedures and SQL statements for creating, updating, and deleting employee address records. This file is used by the EBS HRMS connector (for a Target application).
scripts/OIM_EMPLOYEE_ADDRESS_WRAPPER_APPS.pck	This package file contains procedures and SQL statements for creating, updating, and deleting employee address records for APPS user. This file is used by the EBS HRMS Target connector.
scripts/OIM_EMPLOYEE_WRAPPER.pck	This package file contains the procedures and SQL statements for creating, updating, deleting, and terminating person records. In addition, it contains the SQL statements for creating, updating, and deleting person assignments.
scripts/OIM_FND_GLOBAL.pck	This file contains the procedures that are called to initialize the global security context for a database session during a provisioning operation.
scripts/OIM_TYPES.pck	This package file contains SQL statements used for creating Oracle types. Oracle types are used for storing OIM schema.

Table C-1   (Cont.) Files and Directories in the Connector Installation Package

File in the Installation Package	Description
scripts/OimHRMSAppstablesSynonyms.sql scripts/OimHRMSUser.sql scripts/OimHRMSUserAcl.sql scripts/OimHRMSUserAD_ZDGrants scripts/OimHRMSUserGrants.sql scripts/OimHRMSUserSynonyms.sql	These files contain the SQL scripts to create a target system user account, grant the required rights to the user, and create synonyms of various database objects to be used by the connector.
xml/EBS-HRMS-auth-template.xml	This file contains definitions for the connector objects required for creating an Authoritative application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/EBS-HRMS-ConnectorConfig.xml **Note:** This file is applicable only for a CI-based connector.	This XML file contains definitions for the following components of the EBS HRMS Target connector: • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Prepopulate rules • Lookup definitions • Reconciliation rules • Scheduled tasks
xml/EBS-HRMS-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User objects such as Address, Assignment, and so on.
xml/EBS-HRMS-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system . It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/EBS-HRMS-Trusted-ConnectorConfig.xml	This XML file contains definitions for the following components of the EBS HRMS Trusted connector: • Resource objects • IT resource types • IT resource instance • Lookup definitions • Reconciliation rules • Scheduled tasks

ORACLE®

C-2

D

Privileges Granted to the User Account

This section lists the privileges that are granted to the user account created earlier. The synonyms created for tables are also listed here.

This section lists the privileges that are granted to the user account created earlier. The synonyms created for tables are also listed here.

Execute permission granted to the following packages:

APPS.HR_EMPLOYEE_API

APPS.HR_PERSON_API

APPS.HR_PERSON_ADDRESS_API

APPS.HR_PERSON_ADDRESS_BK1

APPS.HR_API

APPS.HR_CONTINGENT_WORKER_API

APPS.HR_ASSIGNMENT_API

Select privilege has been granted to the following tables:

APPS.PER_ALL_ASSIGNMENTS_F

APPS.PER_PEOPLE_F

APPS.PER_PERSON_TYPES

APPS.PER_PERIODS_OF_SERVICE

APPS.PER_PERIODS_OF_PLACEMENT

APPS.PER_ADDRESSES

APPS.PER_PERSON_TYPE_USAGES_F

APPS.PER_ALL_PEOPLE_F

Execute privileges granted to the following wrapper packages created in APPS schema:

APPS.OIM_EMPLOYEE_WRAPPER

APPS.OIM_EMPLOYEE_ADDRESS_WRAPPER

APPS.HZ_PARTIES

APPS.PER_JOBS

APPS.PER_GRADES

APPS.HR_ALL_ORGANIZATION_UNITS

APPS.PER_VALID_GRADES

APPS.FND_LOOKUP_VALUES_VL

Synonyms created or replaced for tables as follows:

synonym PER_PEOPLE_F for APPS.PER_PEOPLE_F

synonym PER_ALL_ASSIGNMENTS_F for APPS.PER_ALL_ASSIGNMENTS_F

synonym PER_PERIODS_OF_SERVICE for APPS.PER_PERIODS_OF_SERVICE

synonym PER_PERIODS_OF_PLACEMENT for
APPS.PER_PERIODS_OF_PLACEMENT

synonym HR_EMPLOYEE_API for APPS.HR_EMPLOYEE_API

synonym HR_PERSON_API for APPS.HR_PERSON_API

synonym PER_ADDRESSES for APPS.PER_ADDRESSES

synonym PER_PERSON_TYPE_USAGES_F for
APPS.PER_PERSON_TYPE_USAGES_F

synonym PER_ALL_PEOPLE_F for APPS.PER_ALL_PEOPLE_F

synonym PER_JOBS for APPS.PER_JOBS

synonym PER_GRADES for APPS.PER_GRADES

synonym HR_ALL_ORGANIZATION_UNITS for
APPS.HR_ALL_ORGANIZATION_UNITS

synonym HR_PERSON_ADDRESS_API for APPS.HR_PERSON_ADDRESS_API

synonym HR_CONTINGENT_WORKER_API for
APPS.HR_CONTINGENT_WORKER_API

synonym HR_ASSIGNMENT_API for APPS.HR_ASSIGNMENT_API

synonym HR_PERSON_ADDRESS_BK1 for APPS.HR_PERSON_ADDRESS_BK1

synonym HR_API for APPS.HR_API

synonym HZ_PARTIES for APPS.HZ_PARTIES

synonym PER_PERSON_TYPES for APPS.PER_PERSON_TYPES

synonym PER_VALID_GRADES for APPS.PER_VALID_GRADES

synonym FND_LOOKUP_VALUES_VL for APPS.FND_LOOKUP_VALUES_VL

Synonyms created or replaced for OIM database user as follows:

synonym OIM_EMPLOYEE_WRAPPER for APPS.OIM_EMPLOYEE_WRAPPER

synonym OIM_EMPLOYEE_ADDRESS_WRAPPER for
APPS.OIM_EMPLOYEE_ADDRESS_WRAPPER

synonym attributeinfo for APPS.attributeinfo

synonym attributelist for APPS.attributelist

synonym schema_object for APPS.schema_object

synonym schemalist for APPS.schemalist