Oracle® Identity Manager

Connector Guide for Database Application Tables

Release 9.1.0

E11194-14

September 2018

ORACLE

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

E11194-14

Copyright © 2013, 2018, Oracle and/or its affiliates. All rights reserved.

Primary Author: Gowri.G.R

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

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

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

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

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

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

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

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

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

Contents

3 Creating the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate 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

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

Access to Oracle Support

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

Related Documents

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

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

For information about Oracle Identity Manager 9.1.x Connectors documentation, visit the following Oracle Help Center page:

https://docs.oracle.com/cd/E11223_01/index.htm

Conventions

The following text conventions are used in this document:

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

What's New in 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 9.1.0.5.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

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

Software Updates

The following sections discuss software updates:

- Software Updates in Release 9.1.0.5
- Software Updates in Release 9.1.0.4
- Software Updates in Release 9.1.0.3
- Software Updates in Release 9.1.0.2
- Software Updates in Release 9.1.0.1

Software Updates in Release 9.1.0.5

The following is the software update in release 9.1.0.5:

- Support for New Oracle Identity Manager Release
- Support for New Target System Versions

Support for New Oracle Identity Manager Release

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

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for New Target System Versions

From this release onward, MySQL 5.3 and Oracle Database 11*g* Release 2 (11.2) have been added to the list of supported target systems.

See Section 1.1, "Certified Components" for the full list of supported target systems.

Software Updates in Release 9.1.0.4

The following are software updates in release 9.1.0.4:

- Support for New Target Systems
- Resolved Issues in Release 9.1.0.4

Support for New Target Systems

From this release onward, MySQL 5.1.30 has been added to the list of certified target systems.

This target system is mentioned in the "Certified Components" section.

Resolved Issues in Release 9.1.0.4

The following are issues resolved in release 9.1.0.4:

Bug Number	Issue	Resolution
9563242	In the earlier release, JDK 1.6 was required to run the connector. This JDK version was not the same as the JDK version required for Oracle Identity Manager release 9.1.0.1, which was the minimum Oracle Identity Manager requirement for the connector.	This issue has been resolved. From this release onward, the JDK requirement is JDK 1.5.

Software Updates in Release 9.1.0.3

The following are software updates in release 9.1.0.3:

- Change in Requirement for Oracle Identity Manager
- Resolved Issues in Release 9.1.0.3

Change in Requirement for Oracle Identity Manager

The minimum Oracle Identity Manager requirement for the current release of the connector is Oracle Identity Manager release 9.1.0.1 BP03.

Resolved Issues in Release 9.1.0.3

The following are issues resolved in release 9.1.0.3:

Bug Number	Issue	Resolution
8843835	If you were using Sybase Adaptive Server Enterprise as the target system, then the connector did not support child table views.	This issue has been resolved. The connector now supports child table views on the Sybase Adaptive Server Enterprise target system.
8666410	On the Step 3: Modify Connector Configuration page of the Administrative and User Console, data types of all target database columns were set to String by default. The actual data types of these columns were ignored.	This issue has been resolved. The actual data types of the columns are now displayed on the Step 3: Modify Connector Configuration page.

Software Updates in Release 9.1.0.2

The following are software updates in release 9.1.0.2:

- Support for New Target System Versions
- Support for Creating a Connector for a Target System with the Autoincrement Option Set on the Primary Key Column
- Reconciliation Is Not Specific to the Type of Target System Database
- Resolved Issues in Release 9.1.0.2

Support for New Target System Versions

From this release onward, the connector adds support for Microsoft SQL Server 2008, Oracle Database 10*g*, 11*g* as Oracle RAC implementation, and Sybase Adaptive Server Enterprise 15.x as target systems.

These target systems are mentioned in the "Certified Components" section. In addition, the JDBC drivers required for the new target systems are also mentioned in this section.

Note: If you are using Sybase Adaptive Server Enterprise as the target system, then this connector does not support child table views.

If you are using Microsoft SQL Server 2008 as the target system, then this connector does not support the Date data type.

This information has been mentioned in the "Known Issues, Workarounds, and Troubleshooting" chapter.

For information about the JDBC drivers that need to be used for the newly supported target system versions, see the "Copying the JDBC Drivers" section of the connector guide.

For information about the Database URL and Connection Properties parameters for Oracle RAC and Sybase Adaptive Server Enterprise, see the "Database URL and Connection Properties for Oracle RAC" and "Database URL and Connection Properties for Sybase Adaptive Server Enterprise" sections, respectively.

For information about configuring secure communication between Sybase Adpative Server Enterprise and Oracle Identity Manager, see "Configuring Secure Communication Between Sybase Adaptive Server Enterprise and Oracle Identity Manager" section.

Support for Creating a Connector for a Target System with the Autoincrement Option Set on the Primary Key Column

From this release onward, you can create a connector for a target system that has the primary key column defined with the autoincrement option. During a Create User provisioning operation, the process form field corresponding to the primary key field is updated after the account is created on the target system. In other words, you need not specify this value on the process form.

The Is Primary Key Auto Incremented parameter has been added to implement this feature. For information about this parameter, see the "Step 2: Specify Parameter Values Page" section.

Note: If you are using IBM DB2/UDB as the target system and the autoincrement option has been set on the primary key column, then you must install db2jcc4.jar and jdk 1.6.

This information has been mentioned in the "Copying the JDBC Drivers" section of the connector guide.

For information about creating a connector for a target system that has a primary key column defined with the autoincrement option, see the "Step 3: Modify Connector Configuration Page" section.

If you are using Oracle Database as the target system, then see the "Configuring Oracle Database" section for information about configuring the target system for this feature.

Reconciliation Is Not Specific to the Type of Target System Database

From this release onward, implementation of the reconciliation functionality is independent of the type of target system database.

Resolved Issues in Release 9.1.0.2

The following are issues resolved in release 9.1.0.2:

Bug Number	Issue	Resolution
8282035	While updating a provisioned resource, an error was encountered if the column names of the target database tables were in lowercase.	This issue has been resolved. No error is encountered while updating a provisioned resource if the target database column names are in lowercase.
8314294	After the Create User provisioning operation, the account status value for a target system was `Null`.	This issue has been resolved. The appropriate account status value is being displayed after a provisioning operation.

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 Components" 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, Workarounds, and Troubleshooting" 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 sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 9.1.0.5
- Documentation-Specific Updates in Release 9.1.0.4
- Documentation-Specific Updates in Release 9.1.0.3
- Documentation-Specific Updates in Release 9.1.0.2
- Documentation-Specific Updates in Release 9.1.0.1

Documentation-Specific Updates in Release 9.1.0.5

The following documentation-specific updates have been made in revision "14" of release 9.1.0.5:

- The "Oracle Identity Manager" row has been modified in Table 1–1, " Certified Components".
- An issue related to running the Evaluate User Policy scheduled job has been added to Section 4.1, "Known Issues and Workarounds".

The following documentation-specific updates have been made in the revision "13" of the release 9.1.0.5:

- The name of the "Known Issues and Workarounds" chapter has been changed to "Known Issues, Workarounds, and Troubleshooting." In addition, Chapter 4, "Known Issues, Workarounds, and Troubleshooting" has been restructured.
- A problem related to database column type has been added to Section 4.2, "Troubleshooting."

The following documentation-specific updates have been made in the revision "12" of the release 9.1.0.5:

- The "Usage Recommendations" section has been removed as the information in that section is not valid.
- MySQL 5.5 has been added to the "Target System" row of Section 1.1, "Certified Components."
- Section 2.1.7, "Prerequisites for Creating the Connector" has been added.

- The "Configuring IBM DB2/UDB Running on IBM z/OS" section has been removed as the connector does not support the use of stored procedures to perform CRUD operations.
- Section 2.1.4, "Copying the JDBC Drivers" has been modified.
- In Section 2.1.4, "Copying the JDBC Drivers," information about Oracle Database 11*g* release 2 (11.2) drivers has been added under the "For Oracle Database" list item.
- Section 3.6, "Localizing Field Lables in UI Forms" has been added.
- The procedure to modify the field length of provider parameters in Oracle Identity Manager release 11.1.1 and 11.1.2.*x* has been deleted from the Section 3.3, "Modifying Field Lengths of the Provider Parameters."
- Section 2.2.4, "Creating Target System User Accounts for Connector Operations" has been added.

The following documentation-specific updates have been made in the revision "11" of the release 9.1.0.5:

- The "Oracle Identity Manager" and JDK rows in Table 1–1, " Certified Components" has been modified.
- The following sections have been added:
  - "Usage Recommendation"
  - Section 3.5, "Configuring Oracle Identity Manager 11.1.2 or Later"
  - Section 3.8, "Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later"
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added as required throughout the guide.

The following documentation-specific update has been made in the revision "10" of the release 9.1.0.5:

In Chapter 4, "Known Issues, Workarounds, and Troubleshooting," the following item has been added:

Bug 10206089

Suppose a target system table has a primary key defined. While configuring a connector, if you designate a column as Unique, then the connector fails.

Documentation-Specific Updates in Release 9.1.0.4

The following are documentation-specific updates in release 9.1.0.4:

- Section 1.4, "Supported Data Types" has been modified.
- In Section 4, "Known Issues, Workarounds, and Troubleshooting":
  - The following items have been removed:

    Bugs 6689376, 8841689

    The number of characters in the Provider definition fields cannot be more than 200.
  - The following item has been moved to the limitations section because this issue is a limitation of the target system:

    Bug 8854612

If you are using Microsoft SQL Server 2008 as the target system, then this connector does not support the Date data type. A workaround for this issue is to use the DateTime data type.

Documentation-Specific Updates in Release 9.1.0.3

The following are documentation-specific updates in release 9.1.0.3:

- In Section 1.1, "Certified Components," the JDK requirement has been added.
- Section 1.4, "Supported Data Types" has been added.
- In Section 4, "Known Issues, Workarounds, and Troubleshooting":
  - The following item has been removed:

    Bug 8843835

    If you are using Sybase Adaptive Server Enterprise as the target system, then the Database Application Tables connector does not support child table views.
  - Issues tracked by Bug 8843835 and Bug 8805516 have been added.

Documentation-Specific Updates in Release 9.1.0.2

The following are documentation-specific updates in release 9.1.0.2:

- In Section 4, "Known Issues, Workarounds, and Troubleshooting":
  - The following item has been removed:

    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.
  - Issues tracked by bug numbers 8843835 and 8805516 have been added.
- Section 3.3, "Modifying Field Lengths of the Provider Parameters" has been added.

Documentation-Specific Updates in Release 9.1.0.1

The following sections discuss documentation-specific updates:

- In Section 4, "Known Issues, Workarounds, and Troubleshooting," 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 Section 1.1, "Certified Components," changes have been made in the "Target System" 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:

1.1 Certified Components

Table 1–1 lists the certified components for this connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	■ Oracle Identity Manager release 9.1.0.2 BP03 and future releases in this release track **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.2 BP03 and future releases in the 9.1.0.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* release 1 (11.1.1.3.0) and future releases in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1). ■ Oracle Identity Manager 11g release 1 PS1 (11.1.1.5.0) and future releases in this release track ■ Oracle Identity Manager 11g release 1 PS2 (11.1.1.7.0) and future releases in this release track ■ Oracle Identity Manager 11*g* release 2 (11.1.2.0.4) and future releases in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.2.*x*** has been used to denote Oracle Identity Manager release 11.1.2.0.4 and future releases in the 11.1.2.*x* series that the connector will support. ■ Oracle Identity Manager 11g release 2 PS1 (11.1.2.1.0) and future releases in this release track ■ Oracle Identity Manager 11g release 2 PS2 (11.1.2.2.0) and future releases in this release track
JDK	For Oracle Identity Manager release 9.1.0.*x*, JDK 1.5 or later For Oracle Identity Manager release 11.1.1 and 11.1.2.*x*, JDK 1.6 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, 2008 ■ MySQL 5.1.30, 5.3, 5.5 ■ Oracle Database 10*g*, 11*g*R1, 11*g* Release 2 (11.2.0.*x*), as either single database or Oracle RAC implementation. ■ Sybase Adaptive Server Enterprise 15.*x*

Table 1–1 (Cont.) Certified Components

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 IBM DB2/UDB with the autoincrement option set on the primary key column: db2jcc4.jar and jdk 1.6 For Microsoft SQL Server: ■ For Microsoft SQL Server 2005: sqljdbc.jar version 1.2 ■ For Microsoft SQL Server 2008: sqljdbc4.jar version 2.0 For MySQL, you need the mysql-connector-java-5.1.8-bin.jar driver. For Oracle Database ■ Oracle Database 10*g* drivers ■ Oracle Database 11*g* drivers ■ For Oracle RAC: ojdbc14.jar For Sybase Adaptive Server Enterprise, you need the jconn3.jar JDBC driver for all platforms. 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 2-14.

Table 1–1 (Cont.) Certified Components

Item	Requirement
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 2-14 for the description of a workaround to this requirement. ■ Names of foreign key columns must 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. For Oracle Identity Manager release 9.1.0.*x*, 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. For Oracle Identity Manager release 11.1.1 and 11.1.2.*x*, see "Names of Fields" in the "Creating and Managing Generic Technology Connectors" chapter of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information.

1.2 Usage Recommendation

Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of the following connectors:

- If you are using an Oracle Identity Manager release that is 9.1.0.2 BP03 or later and earlier than Oracle Identity Manager Release 11*g* Release 2 BP10 (11.1.2.0.10), then you must use the 9.1.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 2 BP10 (11.1.2.0.10) or later, then you must use the latest 11.1.1.*x* version of this connector.

1.3 Certified Languages

The connector supports the following languages:

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

See Also: One of the following guides for information about supported special characters:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Globalization Guide*.
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.*

1.4 Supported Data Types

The data types supported for reconciliation and provisioning operations are listed in the following section:

Note: Complex data types, such as RAW, Binary File, CLOB, and BLOB, are not supported. Any data type that is not supported *and* is not a complex data type is treated as a String data type.

For IBM DB2 Database:

- SMALLINT
- BIGINT
- INTEGER
- REAL
- FLOAT
- DOUBLE
- DECIMAL
- CHARACTER
- VARCHAR
- DATE
- TIMESTAMP

For Microsoft SQL Server:

- CHAR
- VARCHAR
- TINYINT
- SMALLINT
- INT
- BIGINT
- DECIMAL
- NUMERIC
- FLOAT
- REAL
- SMALLDATETIME
- DATETIME

For MySQL:

- TINYINT
- SMALLINT
- MEDIUMINT
- INT
- BIGINT
- FLOAT
- DOUBLE
- DECIMAL
- CHAR
- VARCHAR
- TINYTEXT
- DATE
- DATETIME
- TIMESTAMP

For Oracle Database:

- VARCHAR2
- CHAR
- NUMBER
- NUMERIC
- INTEGER
- INT
- SMALLINT
- DOUBLE
- FLOAT
- DECIMAL
- DEC
- REAL
- DATE
- TIMESTAMP

For Sybase Database:

- CHAR
- DATE
- VARCHAR
- TINYINT
- SMALLINT
- INT

- NUMERIC
- DECIMAL
- FLOAT
- REAL
- DATETIME

1.5 Features of the Connector

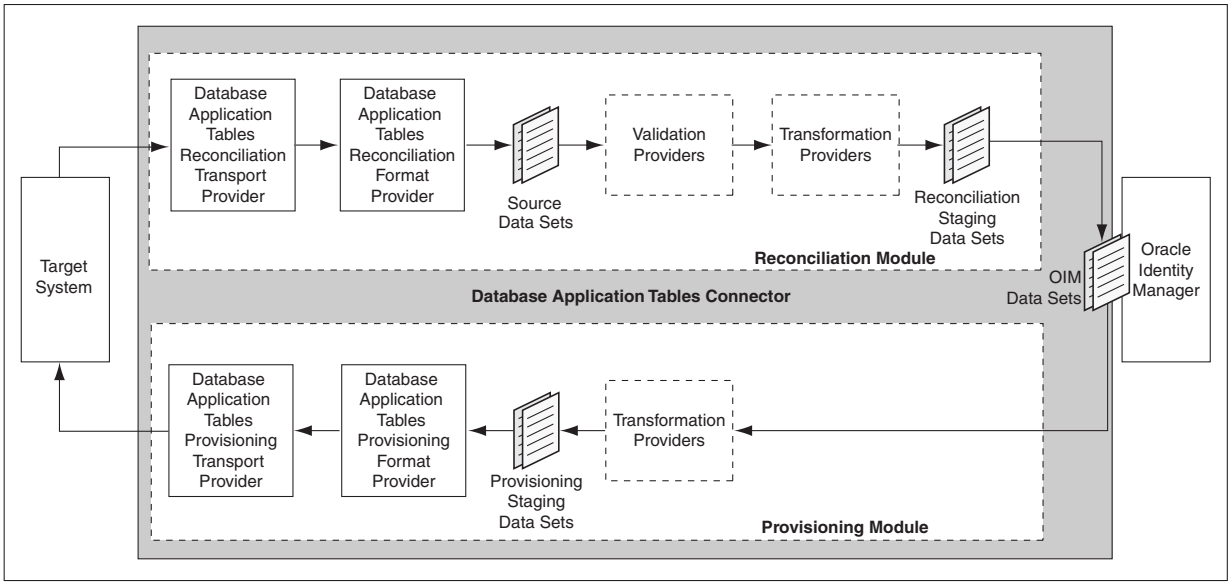
This section discusses the following topics:

- 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.

1.5.1 Connector Architecture

Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of a Database Application Tables Connector



The connector can be logically divided into the Provisioning module and Reconciliation module.

The Provisioning module consists of optional Transformation Providers, the Provisioning Staging data sets, the Database Application Tables Provisioning Format Provider, and the Database Application Tables Provisioning Transport Provider.

The Reconciliation module consists of the Database Application Tables Reconciliation Transport Provider, the Database Application Tables Reconciliation Format Provider,

the Source data sets, optional Validation Providers, optional Transformation Providers, and the Reconciliation Staging data sets.

****

See Also: One of the following guides for conceptual information about providers and data sets:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.*

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.

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 3-20. 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 unique key column.

  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.

Note: If a referential integrity constraint can be set, then ensure that the name of the primary key column in the parent table is the same as the name of the foreign key column in the child table. If this requirement is not met, then the connector cannot detect the referential integrity constraint.

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.

Note: The Database Application Tables connector does not support the use of stored procedures to perform CRUD operations against a table.

1.5.2 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.

Note: In Oracle Identity Manager release 11.1.1 and 11.1.2.*x*, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term scheduled job in the context of Oracle Identity Manager release 11.1.1 and 11.1.2.*x*.

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

See Also: One of the following guides:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.*

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 3-20.

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.

1.5.3 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

1.5.4 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 3-20.

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.

1.6 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 one of the following guides:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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 procedure to create generic technology connectors given in one of the following guides:
  - For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide*
  - For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
- Chapter 4, "Known Issues, Workarounds, and Troubleshooting" 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
- Prerequisites for Creating the Connector

2.1.1 Enabling Logging

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

- Section 2.1.1.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"
- Section 2.1.1.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1 and 11.1.2.x"

2.1.1.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.*x*

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

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

- ALL

  This level enables logging for all events.

- DEBUG

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

- INFO

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

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

- FATAL

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

- OFF

  This level disables logging for all events.

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

- **Oracle 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

2.1.1.2 Enabling Logging on Oracle Identity Manager Release 11.1.1 and 11.1.2.*x*

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

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

These log levels are mapped to ODL message type and level combinations as shown in Table 2–1.

Table 2–1 Log Levels and ODL Message Type:Level Combinations

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

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

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

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

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

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

<logger name="OIMCP.DATC" level="[LOG_LEVEL]" useParentHandlers="false">
     <handler name="dbat-handler"/>
     <handler name="console-handler"/>
```

```
</logger>
```

b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–1 lists the supported message type and level combinations.

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

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

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

<logger name="OIMCP.DATC" level="NOTIFICATION:1" useParentHandlers="false">
     <handler name="dbat-handler"/>
     <handler name="console-handler"/>
   </logger>
```

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

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

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

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

4. Restart the application server.

2.1.2 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 3-20, 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). For information about creating UDFs, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x*, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

The following are the standard OIM User fields on Oracle Identity Manager release 9.1.0.*x*:

- User ID
- First Name
- Last Name
- Organization Name
- User Type
- Employee Type
- Role
- Password
- Middle Name
- Status
- Provisioned Date
- Creation Date
- Manager ID
- End Date
- Start Date
- Email

The following are the standard OIM User fields on Oracle Identity Manager release 11.1.1 and 11.1.2.*x:*

- User Login
- First Name
- Last Name
- Organization
- User Type
- Password
- Middle Name
- Status
- Provisioning Date
- Creation Date
- Manager
- 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 one of the following guides for information about creating lookup definitions:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x*, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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 3-20, 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:

Note: If the target system has the primary key column defined with the autoincrement option, then:

- Ensure that you use JDBC3-compliant database drives.
- Ensure that the autoincrement mechanism is implemented on the target system. The connector does not generate and insert values in the autoincrementing field.
- A target system with Composite Primary Keys is not supported.

- 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 IBM DB2/UDB with the autoincrement option set on the primary key column: db2jcc4.jar and jdk 1.6
- For Microsoft SQL Server:
  - For Microsoft SQL Server 2005: sqljdbc.jar version 1.2
  - For Microsoft SQL Server 2008: sqljdbc4.jar
- For MySQL, you need the mysql-connector-java-5.1.8-bin.jar driver.
- 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
  - Oracle Database 11*g* release 2 (11.2) drivers

Note: If you are using Oracle Database 11*g* release 2 (11.2) drivers, then add the following system property to the startup parameter of the WebLogic Application Server:

```
-Doracle.jdbc.J2EE13Compliant=true
```

  - Oracle RAC: Use the ojdbc14.jar file for JBoss Application Server. For all other application servers, use the ojdbc6.jar file.

Note: The following is also mentioned as a limitation in the "Known Issues, Workarounds, and Troubleshooting" chapter:

If you are using the ojdbc6.jar file, then the ArrayIndexOutOfBounds exception is encountered during a provisioning operation on Oracle Identity Manager 9.1.0.2 BP02 or later. To resolve this issue:

On JBoss Application Server, replace the ojdbc6.jar file with the ojdbc14.jar file in the following directory:

OIM_HOME/xellerate/ext and *JBOSS_HOME*/server/default/lib

For all other certified application servers, apply Patch 7112447. This patch is available on My Oracle Support (formerly Oracle*MetaLink*).

- For Sybase Adaptive Server Enterprise, use the jconn3.jar JDBC driver for all platforms.

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

Note: In an Oracle Identity Manager cluster, copy the JDBC drivers into this directory on each node of the cluster.

- For Oracle Identity Manager release 9.1.0.*x*:
  - For Oracle 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:

    There is no need to copy JDBC drivers to any specific location as they are already present in the specified application server directories on Oracle Identity Manager.
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x* on Oracle WebLogic Server:

  There is no need to copy JDBC drivers as they are already present in the specified application server directories on Oracle Identity Manager.

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 one of the following chapters:

- For Oracle Identity Manager release 9.1.0.*x:* "Predefined Generic Technology Connector Providers Shipped with Oracle Identity Manager" chapter in *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Predefined Providers for Generic Technology Connectors" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

---

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: The "Lookup Definition Form" section in one of the following guides for information about creating lookup definitions:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x*, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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 3-14:
   - 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 3-20, 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 install the connector.

To install the connector:

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

   For Oracle Identity Manager release 9.1.0.*x*:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

   For Oracle Identity Manager release 11.1.1 and 11.1.2.*x*:

   OIM_HOME/server/ConnectorDefaultDirectory
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.*x*:

a. 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.*

b. Click **Deployment Management**, and then click **Install Connector**.

- For Oracle Identity Manager release 11.1.1:

a. 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 Fusion Middleware Administrator's Guide for Oracle Identity Manager.*

b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector.**

c. In the Manage Connector page, click **Install.**

- For Oracle Identity Manager release 11.1.2.*x:*

a. Log in to Oracle Identity System Administration by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager.*

b. In the left pane, under System Management, click **Manage Connector.**

c. In the Manage Connector page, click **Install.**

3. 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.

4. Click **Load**.

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

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

6. Click **Finish**.

7. Restart Oracle Identity Manager.

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

Note: If you are using Oracle Identity Manager release 9.1.0.*x,* then the provider files must be manually copied to the destination directories. On Oracle Identity manager release 11.1.*x,* when you install the connector, the provider files are automatically copied to the destination directories. Additionally, you must manually copy the lib/DatabaseApplicationTables.jar file to the *OIM_HOME*/server/JavaTasks directory.

Table 2–2 Provider Files for the Connector

File in the Installation Media Directory	Description	Destination Directory on OIM 9.1.0.x	Destination Directory on OIM 11.1.x
lib/DatabaseApplicationTables.jar	This file contains the code implementation of all the providers.	*OIM_HOME*/xellerate/JavaTasks	■ Oracle Identity Manager database ■ *OIM_HOME*/server/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	/db/GTC/ProviderDefinitions location in MDS
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 include GUI element labels and messages.	*OIM_HOME*/xellerate/connectorResources	Oracle Identity Manager database

2.1.7 Prerequisites for Creating the Connector

Note: Perform the instructions described in this section *only* if both conditions are true:

- You are using Oracle Identity Manager release 11.1.2.*x*.
- Oracle Identity manager 11.1.2.*x* is running on IBM WebSphere Application Server.

The following procedure is a prerequisite for creating the connector:

1. Stop the IBM WebSphere Application Server.
2. Copy the commons-pool-1.2.jar file from oim.ear/xlWebApp.war/WEB-INF/lib/ directory to the oim.ear/APP-INF/lib directory.
3. Restart IBM WebSphere Application Server.

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
- Configuring Oracle Database
- Creating Target System User Accounts for Connector Operations

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 Oracle Database

Note: This is an optional procedure. Perform this procedure on an Oracle database table only if you want an autoincrementing primary key.

At any time after creating the Oracle database table, you can set up an autoincrementing primary key column for that database table. To set the autoincrementing primary key, create a sequence, and then create a trigger that inserts a unique autogenerated number in the primary key field while inserting a new record into the parent table. The following is a trigger that you can use:

```
CREATE OR REPLACE TRIGGER trigger_name
BEFORE INSERT ON table_name FOR EACH ROW
BEGIN
SELECT sequence_name.nextval INTO :new.primaty_Key_column_name FROM DUAL;
END;
```

2.2.4 Creating Target System User Accounts for Connector Operations

Oracle Identity Manager requires a target system user account to access target system tables during reconciliation and provisioning operations. You provide the credentials of this user account while configuring the IT Resource for the target system.

The target system user account for performing connector operations on database tables must have the following permissions:

- For provisioning operations: The user account must have permissions to perform select, insert, update, and delete operations on the tables to be managed by this connector.
- For reconciliation: The user account must have permissions to run Select statements on the tables that must be managed by this connector.

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 MySQL and Oracle Identity Manager
- Configuring Secure Communication Between Oracle Database and Oracle Identity Manager
- Configuring Secure Communication Between Sybase Adaptive Server Enterprise 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, Workarounds, and Troubleshooting" 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 2–4. This table shows the location of the truststore for each of the supported application servers.

Note: In an Oracle Identity Manager cluster, 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
For Oracle Identity Manager release 9.1.0.*x* on Oracle WebLogic Server	*WEBLOGIC_HOME*/java/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on IBM WebSphere Application Server	*WEBSPHERE_HOME*/java/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts
For Oracle Identity Manager release 11.1.1 and 11.1.2.*x* on Oracle Application Server	*JAVA_HOME*/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 2–4. This table shows the location of the truststore for each of the supported application servers.

Note: In an Oracle Identity Manager cluster, 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
For Oracle Identity Manager release 9.1.0.*x* on Oracle WebLogic Server	*WEBLOGIC_HOME*/java/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on IBM WebSphere Application Server	*WEBSPHERE_HOME*/java/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts
For Oracle Identity Manager release 11.1.1 and 11.1.2.*x* on Oracle Application Server	*JAVA_HOME*/jre/lib/security/cacerts

2.3.3 Configuring Secure Communication Between MySQL and Oracle Identity Manager

To configure secure communication between MySQL and Oracle Identity Manager:

1. See MySQL documentation for information about enabling SSL communication between MySQL and a client system. In this context, the client is Oracle Identity Manager.
2. Export the certificate on the MySQL host computer.
3. Restart the MySQL database service by using the certificate exported in the preceding step. See MySQL documentation for information on restarting the database service.
4. Copy the ca-cert.pem and client-cert.pem certificates to the Oracle Identity Manager host computer.
5. Import the certificates into the JVM truststore of the application server on which Oracle Identity Manager is running.

   To import the certificates into the truststore, run the following command for each certificate:

   ```
   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 2–5. This table shows the location of the truststore for each of the supported application servers.

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

Table 2–5 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
For Oracle Identity Manager release 9.1.0.*x* on IBM WebSphere Application Server	For any supported IBM WebSphere Application Server release, import the certificate into the following certificate store: *WEBSPHERE_HOME*/java/jre/lib/security/cacerts In addition to importing the certificate into the cacerts certificate store, you must import the certificate into one of the following certificate stores: ▪ For IBM WebSphere Application Server 6.1.*x*, import the certificate into the following certificate store: *WEBSPHERE_HOME*/Web_Sphere/profiles/*SERVER_NAME*/config/cells/*CELL_NAME*/nodes/*NODE_NAME*/trust.p12 For example: C:/Web_Sphere/profiles/AppSrv01/config/cells/tcs055071Node01Cell/nodes/tcs055071Node0/trust.p12 ▪ For IBM WebSphere Application Server 5.1.*x*, in addition to the cacerts certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/etc/*KEY_STORE* Here, *KEY_STORE* is the name of the keystore.
For Oracle Identity Manager release 9.1.0.*x* on JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on Oracle WebLogic Server	▪ If you are using Oracle jrockit_R27.3.1-jdk, then import the certificate into the keystore in the following directory: *JROCKIT_HOME*/jre/lib/security ▪ If you are using the default Oracle WebLogic Server JDK, then import the certificate into the keystore in following directory: *WEBLOGIC_HOME*/java/jre/lib/security/cacerts ▪ If you are using a JDK other than Oracle jrockit_R27.3.1-jdk or Oracle WebLogic Server JDK, then import the certificate into your keystore at the following directory: *JAVA_HOME*/jre/lib/security/cacerts
For Oracle Identity Manager release 11.1.1and 11.1.2.*x* on Oracle WebLogic Server	*JAVA_HOME*/jre/lib/security/cacerts

2.3.4 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

2.3.4.1 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.

2.3.4.2 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, Workarounds, and Troubleshooting" 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 2–6. This table shows the location of the truststore for each of the supported application servers.

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

Table 2–6 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
For Oracle Identity Manager release 9.1.0.*x* on Oracle WebLogic Server	*WEBLOGIC_HOME*/java/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
For Oracle Identity Manager release 11.1.1 and 11.1.2.*x* on Oracle WebLogic Server	*JAVA_HOME*/jre/lib/security/cacerts

2.3.5 Configuring Secure Communication Between Sybase Adaptive Server Enterprise and Oracle Identity Manager

To configure secure communication between Sybase Adaptive Server Enterprise and Oracle Identity Manager:

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

   Export the certificate on the Sybase Adaptive Server Enterprise 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 2–7. This table shows the location of the truststore for each of the supported application servers.

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

Table 2–7 Truststore Locations on Supported Application Servers

Application Server	Truststore Location
For Oracle Identity Manager release 9.1.0.*x* on Oracle WebLogic Server	*WEBLOGIC_HOME*/java/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on IBM WebSphere Application Server	*WEBSPHERE_HOME*/java/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
For Oracle Identity Manager release 9.1.0.*x* on Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts
For Oracle Identity Manager release 11.1.1 and 11.1.2.*x* on Oracle WebLogic 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" section discusses the Database URL and Connection Properties parameters.
- The "Modifying Field Lengths of the Provider Parameters" section described the procedure to modify field lengths of the provider parameters.
- The "Creating the Connector" section describes the procedure to create the connector.
- The "Localizing Field Lables in UI Forms" section describes the procedure to
- The "Configuring Oracle Identity Manager 11.1.2 or Later" section describes the procedures to be performed for creating additional metadata, if you are using Oracle Identity Manager release 11.1.2 or later.
- The "Performing Connector Operations" section provides a link to guidelines that you must apply when you start using the connector.
- The "Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later" section provides instructions for performing provisioning operations in Oracle Identity Manager release 11.1.2.*x*.

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 3-14.

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 3-14, 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 3-14.

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

- Database URL and Connection Properties for IBM DB2/UDB
- Database URL and Connection Properties for Microsoft SQL Server
- Database URL and Connection Properties for MySQL

- Database URL and Connection Properties for Oracle Database
- Database URL and Connection Properties for Sybase Adaptive Server Enterprise

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.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.

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[;PROP
ERTY=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 MySQL

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:mysql://[SERVER_NAME]/[DATABASE_NAME]
  ```

  In this format:

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

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

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

  ```
  jdbc:mysql://192.168.1.251/mysql
  ```

- **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=3306
```

If you enable SSL communication between MySQL 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.

3.2.4 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

If you are using Oracle Database with Oracle RAC implementation as the target system, then enter a value for the Database URL property in the format specified in the following section:

Database URL and Connection Properties for Oracle RAC

3.2.4.1 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)
```

3.2.4.2 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.

3.2.4.3 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.

3.2.4.4 Database URL and Connection Properties for Oracle RAC

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

- **Database URL parameter**

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

  > **Note:** The JDBC URL connection string must not exceed 200 characters.

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

  Sample value:

jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=
host1.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=
host2.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=
host3.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=
host4.example.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=
srvce1)))

- **Connection Properties parameter**

  While creating the connector, do not specify any value for the Connection Properties parameter.

3.2.5 Database URL and Connection Properties for Sybase Adaptive Server Enterprise

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:sybase:Tds:`*`SERVER_NAME`*`:`*`PORT_NUMBER`*`/`*`DATABSE_NAME`*

  In this format:

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

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

  ```
  jdbc:sybase:Tds:172.21.109.62:9050/master
  ```

- **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.

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

  ```
  databaseName=sales,port=9000
  ```

  If you enable SSL communication between Sybase Adaptive Server Enterprise and Oracle Identity Manager, then you must include the `SYBSOCKET_FACTORY` property 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:

  `SYBSOCKET_FACTORY=`*`VALUE`*

Replace *VALUE* with the of the class that implements `com.sybase.jdbcx.SybSocketFactory;` or `"DEFAULT"`, which instantiates a new `java.net.Socket( ).`

3.3 Modifying Field Lengths of the Provider Parameters

Note: This section describes an optional procedure.

Perform the procedure described in this section only if both the following conditions are true:

- You are using Oracle Identity Manager release 9.1.0.*x.*
- You want to modify the field lengths of the provider parameters.

By default, the maximum number of characters that you can enter in a provider parameter field is 200. If the value that you enter in the provider parameters field will be greater than 200 characters, then you must increase the length of that parameter field.

See Also: Table 3–1 for information about provider parameter fields and their description

To modify the length of a provider parameter:

1. In a text editor, open the SharedDriveReconTransport.xml file located in the *OIM_HOME*\xellerate\GTC\ProviderDefinitions directory.
2. Search for the name of the provider parameter field whose length has to be modified.
3. Edit the Parameter element (corresponding the provider parameter field that you searched) to specify the length of the provider parameter field as follows:
   - Add the dataLength attribute.
   - Enter the field length as a value of the dataLength attribute.

   The following XML code block from the *OIM_HOME*\xellerate\GTC\ProviderDefinitions\SharedDriveReconTransport.xml file shows sample values entered for the dataLength attribute of the Parameter element:

```
<Parameter datatype="String" name="customizedQueries" type="Runtime"
encrypted="NO" required="NO" dataLength="400" />
```

4. Repeat Steps 2 and 3 for modifying the length of every provider parameter field.
5. Save and close the file.
6. Repeat Steps 1 through 5 for the DBProvisioningTransport.xml and DBReconTransport.xml files located in the *OIM_HOME*\xellerate\GTC\ProviderDefinitions directory.

3.4 Creating the Connector

The initial steps to create a connector depend on the release of Oracle Identity Manager that you are using:

- For Oracle Identity Manager release 9.1.0.*x*:

  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**.

  Note: While performing the rest of the procedure, read the instructions given in the corresponding sections of *Oracle Identity Manager Administrative and User Console Guide.*

- For Oracle Identity Manager release 11.1.1:

  To navigate to the first Administrative page for creating generic technology connectors, log in to the Administrative User console and then click **Advanced**. Then, in the Configuration region of the Welcome to Identity Manager Advanced Administration page, click **Create Generic Connector**.

  Note: While performing the rest of the procedure, read the instructions given in the corresponding sections of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.*

- For Oracle Identity Manager release 11.1.2.*x:*

  To navigate to the first Administrative page for creating generic technology connectors, log in to Oracle Identity System Administration and then in the Configuration region, click **Generic Connector**.

  Note: While performing the rest of the procedure, read the instructions given in the corresponding sections of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.*

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

- 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

3.4.1 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 one of the following guides:

- For Oracle Identity Manager release 11.1.1: *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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.

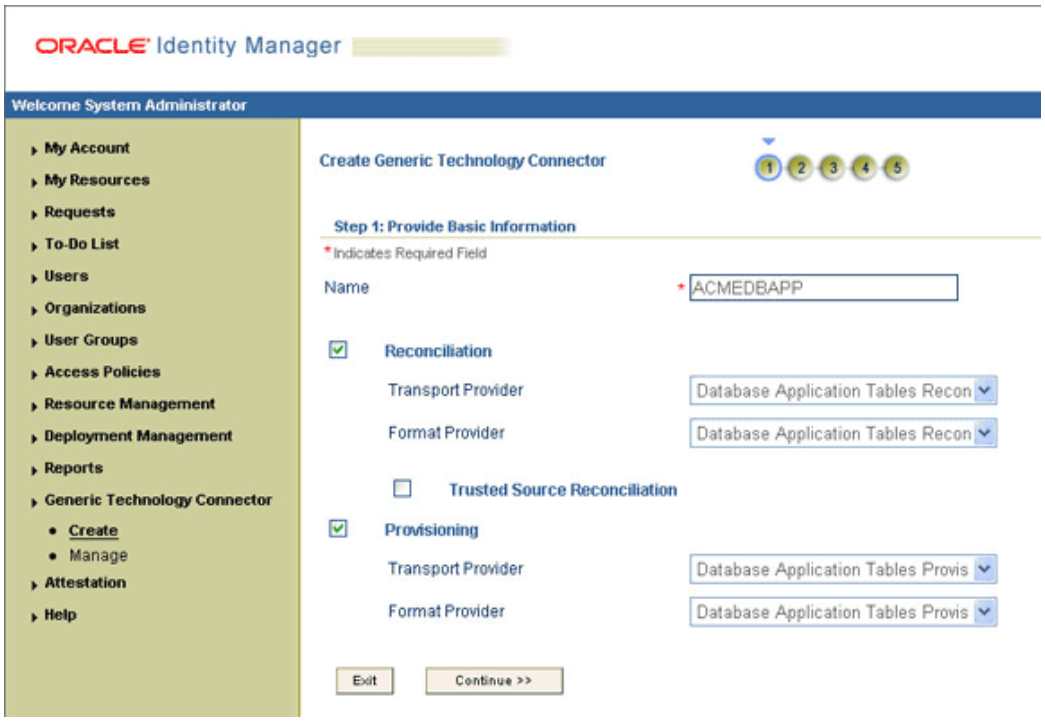
3. If you want to use the connector for provisioning, select **Provisioning** and then perform the following steps:

   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



This screenshot shows the Step 1: Provide Basic Information page. Sample entries have been made in the fields on this page.

****

3.4.2 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 1-8, 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 MySQL Database: `com.mysql.jdbc.Driver` For Oracle Database: `oracle.jdbc.driver.OracleDriver` For Oracle RAC Database: `oracle.jdbc.driver.OracleDriver` For Sybase Adaptive Server Enterprise: `com.sybase.jdbc3.jdbc.SybDriver`
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.
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	

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

Parameter	Description
Parent Table/View Name	Enter the name of the parent table or view. **Note:** You must enter the name of the parent table or view in the same case as it appears in the target system database. For example, if the name of the parent table in the target system database is `ACMEDBAPP`, then you must enter `ACMEDBAPP` in the Parent Table/View Name parameter. The value that you must enter in the Parent Table/View Name parameter 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. **Note:** You must enter the name of the child table or view in the same case as it appears in the target system database. For example, if the name of the child table in the target system database is `acmedbroles`, then you must enter `acmedbroles` in the Child Table/View Names parameter. 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, then do not specify a value for the Unique Attribute parameter. If a referential integrity constraint can be set, then ensure that the name of the primary key column in the parent table is the same as the name of the foreign key column in the child table. If this requirement is not met, then the connector cannot detect the referential integrity constraint.
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 2-10 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 2-10. **Note:** This parameter is used only during provisioning.

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

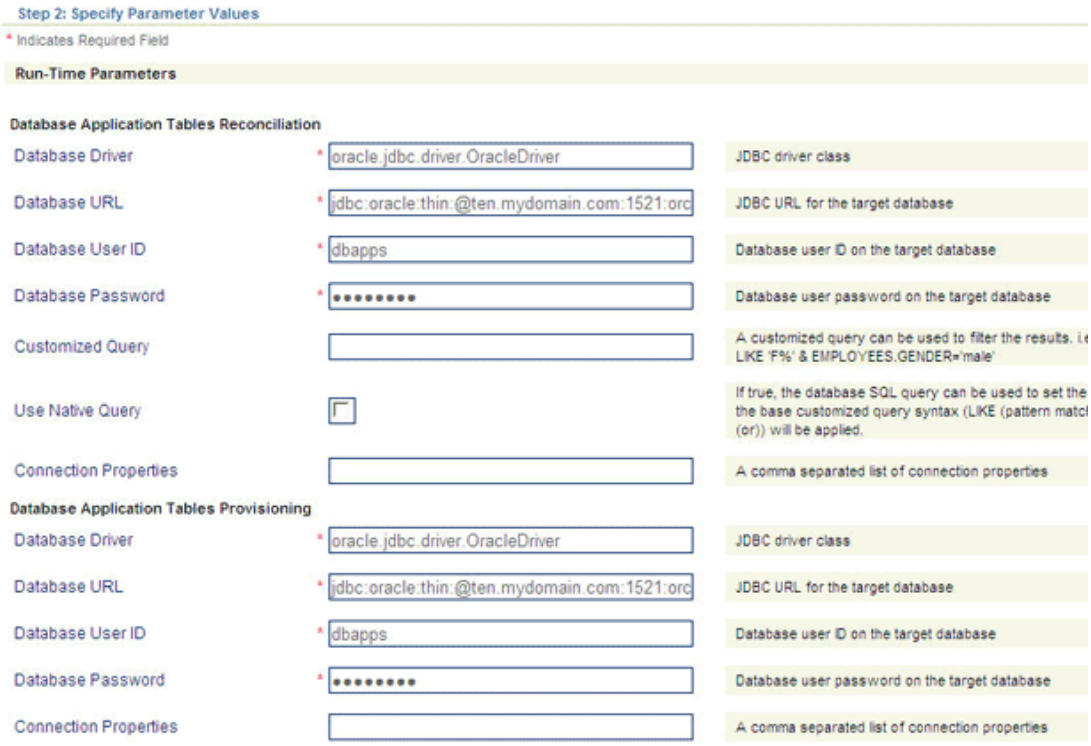
Parameter	Description
Database Date Format	■ Database Date Format parameter for reconciliation: Enter the *same* value that you enter for the Source Date Format parameter. This parameter is described later in this table. Do not enter a value for this parameter if you do not enter a value for the Source 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.
Is Primary Key Auto Incremented	Select this option *only* if the primary key column of the target system is defined with the autoincrement option.
Target Date Format	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. See "Step 2: Specify Parameter Values Page" in one of the following guides for detailed information about this parameter: ■ For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide* ■ For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
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:** One of the following guides for detailed information about this parameter: ■ For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide* ■ For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
Stop Threshold Minimum Records	Enter a value for this parameter only if you specify a value for the Stop Reconciliation Threshold parameter. **See Also:** One of the following guides for detailed information about this parameter: ■ For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide* ■ For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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

Parameter	Description
Source Date Format	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. See "Step 2: Specify Parameter Values Page" in one of the following guides for detailed information about this parameter: ■ For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide* ■ For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
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



This screenshot shows the first section of the Step 2: Specify Parameter Values page. Sample entries have been made in the fields in this section.

****

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

This screenshot shows the second section of the Step 2: Specify Parameter Values page. Sample entries have been made in the fields in this section.

****

3.4.3 Step 3: Modify Connector Configuration Page

Note: See "Step 3: Modify Connector Configuration Page" in one of the following guides for detailed information about the terms and procedures given in this section:

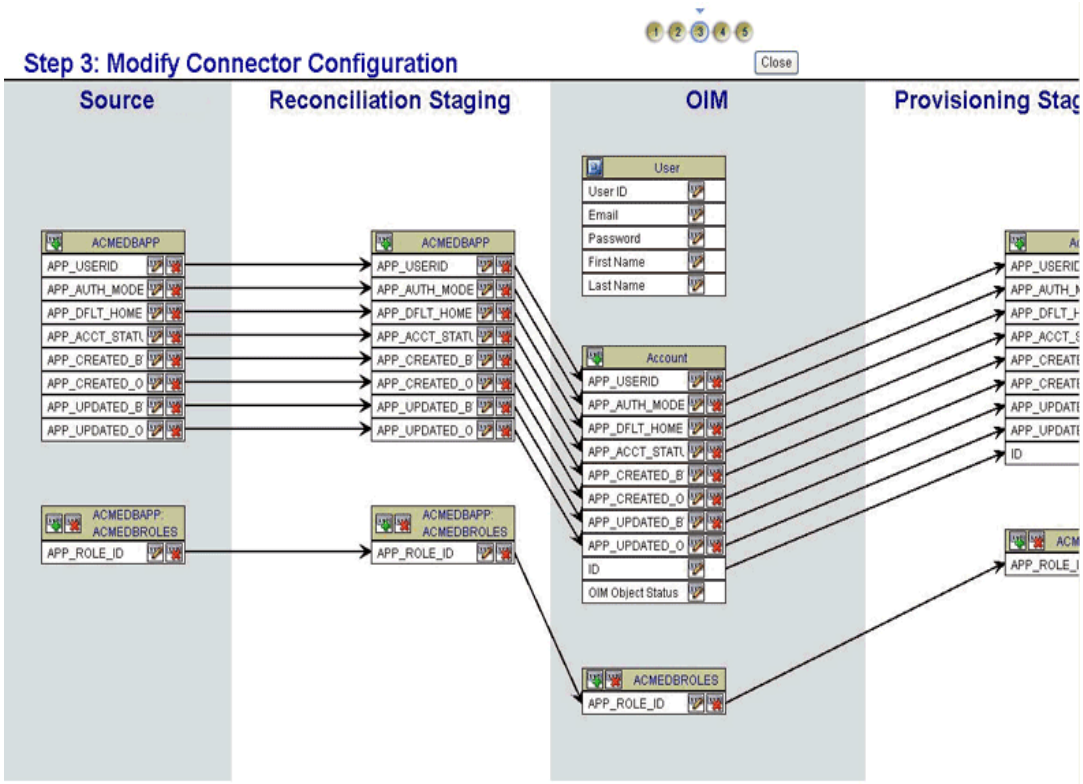
- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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



This screenshot shows the Step 3: Modify Connector Configuration page after metadata detection. Fields identified during metadata detection are displayed in the Source, Reconciliation Staging, OIM, and Provisioning Staging data sets on this page.

****

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 the "Display of Data Sets and Fields Under Various Input Conditions" table in one of the following guides for more information:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide*

- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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 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 3-28 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. The data type and field size of the attribute are automatically detected for the supported data types by the connector itself. If you want to change the data type or size, you may have to edit the 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 may have to 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 2-9 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 2-7.
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 3-28 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 2-5 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. See one of the following guides for information on creating UDFs: ■ For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Design Console Guide.* ■ For Oracle Identity Manager release 11.1.1: See the "Configuring User Attributes" chapter of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*. ■ For Oracle Identity Manager release 11.1.2.*x:* See the "Configuring Custom Attributes" chapter of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*. 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.

If you are creating a connector for a target system that has a primary key column defined with the autoincrement option, then perform the following steps:

Note: If you are creating a provisioning-only connector, then perform *only* Steps 1 through 4. If you are creating a connector for both provisioning and reconciliation, then perform all the steps.

1. From the OIM data sets, to remove the primary key field defined with the auto-increment option, click the Delete icon corresponding to this field.
2. In the Delete Field Confirmation dialog box, confirm that you want to proceed with the deletion of the primary key field by clicking **Confirm.**
3. In the Delete Field Success dialog box, click **Close.**
4. Repeat Steps 1 through 3 to remove the primary key field from the Provisioning Staging data sets.
5. Create a mapping between the primary key field in the Reconciliation Staging data sets and the ID field in the OIM - Account data set by performing the following steps:

Note: Perform Step 5 *only* if you are creating a connector that can be used for both provisioning and reconciliation.

   a. Click the Edit icon for the ID field in the OIM - Account data set.
   b. On the Step 1: Provide Field Information page, select the **Matching Only** check box, and then click **Continue.**

c. On the Step 3: Provide Mapping Information page, from the Field Name list, select the primary key field, and then click **Continue.**

d. In the Modify Generic Technology Connector dialog box, click **Close.**

3.4.4 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

This screenshot shows the Step 4: Verify Connector Form Names page. Default process form and child form names are displayed on this page.

****

3.4.5 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 one of the following sections for troubleshooting information:

- For Oracle Identity Manager release 9.1.0.*x:* "Errors Encountered at the End of the Connector Creation Process" in *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Errors During Connector Creation" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

Creation of the connector involves creation of all the objects that constitute the connector. For information about the connector objects that are created, see the following:

- For Oracle Identity Manager release 9.1.0.*x:* "Connector Objects Created by the Generic Technology Connector Framework" chapter in *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Connector Objects Created by the Generic Technology Connector Framework" section in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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.

3.4.6 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 one of the following guides for information about this procedure:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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 following guides:

- For Oracle Identity Manager release 9.1.0.*x:* "Known Issues of Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Troubleshooting Generic Technology Connectors" chapter of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

3.4.7 Configuring Reconciliation

See "Configuring Reconciliation" section in the following guides:

- For Oracle Identity Manager release 9.1.0.*x:* "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Creating and Managing Generic Technology Connectors" chapter of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

3.4.8 Configuring Provisioning

See "Configuring Provisioning" section in the following guides:

- For Oracle Identity Manager release 9.1.0.*x:* "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Creating and Managing Generic Technology Connectors" chapter of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

3.5 Configuring Oracle Identity Manager 11.1.2 or Later

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

- Tagging Parent Form Fields
- Tagging Child Form Fields
- Creating and Activating a Sandbox
- Creating a New UI Form
- Attaching the UI Form to an Application Instance
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog

3.5.1 Tagging Parent Form Fields

After creating the connector, you must tag the properties of parent form fields such as AccountName, AccountID, ITResource and Type.

The "AccountName" property of a process form field that represents the login ID of an account in the target system must be set to `true`. Otherwise, the Account Name column on the Accounts tab of the My Access page in the Self Service console for a user displays the database numeric key, instead of the correct account name.

The "AccountID" property of a process form field that represents the immutable GUID of the account (if one exists) must be set to `true`. Otherwise, you cannot integrate Oracle Identity Manager with Oracle Identity Analytics (OIA).

The "ITResource" property must be set to `true` to identify the IT Resource field of the process form.

The "Type" property of the IT Resource process form field must be set on the ITResource form field. Otherwise, Design Console automatically makes the form active.

To tag all the properties (discussed in the preceding paragraphs) of the parent form fields:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools,** and then double-click **Form Designer.**
3. Search for and open the parent form. For example, **ACMEDBAPP.**
4. Click **Create New Version.**
5. On the Properties tab, as per your requirements, add properties for all the required fields. See the following table for details:

Configuration	Form Field	Example	Property Name	Property Value
To display Account Name in the Accounts Tab of the user	Login ID Field	APP_USERID	AccountName	`True`
To represent the immutable GUID of the specific account. Used for OIA Integration	Unique ID Field	APP_USERID	AccountId	`True`
To identify the ITResource field	ITResource Lookup Field	IT Resource2	ITResource	`True`
To set the IT Resource Type	ITResource Lookup Field	IT Resource2	Type	For example, `ACMEDBAPP_GTC`

Note: IT Resource Type is a mandatory property that must be set on the ITResource form field. If this property is not set, then the Design Console will make the form active.

6. Click **Save,** and then click **Make Version Active.**

3.5.2 Tagging Child Form Fields

You must tag the "Entitlement" property of child form fields. In other words, you must set the "Entitlement" property of child form attributes to `true`.

If the "Entitlement" property is not set to `true`, then the child form attributes are not displayed in the catalog during a provisioning operation. This prevents users from adding such entitlements provided by the connector to the shopping cart.

To tag the "Entitlement" property of child form fields:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools,** and then double-click **Form Designer.**
3. Search for and open the parent form. For example, **ACMEROLE.**
4. Click **Create New Version.**
5. On the Additional Columns tab, search for the entry corresponding to the child form field (for example, role_id), change the value in the Field Type column to `LookupField`.
6. On the Properties tab, add the following properties to the child form field (for example, role_id):

Property Name	Value
Entitlement	`True`
Lookup Code	Name of the lookup definition that holds child form field values. Sample value: `Lookup.ACMEDBAPP.roles`

Note: The lookup definition containing values for the child form field (for example, Lookup.ACMEDBAPP.roles) must be manually created and populated with values.

7. Click **Save,** and then click **Make Version Active.**
8. Assign the new child form version to the parent form as follows:
   a. Search for and open the parent form. For example, **ACMEDBAPP.**
   b. On the Child Table(s) tab, click **Create New Version.**
   c. Ensure the child table version is the active version.
   d. Click **Save,** and then click **Make Version Active.**
9. Run the Entitlement List and Catalog Synchronization Job scheduled jobs. See "Harvesting Entitlements and Sync Catalog" on page 3-33 for more information.

3.5.3 Creating and Activating a Sandbox

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

1. Log in to Oracle Identity System Administration.
2. In the upper right corner of the page, click the **Sandboxes** link.

   The Manage Sandboxes page is displayed.
3. On the toolbar, click **Create Sandbox.**
4. In the Create Sandbox dialog box, enter values for the following fields:
   – **Sandbox Name:** Enter a name for the sandbox.

- **Sandbox Description:** Enter a description of the sandbox.

5. Click **Save and Close.**
6. Click **OK** on the confirmation message that is displayed.

   The sandbox is created and displayed in the Available Sandboxes section of the Manage Sandboxes page. Note that the newly created sandbox is in the active state by default.
7. Select the newly created sandbox.

3.5.4 Creating a New UI Form

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

1. In the left pane, under Configuration, click **Form Designer.** The Form Designer page is displayed.
2. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Form page is displayed.
3. On the Create Form page, enter values for the following UI fields:
   - **Resource Type:** Select the resource object that you want to associate the form with.
   - **Form Name:** Enter a name for the form.
4. Click **Create.**

   A message is displayed stating that the form is created.

3.5.5 Attaching the UI Form to an Application Instance

For a generic technology connector, and application instance by the name *PARENTFORM*_GTC is created by default. For example, if the name of the parent form is ACMEDBAPP, then the name of the application instance that is created is ACMEDBAPP_GTC.

You must associate the newly created UI form with the application instance of your target system (*PARENTFORM*_GTC). To do so, open the existing application instance for your resource, from the Form field, select the form (created in "Creating a New UI Form" on page 3-32), and then save the application instance.

Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See the "Managing Organizations Associated With Application Instances" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed instructions.

3.5.6 Publishing a Sandbox

To publish the sandbox that you created in "Creating and Activating a Sandbox" on page 3-31:

1. Close all the open tabs and pages.
2. In the upper right corner of the page, click the **Sandboxes** link.

   The Manage Sandboxes page is displayed.

3. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in "Creating and Activating a Sandbox" on page 3-31.
4. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
5. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

3.5.7 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

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

3.6 Localizing Field Lables in UI Forms

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

To localize field label that is added in the UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:
   a. Search for the following text:

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

   b. Replace with the following text:

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

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

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

c. Search for the application instance code. This procedure shows a sample edit for Database Application Tables application instance. The original code is:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_ACMEDBAP_APP_DFLT_HOME__c_description']}">
<source>APP_DFLT_HOME</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ACMEFORM.entity.ACMEFORMEO.
UD_ACMEDBAP_APP_DFLT_HOME__c_LABEL">
<source>APP_DFLT_HOME</source>
<target/>
</trans-unit>
```

d. Open the resource file from the connector package, for example DatabaseApplicationTables_ja.properties, and get the value of the attribute from the file.

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

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_ACMEDBAP_APP_DFLT_HOME__c_description']}">
<source>APP_DFLT_HOME</source>
<target>\u4567d</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ACMEFORM.entity.ACMEFORMEO.
UD_ACMEDBAP_APP_DFLT_HOME__c_LABEL">
<source>APP_DFLT_HOME</source>
<target>\u4567d</target>
</trans-unit>
```

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

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

Sample file name: BizEditorBundle_ja.xlf.

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

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

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

3.7 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, Workarounds, and Troubleshooting" chapter

3.8 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

To perform provisioning operations in Oracle Identity Manager release 11.1.2 or later:

1. Log in to Oracle Identity Self Service.
2. Create a user. See the "Managing Users" chapter in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance for your target system (*PARENTFORM*_GTC) and then click **Checkout.**
5. Specify value for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**
7. If the generic technology connector has child tables and you want to provision entitlements (child table values), then:
   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

   Alternatively, you can insert or delete child table values to or from a user account in Oracle Identity Manager as follows:
   1. In the left pane, under Administration, click **Users.**
   2. On the Users page, search for and select the user.
   3. On the User Details page, click the **Accounts** tab.
   4. Search for and select the user account to or from which child tables values must be inserted or deleted, and then click **Modify Accounts.**
   5. Depending on whether you want to insert of delete child table values, perform one of the following steps:
      - To insert child table values, add the child table data in the child table displayed below the parent table data.
      - To delete child table values, select the child table row, and then click **Delete.**

6. Click **Ready to Submit.**
7. Click **Submit.**

4

Known Issues, Workarounds, and Troubleshooting

This chapter discusses the following topics related to connector testing:

- Section 4.1, "Known Issues and Workarounds"
- Section 4.2, "Troubleshooting"

4.1 Known Issues and Workarounds

This chapter describes known issues that you might encounter while creating or using Database Application Tables connectors. It includes the following topics:

See Also:

- For Oracle Identity Manager release 9.1.0.*x:* "Known Issues of Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Troubleshooting Generic Technology Connectors" chapter of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

- Connector Issues
- Oracle Identity Manager Issues

4.1.1 Connector Issues

The following are issues and workarounds associated with the connector:

- Deletion of a Record from the Target System is not Reconciled into Oracle Identity Manager
- Update Child Record Provisioning Operations
- Stored Procedure for Performing CRUD Operations
- ArrayIndexOutOfBounds Exception
- Connector is Not Created when No Value is Specified for the Unique Attribute
- No Support for Date Data Type in Microsoft SQL Server 2008 Target System
- Error While Running the Evaluate User Policy Scheduled Job

4.1.1.1 Deletion of a Record from the Target System is not Reconciled into Oracle Identity Manager

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.

This is a known issue, and a workaround is currently not available.

4.1.1.2 Update Child Record Provisioning Operations

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.

4.1.1.3 Stored Procedure for Performing CRUD Operations

The Database Application Tables connector does not support the use of stored procedures to perform CRUD operations against a table.

This is a known issue, and a workaround is currently not available.

4.1.1.4 ArrayIndexOutOfBounds Exception

If you are using the ojdbc6.jar file, then the ArrayIndexOutOfBounds exception is encountered during a provisioning operation on Oracle Identity Manager 9.1.0.2 BP02 or later.

To resolve this issue:

- On JBoss Application Server, replace the ojdbc6.jar file with the ojdbc14.jar file in the following directory:

  OIM_HOME/xellerate/ext and *JBOSS_HOME*/server/default/lib

- For all other certified application servers, apply Patch 7112447. This patch is available on My Oracle Support (formerly Oracle*MetaLink*).

4.1.1.5 Connector is Not Created when No Value is Specified for the Unique Attribute

In the case of table views (parent table view and child table view), you must specify the name of the Unique attribute while creating the connector. Otherwise, the connector is not created at the end of the procedure.

This is a known issue, and a workaround is currently not available.

4.1.1.6 No Support for Date Data Type in Microsoft SQL Server 2008 Target System

If you are using Microsoft SQL Server 2008 as the target system, then this connector does not support the Date data type.

A workaround for this issue is to use the DateTime data type.

4.1.1.7 Error While Running the Evaluate User Policy Scheduled Job

If you run the Evaluate User Policy scheduled job, the ProvisionAccountActionHandler fails to complete the job and the following error message appears:

```
<Error> <WebLogicServer> <BEA-000337> <[STUCK] ExecuteThread: '76' for
queue: 'weblogic.kernel.Default (self-tuning)' has been busy for "1,238"
seconds working on the request "Workmanager: OIMMDBWorkManager, Version:
0, Scheduled=false, Started=true, Started time: 237436 ms ", which is more
than the configured time (StuckThreadMaxTime) of "1,200" seconds. Stack
trace: java.lang.Object.wait(Native Method)
java.lang.Object.wait(Object.java:503)
org.apache.commons.pool.impl.GenericObjectPool.borrowObject(GenericObjectP
ool.java:810)
org.apache.commons.dbcp.PoolingDataSource.getConnection(PoolingDataSource.
java:95) com.thortech.xl.gc.impl.common.DBFacade.getConnection(Unknown
Source) com.thortech.xl.gc.impl.common.DBFacade.createParentRecord(Unknown
Source)
com.thortech.xl.gc.impl.prov.DBProvisioningTransportProvider.sendData(Unkn
own Source) .....
```

This is due to an issue with the Apache Commons Pool used by the connector.

To resolve this issue:

1. Download commons-pool-1.6.jar file from Apache Commons Pool release 1.6.
2. On the application server, update the com.bea.core.apache.commons.pool_1.3.0.jar and commons-pool-1.2.jar as follows:
   - Copy commons-pool-1.6.jar file to com.bea.core.apache.commons.pool_1.3.0.jar.
   - Copy commons-pool-1.6.jar file to commons-pool-1.2.jar file.
3. Restart the application server.

4.1.2 Oracle Identity Manager Issues

The following is an issue associated with Oracle Identity Manager:

4.1.2.1 UI Text is Displayed in English in non-English Locales

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`

This is a known issue, and a workaround is currently not available.

4.2 Troubleshooting

Table 4–1 lists solutions to some commonly encountered issues associated with the Google Apps connector:

Table 4–1 Troubleshooting

Problem Description	Solution
Database Application Tables connector creation may fail with the following error, if the precise length of the NUMBER field in the Database Column Type is not defined. `DBProvisioningTransportProvider/sendData encounter some problems: DB_CREATE_PARENTRECORD_ERROR`	Define a fixed precise length for the NUMBER field in the Database Column Type. For example: NUMBER (10)

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 Components" 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 2-7 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 2-9 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 2-10 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 the following guides for information about creating UDFs:
   - For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Design Console Guide.*
   - For Oracle Identity Manager release 11.1.1: See the "Configuring User Attributes" chapter of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
   - For Oracle Identity Manager release 11.1.2.*x:* See the "Configuring Custom Attributes" chapter of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
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 2-11 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 following guides:
   - For Oracle Identity Manager release 9.1.0.*x:* "Addressing the Prerequisites for Creating the Generic Technology Connector" section of *Oracle Identity Manager Administrative and User Console Guide*
   - For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Addressing the Prerequisites" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

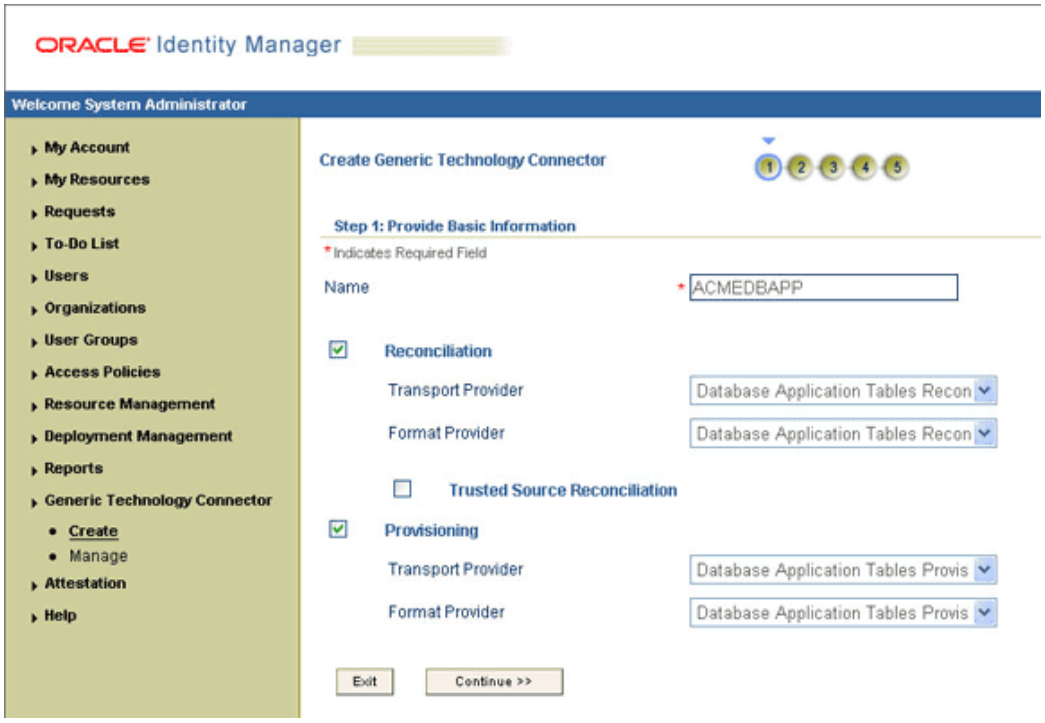
2. To navigate to the first Administrative and User Console page for creating generic technology connectors, expand **Generic Technology Connector**, and then click **Create**.
3. On the Step 1: Provide Basic Information page, specify the values listed in Table A–1 and then click **Continue**.

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

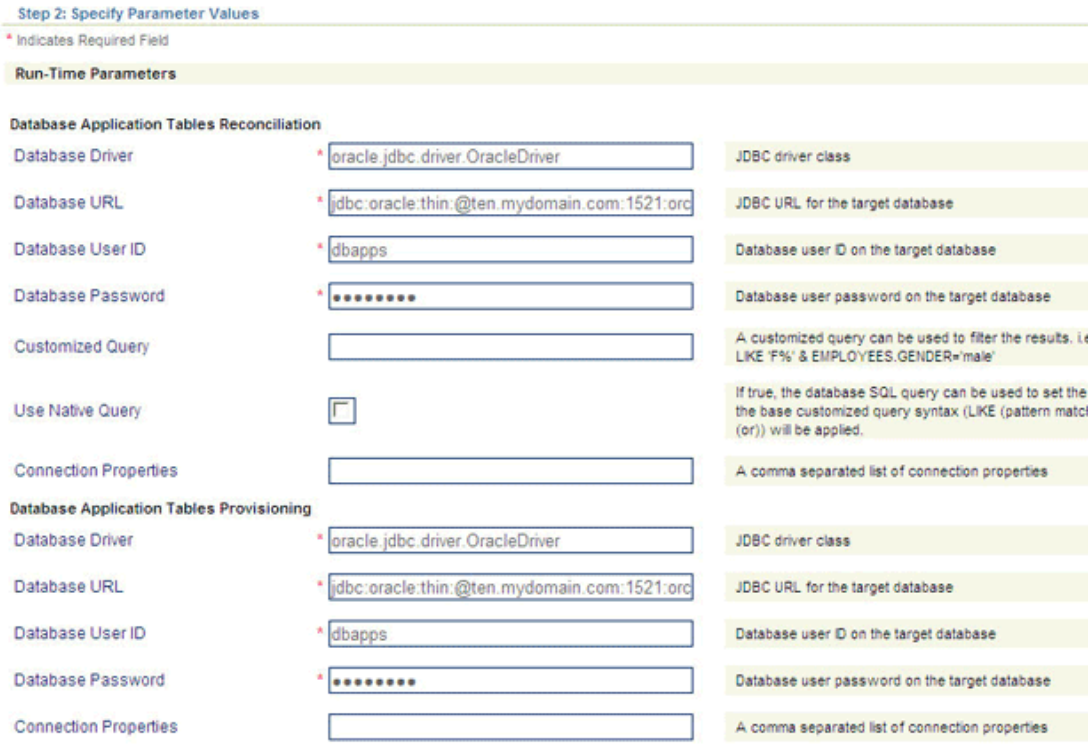
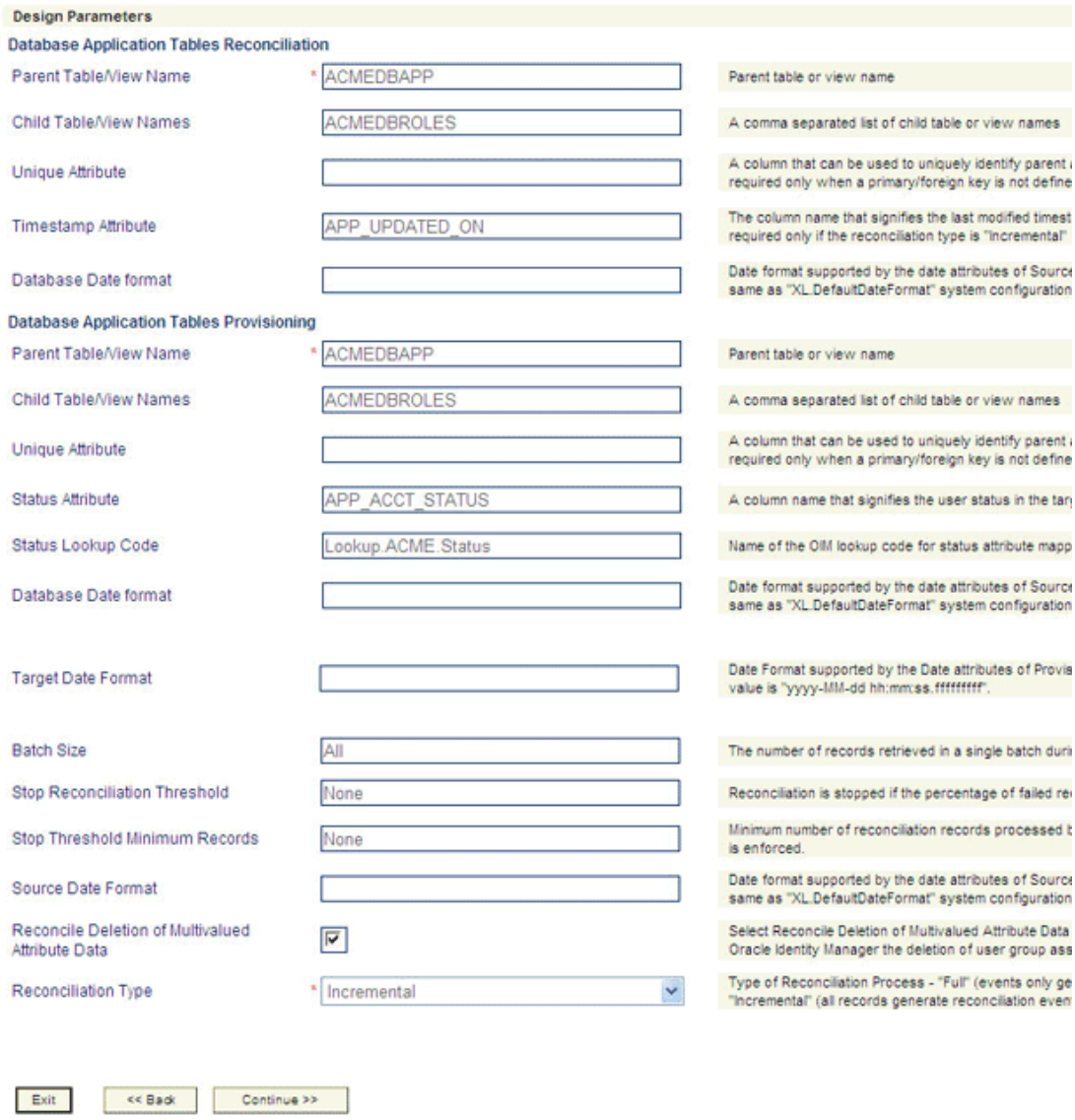


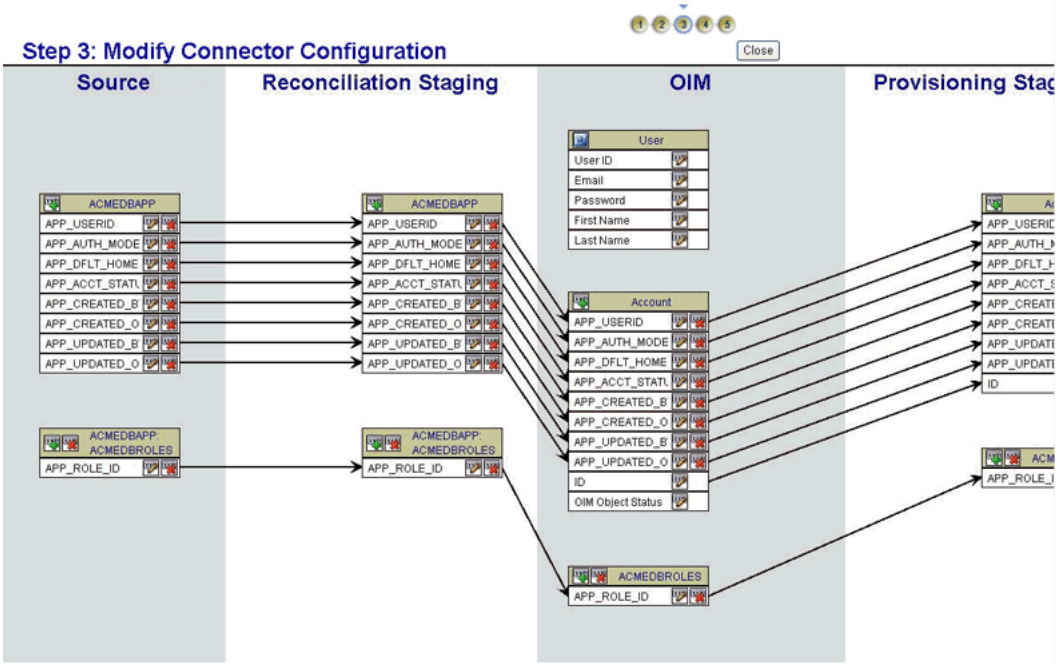
Figure A–3 shows the second section of the Step 2: Specify Parameter Values page on which sample entries have been made.

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

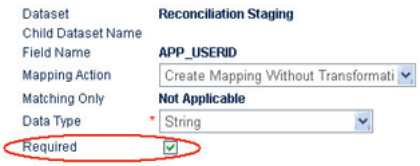


On this page, perform the following actions:

- 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:

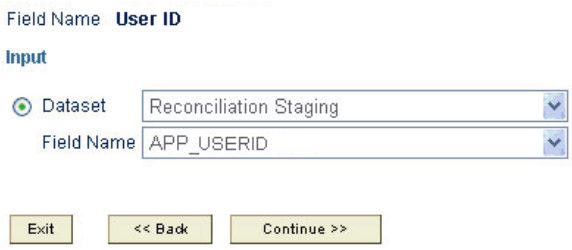
  - From the Mapping Action list, select **Create Mapping Without Transformation**.

  - Select **Matching Only**.

  - Click **Continue**.

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

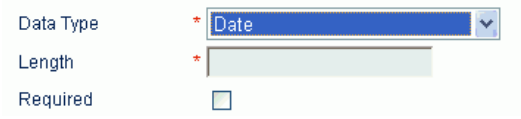
c. On the Step 3: Provide Mapping Information page, select **Reconciliation Staging** from the Dataset list, select **APP_USERID** from the Field Name list, and then click **Continue**. The following screenshot shows the Step 3: Provide Mapping Information page:



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:

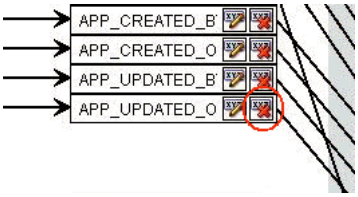


- You want to configure the exchange of account status data between the target system and Oracle Identity Manager.

  See "Exchanging Account Status Data with the Target System" on page 2-9 for details.

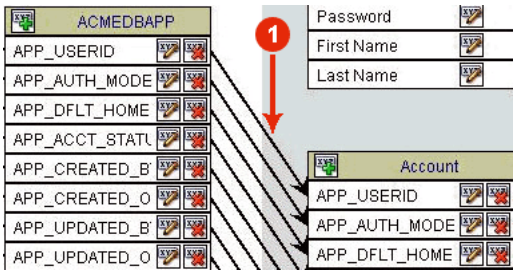
- You do not want to use the APP_CREATED_ON, APP_UPDATED_BY, and APP_UPDATED_ON fields during reconciliation or provisioning. To remove these fields, click the Delete icon for each field and then confirm that you want to proceed with the deletion of the field. You must remove these fields from all the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

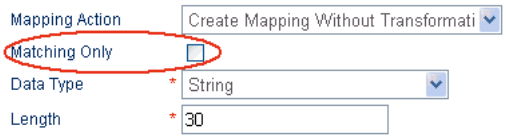
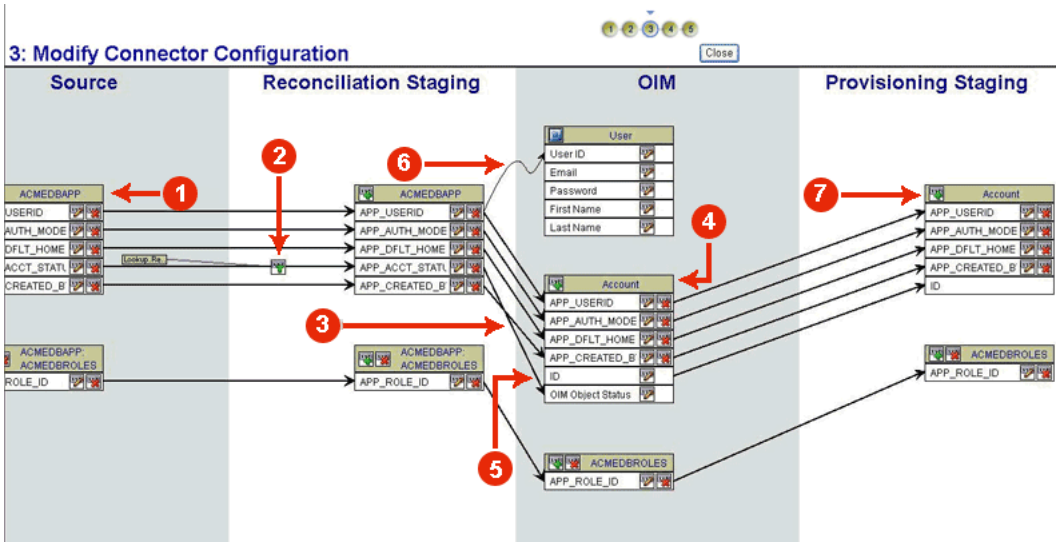


Figure A–5 shows a screenshot of the Step 3: Modify Connector Configuration page that is displayed after you perform the actions described in this section.

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 3-28 for details.
9. Configure reconciliation.

   See "Configuring Reconciliation" section in the following guides:

- For Oracle Identity Manager release 9.1.0.*x:* "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Creating and Managing Generic Technology Connectors" chapter of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

10. Configure provisioning.

    See "Configuring Provisioning" section in the following guides:

    - For Oracle Identity Manager release 9.1.0.*x:* "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*
    - For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Creating and Managing Generic Technology Connectors" chapter of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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:

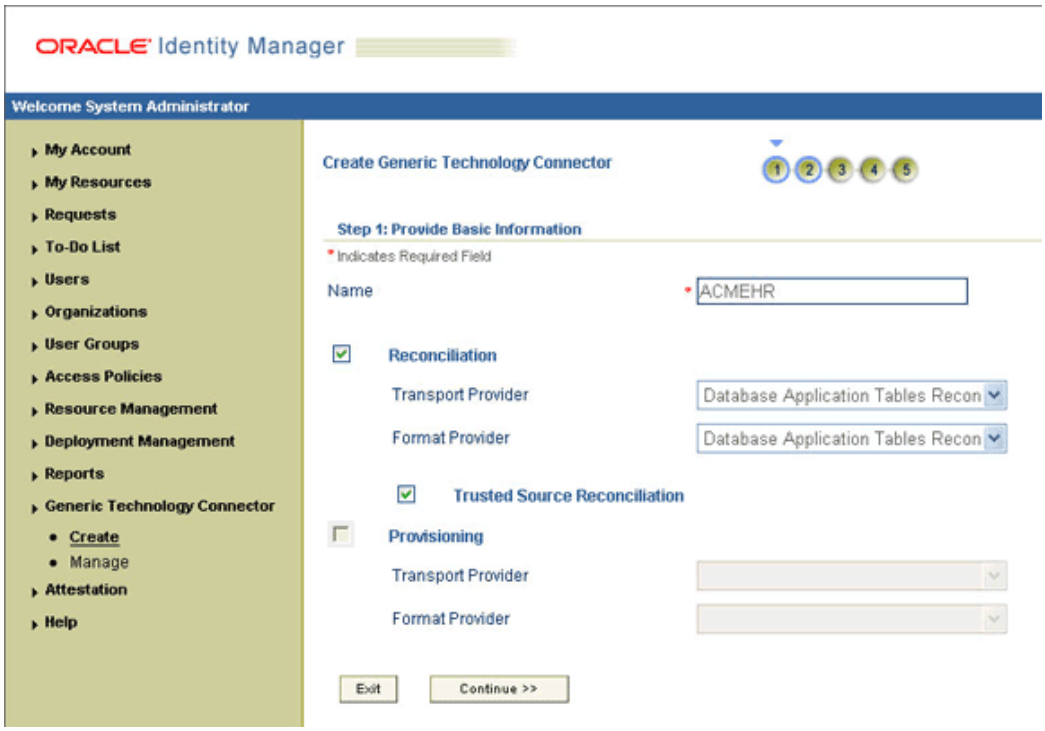
1. Log in to the Administrative and User Console as the user described in the following guides:
    - For Oracle Identity Manager release 9.1.0.*x:* "Addressing the Prerequisites for Creating the Generic Technology Connector" section of *Oracle Identity Manager Administrative and User Console Guide*
    - For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Addressing the Prerequisites" section of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
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**

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
Child Table/View Names field	
Unique Attribute field	
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

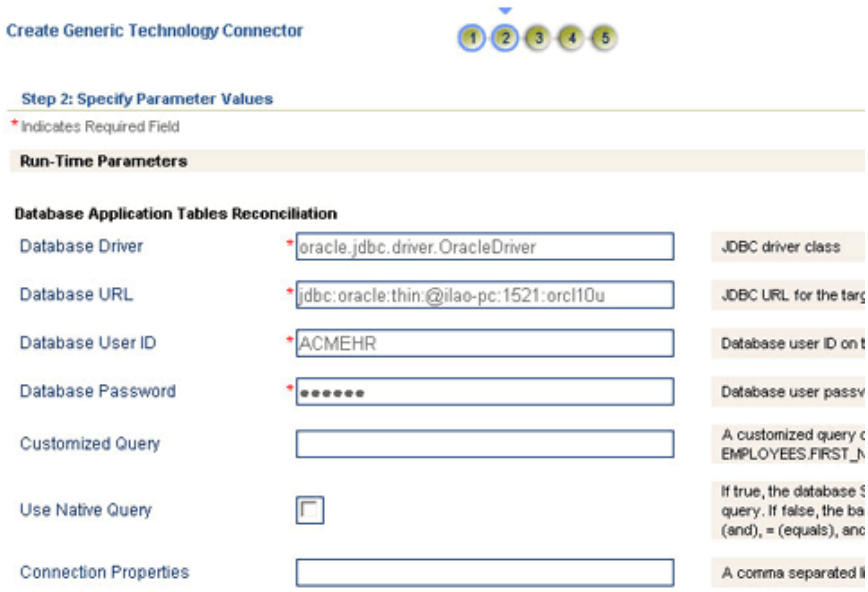
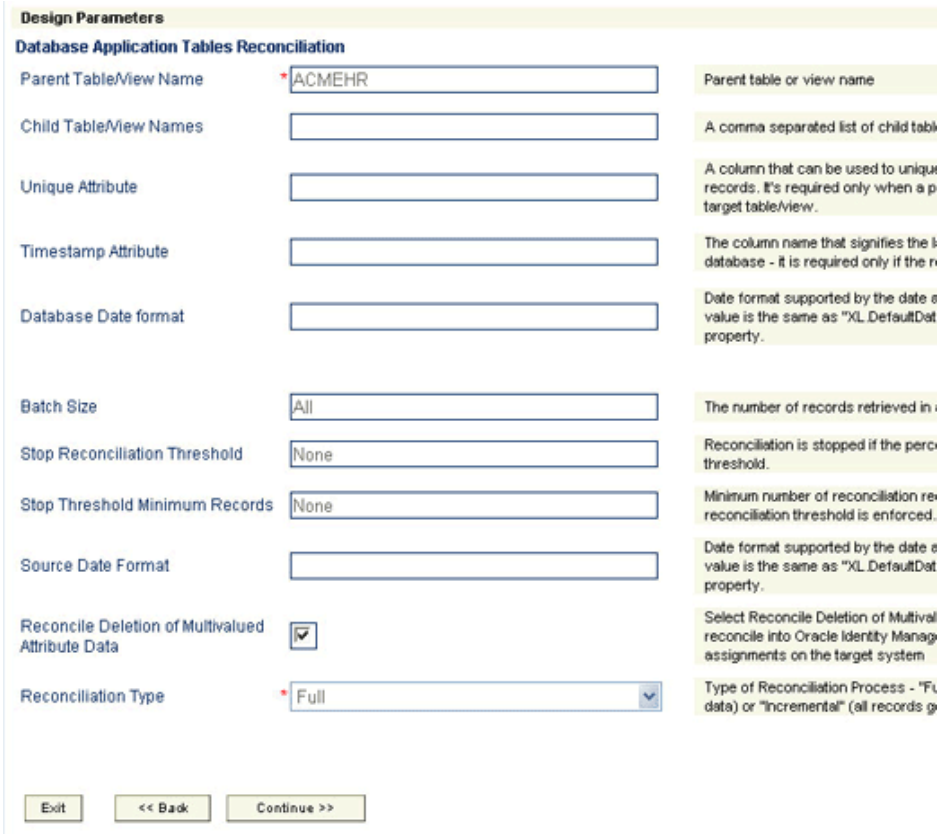


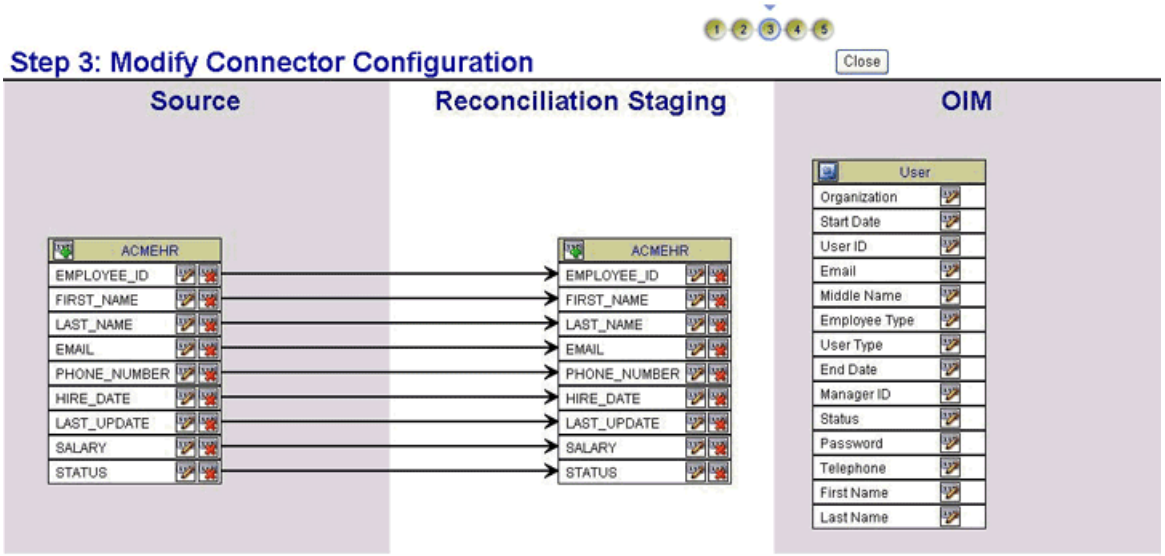
Figure A–9 shows the second section of the Step 2: Specify Parameter Values page on which sample entries have been made.

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

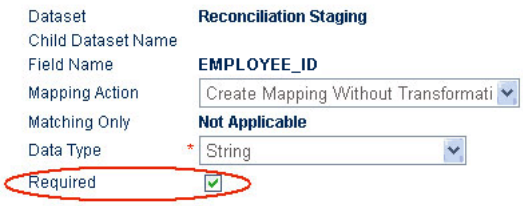


On the Step 3: Modify Connector Configuration page, perform the following actions:

- 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.

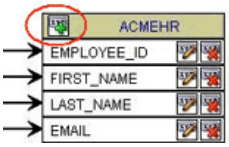
  See "Configuring Account Status Reconciliation" on page 2-9 for details.

- 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.

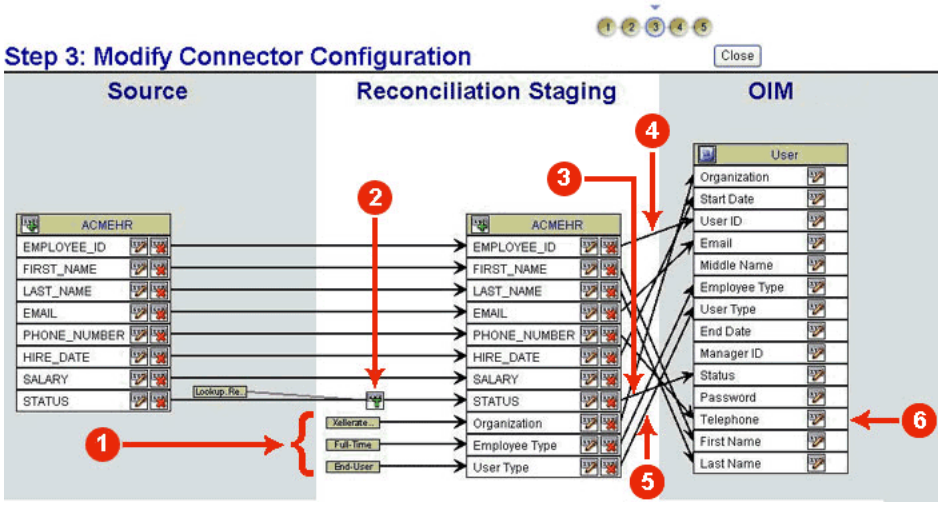
For the Employee Type field, enter **Full-Time**, **Part-Time**, **Temp**, **Intern**, or **Consultant**. These are Code Key values of the Employee Type field.

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 3-28 for details.
8. Configure reconciliation.

   See "Configuring Reconciliation" section in the following guides:

   - For Oracle Identity Manager release 9.1.0.*x:* "Creating Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console Guide*
   - For Oracle Identity Manager release 11.1.1 and 11.1.2.*x:* "Creating and Managing Generic Technology Connectors" chapter of *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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.

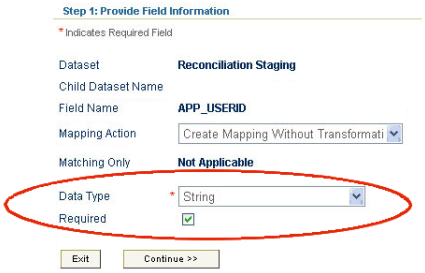
Screenshots for the following actions are described in this appendix:

- 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

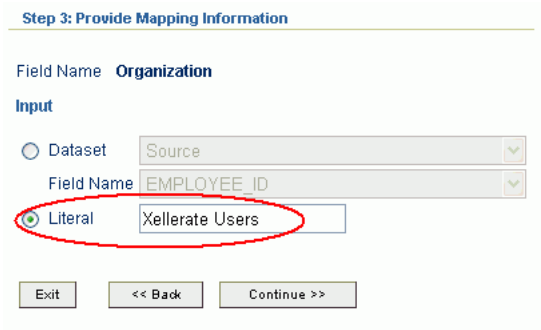
example, date format validation and conversion will not take place if you do not set the Date data type for date fields of the Reconciliation Staging and OIM - Account data sets.

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.

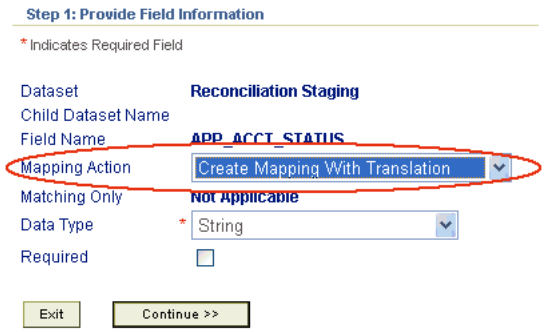
Figure B–3 Encrypted and Password Field Check Boxes

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 the following guides:

- For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Administrative and User Console Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.*x: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

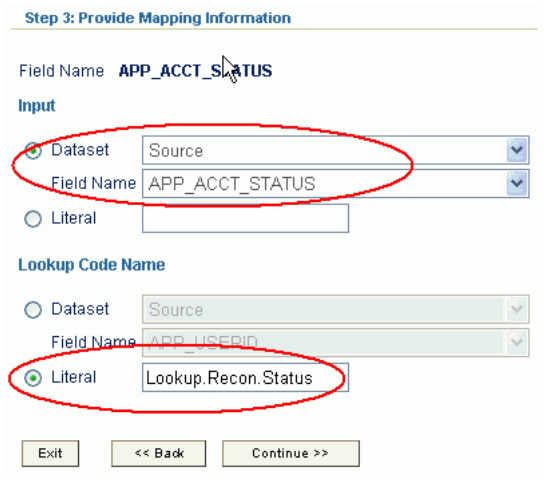
Figure B–4 Translation Transformation Option



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

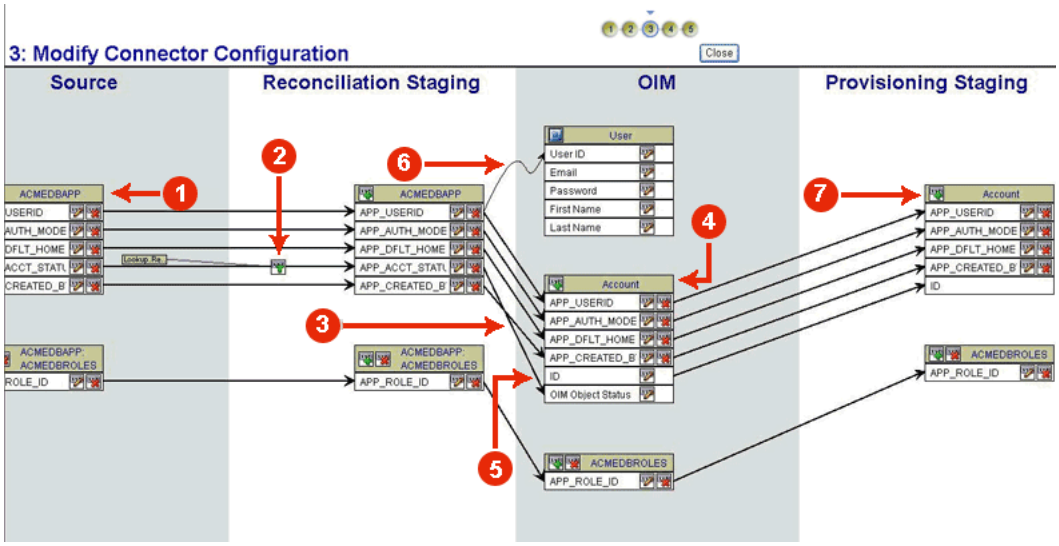


In the Input region of this page, you select **Source** from the Dataset list and then select the name of the status field from the Field Name list. In the Lookup Code Name region, you select **Literal** and then enter the name of the lookup definition that maps target system status values with Oracle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

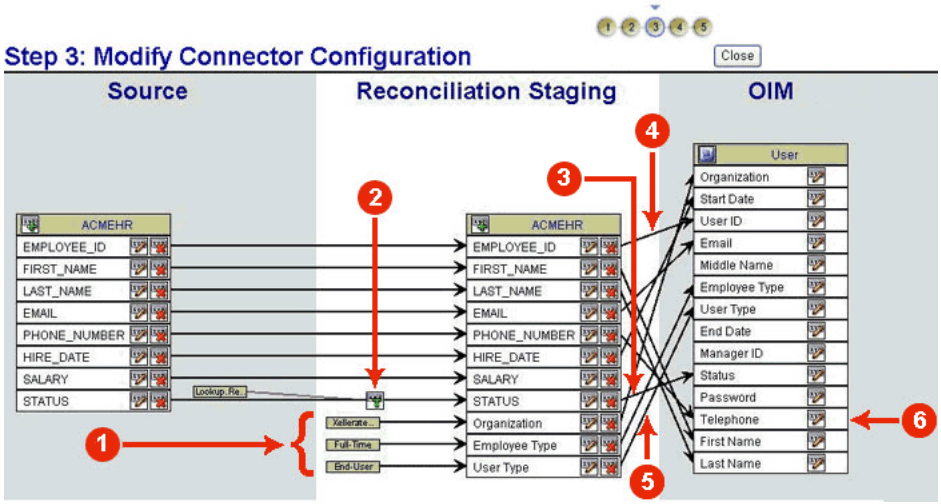
Note: The effect of certain actions, such as setting the attributes of fields in the Reconciliation Staging data set, cannot be seen on this page.

- **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

R

S

T

U

V