Oracle® Identity Manager

Connector Guide for Database Application Tables

Release 9.1.0

E11194-03

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for Database Application Tables, Release 9.1.0

E11194-03

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents x
Documentation Updates x
Conventions x

What's New in Oracle Identity Manager Connector for Database Application Tables? xi

Software Updates xi
Documentation-Specific Updates xii

1 About the Connector

Certified Deployment Configurations 1-2
Certified Languages 1-3
Features of the Connector 1-4
Connector Architecture 1-4
Target Resource Reconciliation 1-6
Provisioning 1-7
Trusted Source Reconciliation 1-7
Roadmap for Deploying and Using the Connector 1-7

2 Tasks to Be Performed Before You Create the Connector

Configuring Oracle Identity Manager 2-1
Enabling Logging 2-1
Adding New User-Defined Fields for the OIM User 2-3
Using Lookup Definitions 2-4
Copying the JDBC Drivers 2-4
Exchanging Account Status Data with the Target System 2-5
Configuring Account Status Reconciliation 2-5
Configuring Account Status Provisioning 2-6
Copying the Provider Files 2-7
Configuring the Target System 2-8

Using Read-Only Views 2-8
Ensuring That There Are No Target System Columns Named ID 2-9
Configuring IBM DB2/UDB Running on IBM z/OS 2-9
Configuring Secure Communication Between the Target System and Oracle Identity Manager ... 2-9
Configuring Secure Communication Between IBM DB2/UDB and Oracle Identity Manager 2-9
Configuring Secure Communication Between Microsoft SQL Server and Oracle Identity Manager 2-10
Configuring Secure Communication Between Oracle Database and Oracle Identity Manager 2-11
Configuring Data Encryption and Integrity in Oracle Database 2-11
Configuring SSL Communication in Oracle Database 2-11

3 Creating the Connector

Limited Reconciliation 3-1
Determining Values for the Database URL and Connection Properties Parameters 3-2
Database URL and Connection Properties for IBM DB2/UDB 3-2
Database URL and Connection Properties for Microsoft SQL Server 3-3
Database URL and Connection Properties for Oracle Database 3-5
Only Data Encryption and Integrity Is Configured 3-5
Only SSL Communication Is Configured 3-6
Both Data Encryption and Integrity and SSL Communication Are Configured 3-7
Creating the Connector 3-8
Step 1: Provide Basic Information Page 3-8
Step 2: Specify Parameter Values Page 3-10
Step 3: Modify Connector Configuration Page 3-15
Step 4: Verify Connector Form Names Page 3-21
Step 5: Verify Connector Information Page 3-21
Modifying the Default Action Rules 3-22
Configuring Reconciliation 3-23
Configuring Provisioning 3-23
Performing Connector Operations 3-23

4 Known Issues

A An Example of the Procedure to Create Connectors

Sample Scenario A-1
Sample Target System to Be Configured As a Target Resource A-1
Sample Target System to Be Configured As a Trusted Source A-2
Tasks to Be Performed Before You Create the Connector A-2
Configuring the Target System As a Target Resource A-3
Configuring the Target System As a Trusted Source A-12

B Screenshots of the Step 3: Modify Connector Configuration Page

Using the Data Type List and Required Check Box B-1
Specifying a Literal Value As Input for a Field B-2

Encrypting the Storage and Display of Field Values B-2
Configuring Account Status Reconciliation: Step 1 ..... B-3
Configuring Account Status Reconciliation: Step 2 ..... B-3
Summary of Changes That You See After Configuring Target Resource Reconciliation B-4
Summary of Changes That You See After Configuring Trusted Source Reconciliation B-5

Index

List of Figures

1–1 Architecture of a Database Application Tables Connector 1-4
3–1 Step 1: Provide Basic Information Page 3-9
3–2 First Section of the Step 2: Specify Parameter Values Page 3-14
3–3 Second Section of the Step 2: Specify Parameter Values Page 3-15
3–4 Step 3: Modify Connector Configuration Page After Metadata Detection 3-16
3–5 Step 4: Verify Connector Form Names Page 3-21
A–1 Step 1: Provide Basic Information Page A-4
A–2 First Section of the Step 2: Specify Parameter Values Page A-6
A–3 Second Section of the Step 2: Specify Parameter Values Page A-7
A–4 Step 3: Modify Connector Configuration Page After Metadata Detection A-8
A–5 Step 3: Modify Connector Configuration Page Displayed After You Configure the Connector A-10
A–6 Step 4: Verify Connector Form Names Page A-11
A–7 Step 1: Provide Basic Information Page A-13
A–8 First Section of the Step 2: Specify Parameter Values Page A-14
A–9 Second Section of the Step 2: Specify Parameter Values Page A-15
A–10 Step 3: Modify Connector Configuration Page After Metadata Detection A-15
A–11 Step 3: Modify Connector Configuration Page Displayed After You Configure the Connector A-18
B–1 Data Type List and Required Check Box B-1
B–2 Literal Value As Input for a Field B-2
B–3 Encrypted and Password Field Check Boxes B-2
B–4 Translation Transformation Option B-3
B–5 Source Field and Lookup Definition Containing Translated Values B-3
B–6 Actions Performed for Configuring Target Resource Reconciliation B-4
B–7 Actions Performed for Configuring Trusted Source Reconciliation B-5

List of Tables

1–1 Certified Deployment Configurations 1-2
2–1 Provider Files for the Connector 2-8
2–2 Truststore Locations on Supported Application Servers 2-10
2–3 Truststore Locations on Supported Application Servers 2-11
2–4 Truststore Locations on Supported Application Servers 2-12
3–1 Parameters Displayed on the Step 2: Specify Parameter Values Page 3-10
3–2 Actions to Be Performed on the Step 3: Modify Connector Configuration Page 3-17
3–3 Action Rules for Target Resource Reconciliation 3-22
3–4 Action Rules for Trusted Source Reconciliation 3-22
A–1 Sample Entries for the Step 1: Provide Basic Information Page A-4
A–2 Sample Entries for the Step 2: Specify Parameter Values Page A-5
A–3 Sample Entries for the Step 1: Provide Basic Information Page A-12
A–4 Sample Entries for the Step 2: Specify Parameter Values Page A-13

Preface

This guide provides information about integrating Oracle Identity Manager with database tables that store user data.

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

For generic information about connectors, see *Oracle Identity Manager Connector Concepts* in the Oracle Identity Manager Connectors documentation library.

To access the Oracle Identity Manager documents mentioned as references in this guide, visit Oracle Technology Network. The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://www.oracle.com/technology/documentation/index.html

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

What's New in Oracle Identity Manager Connector for Database Application Tables?

This chapter provides an overview of the updates made to the software and documentation for the Database Application Tables connector in release 9.1.0.1.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following sections discuss updates made from release 9.0.4 to the current release of the connector:

- Software Updates in Release 9.1.0.1

Software Updates in Release 9.1.0.1

The following are software updates in release 9.1.0.1:

- Support for IBM DB2/UDB Version 9.x on Microsoft Windows, UNIX, and IBM z/OS Platforms
- Resolved Issues in Release 9.1.0.1

Support for IBM DB2/UDB Version 9.x on Microsoft Windows, UNIX, and IBM z/OS Platforms

In addition to the databases supported by the earlier release, this release supports IBM DB2/UDB version 9.*x* running on Microsoft Windows, UNIX, and IBM z/OS platforms.

See "Certified Deployment Configurations" in the connector guide for information about the other target systems. Information specific to IBM DB2/UDB has been added at various places in this guide.

Note: SSL communication is not supported if IBM DB2/UDB is running on IBM z/OS. This has been mentioned in the "Known Issues" chapter.

Resolved Issues in Release 9.1.0.1

The following is an issue resolved in release 9.1.0.1:

Bug Number	Issue	Resolution
7622061	While a connector was being created, the names of target database tables that you specified were changed to uppercase by the generic technology connector framework. If the database was configured to be case-sensitive to table names, then these tables were not found in the database during the connector creation process and the process failed.	This issue has been resolved. During the connector creation process, the table names are not modified.

Documentation-Specific Updates

The following documentation-specific updates have been made in the guide:

- Documentation-Specific Updates in Release 9.1.0.1

Documentation-Specific Updates in Release 9.1.0.1

The following are documentation-specific updates in release 9.1.0.1:

- In the "Known Issues" chapter, the following item has been added:

  Bug 8282035

  If the data type of the primary key column of the target database table is not VARCHAR, then an error is encountered if you try to update a provisioned resource whose data is stored in that target database table.

- In the "Certified Deployment Configurations" section, changes have been made in the "Target systems" and "JDBC drivers" rows.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications.

A custom application in your organization may use relational database tables as a repository for user data. This guide describes the procedure to create the connector for integrating these database tables with Oracle Identity Manager. After you integrate the tables with Oracle Identity Manager, you can use them either as a managed (target) resource or as an authoritative (trusted) source of user data for Oracle Identity Manager.

The connector that you create is known as a **Database Application Tables connector**. The following sample scenario describes the requirement that can be addressed by a Database Application Tables connector:

Example Inc. has some database-driven custom applications. These applications cannot be LDAP enabled, and they do not have any APIs for identity administration. The company wants to deploy an identity management and provisioning system that can be linked with their database.

The Database Application Tables connector is one of the solutions to this business problem. Example Inc. can use this connector to enable the exchange of user data between the database and Oracle Identity Manager.

Note: In this guide:

- The database tables that store user data are collectively referred to as the **target system**.
- The computer on which the database is installed is referred to as the **target system host computer**.

In the target resource configuration, data about users created or modified on the target system is reconciled into Oracle Identity Manager and is used to create or update resources allocated to OIM Users. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the trusted source configuration, data about users created or modified on the target system is reconciled into Oracle Identity Manager and is used to create or update OIM Users.

Note:

- It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.
- See *Oracle Identity Manager Connector Concepts* for detailed information about connector deployment configurations.

This chapter discusses the following topics:

- Certified Deployment Configurations
- Certified Languages
- Features of the Connector
- Roadmap for Deploying and Using the Connector

1.1 Certified Deployment Configurations

Table 1–1 lists the certified deployment configurations for this connector.

Table 1–1 Certified Deployment Configurations

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.1.0 or later
Target systems	The target system can be database tables from any one of the following RDBMSs: ■ IBM DB2/UDB Version 9.*x* running on Microsoft Windows, UNIX, and IBM z/OS platforms ■ Microsoft SQL Server 2005 ■ Oracle Database 10*g*, 11*g*

Table 1–1 (Cont.) Certified Deployment Configurations

Item	Requirement
JDBC drivers	Depending on the target system that you use, you would need one of the following sets of JDBC drivers: For IBM DB2/UDB: ■ For all platforms: db2jcc.jar ■ For Microsoft Windows and UNIX platforms: db2jcc_license_cu.jar ■ For IBM z/OS platforms: db2jcc_license_cisuz.jar For Microsoft SQL Server: ■ sqljdbc.jar version 1.2 For Oracle Database ■ Oracle Database 10*g* drivers ■ Oracle Database 11*g* drivers Instructions to download and use these drivers are provided later in this guide.
Format in which user data is stored in the target system	You can use a Database Application Tables connector only if user data is stored in the target system in any one of the following formats: ■ All user data is in a single table. ■ User data is spread across one parent table and one or more child tables. This target system can be configured only as a target resource, and not as a trusted source. ■ All user data is in a single updatable view (that is based on one or more tables). ■ User data is spread across one updatable view (that is based on one or more tables) and one or more child views (that are based on one or more tables). This target system can be configured only as a target resource, and not as a trusted source. In other words, a trusted source cannot store child data. **Note:** If you use read-only views, then you must create INSTEAD OF triggers to enable modification of the read-only views during provisioning operations. This requirement has also been mentioned in "Using Read-Only Views" on page 2-8.
Other requirements of the target system	The target system must meet the following requirements: ■ The target system must not contain a column named `ID`. See "Ensuring That There Are No Target System Columns Named ID" on page 2-9 for the description of a workaround to this requirement. ■ Names of foreign key columns can be the same in parent and child tables. However, the names of all other columns in the parent table must be different from the names of columns in the child tables. See "Names of Fields" in the "Best Practices for Creating and Using Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide* for more information. The latest version of this guide is available on Oracle Technology Network.

1.2 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)

- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

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

1.3 Features of the Connector

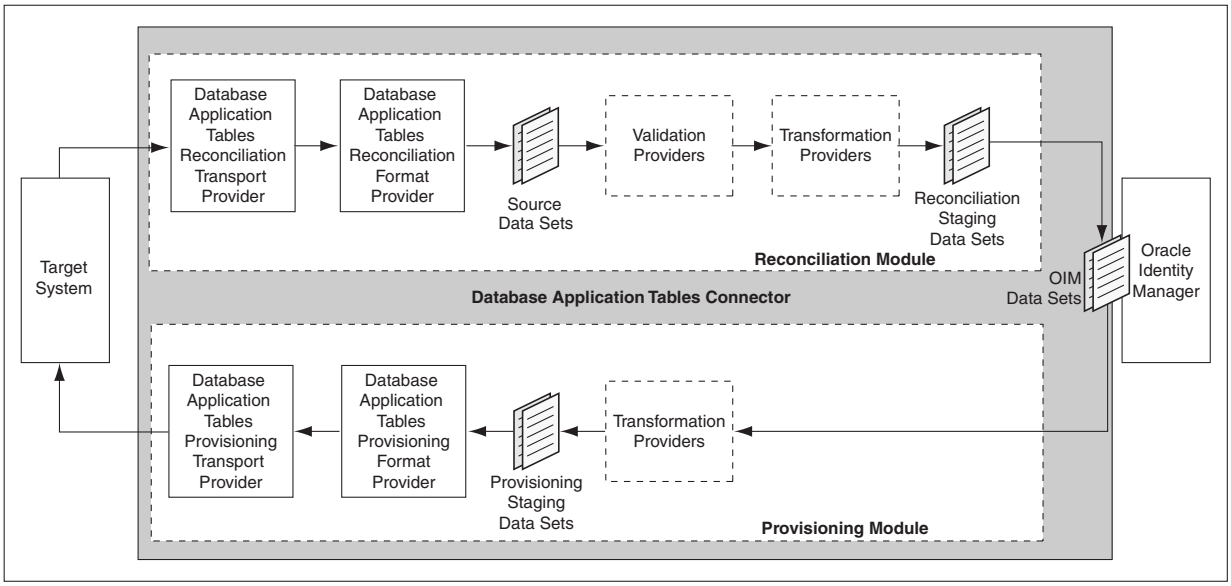
This section discusses the following topics:

- The "Connector Architecture" section describes the architecture of the connector.
- The following sections describe features of the target resource configuration:
  - Target Resource Reconciliation
  - Provisioning
- The "Trusted Source Reconciliation" section describes features of the trusted source configuration.

1.3.1 Connector Architecture

Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of a Database Application Tables Connector



See Also: *Oracle Identity Manager Administrative and User Console Guide* for conceptual information about providers and data sets

The latest version of this guide is available on Oracle Technology Network.

This diagram shows the providers that constitute the connector. The position of each provider is based on its role during reconciliation or provisioning.

The Transformation and Validation Providers are optional elements of the connector. Predefined Transformation and Validation Providers are shipped as part of the generic technology connector framework. Refer to *Oracle Identity Manager Administrative and User Console Guide* for information about these predefined providers.

The following predefined providers are the building blocks of the connector:

Note: The provider parameters mentioned in this section are described later. While creating the connector, you specify values for these parameters. The providers use the parameter values to perform their intended function. For example, the Reconciliation and Provisioning Transport Providers use the Database URL parameter to connect to the target system.

Some of the parameters are common to both the provisioning and reconciliation providers. For example, the Database Driver parameter is common to both the Database Application Tables Reconciliation Transport Provider and the Database Application Tables Provisioning Transport Provider.

- **Database Application Tables Reconciliation Transport Provider**

  This provider uses a SQL query to fetch data from the target system. The column names for the SELECT clause of the SQL query are derived from the field mappings that you create while performing the procedure described in "Step 3: Modify Connector Configuration Page" on page 3-15. The table names for the FROM clause are derived from the values of the Parent Table/View Name and Child Table/View Names parameters. The WHERE clause is derived from the value of the Customized Query parameter. This clause is optional. In other words, it is not mandatory to enter a value for the Customized Query parameter.

  If the primary key constraint cannot be set in the target system, then you use the Unique Attribute parameter to specify the name of the primary key column.

  If the primary key constraint has been set between the parent and child tables (or views), then the provider can automatically detect the primary key. In this scenario, the value of the Unique Attribute parameter is ignored.

  Similarly, if the target system is composed of more than one table or view, then this provider can automatically detect and use referential integrity constraints that have been set between the tables. However, if referential integrity constraints have not been set between parent and child tables, then you can use the Unique Attribute parameter to specify the name of the column that you want to use as the foreign key. The only requirement is that the name of the column must be the same in the parent and child tables.

  The result set fetched by the SQL query is in a format that is supported by the predefined Reconciliation Format Provider.

- **Database Application Tables Reconciliation Format Provider**

This provider converts the format of data fetched by the Database Application Tables Reconciliation Transport Provider into a format supported by Oracle Identity Manager.

- **Database Application Tables Provisioning Format Provider**

  This provider converts the format of data sent from Oracle Identity Manager into a format supported by the target system.

- **Database Application Tables Provisioning Transport Provider**

  This provider uses INSERT, UPDATE, and DELETE statements to perform provisioning operations on the target system. Like the Database Application Tables Reconciliation Transport Provider, this provider can detect primary and foreign key constraints that are set in the target system. Similarly, if the primary and foreign keys have not been set in the target system, then the value of the Unique Attribute parameter is used during connector operations.

1.3.2 Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified users on the target system and using this data to add or modify resources assigned to OIM Users. See *Oracle Identity Manager Connector Concepts* for conceptual information about target resource reconciliation.

The scheduled task that you use to start a target resource reconciliation run is automatically created when you create the connector.

> **See Also:** The "Connector Objects Created by the Generic Technology Connector Framework" chapter in *Oracle Identity Manager Administrative and User Console Guide* on Oracle Technology Network.

Supported Target Resource Reconciliation Functions

The connector supports any of the following actions during a target resource reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.
- Deletion of child data from accounts on the target system results in deletion of the same data from the resource. For example, if user John Doe is removed from the Leave Approvers group on the target system, then the same action is performed on the resource assigned to the OIM User John Doe.

> **Note:** Reconciliation of user account deletion on the target system is not supported in this release.

Reconciliation Rules

You create the reconciliation rule when you perform the procedure described in "Step 3: Modify Connector Configuration Page" on page 3-15.

You can modify the default rule conditions and actions that are created automatically at the end of the connector creation process. The procedure is described later in this guide.

1.3.3 Provisioning

Provisioning involves creating or modifying a user's data on the target system through Oracle Identity Manager. See *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning.

The connector supports the following provisioning functions:

- Create an account
- Update an account
- Enable an account
- Disable an account
- Delete an account

1.3.4 Trusted Source Reconciliation

The connector supports any of the following actions during a trusted source reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

Note: Reconciliation of user account deletion on the target system is not supported in this release.

Reconciliation Rules

You create the reconciliation rule when you perform the procedure described in "Step 3: Modify Connector Configuration Page" on page 3-15.

You can modify the default rule conditions and actions that are created automatically at the end of the connector creation process. The procedure is described later in this guide.

1.4 Roadmap for Deploying and Using the Connector

Note: Before you start creating the connector, it is recommended that you read and familiarize yourself with the generic technology connector information in *Oracle Identity Manager Administrative and User Console Guide*. The latest version of this guide is available on Oracle Technology Network.

The following is a summary of the rest of the content in this guide:

- Chapter 2, "Tasks to Be Performed Before You Create the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system before you can start creating Database Application Tables connectors.
- Chapter 3, "Creating the Connector" describes the procedure to create Database Application Tables connectors. This procedure is based on the "Using the Administrative and User Console to Create the Generic Technology Connector" section in *Oracle Identity Manager Administrative and User Console Guide*.

- Chapter 4, "Known Issues" lists the known issues that you may encounter while using Database Application Tables connectors.
- Appendix A, "An Example of the Procedure to Create Connectors" demonstrates the procedure to create a Database Application Tables connector.
- Appendix B, "Screenshots of the Step 3: Modify Connector Configuration Page" presents screenshots of pages that you encounter while creating Database Application Tables connectors. These screenshots are referenced in Chapter 3.

2

Tasks to Be Performed Before You Create the Connector

The following sections of this chapter describe the procedures that you must perform before you create the connector:

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

2.1 Configuring Oracle Identity Manager

This section describes the following procedures:

- Enabling Logging
- Adding New User-Defined Fields for the OIM User
- Using Lookup Definitions
- Copying the JDBC Drivers
- Exchanging Account Status Data with the Target System
- Copying the Provider Files

2.1.1 Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

  This level enables logging of information about error events that may allow the application to continue running.

- FATAL

  This level enables logging of information about very severe error events that could cause the application to stop functioning.

- OFF

  This level disables logging for all events.

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

- **BEA WebLogic Server**

  To enable logging:

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

     ```
     log4j.logger.OIMCP.DATC=LOG_LEVEL
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.DATC=INFO
     ```

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

  WEBLOGIC_HOME/user_projects/domains/*DOMAIN_NAME*/*SERVER_NAME*/*SERVER_NAME*.log

- **IBM WebSphere Application Server**

  To enable logging:

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

     ```
     log4j.logger.OIMCP.DATC=LOG_LEVEL
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.DATC=INFO
     ```

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

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/startServer.log

- **JBoss Application Server**

  To enable logging:

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

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

```
</category>
```

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

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

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

JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

To enable logging:

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

```
log4j.logger.OIMCP.DATC=LOG_LEVEL
```

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

For example:

```
log4j.logger.OIMCP.DATC=INFO
```

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

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

2.1.2 Adding New User-Defined Fields for the OIM User

Note: This is an optional procedure. Perform this procedure only if you want to add fields to the standard set of OIM User fields.

While creating the connector, when you perform the procedure described in "Step 3: Modify Connector Configuration Page" on page 3-15, you create mappings between the OIM User fields and the corresponding target system fields (columns). If there are additional target system fields that you want to use during reconciliation or provisioning, then you can extend the set of OIM User fields by creating user-defined fields (UDFs). See *Oracle Identity Manager Design Console Guide* for information about creating UDFs.

The following are the standard OIM User fields:

- User ID
- First Name
- Last Name
- Organization Name
- Employee Type
- Role
- Password
- Middle Name
- Status

- Provisioned Date
- Creation Date
- Manager ID
- End Date
- Start Date
- Email

2.1.3 Using Lookup Definitions

Note: This is an optional procedure. Perform this procedure only if you want to use lookup definitions as the input source for some of the fields on the process form during provisioning operations.

If you are configuring the connector for provisioning, then you may want to create lookup fields on the process form. For example, during provisioning operations, you may want to select the Country Code value from a lookup field. While creating the connector, you can set up this field as a lookup field by specifying an input source (other than the target system) for the field.

You can use a lookup definition as the input source. For example, you can create a lookup definition containing country codes and then set up the lookup definition as the input source for the Country field. If you want to use a lookup definition as the input source, then you must first create it.

See Also: The "Lookup Definition Form" section in *Oracle Identity Manager Design Console Guide* for information about creating lookup definitions

Alternatively, you can create a lookup field that uses columns from Oracle Identity Manager database tables as its input source. For example, if country code values are stored in any Oracle Identity Manager database table, then you can use the columns of that table as the input source for the Country Code lookup field.

While performing the procedure described in "Step 3: Modify Connector Configuration Page" on page 3-15, you specify the custom lookup definition as the input source.

2.1.4 Copying the JDBC Drivers

Note: If the target system version is the same as the version of the database that Oracle Identity Manager is using, then you need not perform the procedure described in this section. This is because the JDBC drivers have already been copied into the specified application server directories on Oracle Identity Manager.

Depending on the target system that you use, download one of the following sets of JDBC drivers from the vendor's Web site:

- For IBM DB2/UDB:
  - For all platforms: db2jcc.jar

  - For Microsoft Windows and UNIX platforms: db2jcc_license_cu.jar
  - For IBM z/OS platforms: db2jcc_license_cisuz.jar
- For Microsoft SQL Server:
  - sqljdbc.jar version 1.2
- For Oracle Database:
  - Oracle Database 10*g* release 2 (10.2.0.1), (10.2.0.2), or (10.2.0.3) drivers
  - Oracle Database 11*g* release 1 (11.1.0.6) drivers

Depending on the application server that you use, copy the JDBC drivers into one of the following directories:

Note: In a clustered environment, copy the JDBC drivers into this directory on each node of the cluster.

- For BEA WebLogic Server:

  WEBLOGIC_HOME/java/jre/lib/ext
- For JBoss Application Server:

  JAVA_HOME/jre/lib/ext
- For IBM WebSphere Application Server:

  WEBSPHERE_HOME/java/jre/lib/ext
- For Oracle Application Server:

  ORACLE_HOME/jdk/jre/lib/ext

2.1.5 Exchanging Account Status Data with the Target System

This section discusses the following topics:

- Configuring Account Status Reconciliation
- Configuring Account Status Provisioning

2.1.5.1 Configuring Account Status Reconciliation

For a target system that you configure as a target resource, Oracle Identity Manager expects the following account status values during reconciliation:

- Enabled
- Disabled

If you are configuring the target system as a target resource and if the target system uses the same status values, then you need not perform the procedure to configure account status reconciliation.

Similarly, for a target system that you configure as a trusted source, Oracle Identity Manager expects the following account status values during reconciliation:

- Active
- Disabled

If you are configuring the target system as a trusted source and if the target system uses the same status values, then you need not perform the procedure to configure account status reconciliation.

However, if the target system does not use status values that are compatible with Oracle Identity Manager, then you must configure account status reconciliation as follows:

Note: For detailed instructions to perform these steps, see "Configuring Account Status Reconciliation" in the "Predefined Generic Technology Connector Providers Shipped with Oracle Identity Manager" chapter of *Oracle Identity Manager Administrative and User Console Guide*. The latest version of this guide is available on Oracle Technology Network.

---

1. Create a lookup definition that maps the status values used in the target system with the status values used in Oracle Identity Manager.
2. While creating the connector, use the Translation Transformation Provider to create a transformation mapping between the fields that hold account status values in the Source and Reconciliation Staging data sets. The Translation Transformation Provider converts the target system status values into values that are compatible with Oracle Identity Manager.
3. Create a mapping between the field that holds account status values in the Reconciliation Staging data set and one of the following fields:
   - The OIM Object Status field of the OIM - Account data set, for target resource reconciliation

     ---

     Note: You must remove the status field that is shown in the OIM - Account data set after metadata detection.

   - The Status field of the OIM - User data set, for trusted source reconciliation

2.1.5.2 Configuring Account Status Provisioning

For a target system that you configure as a target resource, Oracle Identity Manager sends the following account status values during provisioning:

- enable
- disable

If the target system does not use the same values, then you must perform the following steps:

1. Create a lookup definition that maps the status values used in Oracle Identity Manager with the status values used in the target system.

   See Also: *Oracle Identity Manager Design Console Guide* for information about creating lookup definitions

   The following table shows the Code Key and Decode values for the lookup definition that you must create:

Code Key	Decode
enable	*Status value used in the target system for an account that is in the Enabled state*
disable	*Status value used in the target system for an account that is in the Disabled state*

2. While performing the procedure described in "Step 2: Specify Parameter Values Page" on page 3-10:
   - Use the Status Attribute parameter to enter the name of the target system column that stores account status values.
   - Use the Status Lookup Code parameter to enter the name of the lookup definition that you create.
3. While performing the procedure described in "Step 3: Modify Connector Configuration Page" on page 3-15, remove the status field from the Provisioning Staging data sets and from the OIM - Account data set.

2.1.6 Copying the Provider Files

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

The files that contain the definitions of the predefined providers are placed in the Database Application Tables directory on the installation media. You must run the Connector Installer to copy these files to specified directories on the Oracle Identity Manager computer.

To copy the provider files to Oracle Identity Manager:

1. Copy the Database Application Tables directory from the installation media into the following directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory
2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console Guide*. The latest version of this guide is available on Oracle Technology Network.
3. Click **Deployment Management**, and then click **Install Connector**.
4. From the **Connector List** list, select the connector that you want to install. This list displays the names and release numbers of connectors whose installation files you copy into the ConnectorDefaultDirectory directory.

   If you have copied the Database Application Tables directory into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the **Connector List** list, select the connector that you want to install.
5. Click **Load**.

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

   You can ignore the messages that are displayed after the process is completed.

7. Click **Finish**.

8. Restart Oracle Identity Manager.

Table 2–1 lists the provider files and their destination directories on Oracle Identity Manager.

Table 2–1 Provider Files for the Connector

File in the Installation Media Directory	Description	Destination Directory
lib/DatabaseApplicationTables.jar	This file contains the code implementation of all the providers.	*OIM_HOME*/xellerate/JavaTasks
Files in the ProviderDefinitions directory ■ DBProvisioningFormat.xml ■ DBProvisioningTransport.xml ■ DBReconFormat.xml ■ DBReconTransport.xml	Each XML file in this directory contains the definition of one of the predefined providers.	*OIM_HOME*/xellerate/GTC/ProviderDefinitions
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.	*OIM_HOME*/xellerate/connectorResources

2.2 Configuring the Target System

Configuring the target system involves performing the following optional procedures:

- Using Read-Only Views
- Ensuring That There Are No Target System Columns Named ID

2.2.1 Using Read-Only Views

Note: This is an optional procedure. Perform this procedure only if the target system is composed of read-only views.

Provisioning involves updating data stored in the target system. If the target system is composed of read-only views, then you must create INSTEAD OF triggers to enable modification of the read-only views during provisioning operations. For information about creating INSTEAD OF triggers, refer to the documentation for the target system database.

2.2.2 Ensuring That There Are No Target System Columns Named ID

Note: This is an optional procedure. Perform this procedure only if you are creating a connector for target resource reconciliation.

When you start creating the connector by using the Administrative and User Console, the ID field is added by default to the OIM - Account data set. Database Application Tables connectors do not need to use this field. If the target system were to contain a column named ID, then that column would overwrite the default ID field and the connector would not be created correctly. As a workaround, you can create a view based on the table and provide a different name for the column named ID.

2.2.3 Configuring IBM DB2/UDB Running on IBM z/OS

During a provisioning operation, the connector runs Java stored procedures to perform the required action on the target system. If your IBM DB2/UDB installation is running on IBM z/OS, then you must configure the WLM to enable the running of these stored procedures. See IBM z/OS documentation for detailed information about configuring the WLM.

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

Note: It is recommended that you perform the procedure described in this section to secure communication between the target system and Oracle Identity Manager.

The procedure to secure communication depends on the database that you are using:

- Configuring Secure Communication Between IBM DB2/UDB and Oracle Identity Manager
- Configuring Secure Communication Between Microsoft SQL Server and Oracle Identity Manager
- Configuring Secure Communication Between Oracle Database and Oracle Identity Manager

2.3.1 Configuring Secure Communication Between IBM DB2/UDB and Oracle Identity Manager

Note: IBM DB2/UDB version 9.1 Fix Pack 2 and later support secure communication over SSL.

SSL communication is not supported if IBM DB2/UDB is running on IBM z/OS. This has been mentioned in the "Known Issues" chapter.

To configure secure communication between IBM DB2/UDB and Oracle Identity Manager:

1. Refer to IBM DB2/UDB documentation for information about enabling SSL communication between IBM DB2/UDB and a client system. In this context, the client is Oracle Identity Manager.

   Export the certificate on the IBM DB2/UDB host computer.

2. Copy the certificate to the Oracle Identity Manager host computer.

3. Import the certificate into the JVM truststore of the application server on which Oracle Identity Manager is running.

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

   ```
   ..\..\bin\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 truststore.
   - Replace *TRUSTSTORE_LOCATION* with one of the truststore paths from Table 2–3. This table shows the location of the truststore for each of the supported application servers.

     Note: For a clustered configuration, you must import the file into the truststore on each node of the cluster.

Table 2–2 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
BEA WebLogic Server	*BEA_HOME*/java/jre/lib/security/cacerts
IBM WebSphere Application Server	*WEBSPHERE_HOME*/java/jre/lib/security/cacerts
JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts

2.3.2 Configuring Secure Communication Between Microsoft SQL Server and Oracle Identity Manager

To configure secure communication between Microsoft SQL Server and Oracle Identity Manager:

1. Refer to Microsoft SQL Server documentation for information about enabling SSL communication between Microsoft SQL Server and a client system. In this context, the client is Oracle Identity Manager.

   Export the certificate on the Microsoft SQL Server host computer.

2. Copy the certificate to the Oracle Identity Manager host computer.

3. Import the certificate into the JVM truststore of the application server on which Oracle Identity Manager is running.

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

   ```
   ..\..\bin\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 truststore.
- Replace *TRUSTSTORE_LOCATION* with one of the truststore paths from Table 2–3. This table shows the location of the truststore for each of the supported application servers.

Note: For a clustered configuration, you must import the file into the truststore on each node of the cluster.

Table 2–3 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
BEA WebLogic Server	*BEA_HOME*/java/jre/lib/security/cacerts
IBM WebSphere Application Server	*WEBSPHERE_HOME*/java/jre/lib/security/cacerts
JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts

2.3.3 Configuring Secure Communication Between Oracle Database and Oracle Identity Manager

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

- Configuring Data Encryption and Integrity in Oracle Database
- Configuring SSL Communication in Oracle Database

2.3.3.1 Configuring Data Encryption and Integrity in Oracle Database

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

2.3.3.2 Configuring SSL Communication in Oracle Database

Note: Database Application Tables connectors do not support SSL communication between an Oracle Database target system and Oracle Identity Manager running on IBM WebSphere Application Server or Oracle Application Server. This is also mentioned in the "Known Issues" chapter (see Bug 6696248).

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

1. Refer to *Oracle Database Advanced Security Administrator's Guide* for information about enabling SSL communication between Oracle Database and Oracle Identity Manager.

   Export the certificate on the Oracle Database host computer.

2. Copy the certificate to Oracle Identity Manager.
3. Import the certificate into the JVM truststore of the application server on which Oracle Identity Manager is running.

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

   ```
   ..\..\bin\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 truststore.
   - Replace *TRUSTSTORE_LOCATION* with one of the truststore paths from Table 2–4. This table shows the location of the truststore for each of the supported application servers.

     Note: For a clustered configuration, you must import the file into the truststore on each node of the cluster.

Table 2–4 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
BEA WebLogic Server	*WEBLOGIC_HOME*/java/jre/lib/security/cacerts
JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts

3

Creating the Connector

This chapter contains the following sections:

- The "Limited Reconciliation" section discusses the Customized Query and Use Native Query parameters.
- The "Determining Values for the Database URL and Connection Properties Parameters" discusses the Database URL and Connection Properties parameters.
- The "Creating the Connector" section describes the procedure to create the connector.
- The "Performing Connector Operations" section provides a link to guidelines that you must apply when you start using the connector.

3.1 Limited Reconciliation

This section discusses the Customized Query and Use Native Query parameters. You apply the information in this section while performing the procedure described in "Step 2: Specify Parameter Values Page" on page 3-10.

By default, all target system records that are added or modified after the previous reconciliation run are reconciled during the current reconciliation run. You can filter records for reconciliation by specifying the subset of newly added or modified records that must be reconciled. You implement this form of limited reconciliation by using a customized query for reconciliation.

You create a customized query by specifying a value for the Customized Query parameter. The value of this parameter becomes a component of the WHERE clause in the SQL query that is used to fetch records from the target system.

Note: While performing the procedure described in "Step 2: Specify Parameter Values Page" on page 3-10, if you specify a value for the Timestamp Attribute parameter, then you need not include the time-stamp column in the Customized Query parameter.

The following are examples of the WHERE clause that you can specify as the value of the Customized Query parameter. In these examples, `jdoe` is the database user ID and `employees` is the name of the table that holds user data.

- The following WHERE clause component returns records of employees whose last names begin with `Roe` and who belong to the `Finance` department.

```
jdoe.employees.last_name LIKE 'Roe%' & jdoe.employees.dept_id = 'Finance'
```

- The following WHERE clause component returns records of employees who report to the manager with the ID `856` or employees who belong to the `Finance` department.

```
jdoe.employees.mgr_id = 856 | jdoe.employees.dept_id = 'Finance'
```

Note:

- The value that you specify must not contain the keyword `WHERE`.
- The value that you specify must not contain a SQL join between parent and child tables.

Instead of using the & and | operators, you can use any of the logical operators supported by the target system database. To specify the operators that you want to use, use the Use Native Query check box as follows:

- Select the Use Native Query check box if you want to use logical operators that are native to the target system database.
- Do not select the Use Native Query check box if you want to use the & and | operators.

If you do not want to use a customized query, then do not specify a value for this parameter. If you do not specify a value, then regular (that is, not limited) reconciliation is performed.

3.2 Determining Values for the Database URL and Connection Properties Parameters

This section discusses the Database URL and Connection Properties parameters. You apply the information in this section while performing the procedure described in "Step 2: Specify Parameter Values Page" on page 3-10.

The values that you specify for the Database URL and Connection Properties parameters depend on the target system:

- Database URL and Connection Properties for Microsoft SQL Server
- Database URL and Connection Properties for Oracle Database

3.2.1 Database URL and Connection Properties for IBM DB2/UDB

The following are guidelines on specifying the Database URL and Connection Properties parameters:

- **Database URL parameter**

  Enter the following component of the connection URL as the value of the Database URL provider:

```
jdbc:db2://[SERVER_NAME[\INSTANCE_NAME][:PORT_NUMBER]]
```

  In this format:

  – *SERVER_NAME* is the IP address (not the host name) of the target system host computer.

  – *INSTANCE_NAME* is the name of the target system database.

– *PORT_NUMBER* is the port at which the target system database is listening.

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

```
jdbc:db2://192.168.16.76:50000
```

- **Connection Properties parameter**

  Enter the following component of the connection URL as the value of the Connection Properties parameter:

  ```
  [,PROPERTY=VALUE[,PROPERTY=VALUE]] . . .
  ```

  In this format:

  – *PROPERTY* is the name of one or more database connection properties, such as `applicationName` and `disableStatementPooling`.

  – *VALUE* is the value of each database connection property whose name you specify by using the *PROPERTY* placeholder.

  Note: Semicolons must be changed to commas in the value that you specify.

  The following is a sample value for the Connection Properties parameter:

  ```
  databaseName=sales,port=50000
  ```

  If you enable SSL communication between IBM DB2/UDB and Oracle Identity Manager, then you must include the `sslConnection`, `javax.net.ssl.trustStore`, and `javax.net.ssl.trustStorePassword` properties in the value that you specify for the Connection Properties parameter. In other words, the following must be part of the string that you enter as the value of the parameter:

  ```
  sslConnection=true,javax.net.ssl.trustStore=STORE_LOCATION,javax.net.ssl.trustS
  torePassword=STORE_PASSWORD
  ```

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

  For example:

  ```
  sslConnection=true,Djavax.net.ssl.trustStore=C:/j2sdk1.4.2_12/jre/lib/security/
  cacerts,javax.net.ssl.trustStorePassword=changeit
  ```

3.2.2 Database URL and Connection Properties for Microsoft SQL Server

Note: In Microsoft SQL Server documentation, the term "connection URL" is used instead of "database URL."

In Oracle Identity Manager release 9.1.0, the semicolon (;) is one of the special characters that cannot be entered in any of the fields of the Administrative and User Console. This restriction has been introduced for security reasons. However, a typical Microsoft SQL Server connection URL contains a semicolon-separated property-value pair in the following format:

```
jdbc:sqlserver://[SERVER_NAME[\INSTANCE_NAME][:PORT_NUMBER]][;PROPERTY=VALUE[;PROPERTY=VALUE]]
```

> **See Also:** The "Setting the Connection Properties" section on the Microsoft Web site for detailed information about the properties that you can specify by using this format

To work around the restriction on entering semicolons, you can specify the connection URL as the value of the following provider parameters:

- **Database URL parameter**

  Enter the following component of the connection URL as the value of the Database URL provider:

  ```
  jdbc:sqlserver://[SERVER_NAME[\INSTANCE_NAME][:PORT_NUMBER]]
  ```

  In this format:

  - *SERVER_NAME* is the IP address (not the host name) of the target system host computer.
  - *INSTANCE_NAME* is the name of the target system database.
  - *PORT_NUMBER* is the port at which the target system database is listening.

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

  ```
  jdbc:sqlserver://192.168.16.76:1433
  ```

- **Connection Properties parameter**

  Enter the following component of the connection URL as the value of the Connection Properties parameter:

  ```
  [,PROPERTY=VALUE[,PROPERTY=VALUE]] . . .
  ```

  In this format:

  - *PROPERTY* is the name of one or more database connection properties, such as `applicationName` and `disableStatementPooling`.
  - *VALUE* is the value of each database connection property whose name you specify by using the *PROPERTY* placeholder.

  > **Note:** Semicolons must be changed to commas in the value that you specify.

  The following is a sample value for the Connection Properties parameter:

  ```
  databaseName=sales,port=1433
  ```

  If you enable SSL communication between Microsoft SQL Server and Oracle Identity Manager, then you must include the `encrypt` and `hostNameInCertificate` properties in the value that you specify for the Connection Properties parameter. In other words, the following must be part of the string that you enter as the value of the parameter:

  ```
  encrypt=true,hostNameInCertificate=HOST_NAME
  ```

  Replace *HOST_NAME* with the host name given in the certificate that you use.

In addition, you must specify the location of the truststore if you import the certificate into a truststore other than the JVM truststore of Oracle Identity Manager. To specify the location of the truststore, include the following properties in the value that you specify for the Connection Properties parameter:

```
encrypt=true,hostNameInCertificate=HOST_NAME,trustStore=STORE_LOCATION,trustStorePassword=STORE_PASSWORD
```

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

3.2.3 Database URL and Connection Properties for Oracle Database

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

- Only Data Encryption and Integrity Is Configured
- Only SSL Communication Is Configured
- Both Data Encryption and Integrity and SSL Communication Are Configured

3.2.3.1 Only Data Encryption and Integrity Is Configured

If you have configured only data encryption and integrity, then enter the following values:

- **Database URL parameter**

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

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

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

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

- **Connection Properties parameter**

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

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

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

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

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

Note:

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

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

3.2.3.2 Only SSL Communication Is Configured

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

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

Sample Format 1:

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

Sample Format 2:

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

Sample Format 3:

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

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

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

Database URL parameter

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

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

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

Connection Properties parameter

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

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

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

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

3.2.3.3 Both Data Encryption and Integrity and SSL Communication Are Configured

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

- **Database URL parameter**

  While creating the connector, to specify a value for the Database URL parameter, enter a comma-separated combination of the values for the Database URL parameter described in the "Only Data Encryption and Integrity Is Configured" and "Only SSL Communication Is Configured" sections. For example:

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

- **Connection Properties parameter**

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

```
oracle.net.encryption_client=REQUIRED,oracle.net.encryption_types_client=(3DES1
68),oracle.net.crypto_checksum_client=REQUESTED,oracle.net.crypto_checksum_type
s_client=(MD5),javax.net.ssl.trustStore=STORE_LOCATION,javax.net.ssl.trustStore
Type=JKS,javax.net.ssl.trustStorePassword=STORE_PASSWORD
```

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

3.3 Creating the Connector

To navigate to the first Administrative and User Console page for creating generic technology connectors, log in to the Administrative and User Console, expand **Generic Technology Connector**, and then click **Create**.

From this point onward, page-wise instructions are provided in the following sections:

Note: While performing the procedures described in these sections, you must read the instructions given in the corresponding sections of *Oracle Identity Manager Administrative and User Console Guide*. The latest version of this guide is on Oracle Technology Network.

- Step 1: Provide Basic Information Page
- Step 2: Specify Parameter Values Page
- Step 3: Modify Connector Configuration Page
- Step 4: Verify Connector Form Names Page
- Step 5: Verify Connector Information Page

The following sections describe additional configuration procedures that can be performed after you create the connector:

- Modifying the Default Action Rules
- Configuring Reconciliation
- Configuring Provisioning

3.3.1 Step 1: Provide Basic Information Page

On the Step 1: Provide Basic Information page, perform the following steps:

1. In the **Name** field, specify a name for the connector.

   See the guidelines on specifying a name for a generic technology connector given in the "Step 1: Provide Basic Information Page" section of *Oracle Identity Manager Administrative and User Console Guide*.

2. If you want to use the connector for reconciliation, select **Reconciliation** and then perform the following steps:

- From the Transport Provider list, select **Database Application Tables Reconciliation Transport Provider**.
- From the Format Provider list, select **Database Application Tables Reconciliation Format Provider**.
- If you want to use the connector to perform trusted source reconciliation with the target system, then select **Trusted Source Reconciliation**.

Note: If you select the Trusted Source Reconciliation check box, then the Provisioning region of the page is disabled. This is because you cannot use the connector for both trusted source reconciliation and provisioning.

3. If you want to use the connector for provisioning, select **Provisioning** and then perform the following steps:

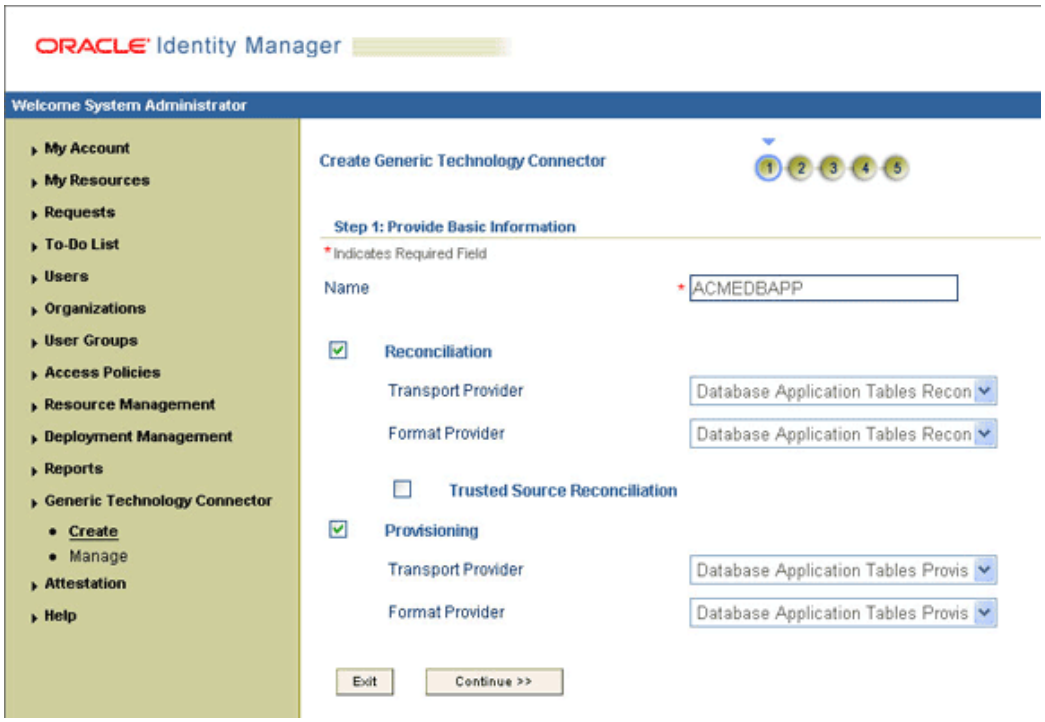
Note: You can select only Reconciliation, only Provisioning, or both Reconciliation and Provisioning.

- From the Transport Provider list, select **Database Application Tables Provisioning Transport Provider**.
- From the Format Provider list, select **Database Application Tables Provisioning Format Provider**.

4. Click **Continue**.

Figure 3–1 shows the Step 1: Provide Basic Information page on which sample entries have been made.

Figure 3–1 Step 1: Provide Basic Information Page



3.3.2 Step 2: Specify Parameter Values Page

On the Step 2: Specify Parameter Values page, specify values for the provider parameters and then click **Continue**.

Table 3–1 lists the parameters that are displayed on the Step 2: Specify Parameter Values page. The display of parameters on this page depends on the options that you select on the Step 1: Provide Basic Information page. For example, the Target Date Format parameter is a provisioning-specific parameter and it is displayed only if you select **Provisioning** on the Step 1: Provide Basic Information page.

As mentioned in "Connector Architecture" on page 1-4, some of the parameters are common to both provisioning and reconciliation providers. If you select both **Reconciliation** and **Provisioning** on the Step 1: Provide Basic Information page, then the common parameters are displayed twice on this page. Unless specified otherwise, the parameters listed in this table are common to both reconciliation and provisioning providers.

Note: For parameters that are common (displayed twice), you must enter the same value in both fields. For example, suppose you enter `dbapps` as the value of the Database User ID parameter for provisioning. You must enter the same value for the Database User ID parameter for reconciliation.

Only the value entered for the first occurrence of the parameter is validated when you submit the data entered on the Step 2: Specify Parameter Values page. In the preceding example, if you enter an incorrect value in the Database User ID parameter for reconciliation, then this error is caught only when you try to use the connector for reconciliation.

Table 3–1 Parameters Displayed on the Step 2: Specify Parameter Values Page

Parameter	Description
Run-Time Parameters	
Database Driver	Specify the JDBC driver class. For IBM DB2/UDB database: com.ibm.db2.jcc.DB2Driver For Microsoft SQL Server: `com.microsoft.sqlserver.jdbc.SQLServerDriver` For Oracle Database: `oracle.jdbc.driver.OracleDriver`
Database URL	Enter the database URL of the target database. The value that you specify depends on the database product that you are using. See "Determining Values for the Database URL and Connection Properties Parameters" on page 3-2 for more information.
Database User ID	Enter the user ID of the database user account that Oracle Identity Manager will use to connect to the target system. For example: `dbapps`
Database Password	Enter the password of the database user account that Oracle Identity Manager will use to connect to the target system.
Customized Query	Enter the WHERE clause specifying the subset of newly added or modified records that you want to reconcile. See "Limited Reconciliation" on page 3-1 for more information about this parameter.

Table 3–1 (Cont.) Parameters Displayed on the Step 2: Specify Parameter Values Page

Parameter	Description
Use Native Query	Select **Use Native Query** if you want to use logical operators native to the target system database in the value that you specify for the Customized Query parameter. Do not select **Use Native Query** if you want to use the & and | operators in the value that you specify for the Customized Query parameter. See "Limited Reconciliation" on page 3-1 for more information about this parameter.
Connection Properties	Specify the connection properties of the target database. The value that you specify depends on the database product that you are using. See "Determining Values for the Database URL and Connection Properties Parameters" on page 3-2 for more information.
Design Parameters	
Parent Table/View Name	Enter the name of the parent table or view. The value that you must enter depends on the target system database: ■ If the target system database is Microsoft SQL Server, then the table name must be provided in the `[Schema].[Table]` format (for example, `hr.employees`). ■ If the target system database is Oracle Database, then only the table name would suffice (for example, `employees`).
Child Table/View Names	If you want to use the connector for trusted source reconciliation, then do *not* enter a value. If you want to use the connector for target resource reconciliation and if user data is spread across parent and child tables, then enter a comma-separated list of child table names. The guidelines for specifying the table names are the same as those described for the Parent Table/View Name parameter.
Unique Attribute	If the primary key constraint cannot be set in the parent table, then enter the name of the column that uniquely identifies each row in the parent table. Similarly, if referential integrity constraints have not been set between parent and child tables, then use the Unique Attribute parameter to specify the name of the column that you want to use as the foreign key. The only requirement is that the name of the column must be the same in the parent and child tables. **Note:** If primary key and referential integrity constraints already exist and if you still specify a value for the Unique Attribute parameter, then the parameter is ignored and the integrity constraints defined in the database are used during reconciliation and provisioning.
Timestamp Attribute	Enter the name of the column (in the parent table or view) that holds time-stamp information. **Note:** If the target system is Oracle Database, then you must ensure that the data type of the column is either Date or Timestamp. This parameter is used only during reconciliation. See the description of the Reconciliation Type parameter later in this table.
Status Attribute	If you want to include account status data in provisioning operations, then enter the name of the target system column that stores account status values. **Note:** This parameter is used only during provisioning. See "Configuring Account Status Provisioning" on page 2-6 for details.
Status Lookup Code	If you want to include account status data in provisioning operations, then enter the name of the lookup definition described in "Configuring Account Status Provisioning" on page 2-6. **Note:** This parameter is used only during provisioning.

Table 3–1 (Cont.) Parameters Displayed on the Step 2: Specify Parameter Values Page

Parameter	Description
Database Date Format	■ Database Date Format parameter for reconciliation: Enter the *same* value that you enter for the Source Date Format parameter. This parameter is described later in this table. Do not enter a value for this parameter if you do not enter a value for the Source Date Format parameter. ■ Database Date Format parameter for provisioning: Enter the *same* value that you enter for the Target Date Format parameter. This parameter is described later in this table. Do not enter a value for this parameter if you do not enter a value for the Target Date Format parameter.
Target Date Format	See "Step 2: Specify Parameter Values Page" in *Oracle Identity Manager Administrative and User Console Guide* for detailed information about this parameter. If you enter a value for the Target Date Format parameter, then you must specify the same value for the Database Date Format parameter for provisioning. **Note:** This parameter is used only during provisioning. It is recommended that you do not enter a value for this parameter.
Batch Size	Enter a batch size (an integer value) for the reconciliation run. By using this parameter, you can break into batches the total number of records that the reconciliation engine fetches from the target system during each reconciliation run. You should specify a batch size that optimizes the performance of the reconciliation run. Default value: `All`
Stop Reconciliation Threshold	Enter a value for this parameter only if you want reconciliation to stop automatically if the percentage of records that fail the validation checks to the total number of reconciliation records processed exceeds the specified value. **See Also:** *Oracle Identity Manager Administrative and User Console Guide* for detailed information about this parameter
Stop Threshold Minimum Records	Enter a value for this parameter only if you specify a value for the Stop Reconciliation Threshold parameter. **See Also:** *Oracle Identity Manager Administrative and User Console Guide* for detailed information about this parameter

Table 3–1 (Cont.) Parameters Displayed on the Step 2: Specify Parameter Values Page

Parameter	Description
Source Date Format	See "Step 2: Specify Parameter Values Page" in *Oracle Identity Manager Administrative and User Console Guide* for detailed information about this parameter. If you want to validate the format of date values that are fetched from the target system during reconciliation, then enter a value for this parameter. Otherwise, do not enter a value for this parameter. If you enter a value for the Source Date Format parameter, then you must specify the same value for the Database Date Format parameter for reconciliation. **Note:** It is recommended that you do not enter a value for this parameter.
Reconcile Deletion of Multivalued Attribute Data	If you are configuring the connector for trusted source reconciliation, then do not select this check box. If you are configuring the connector for target resource reconciliation and if you want to reconcile into Oracle Identity Manager the deletion of child data on the target system, then select this check box.
Reconciliation Type	Use this check box to specify whether you want to use the connector to perform incremental or full reconciliation. In incremental reconciliation, only target system records that are newly added or modified after the last reconciliation run are brought to Oracle Identity Manager. Reconciliation events are created for each of these records. In full reconciliation, all target system records are brought to Oracle Identity Manager. The optimized reconciliation feature identifies and ignores records that have already been reconciled in Oracle Identity Manager. Reconciliation events are created for the remaining records. If you select **Incremental**, then you must also specify a value for the Timestamp Attribute parameter.

Figure 3–2 shows the first section of the Step 2: Specify Parameter Values page on which sample entries have been made.

Figure 3–2 First Section of the Step 2: Specify Parameter Values Page

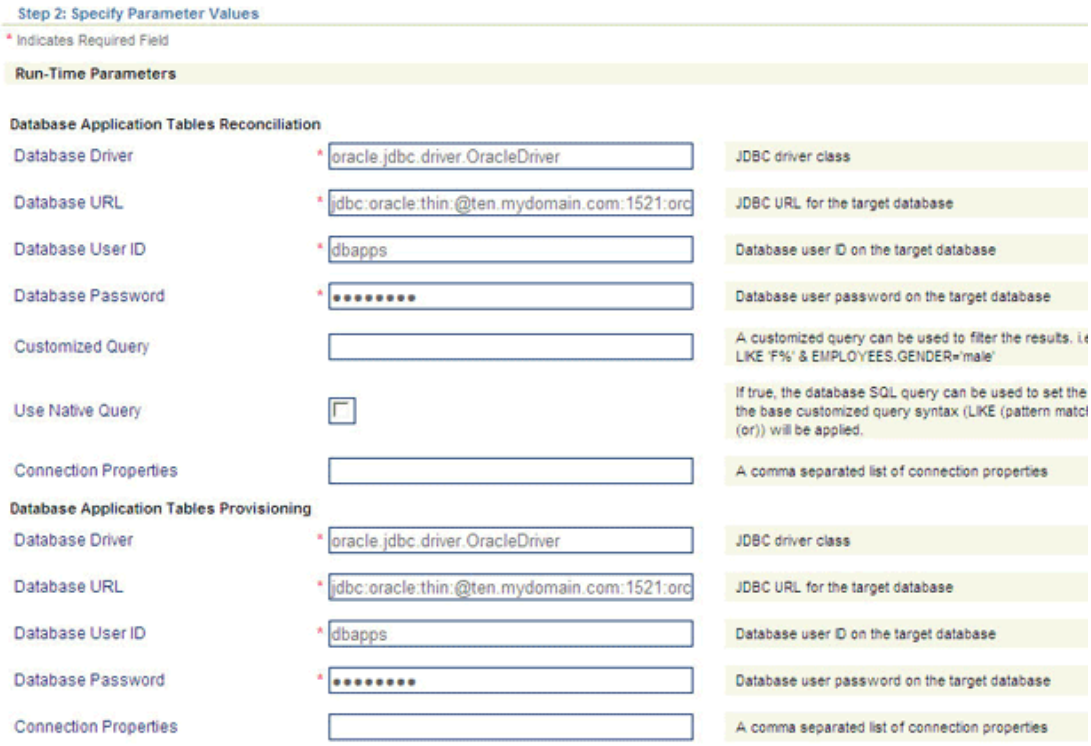


Figure 3–3 shows the second section of the Step 2: Specify Parameter Values page on which sample entries have been made.

Figure 3–3 Second Section of the Step 2: Specify Parameter Values Page

3.3.3 Step 3: Modify Connector Configuration Page

Note: See "Step 3: Modify Connector Configuration Page" in the "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide* for detailed information about the terms and procedures given in this section.

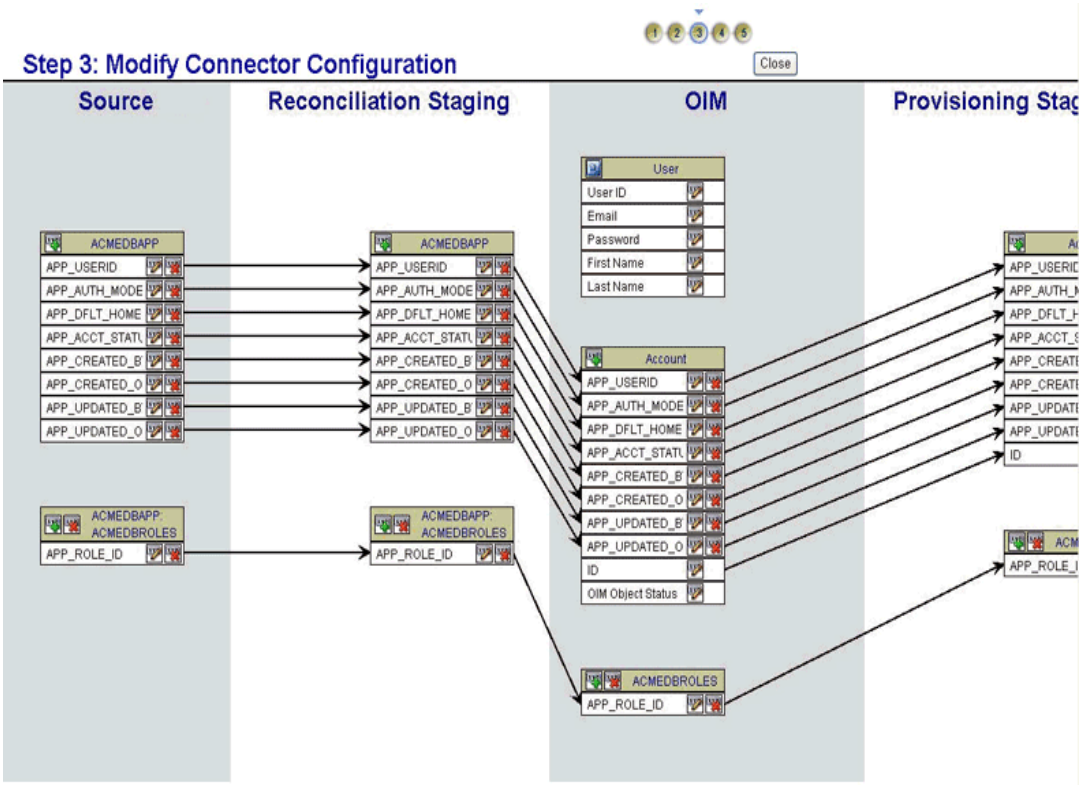
When you click **Continue** on the Step 2: Specify Parameter Values page, the generic technology connector framework tries to read metadata from the target system. If this operation is successful, then metadata is displayed on the Step 3: Modify Connector Configuration page in the form of data sets.

If metadata detection fails, then an error message is displayed and details of the cause of the error are recorded in the log file. If you encounter a metadata detection error,

then you must fix it before resuming the procedure from the Step 2: Specify Parameter Values page.

Figure 3–4 shows a screenshot of the Step 3: Modify Connector Configuration page after metadata detection has run on the sample target system described in the "Step 2: Specify Parameter Values Page" section.

Figure 3–4 Step 3: Modify Connector Configuration Page After Metadata Detection



The elements displayed on the Step 3: Modify Connector Configuration page depend on the input that you provide on the Step 1: Provide Basic Information page and Step 2: Specify Parameter Values page. For example, if you select the Trusted Source Reconciliation check box on the Step 1: Provide Basic Information page, then the OIM - Account data sets and Provisioning Staging data sets are not displayed. See Table 22-3, "Display of Data Sets and Fields Under Various Input Conditions" in the "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide* for more information.

You must perform the actions described in Table 3–2 by using the features provided by the Step 3: Modify Connector Configuration page.

Note:

- You can perform these actions in any sequence. For example, you can create the reconciliation rule before you specify the data type for fields in the Reconciliation Staging and OIM data sets.
- Some of the actions can be performed as parts of the same procedure. For example, while setting the data type and length of a field, you can also create a mapping between the field and a field in a different data set.
- See "Adding or Editing Fields" of *Oracle Identity Manager Administrative and User Console Guide* for details.
- See Appendix A, "An Example of the Procedure to Create Connectors" for sample steps.

Table 3–2 Actions to Be Performed on the Step 3: Modify Connector Configuration Page

Action	Description
Actions common to both target resource and trusted source configurations of the target system	
In the Reconciliation Staging and OIM data sets, you must designate fields as mandatory fields to duplicate NOT NULL constraints (including primary key constraints) of the target system tables.	While adding or editing a field, you can select the **Required** check box to specify that the field is a mandatory field. In the Reconciliation Staging and OIM data sets, you must select the **Required** check box for fields that represent columns for which the NOT NULL constraint has been set. See Figure B–1.
Create the reconciliation rule by creating a matching-only mapping between the primary key field of the Reconciliation Staging data set and the corresponding field of the OIM - User data set.	During reconciliation, the reconciliation rule forms the basis of entity matching in which target system records are compared with existing OIM Users. See *Oracle Identity Manager Connector Concepts* for more information about the reconciliation rule. To create the reconciliation rule, you must create a matching-only mapping between the unique field (primary key) of the Reconciliation Staging data set and the corresponding field of the OIM - User data set. For example, you can create a matching-only mapping between the APP_USERID field of the Reconciliation Staging data set and the User ID field of the OIM - User data set. See Point 4 in Figure B–6. If the primary key is composed of more than one target system field (column), then create matching-only mappings between each primary key field and the corresponding field of the OIM - User data set. **Note:** The outcome of the entity-matching operation is determined by the reconciliation action rules that you configure. See "Modifying the Default Action Rules" on page 3-22 for details.

Table 3–2 (Cont.) Actions to Be Performed on the Step 3: Modify Connector Configuration Page

Action	Description
Set the attributes (such as the data type and length) for the fields of the Reconciliation Staging data sets and the OIM - Account data sets.	At the end of the metadata detection process, default values for field attributes (such as the data type and length) are assigned to the fields displayed in the Reconciliation Staging and OIM - Account data sets. You must edit these fields and set the required attributes for them. For example, suppose the target system contains the HIRE_DATE and LAST_UPDATE columns. On the Step 3: Modify Connector Configuration page, you must edit the fields for these columns and set their data type to Date. Figure B–1 shows the Data Type list, which you can use to set the data type of a field. **Note:** If you select the Provisioning option on the Step 1: page, then after you create the connector, you must not modify the data type of the OIM - Account data sets fields. This is because a data type change does not result in the creation of a new version of the process form.
Remove fields that are not required.	You might not want to read data from (reconcile with) or send data to (provision to) some fields of the target system. You must remove such fields from all the data sets on the Step 3: Modify Connector Configuration page. **Note:** If you do not want to reconcile from or provision to the field that stores time-stamp values, then you can remove it from all the data sets. You can perform this action even if you have specified the name of the field as the value of the Timestamp Attribute parameter on the Step 2: Specify Parameter Values page.
If required, create or edit mappings to establish new flow lines, transform data, and validate data. **Note:** This is not a mandatory action.	In addition to the mappings created through metadata detection, you can create mappings to establish new data flow lines between fields of adjacent data sets. While adding or editing a mapping, you can add Transformation Providers to transform data that is in transit between fields of the following data sets: ▪ Source and Reconciliation Staging ▪ OIM and Provisioning Staging While adding or editing a mapping, you can add Validation Providers to validate data before it is sent to the Reconciliation Staging data sets.
If required, configure the exchange of account status data between the target system and Oracle Identity Manager. **Note:** This is not a mandatory action.	See "Exchanging Account Status Data with the Target System" on page 2-5 for more information. In addition, see Figure B–4, Figure B–5, and Figure B–6.
Specify that you want to encrypt the storage, display, or both storage and display of fields that store confidential data in Oracle Identity Manager.	The target system may store confidential data, such as salaries and passwords of employees. For fields of the OIM data sets that hold confidential data, you can specify that you want to encrypt the field values in the Oracle Identity Manager database (storage of the field) and on the Administrative and User Console (display of the field). See Figure B–3.
Do not add the foreign key field.	If a foreign key is defined in the target system, then the foreign key column is automatically identified during metadata detection. If the foreign key is not defined, then you must use the Unique Attribute parameter to specify the name of the column that links rows of the parent and child tables. In either case, the foreign key column (field) is not displayed on the Step 3: Modify Connector Configuration page. You *must not* add it on this page.
Actions specific to configuring the target system as a target resource	

Table 3–2 (Cont.) Actions to Be Performed on the Step 3: Modify Connector Configuration Page

Action	Description
If required, convert fields to lookup fields. **Note:** This is not a mandatory action.	If you are configuring the connector for provisioning, then you may want to create lookup fields on the process form. For example, during provisioning operations, you may want to select the Country Code value from a lookup field. The generic technology connector framework enables you to specify input sources for the lookup field. You can create a lookup field that uses columns from Oracle Identity Manager database tables as its input source. For example, if country code values are stored in any Oracle Identity Manager database table, then you can use the columns of that table as the input source for the Country Code lookup field. Alternatively, you can specify a lookup definition that you have created as the input source. This is discussed in "Using Lookup Definitions" on page 2-4.
Specify the key field for reconciliation matching.	During target resource reconciliation, the key field for reconciliation matching is used to match target system accounts with accounts provisioned to existing OIM Users. This key field forms the basis of process matching that is performed during reconciliation. To specify the key field for reconciliation matching, create a matching-only mapping between the unique field of the Reconciliation Staging data set and the corresponding field of the OIM - Account data set. See Figure B–6. **Note:** You must not use the ID field to create the key field for reconciliation matching. Ensure that there are no mappings (of any kind) between the ID field and fields of any other data set. Multiple fields of the OIM - Account data set can be (matching-only) mapped to corresponding fields of the Reconciliation Staging data set to create a composite key field for reconciliation matching. **Note:** The outcome of the process-matching operation is determined by the reconciliation action rules that you configure. See "Modifying the Default Action Rules" on page 3-22 for details.
Actions specific to configuring the target system as a trusted source	

Table 3–2 (Cont.) Actions to Be Performed on the Step 3: Modify Connector Configuration Page

Action	Description
Remove password fields from all data sets.	Reconciliation of password information is not supported in Oracle Identity Manager. You must remove password fields from all data sets.
Ensure that the mandatory fields required for creation of an OIM User are present.	If you are creating the connector for trusted source reconciliation and if the target system does not have columns for some of the mandatory fields of the OIM User form, then add these mandatory fields to the Reconciliation Staging data set and specify literal values as the input sources for these fields. The following are the mandatory fields of the OIM User form: ■ User ID ■ First Name ■ Last Name ■ Employee Type ■ User Type ■ Organization During trusted source reconciliation, you must ensure that there are target system fields that provide data for each of these mandatory OIM User fields. To ensure successful reconciliation, you must add fields corresponding to these target system fields in the Reconciliation Staging data set and specify literal values for the fields. To add a field: 1. Click the Add icon of the Reconciliation Staging data set. 2. On the Step 1: Provide Field Information page: - In the **Field Name** field, enter a name for the field. - From the Mapping Action list, select **Create Mapping Without Transformation**. - From the Data Type list, select **String**. 3. Click **Continue**. 4. On the Step 3: Provide Mapping Information page, select **Literal** and enter a value. The value depends on the field for which you are specifying a literal value. For example: - If are creating a field to be mapped to the Organization field, then enter the name of an existing Oracle Identity Manager organization. - If are creating a field to be mapped to the Employee Type field, then enter Full-Time, Part-Time, Temp, Intern, or Consultant. These are Code Key values of the Employee Type field. - If are creating a field to be mapped to the User Type field, then enter End-User or End-User Administrator. These are Code Key values of the User Type field. See Figure B–2. 5. Click **Continue** and then continue with the rest of the tasks that you want to perform on the Step 3: Modify Connector Configuration page. See Figure B–7.

Table 3–2 (Cont.) Actions to Be Performed on the Step 3: Modify Connector Configuration Page

Action	Description
If the target system has more columns than there are fields on the OIM User form, then create mappings between the UDFs that you created earlier and the corresponding fields of the Reconciliation Staging data sets.	The target system may have more columns than there are fields on the OIM User form. For example, the target system may have the Designation column, which has no corresponding field on the OIM User form. To enable the creation of OIM Users during trusted source reconciliation, you must create a UDF for the Designation field on the OIM User form *before* you start creating the connector. See "Adding New User-Defined Fields for the OIM User" on page 2-3 for more information. On the Step 3: Modify Connector Configuration page, you must create mappings between the UDFs in the OIM - User data set and corresponding fields of the Reconciliation Staging data sets. You use the Design Console to create UDFs. See *Oracle Identity Manager Design Console Guide* for information about creating UDFs. After you create the required UDFs, you must create mappings between them and the corresponding fields of the Reconciliation Staging data sets. See Figure B–7.

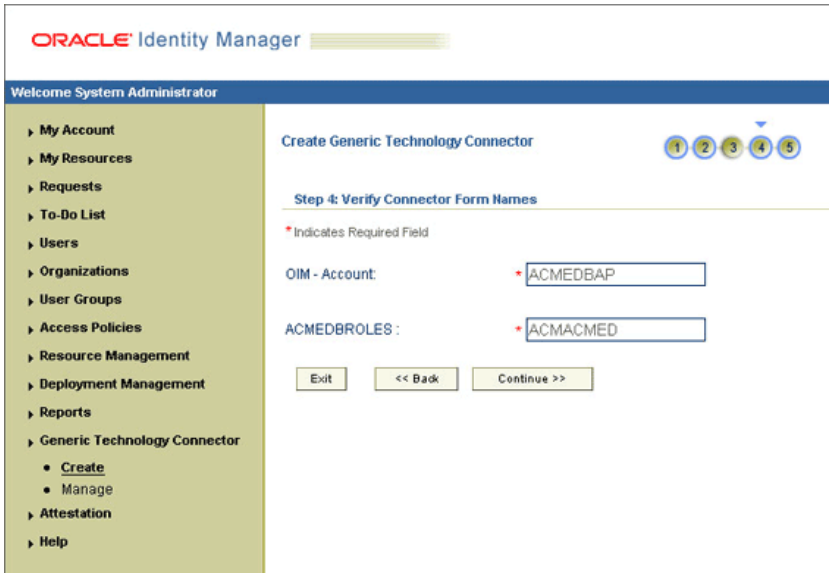
3.3.4 Step 4: Verify Connector Form Names Page

Note: This page is not displayed if you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page.

On the Step 4: Verify Connector Form Names page, click **Continue**.

Figure 3–5 shows the Step 4: Verify Connector Form Names page.

Figure 3–5 Step 4: Verify Connector Form Names Page



3.3.5 Step 5: Verify Connector Information Page

On the Step 5: Verify Connector Information page, click **Save**.

Note: If you encounter any errors at this stage, then see "Errors Encountered at the End of the Connector Creation Process" in *Oracle Identity Manager Administrative and User Console Guide* for troubleshooting information.

Creation of the connector involves creation of all the objects that constitute the connector. See the "Connector Objects Created by the Generic Technology Connector Framework" chapter in *Oracle Identity Manager Administrative and User Console Guide* for information about the connector objects that are created.

Except for the form names, the names of generic technology connector objects are in the *GTC_NAME*_GTC format, where *GTC_NAME* is the name that you assign to the connector.

For example, if you specify DBTables_conn as the name of the connector that you create, then all the connector objects (except the forms) are named DBTables_conn_GTC.

3.3.6 Modifying the Default Action Rules

Table 3–3 lists the default action rules that are created when you create a connector for target resource reconciliation.

Table 3–3 Action Rules for Target Resource Reconciliation

Rule Condition	Action
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Table 3–4 lists the default action rules that are created when you create a connector for trusted source reconciliation.

Table 3–4 Action Rules for Trusted Source Reconciliation

Rule Condition	Action
No matches found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

You can modify these rule conditions and rule actions according to your requirements. See the "Resource Objects Form" section in *Oracle Identity Manager Design Console Guide* for information about this procedure.

Note: If you use the Design Console to modify the objects (for example, the action rules), then do not use the Manage Generic Technology Connector feature to modify the generic technology connector. If you modify the connector, then all the modifications made by using the Design Console would be overwritten.

This limitation is mentioned in the "Connector Objects" section in the "Known Issues of Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*.

3.3.7 Configuring Reconciliation

See "Configuring Reconciliation" in the "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*.

3.3.8 Configuring Provisioning

See "Configuring Provisioning" in the "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*.

3.4 Performing Connector Operations

See "Performing Connector Operations" in *Oracle Identity Manager Connector Concepts* for information about guidelines that you must apply when you start using the connector.

Updating Child Records

Database Application Tables connectors do not support Update Child Record provisioning operations in this release. To work around this problem, you must first delete the record and then add the record with the required data modified.

See Also: The entry for Bug 6614311 in the "Known Issues" chapter

4

Known Issues

The following are known issues that you might encounter while creating or using Database Application Tables connectors:

> **See Also:** The "Known Issues of Generic Technology Connectors" chapter in *Oracle Identity Manager Administrative and User Console Guide*

- **Bug 6644652**

  Reconciliation of account deletion is not supported. In other words, if a record is deleted from the target database, then this deletion is not reconciled into Oracle Identity Manager.

- **Bug 6614311**

  Database Application Tables connectors do not support Update Child Record provisioning operations in this release. To work around this problem, you must first delete the record and then add the record with the required data modified.

- **Bug 6696248**

  Database Application Tables connectors do not support SSL communication between an Oracle Database target system and Oracle Identity Manager running on IBM WebSphere Application Server or Oracle Application Server.

- **Bugs 6813795 and 7008825**

  If you are using any locale other than the English locale, then on the Step 2: Specify Parameter Values page:

  – The following text is displayed as the label and description of the Unique Attribute parameter

    `parentContainerUniqueKey`

  – The following text is displayed as the label and description of the Database Date Format parameter

    `dbDateFormat`

- **Bug 7009308**

  While performing an Update User provisioning operation in the Administrative and User Console, if you try to modify the primary key field of the user, then the task is rejected. If you try to view the rejected task, then an error is thrown. The error message that is displayed is not localized.

- **Bug 8282035**

If the data type of the primary key column of the target database table is not VARCHAR, then an error is encountered if you try to update a provisioned resource whose data is stored in that target database table.

- **Bug 8449404**

  SSL communication is not supported if IBM DB2/UDB is running on IBM z/OS.

A

An Example of the Procedure to Create Connectors

In this appendix, a sample scenario has been used to demonstrate the procedure to create Database Application Tables connectors.

This appendix is divided into the following sections:

- Sample Scenario
- Tasks to Be Performed Before You Create the Connector
- Configuring the Target System As a Target Resource
- Configuring the Target System As a Trusted Source

A.1 Sample Scenario

Example Inc. has some database-driven custom applications. These applications store user and transaction data in an installation of Oracle Database 10*g* release 2 (10.2.0.3). The applications cannot be LDAP enabled, and they do not have any APIs for identity administration. The company wants to deploy an identity management and provisioning system that can be linked with their database.

Oracle Identity Manager is the solution to this business problem. The company can create and use a Database Application Tables connector to enable the exchange of user data between the database and Oracle Identity Manager.

The following sections describe the sample target system:

- Sample Target System to Be Configured As a Target Resource
- Sample Target System to Be Configured As a Trusted Source

A.1.1 Sample Target System to Be Configured As a Target Resource

The ACMEDBAPP table stores parent user data. The following is the structure of this table:

Column Name	Data Type	Nullable
APP_USERID	VARCHAR2	No
Note: This is the primary key.		
APP_AUTH_MODE	VARCHAR2	Yes
APP_DFLT_HOME	VARCHAR2	Yes
APP_ACCT_STATUS	VARCHAR2	Yes

Column Name	Data Type	Nullable
APP_CREATED_BY	DATE	Yes
APP_CREATED_ON	DATE	Yes
APP_UPDATED_BY	TIMESTAMP	Yes
APP_ UPDATED_ON	TIMESTAMP	Yes

The ACMEDBROLES table stores child user data. The following is the structure of this table:

Column Name	Data Type	Nullable
APP_USERID **Note:** This is the foreign key.	VARCHAR2	No
APP_ROLE_ID	VARCHAR2	No

A.1.2 Sample Target System to Be Configured As a Trusted Source

The ACMEHR table stores user data. The following is the structure of this table:

Column Name	Data Type	Nullable
EMPLOYEE_ID	VARCHAR2	No
FIRST_NAME	VARCHAR2	No
LAST_NAME	VARCHAR2	No
EMAIL	VARCHAR2	Yes
PHONE_NUMBER	VARCHAR2	Yes
HIRE_DATE	DATE	Yes
LAST_UPDATE	TIMESTAMP	Yes
SALARY	NUMBER	Yes
STATUS	VARCHAR2	Yes

A.2 Tasks to Be Performed Before You Create the Connector

Note: Unless specified otherwise, the steps listed in this section are common to both target resource and trusted source configurations.

Before you start creating the connector, perform the following steps:

1. Verify that the target system meets the requirements for creating and using the connector.

   See "Certified Deployment Configurations" on page 1-2 for details.

2. Enable logging for the connector.

   See "Enabling Logging" on page 2-1 for details.

3. Copy the JDBC drivers to the specified application server directories.

   See "Copying the JDBC Drivers" on page 2-4 for details.

4. You want to configure account status reconciliation. To achieve this, create a lookup definition that maps the status values stored in one of the following fields with the status values used by Oracle Identity Manager during reconciliation:
   - For the target resource scenario, the APP_ACCT_STATUS field of the target system
   - For the trusted source scenario, the STATUS field of the target system

   Note: Status values used in Oracle Identity Manager are different for target resource and trusted source reconciliation.

   See "Configuring Account Status Reconciliation" on page 2-5 for details.
5. For the target resource scenario, you want to configure account status provisioning. To achieve this, create the Lookup.ACME.Status lookup definition that maps the status values stored in the APP_ACCT_STATUS field of the target system with the status values used in Oracle Identity Manager for provisioning operations.

   See "Configuring Account Status Provisioning" on page 2-6 for details.
6. For the trusted source scenario, the PHONE_NUMBER field is a mandatory field of the target system. There is no corresponding OIM User field. Therefore, you must create a UDF that can accept and store values from the PHONE_NUMBER field during trusted source reconciliation. For this example, it is assumed that you have created the Telephone UDF.

   See *Oracle Identity Manager Design Console Guide* for information about creating UDFs.
7. Run the Connector Installer to copy the provider files to specified destination directories on Oracle Identity Manager.

   See "Copying the Provider Files" on page 2-7 for details.

A.3 Configuring the Target System As a Target Resource

You want to configure the target system as a target resource of Oracle Identity Manager. To create the connector for this purpose:

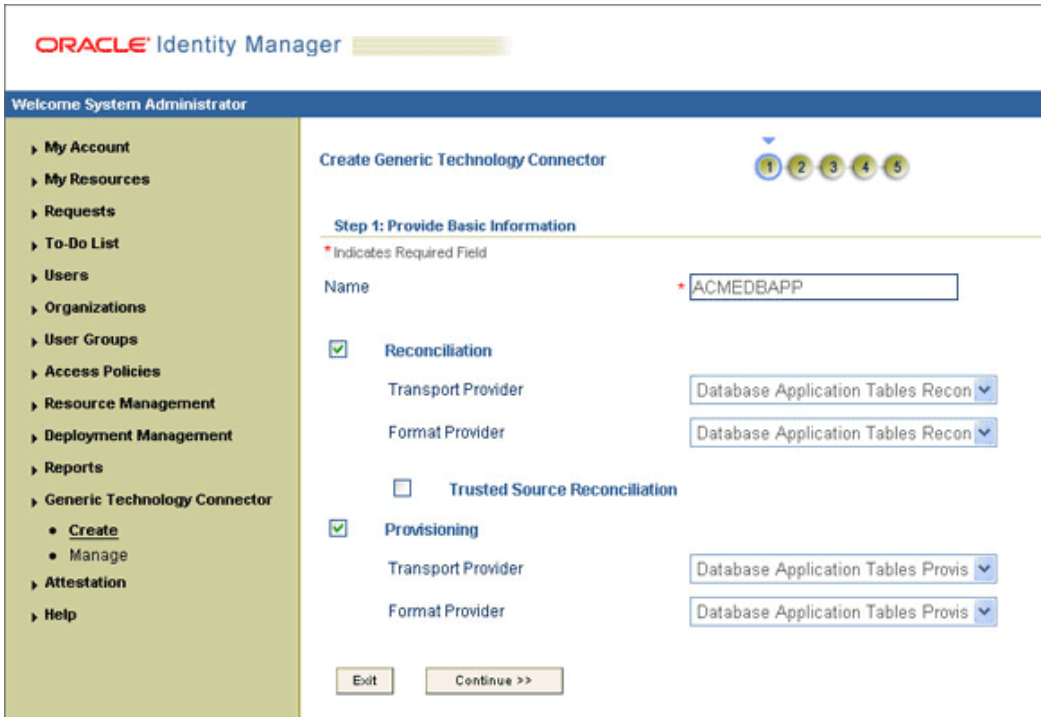
1. Log in to the Administrative and User Console as the user described in the "Addressing the Prerequisites for Creating the Generic Technology Connector" section of *Oracle Identity Manager Administrative and User Console Guide*.
2. To navigate to the first Administrative and User Console page for creating generic technology connectors, expand **Generic Technology Connector**, and then click **Create**.
3. On the Step 1: Provide Basic Information page, specify the values listed in Table A–1 and then click **Continue**.

Table A–1 Sample Entries for the Step 1: Provide Basic Information Page

Label on the Step 1: Provide Basic Information Page	Value/Action
Name field	**ACMEDBAPP**
Reconciliation check box	Select this check box.
Transport Provider list	**Database Application Tables Reconciliation Transport Provider**
Format Provider list	**Database Application Tables Reconciliation Format Provider**
Trusted Source Reconciliation check box	Do not select this check box.
Provisioning check box	Select this check box.
Transport Provider list	**Database Application Tables Provisioning Transport Provider**
Format Provider list	**Database Application Tables Provisioning Format Provider**

Figure A–1 shows the Step 1: Provide Basic Information page on which sample entries have been made.

Figure A–1 Step 1: Provide Basic Information Page



4. On the Step 2: Specify Parameter Values page, specify the values listed in Table A–2 and then click **Continue**.

Table A–2 Sample Entries for the Step 2: Specify Parameter Values Page

Label on the Step 2: Specify Parameter Values Page	Value/Action
Run-Time Parameters	
Database Driver field	**oracle.jdbc.driver.OracleDriver**
Database URL field See "Determining Values for the Database URL and Connection Properties Parameters" on page 3-2 for information about this parameter.	**jdbc:oracle:thin:@ten.mydomain.com:1521:orcl**
Database User ID field	**dbapps**
Database Password field	**dbappsPd**
Customized Query field	
Use Native Query check box	Do not select this check box.
Connection Properties field See "Determining Values for the Database URL and Connection Properties Parameters" on page 3-2 for information about this parameter.	
Design Parameters	
Parent Table/View Name field	**ACMEDBAPP**
Child Table/View Names field	**ACMEDBROLES**
Unique Attribute field	
Timestamp Attribute field	**APP_UPDATED_ON**
Status Attribute field	**APP_ACCT_STATUS**
Status Lookup Code field	**Lookup.ACME.Status** This is the lookup definition that you create by performing Step 5 of the procedure in the "Tasks to Be Performed Before You Create the Connector" section.
Database Date Format field	
Target Date Format field	
Batch Size field	**All**
Stop Reconciliation Threshold field	**None**
Stop Threshold Minimum Records field	**None**
Source Date Format field	
Reconcile Deletion of Multivalued Attribute Data check box	Select this check box.
Reconciliation Type list	**Incremental**

Figure A–2 shows the first section of the Step 2: Specify Parameter Values page on which sample entries have been made.

Figure A–2 First Section of the Step 2: Specify Parameter Values Page

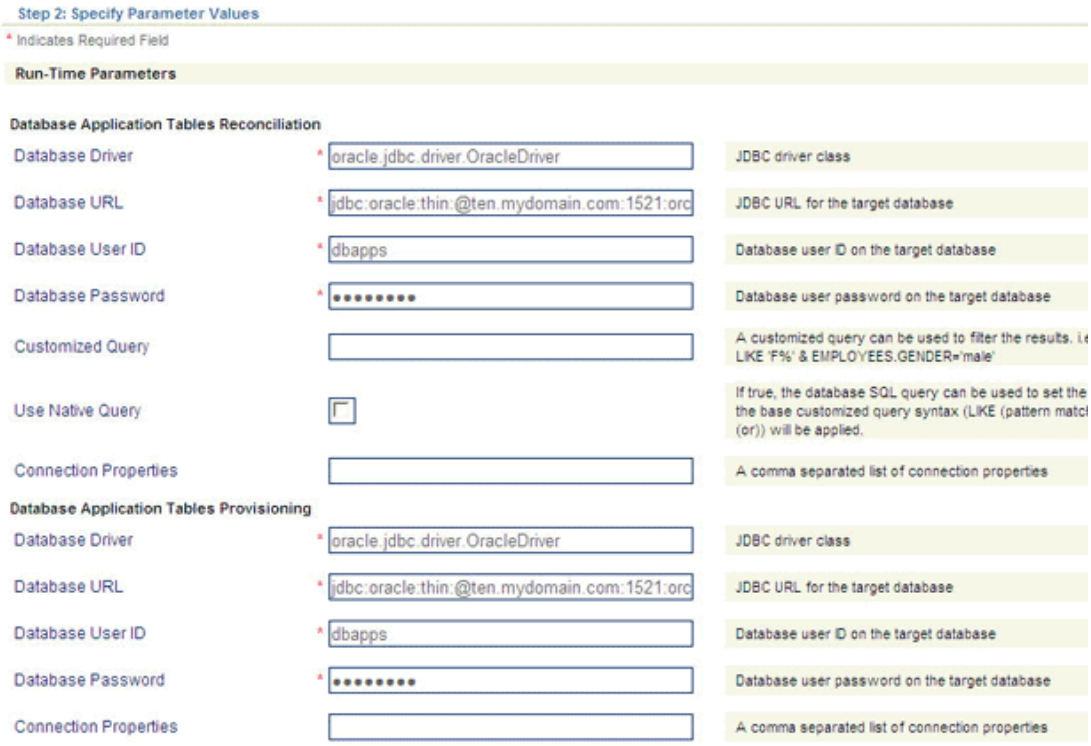
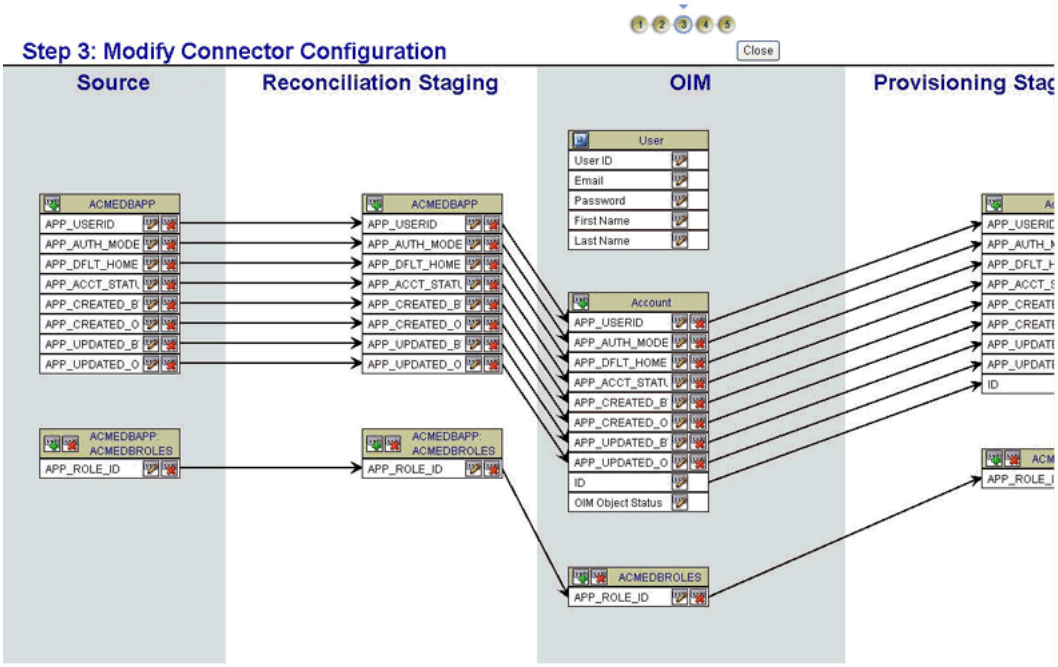


Figure A–3 shows the second section of the Step 2: Specify Parameter Values page on which sample entries have been made.

Figure A–3 Second Section of the Step 2: Specify Parameter Values Page

5. Figure A–4 shows a screenshot of the Step 3: Modify Connector Configuration page after metadata detection has run on the sample target system. As mentioned in Table 3–2, the APP_USERID field (foreign key) is not included in the child data sets shown on this page.

Figure A–4 Step 3: Modify Connector Configuration Page After Metadata Detection

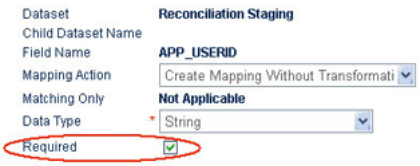


On this page, perform the following actions:

- Designate the APP_USERID field of the Reconciliation Staging and OIM - Account data sets as a mandatory field.

  To designate a field as a mandatory field, click the Edit icon for the field and select **Required** on the Step 1: Provide Field Information page.

  The following screenshot shows the Required check box highlighted for the APP_USERID field:



- Create the reconciliation rule by creating a matching-only mapping between the APP_USERID (primary key) field of the Reconciliation Staging data set and the User ID field of the OIM - User data set.

  To create the matching-only mapping for the reconciliation rule:

  a. Click the Edit icon of the User ID field of the OIM - User data set.

  b. On the Step 1: Provide Field Information page:

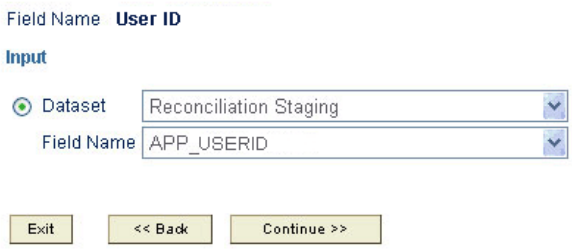
  - From the Mapping Action list, select **Create Mapping Without Transformation**.

  - Select **Matching Only**.

  - Click **Continue**.

  The following screenshot shows the Step 1: Provide Field Information page for the User ID field:

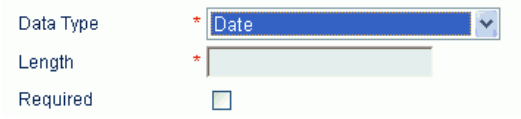
c. On the Step 3: Provide Mapping Information page, select **Reconciliation Staging** from the Dataset list, select **APP_USERID** from the Field Name list, and then click **Continue**. The following screenshot shows the Step 3: Provide Mapping Information page:



d. Close the wizard.

- Set the attributes (such as the data type and length) for the fields of the Reconciliation Staging data sets and the OIM - Account data sets.

  The following screenshot shows the Data Type list and Length field on the Step 1: Provide Field Information page:

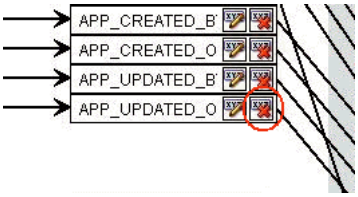


- You want to configure the exchange of account status data between the target system and Oracle Identity Manager.

  See "Exchanging Account Status Data with the Target System" on page 2-5 for details.

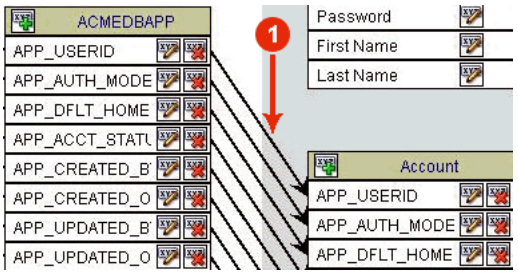
- You do not want to use the APP_CREATED_ON, APP_UPDATED_BY, and APP_UPDATED_ON fields during reconciliation or provisioning. To remove these fields, click the Delete icon for each field and then confirm that you want to proceed with the deletion of the field. You must remove these fields from all the data sets in which they are displayed.

  The following screenshot shows the Delete icon highlighted for the APP_UPDATED_ON field:



- Specify the key field for reconciliation matching.

The following screenshot shows the default mapping between the APP_USERID fields of the Reconciliation Staging and OIM - Account data sets:



You must change this mapping to a matching-only mapping by clicking the Edit icon for the APP_USERID field of the OIM - Account data set, selecting **Matching Only** on the Step 1: Provide Field Information page, and then continuing to the last page of the wizard. The following screenshot shows the Matching Only check box highlighted:

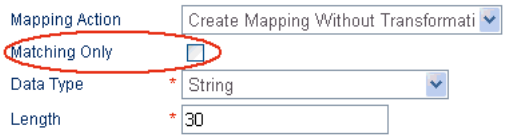
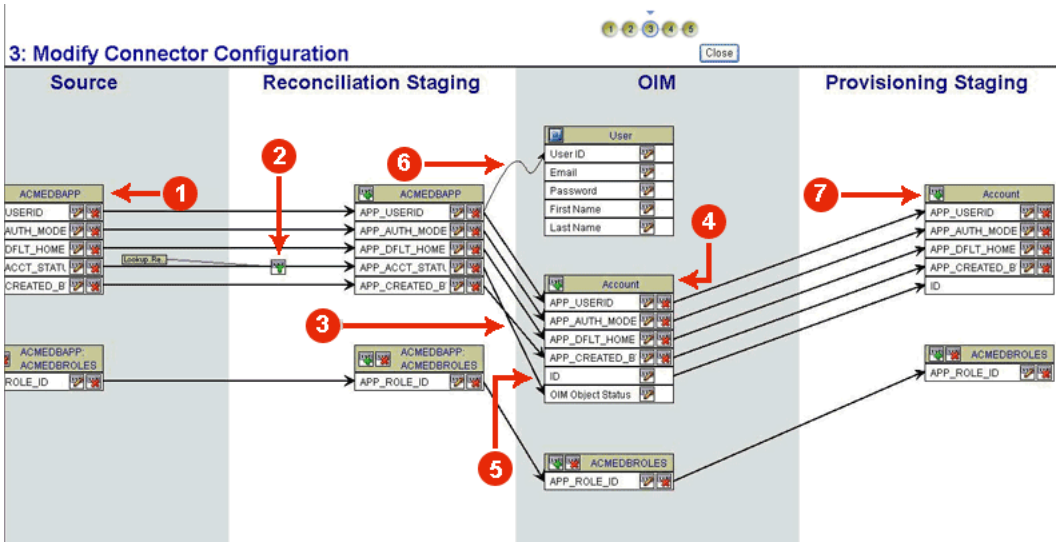


Figure A–5 shows a screenshot of the Step 3: Modify Connector Configuration page that is displayed after you perform the actions described in this section.

Figure A–5 Step 3: Modify Connector Configuration Page Displayed After You Configure the Connector



The following are some of the changes seen on the Step 3: Modify Connector Configuration page after you perform the actions described earlier in this section:

Note: The effect of certain actions, such as setting the attributes of fields in the Reconciliation Staging data set, cannot be seen on this page.

- **1.** You removed the APP_CREATED_ON, APP_UPDATED_BY, and APP_UPDATED_ON fields from all the data sets, starting with the Source data set.
- You configured account status reconciliation by:
  - **2.** Using the Translation Transformation provider to create a transformation mapping between the APP_ACCT_STATUS fields of the Source and Reconciliation Staging data sets.
  - **3.** Creating a mapping between the APP_ACCT_STATUS field of the Reconciliation Staging data set and the OIM Object Status field of OIM - Account data set.
  - **4.** Removing the APP_ACCT_STATUS field from the OIM - Account data set.
- **5.** You ensured that there are no mappings between the ID field of the OIM - Account data set and any field of the Reconciliation Staging data set.
- **6.** You created the reconciliation rule by creating a matching-only mapping between the APP_USERID field of the Reconciliation Staging data set and the User ID field of the OIM - User data set.
- **7.** As part of the procedure to configure account status provisioning, you removed the APP_ACCT_STATUS field from the Provisioning Staging data set.

6. On the Step 4: Verify Connector Form Names page, click **Continue**.

   Figure A–6 shows the Step 4: Verify Connector Form Names page.

Figure A–6 Step 4: Verify Connector Form Names Page

7. On the Step 5: Verify Connector Information page, click **Save**.
8. Modify the default rule actions.

   See "Modifying the Default Action Rules" on page 3-22 for details.
9. Configure reconciliation.

See "Configuring Reconciliation" in the "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*.

10. Configure provisioning.

    See "Configuring Provisioning" section in the "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*.

A.4 Configuring the Target System As a Trusted Source

You want to configure the target system as a trusted source of Oracle Identity Manager. To create the connector for this purpose:

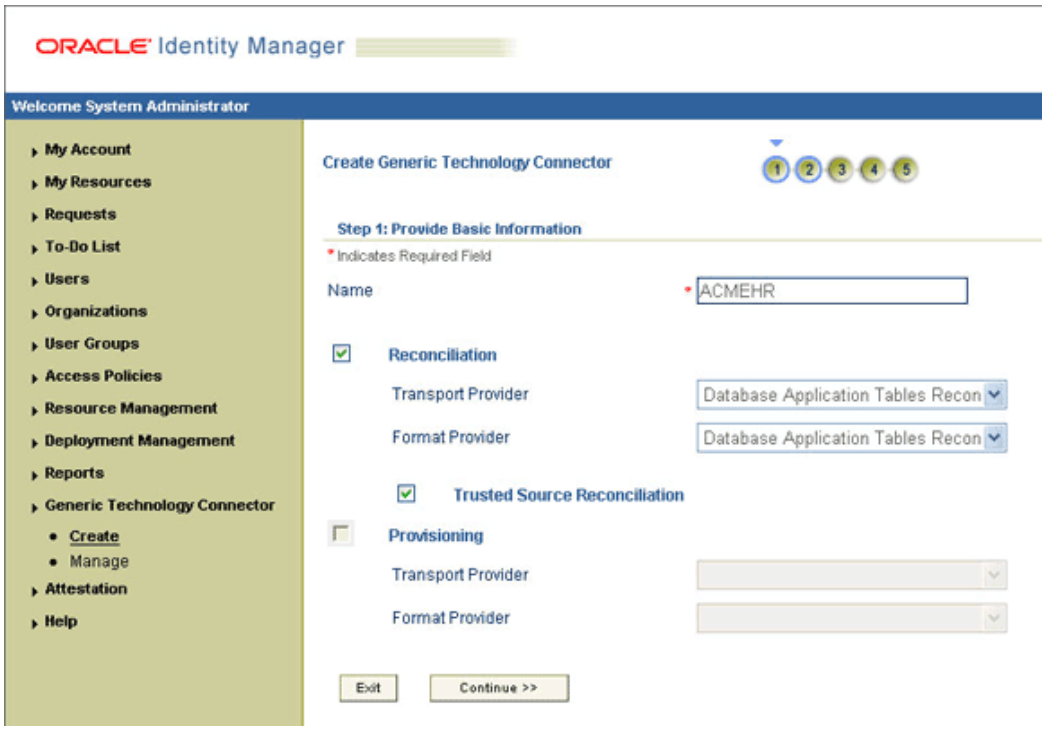
1. Log in to the Administrative and User Console as the user described in "Addressing the Prerequisites for Creating the Generic Technology Connector" of *Oracle Identity Manager Administrative and User Console Guide*.
2. To navigate to the first Administrative and User Console page for creating generic technology connectors, expand **Generic Technology Connector**, and then click **Create**.
3. On the Step 1: Provide Basic Information page, specify the values listed in Table A–3 and then click **Continue**.

Table A–3 Sample Entries for the Step 1: Provide Basic Information Page

Label on the Step 1: Provide Basic Information Page	Value/Action
Name field	**ACMEHR**
Reconciliation check box	Select this check box.
Transport Provider list	**Database Application Tables Reconciliation Transport Provider**
Format Provider list	**Database Application Tables Reconciliation Format Provider**
Trusted Source Reconciliation check box	Select this check box.
Provisioning check box	Do not select this check box.
Transport Provider list	Do not select a provider.
Format Provider list	Do not select a provider.

Figure A–7 shows the Step 1: Provide Basic Information page on which sample entries have been made.

Figure A–7 Step 1: Provide Basic Information Page



4. On the Step 2: Specify Parameter Values page, perform the actions described in Table A–4 and then click **Continue**.

Table A–4 Sample Entries for the Step 2: Specify Parameter Values Page

Label on the Step 2: Specify Parameter Values Page	Value to Be Entered/Action to Be Performed
Run-Time Parameters	
Database Driver field	**oracle.jdbc.driver.OracleDriver**
Database URL field See "Determining Values for the Database URL and Connection Properties Parameters" on page 3-2 for information about this parameter.	**jdbc:oracle:thin:@ilao-pc:1521:orcl10u**
Database User ID field	**ACMEHR**
Database Password field	**AcmeHr**
Customized Query field	
Use Native Query check box	Do not select this check box.
Connection Properties field See "Determining Values for the Database URL and Connection Properties Parameters" on page 3-2 for information about this parameter.	
Design Parameters	
Parent Table/View Name field	**ACMEHR**
Child Table/View Names field	
Unique Attribute field	

Table A–4 (Cont.) Sample Entries for the Step 2: Specify Parameter Values Page

Label on the Step 2: Specify Parameter Values Page	Value to Be Entered/Action to Be Performed
Timestamp Attribute field	
Database Date Format field	
Batch Size field	**All**
Stop Reconciliation Threshold field	**None**
Stop Threshold Minimum Records field	**None**
Source Date Format field	
Reconcile Deletion of Multivalued Attribute Data check box	Select this check box.
Reconciliation Type list	**Full**

Figure A–8 shows the first section of the Step 2: Specify Parameter Values page on which sample entries have been made.

Figure A–8 First Section of the Step 2: Specify Parameter Values Page

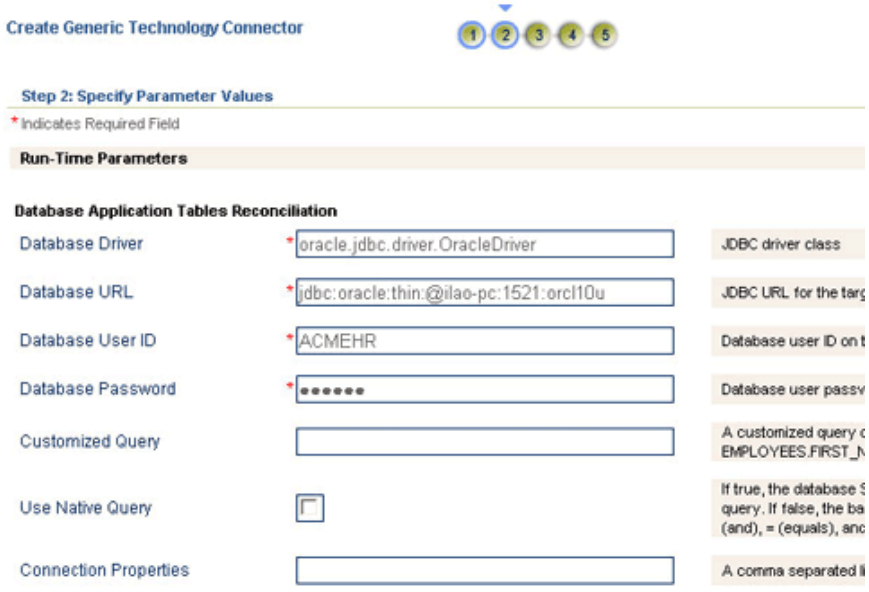
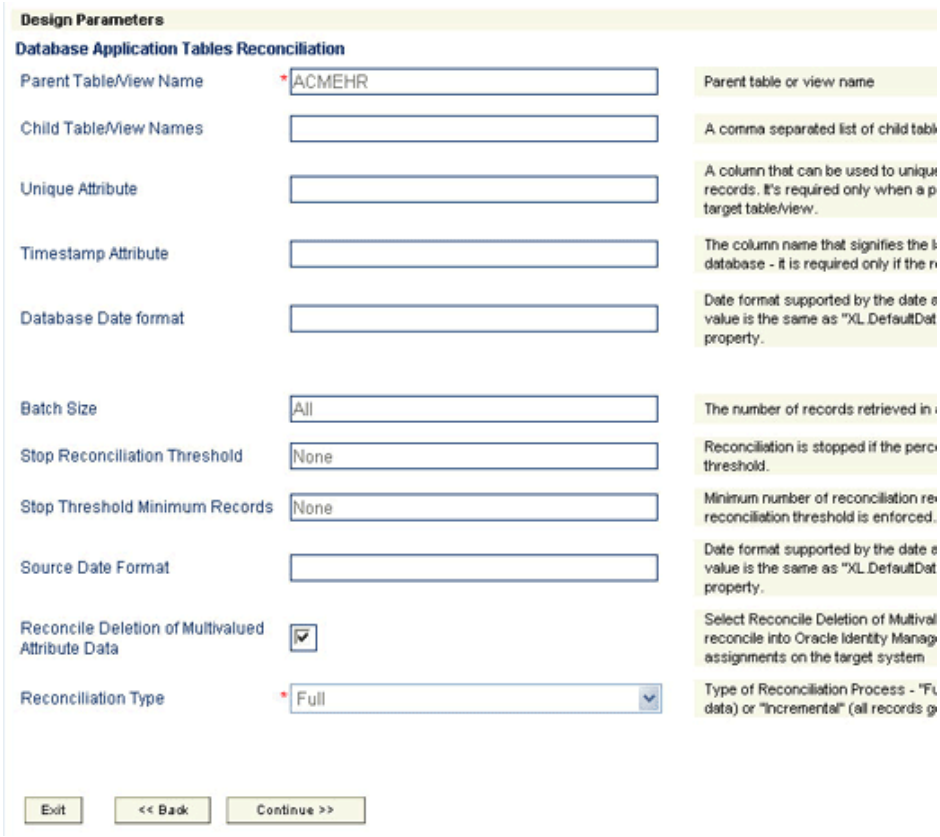


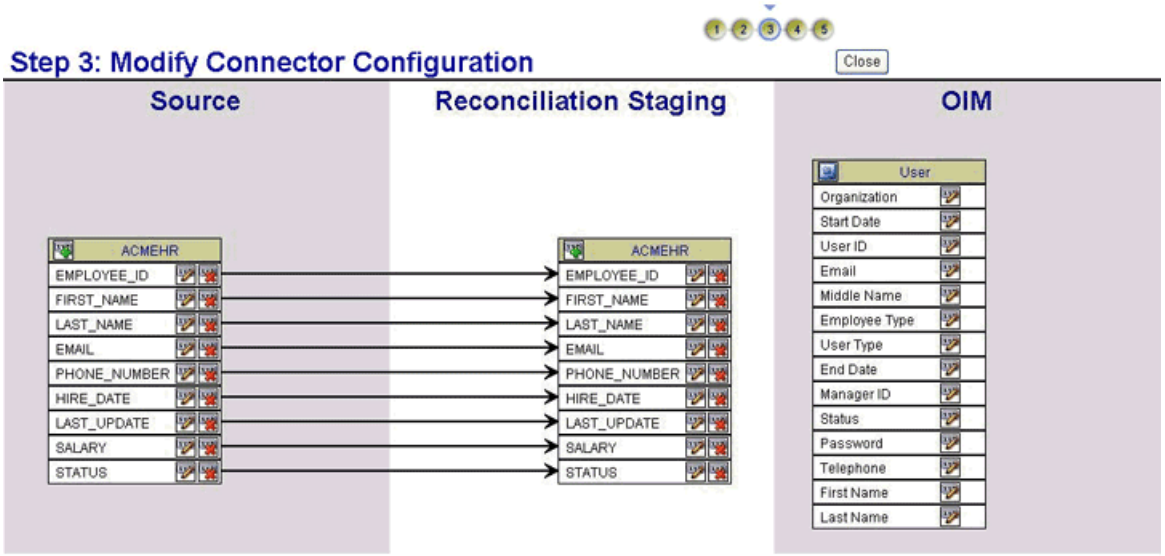
Figure A–9 shows the second section of the Step 2: Specify Parameter Values page on which sample entries have been made.

Figure A–9 Second Section of the Step 2: Specify Parameter Values Page



5. Figure A–10 shows a screenshot of the Step 3: Modify Connector Configuration page after metadata detection has run on the sample target system. The Telephone field shown in the OIM - User data set represents the UDF that you added by performing Step 6 of the procedure described in "Tasks to Be Performed Before You Create the Connector" on page A-2.

Figure A–10 Step 3: Modify Connector Configuration Page After Metadata Detection

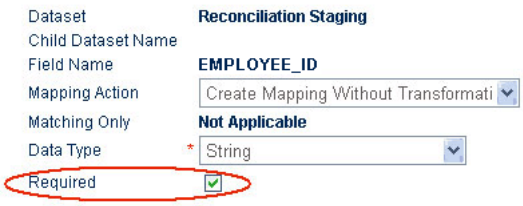


On the Step 3: Modify Connector Configuration page, perform the following actions:

- Designate the EMPLOYEE_ID, FIRST_NAME, and LAST_NAME fields of the Reconciliation Staging data set as mandatory fields.

  To designate a field as a mandatory field, click the Edit icon for the field and select **Required** on the Step 1: Provide Field Information page.

  The following screenshot shows the Required check box highlighted for the EMPLOYEE_ID field:



- Create the reconciliation rule by creating a matching-only mapping between the EMPLOYEE_ID (primary key) field of the Reconciliation Staging data set and the User ID field of the OIM - User data set.

  To create the matching-only mapping for the reconciliation rule:

  a. Click the Edit icon of the User ID field of the OIM - User data set.

  b. On the Step 1: Provide Field Information page:

  - From the Mapping Action list, select **Create Mapping Without Transformation**.

  - Select **Matching Only**.

  - Click **Continue**.

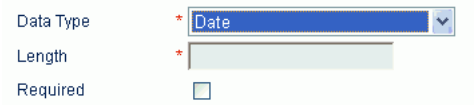
  The following screenshot shows the Step 1: Provide Field Information page for the User ID field:

  c. On the Step 3: Provide Mapping Information page, select **Reconciliation Staging** from the Dataset list, select **EMPLOYEE_ID** from the Field Name list, and then click **Continue**.

d. Close the wizard.

- Create mappings between the remaining fields of the Reconciliation Staging data set and corresponding fields of the OIM - User data set.
- Set the attributes (such as the data type and length) for the fields displayed in the Reconciliation Staging data set.

  The following screenshot shows the Data Type list and Length field on the Step 1: Provide Field Information page:



- You want to configure the reconciliation of account status data between the target system and Oracle Identity Manager.

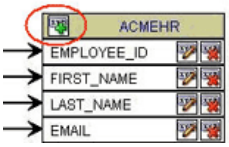
  See "Configuring Account Status Reconciliation" on page 2-5 for details.

- Ensure that the mandatory fields required for creation of an OIM User are present.

  The Organization, Employee Type, and User Type fields are mandatory OIM User fields. If an OIM User is to be created through trusted source reconciliation, then values must be specified for these fields. However, these fields do not exist in the target system. To add these fields to the Reconciliation Staging data set and set up literal values as the input for these fields, perform the following procedure for *each* field:

  a. Click the Add icon for the Reconciliation Staging data set.

  The following screenshot shows the Add icon of the ACMEHR data set highlighted:



  b. On the Step 1: Provide Field Information page:

  In the Field Name field, enter a name for the field:

  - For the Organization field, enter **Organization**.

  - For the Employee Type field, enter **Employee Type**.

  - For the User Type field, enter **User Type**.

  From the Mapping Action list, select **Create Mapping Without Transformation**.

  From the Data Type list, select **String**.

  c. Click **Continue**.

  d. On the Step 3: Provide Mapping Information page, select **Literal** and enter one of the following values:

  For the Organization field, enter the name of an existing organization in Oracle Identity Manager.

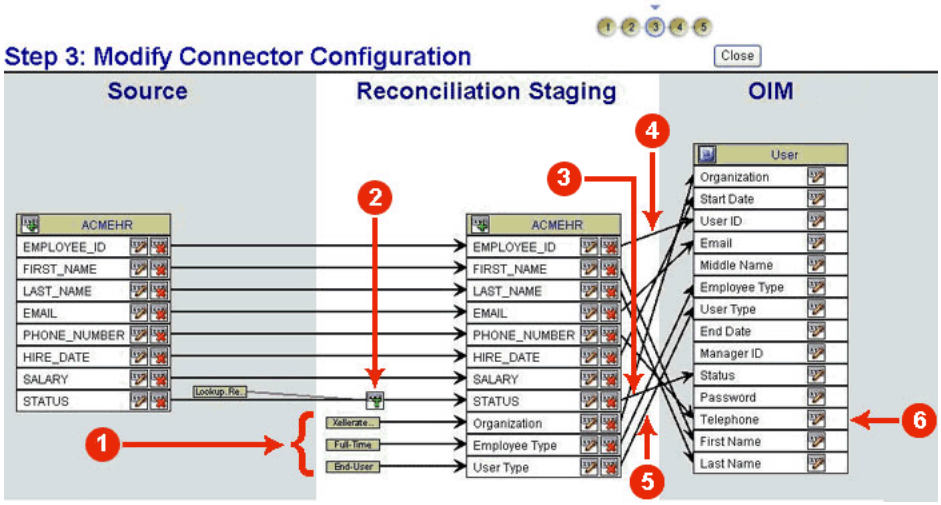
For the Employee Type field, enter **Full-Time**, **Part-Time**, **Temp**, **Intern**, or **Consultant**. These are Code Key values of the Employee Type field.

For the User Type field, enter **End-User** or **End-User Administrator**. These are Code Key values of the User Type field.

e. Complete the procedure and then close the wizard.

Figure A–11 shows a screenshot of the Step 3: Modify Connector Configuration page that is displayed after you perform the actions described in this section.

Figure A–11 Step 3: Modify Connector Configuration Page Displayed After You Configure the Connector



The following are some of the changes seen on the Step 3: Modify Connector Configuration page after you perform the actions described earlier in this section:

Note: The effect of certain actions, such as setting the attributes of fields in the Reconciliation Staging data set, cannot be seen on this page.

- **1.** You added the Organization, Employee Type, and User Type fields to the Reconciliation Staging data sets, and then set up literal values as the input sources for these fields.
- You configured account status reconciliation by:
  - **2.** Using the Translation Transformation provider to create a transformation mapping between the STATUS fields of the Source and Reconciliation Staging data sets.
  - **3.** Creating a mapping between the STATUS field of the Reconciliation Staging data set and the Status field of the OIM - User data set. This change is represented by the arrow between the STATUS and Status fields.
- **4.** You created the reconciliation rule by creating a matching-only mapping between the EMPLOYEE_ID field of the Reconciliation Staging data set and the User ID field of the OIM - User data set.
- **5.** You mapped fields of the Reconciliation Staging data set with corresponding fields of the OIM - User data set.

- **6.** You created the Telephone UDF to map the PHONE_NUMBER field of the target system.

6. On the Step 5: Verify Connector Information page, click **Save**.
7. Modify the default rule actions.

   See "Modifying the Default Action Rules" on page 3-22 for details.
8. Configure reconciliation.

   See "Configuring Reconciliation" in the "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*.

B

Screenshots of the Step 3: Modify Connector Configuration Page

The screenshots presented in this appendix show the outcome of various actions performed on the Step 3: Modify Connector Configuration page. See Table 3–2 for information about the context in which these pages are displayed.

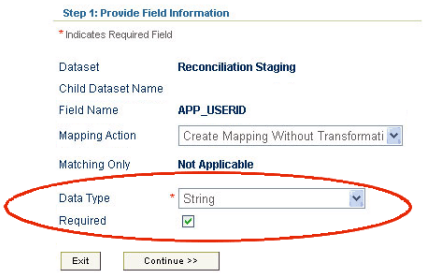
Screenshots for the following actions are described in this appendix:

- Using the Data Type List and Required Check Box
- Specifying a Literal Value As Input for a Field
- Encrypting the Storage and Display of Field Values
- Configuring Account Status Reconciliation: Step 1
- Configuring Account Status Reconciliation: Step 2
- Summary of Changes That You See After Configuring Target Resource Reconciliation
- Summary of Changes That You See After Configuring Trusted Source Reconciliation

B.1 Using the Data Type List and Required Check Box

Figure B–1 shows the Step 1: Provide Field Information page that is displayed when you click the Edit icon of any field in the Reconciliation Staging data set. The name of the field whose Edit icon you click (in this example, APP_USERID) is displayed on this page.

Figure B–1 Data Type List and Required Check Box



You use the Data Type list to set the data type for the fields that are detected through metadata detection. The connector will not work correctly if you do not perform this action for all the fields of the Reconciliation Staging and OIM - Account data sets. For

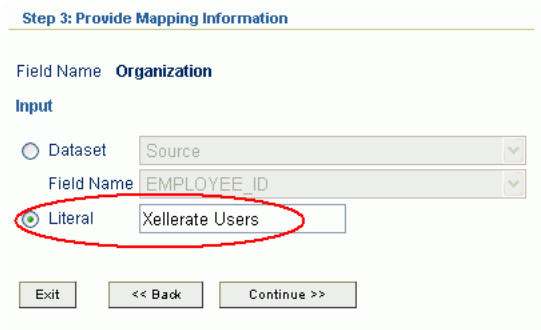
example, date format validation and conversion will not take place if you do not set the Date data type for date fields of the Reconciliation Staging and OIM - Account data sets.

You use the Required check box to specify that the field must contain a value during reconciliation. In other words, you designate the field as a mandatory field.

B.2 Specifying a Literal Value As Input for a Field

Figure B–2 shows the Step 3: Provide Mapping Information page. On this page, you can either select an input field for the mapping or enter a literal value. This page is displayed if you select **Create Mapping Without Transformation** from the Mapping Action list on the Step 1: Provide Field Information page.

Figure B–2 Literal Value As Input for a Field



B.3 Encrypting the Storage and Display of Field Values

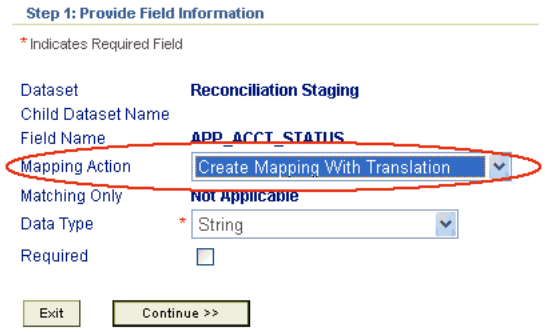
Figure B–3 shows the Step 1: Provide Field Information that is displayed when you click the Edit icon of any field in the OIM - Account data set. You use the Encrypted and Password Field check boxes to specify that you want to encrypt the storage, display, or both storage and display of fields that store confidential data.

Figure B–3 Encrypted and Password Field Check Boxes

B.4 Configuring Account Status Reconciliation: Step 1

Figure B–4 shows the start of the second step for configuring account status reconciliation. You open this page by clicking the Edit icon for the status field in the Reconciliation Staging data set. On this page, you select **Create Mapping with Translation** from the Mapping Action list. The procedure to configure account status reconciliation is described in *Oracle Identity Manager Administrative and User Console Guide*.

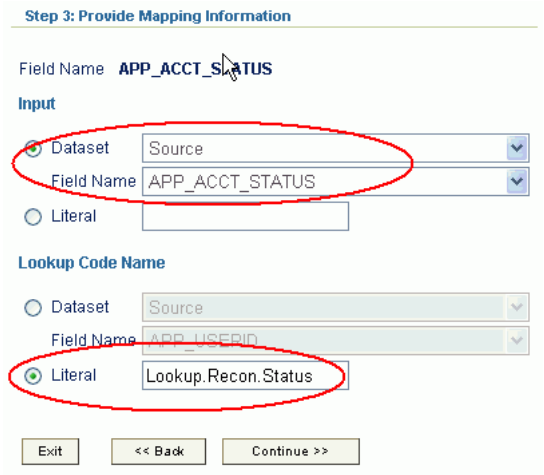
Figure B–4 Translation Transformation Option



B.5 Configuring Account Status Reconciliation: Step 2

Figure B–5 shows the outcome of the input that you provide on the page shown in Figure B–4.

Figure B–5 Source Field and Lookup Definition Containing Translated Values

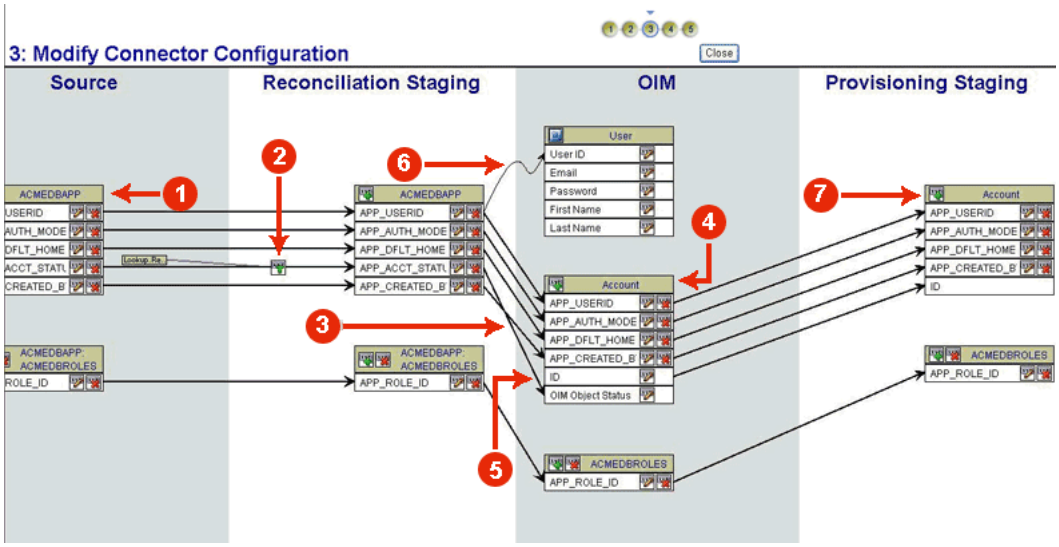


In the Input region of this page, you select **Source** from the Dataset list and then select the name of the status field from the Field Name list. In the Lookup Code Name region, you select **Literal** and then enter the name of the lookup definition that maps target system status values with Oracle Identity Manager status values.

B.6 Summary of Changes That You See After Configuring Target Resource Reconciliation

Figure B–6 shows the Step 3: Modify Connector Configuration page that is displayed after you configure the connector for target resource reconciliation.

Figure B–6 Actions Performed for Configuring Target Resource Reconciliation



The following are some of the changes seen on this page after you configure the connector for target resource reconciliation:

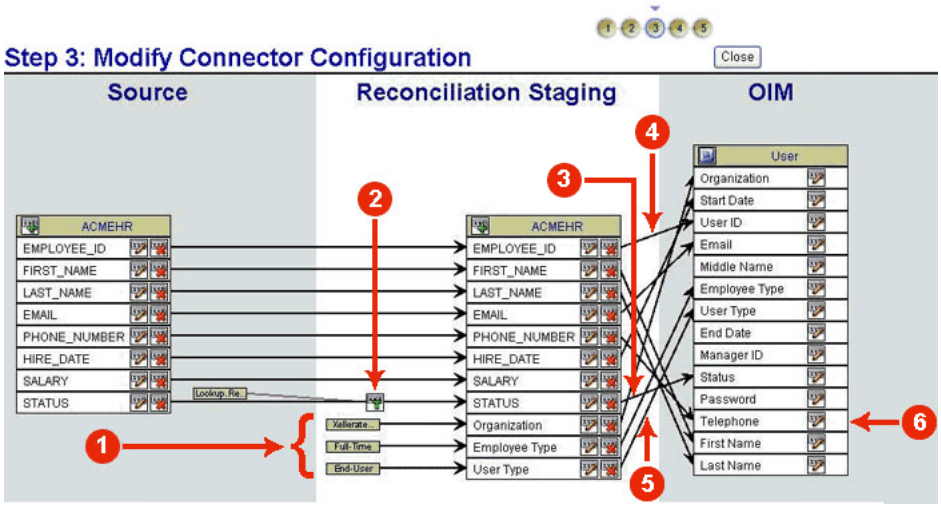
Note: The effect of certain actions, such as setting the attributes of fields in the Reconciliation Staging data set, cannot be seen on this page.

- **1.** You removed the APP_CREATED_ON, APP_UPDATED_BY, and APP_UPDATED_ON fields from all the data sets, starting with the Source data set.
- You configured account status reconciliation by:
  - **2.** Using the Translation Transformation provider to create a transformation mapping between the APP_ACCT_STATUS fields of the Source and Reconciliation Staging data sets.
  - **3.** Creating a mapping between the APP_ACCT_STATUS field of the Reconciliation Staging data set and the OIM Object Status field of OIM - Account data set.
  - **4.** Removing the APP_ACCT_STATUS field from the OIM - Account data set.
- **5.** You ensured that there are no mappings between the ID field of the OIM - Account data set and any field of the Reconciliation Staging data set.
- **6.** You created the reconciliation rule by creating a matching-only mapping between the APP_USERID field of the Reconciliation Staging data set and the User ID field of the OIM - User data set.
- **7.** As part of the procedure to configure account status provisioning, you removed the APP_ACCT_STATUS field from the Provisioning Staging data set.

B.7 Summary of Changes That You See After Configuring Trusted Source Reconciliation

Figure B–7 shows the Step 3: Modify Connector Configuration page that is displayed after you configure the connector for trusted source reconciliation.

Figure B–7 Actions Performed for Configuring Trusted Source Reconciliation



The following are some of the changes seen on this page after you configure the connector for trusted source reconciliation:

> **Note:** The effect of certain actions, such as setting the attributes of fields in the Reconciliation Staging data set, cannot be seen on this page.

- **1.** You added the Organization, Employee Type, and User Type fields to the Reconciliation Staging data sets, and then set up literal values as the input sources for these fields.
- You configured account status reconciliation by:
  - **2.** Using the Translation Transformation provider to create a transformation mapping between the STATUS fields of the Source and Reconciliation Staging data sets.
  - **3.** Creating a mapping between the STATUS field of the Reconciliation Staging data set and the Status field of the OIM - User data set. This change is represented by the arrow between the STATUS and Status fields.
- **4.** You created the reconciliation rule by creating a matching-only mapping between the EMPLOYEE_ID field of the Reconciliation Staging data set and the User ID field of the OIM - User data set.
- **5.** You mapped fields of the Reconciliation Staging data set with corresponding fields of the OIM - User data set.
- **6.** You created the Telephone UDF to map the PHONE_NUMBER field of the target system.

Index

B

Batch Size parameter, 3-12, A-5, A-14

C

certified
  languages, 1-3
certified deployment configurations, 1-2
child table provisioning, 2-4
Child Table/View Names parameter, 3-11, A-5, A-13
configurations, certified, 1-2
Connection Properties parameter, 3-2, 3-3, 3-5, 3-11, A-5, A-13
connector features, 1-4
connector files
  copying, 2-7
copying connector files, 2-7
Customized Query parameter, 3-1, 3-10, 3-11, A-5, A-13

D

data encryption and integrity, 2-9, 2-10, 2-11
Database Application Tables Provisioning Format Provider, 1-6, 3-9, A-4
Database Application Tables Provisioning Transport Provider, 1-5, 1-6, 3-9, A-4
Database Application Tables Reconciliation Format Provider, 1-5, 3-9, A-4, A-12
Database Application Tables Reconciliation Transport Provider, 1-5, 1-6, 3-9, A-4, A-12
Database Date Format parameter, 3-12, 3-13, 4-1, A-5, A-14
Database Driver parameter, 3-10, A-5, A-13
Database Password parameter, 3-10, A-5, A-13
Database URL parameter, 3-2, 3-3, 3-5, 3-10, A-5, A-13
Database User ID parameter, 3-10, A-5, A-13
deployment configurations, certified, 1-2
design parameters, 3-11

E

enabling logging, 2-1

F

features of connector, 1-4

G

globalization features, 1-3

I

IBM DB2/UDB, 1-2, 1-3, 2-4, 2-9, 3-2, 3-10

L

languages, certified, 1-3
limited reconciliation, 3-1
logging enabling, 2-1
lookup definitions, 2-4

M

Microsoft SQL Server, 1-2, 1-3, 2-5, 2-10, 3-3, 3-10, 3-11
multilanguage support, 1-3

O

Oracle Database, 1-2, 1-3, 2-5, 2-11, 3-5, 3-10, 3-11, 4-1, A-1

P

parameters
  design, 3-11
  run-time, 3-10
Parent Table/View Name parameter, 3-11, A-5, A-13
provider parameters
  Batch Size, 3-12, A-5, A-14
  Child Table/View Names, 3-11, A-5, A-13
  Connection Properties, 3-2, 3-3, 3-5, 3-11, A-5, A-13
  Customized Query, 3-1, 3-10, 3-11, A-5, A-13
  Database Date Format, 3-12, 3-13, 4-1, A-5, A-14
  Database Driver, 3-10, A-5, A-13
  Database Password, 3-10, A-5, A-13
  Database URL, 3-2, 3-3, 3-5, 3-10, A-5, A-13

Database User ID, 3-10, A-5, A-13
Parent Table/View Name, 3-11, A-5, A-13
Reconcile Deletion of Multivalued Attribute Data, 3-13, A-5, A-14
Reconciliation Type, 3-11, 3-13, A-5, A-14
Source Date Format, 3-12, 3-13, A-5, A-14
Status Attribute, 2-7, 3-11, A-5
Status Lookup Code, 2-7, 3-11, A-5
Stop Reconciliation Threshold, 3-12, A-5, A-14
Stop Threshold Minimum Records, 3-12, A-5, A-14
Target Date Format, 3-10, 3-12, A-5
Timestamp Attribute, 3-1, 3-11, 3-13, 3-18, A-5, A-14
Unique Attribute, 1-5, 1-6, 3-11, 3-18, 4-1, A-5, A-13
Use Native Query, 3-1, 3-11, A-5, A-13
provisioning, 1-1, 1-2, 1-3, 1-7, 2-4, 2-6, 2-8, 3-9, 3-10, 3-11, 3-12, 3-18, 3-19, 3-23, 4-1

R

Reconcile Deletion of Multivalued Attribute Data parameter, 3-13, A-5, A-14
Reconciliation Type parameter, 3-11, 3-13, A-5, A-14
run-time parameters, 3-10

S

Source Date Format parameter, 3-12, 3-13, A-5, A-14
Status Attribute parameter, 2-7, 3-11, A-5
Status Lookup Code parameter, 2-7, 3-11, A-5
Step 1 Provide Basic Information page, 3-8, A-4, A-12, A-13
Step 1 Provide Field Information page, 3-20, A-8, A-9, A-10, A-16, A-17, B-1, B-2
Step 2 Specify Parameter Values page, 3-10, 3-12, 3-13, 3-14, 3-15, A-5, A-6, A-7, A-13, A-14, A-15
Step 3 Modify Connector Configuration page, 3-15, A-8, A-10, A-15, A-18, B-1
Step 3 Provide Mapping Information page, 3-20, A-9, A-16, A-17, B-2
Step 4 Verify Connector Form Names page, 3-21, A-11
Step 5 Verify Connector Information page, 3-21, A-11, A-19
Stop Reconciliation Threshold parameter, 3-12, A-5, A-14
Stop Threshold Minimum Records parameter, 3-12, A-5, A-14
supported
releases of Oracle Identity Manager, 1-2
target systems, 1-2

T

Target Date Format parameter, 3-10, 3-12, A-5
target resource reconciliation, 1-1, 1-2, 1-3, 1-4, 1-6, 2-5, 2-6, 2-9, 3-11, 3-12, 3-13, 3-17, 3-18, 3-22, 3-23
target systems, supported, 1-2
Timestamp Attribute parameter, 3-1, 3-11, 3-13, 3-18, A-5, A-14
Transformation Providers, 1-5, 2-6, 3-18, A-11, A-18, B-4, B-5
Translation Transformation Provider, 2-6, A-11, A-18, B-4, B-5
trusted source reconciliation, 1-1, 1-2, 1-3, 1-4, 1-7, 2-5, 2-6, 3-9, 3-11, 3-12, 3-13, 3-16, 3-17, 3-19, 3-21, 3-22, 3-23, A-12, B-5

U

Unique Attribute parameter, 1-5, 1-6, 3-11, 3-18, 4-1, A-5, A-13
Use Native Query parameter, 3-1, 3-11, A-5, A-13

V

Validation Providers, 1-5, 3-18