Oracle® Identity Manager

Connector Guide for Siebel User Management

Release 9.0.4

E10445-15

September 2013

Oracle Identity Manager Connector Guide for Siebel User Management, Release 9.0.4

E10445-15

Primary Author: Sridhar Machani

Contributing Authors: Debapriya Datta, Gowri.G.R, Devanshi Mohan, Alankrita Prakash

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

5 Testing and Troubleshooting

6 Known Issues

Index

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Siebel User Management.

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 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*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

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

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

What's New in Oracle Identity Manager Connector for Siebel User Management?

This chapter provides an overview of the updates made to the software and documentation for the Siebel User Management connector in release 9.0.4.15.

Note: Release 9.0.4.15 of the connector comes after release 9.0.4.12. Release numbers from 9.0.4.13 and 9.0.4.14 have not been used.

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 9.0.4.1
- Software Updates in Release 9.0.4.1_6713023
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.6
- Software Updates in Release 9.0.4.7
- Software Updates in Release 9.0.4.8
- Software Updates in Release 9.0.4.9
- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.15

Software Updates in Release 9.0.4.1

The following is a software update in release 9.0.4.1:

- Changes in the Directory Structure of the Connector Files on the Installation Media

Changes in the Directory Structure of the Connector Files on the Installation Media

The xlSiebel.jar file has been split into two files, xlSiebel.jar and SiebelRecon.jar. Corresponding changes have been made in the following sections:

- Section 2.1.1, "Files and Directories on the Installation Media"
- Section 2.1.2, "Determining the Release Number of the Connector"
- Section 5.1, "Running Test Cases"

Software Updates in Release 9.0.4.1_6713023

The following are issues resolved in release 9.0.4.1_6713023:

Bug Number	Issue	Resolution
6713023	User reconciliation and provisioning did not work due to connection failure.	The issue has been resolved.

Software Updates in Release 9.0.4.2

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
7014401	Time zone values that you set during provisioning was not displayed on the target system.	This issue has been resolved. The time zone value is correctly stored during provisioning.

Software Updates in Release 9.0.4.3

The following are software updates implemented in release 9.0.4.3:

- Using the Connector Installer

Using the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See Section 2.2.1, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1" for details.

Software Updates in Release 9.0.4.4

The following are issues resolved in release 9.0.4.4:

Bug Number	Issue	Resolution
7308907	Incremental reconciliation failed if the target system database was set to any time zone other than GMT. For example, if the time zone of the target system database was set to GMT+08:00, then incremental reconciliation would fail.	This issue has been resolved. The SiebelDatabaseTimeZone attribute has been added to the Siebel Recon scheduled task. You can use this attribute to specify the time zone of the target system database. See Section 3.4.4, "User Reconciliation Scheduled Task" for more information about the SiebelDatabaseTimeZone attribute.

Software Updates in Release 9.0.4.5

The following are issues resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
7308907	The connector uses the time stamp stored in the TimeStamp IT resource parameter to identify target system records that must be reconciled. However, daylight savings time was not taken into account.	This issue has been resolved. The DayLightSaving attribute has been added to the SiebelRecon task. You use this attribute to specify the time (in minutes) that must be added to the time stamp. Sample value: `60` With this sample value, 60 minutes are added to the time stamp stored in the TimeStamp parameter, and the new time stamp is used to identify records that have been created or modified after the last reconciliation run. Default value: `0` **Note:** The SiebelDatabaseTimeZone attribute of the SiebelRecon scheduled task has been renamed to SiebelServerTimeZone.
7163582	The following issue was observed when the target system was Siebel 8.0: In a provisioning operation, if you tried to assign a responsibility to a user who had no responsibilities, then the connection exception was encountered.	This issue has been resolved. In a provisioning operation, you can now assign responsibilities to a user who does not have any responsibilities.
7561587	You could not set a primary responsibility to a user through a provisioning operation.	This issue has been resolved. You can now use the PrimaryResponsibility lookup field to set a primary responsibility during provisioning. **See Also:** Bug 7703095 in the "Known Issues" chapter for information about an issue related to this feature.
6847114	On the target system, if a position name was used across more than one division, then only one occurrence of the position name was reconciled into the Lookup.Siebel.Position lookup definition.	This issue has been resolved. Position names are reconciled according to their unique IDs on the target system. The following are sample entries from the Lookup.Siebel.Position lookup definition: Code Key1: `0-55RNY` Decode1: `Finance, General Manager` Code Key2: `0-57T1J` Decode2: `Sales, General Manager`

Bug Number	Issue	Resolution
7668306	If a responsibility name reconciled from the target system contained a special character, then that responsibility could not be assigned to a user through a provisioning operation.	This issue has been resolved. Responsibilities whose names contain special characters, except the single quotation mark character ('), can now be assigned to user through provisioning. **Note:** A responsibility whose name contains the single quotation mark (') character cannot be assigned to a user through provisioning. This is because the target system cannot search for a responsibility name if it contains a single quotation mark.
7667566	An exception was encountered if you deleted a user's position through a provisioning operation.	This issue has been resolved. You can delete a user's responsibility through provisioning.
7673332	A user's status was Inactive even when one or more responsibilities were assigned to the user through provisioning.	This issue has been resolved. If a user has no responsibilities assigned, then the status of the user is set to Inactive. If you assign responsibilities to the user through provisioning, then the status is changed to Active.

Software Updates in Release 9.0.4.6

The following are software updates implemented in release 9.0.4.6:

- Support for Siebel 8.1.1
- Resolved Issues in Release 9.0.4.6

Support for Siebel 8.1.1

From this release onward, the connector supports Siebel 8.1.1. This is mentioned in Section 1.1, "Certified Components."

Resolved Issues in Release 9.0.4.6

The following table describes issues resolved in release 9.0.4.6:

Bug Number	Issue	Resolution
8223113	When you assign a primary position to an employee through a provisioning operation on Oracle Identity Manager, the change is correctly reflected in the Administration – User module on the target system. However, in the Administration – Group module, the check box designating that the position is primary for that particular employee remains deselected.	This issue has been resolved. The relationship between an employee and a primary position is correctly shown in the Administration – Group module. The "Assigning a Position to Users" section has been removed from the connector guide.

Software Updates in Release 9.0.4.7

The following table describes issues resolved in release 9.0.4.7:

Bug Number	Issue	Resolution
7579522	When you assigned a primary position to an employee through a provisioning operation on Oracle Identity Manager, the employee became the primary user for the position. When you assigned the same primary position to another employee, this employee became the new primary user for the position. In this way, the primary user of the position kept changing with each assignment of the position.	This issue has been resolved. The first employee to whom the position is assigned remains the primary user of the position.

Software Updates in Release 9.0.4.8

The following table describes issues resolved in release 9.0.4.8:

Bug Number	Issue	Resolution
8362522	The connector did not work correctly if Oracle Identity Manager and Oracle Access Manager both used the same object manager (CommunicationsObjMgr_enu). The following error was encountered during password operations: `The password you have entered is not correct. Please enter your password again.(SBL-DAT-00569)`	This issue has been resolved. The connector functions as expected even if Oracle Identity Manager and Oracle Access Manager are using the same object manager. The SSO and Trusted Token parameters have been added in the IT resource definition.

Software Updates in Release 9.0.4.9

The following are software updates implemented in release 9.0.4.9:

- Support for Adding Single-Valued and Multivalued Attributes for Reconciliation and Provisioning
- Addition of the Configuration and Constants Lookup Definitions
- Support for Transformation of Data During Reconciliation
- Resolved Issues in Release 9.0.4.9

Support for Adding Single-Valued and Multivalued Attributes for Reconciliation and Provisioning

From this release onward, you can add single-valued and multivalued attributes for target resource reconciliation and provisioning. See Chapter 4, "Extending the Functionality of the Connector" for more information.

Addition of the Configuration and Constants Lookup Definitions

The following lookup definitions have been added in this release:

- Lookup.Configuration.Siebel

  This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.

- Lookup.Siebel.Constants

  This lookup definition stores values that are used internally by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector.

Support for Transformation of Data During Reconciliation

From this release onward, you can configure transformation of data during reconciliation.

See Section 1.4.6, "Support for Transformation of Data During Reconciliation" for more information.

Resolved Issues in Release 9.0.4.9

The following table describes issues resolved in release 9.0.4.9:

Bug Number	Issue	Resolution
8734174	The logging feature did not record some exceptions.	This issue has been resolved. All exceptions are now recorded by the logging feature.

Software Updates in Release 9.0.4.12

The following are software updates implemented in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning

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 Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 3.6.2, "Request-Based Provisioning" for more information.

Software Updates in Release 9.0.4.15

The following are software updates implemented in release 9.0.4.15:

- Support for Importing Request Dataset XML Files
- Resolved Issues in Release 9.0.4.15

Support for Importing Request Dataset XML Files

From this release onward, the connector provides support for importing a request dataset XML file into Oracle Identity Manager by using the Deployment Manager on Oracle Identity Manager 11*g* release 1 (11.1.1).

The installation media of this release includes a request dataset file, SiebelConnectorRequestDatasets.xml, which is available in the xml directory.

See Section 2.3.1.8.1, "Importing Request Datasets Using Deployment Manager" for more information.

Resolved Issues in Release 9.0.4.15

The following table describes issues resolved in release 9.0.4.15:

Bug Number	Issue	Resolution
11871430	When you provision a Siebel resource to a user having special characters, an error was encountered.	This issue has been resolved. Resources can be provisioned to users having special characters.
11665189	During a full reconciliation operation, if there was a special character in a user name, an error was encountered.	This issue has been resolved. Users having special characters in their user names are reconciled without any errors.
10373871	Reconciliation of a new Siebel user to Oracle Identity Manager failed if the user record did not exist in Oracle Identity Manager.	This issue has been resolved. New Siebel users can be reconciled to Oracle Identity Manager.
9432044	When adding a secondary responsibility to a user, an error was encountered.	This issue has been resolved. A secondary responsibility can be added to a user.
9358528	After upgrading Siebel connector from release 9.0.4.8, an error was encountered during provisioning.	This issue has been resolved. Upgrading the connector from release 9.0.4.12 to this release prevents the error caused during provisioning.
9238731	During a provisioning operation, using custom process forms failed because the form names were included in the software code.	This issue has been resolved. The names of the custom process forms use the Lookup.Siebel.Constants lookup definitions.
12403295	When a user of type User is provisioned with a value for work phone, the WorkPhone field was not updated.	This issue has been resolved. The WorkPhone field is updated when provisioning to users of type User.
12403335	When a user of type User is provisioned with a value for primary responsibility, the PrimaryResponsibility field was not updated.	This issue has been resolved. The PrimaryResponsibility field is updated when provisioning to users of type User.
12380304	During a full trusted source reconciliation operation, an error was encountered for users of type User if the TimeStamp IT resource parameter is empty.	This issue has been resolved. The full trusted source reconciliation operation for users of type User is successful.
12374876	During target resource reconciliation, the UserType and the SiebelServerTimeZone attribute values of a user were not reconciled.	This issue has been resolved. The the UserType and the SiebelServerTimeZone attribute values of a user are reconciled.
12369295	When a primary responsibility was added, the user status in the Siebel process form was not set to ACTIVE.	This issue has been resolved. The user status is set to ACTIVE after adding a primary responsibility.
12365104	When a trusted source reconciliation scheduled task was run, if the IsTrusted attribute was set to True, the task also triggered a target system reconciliation event.	This issue has been resolved. The trusted source reconciliation scheduled task does not trigger a target system reconciliation event.
12365135	During a provisioning operation, setting a value for the Position field was mandatory for users of type User.	This issue has been resolved. The users of type User can be provisioned without setting a value for the Position field.
12561788	After a provisioning operation, if the Siebel process form was customized and the Position field was made optional, the user was not found on the target system.	This issue has been resolved. A user can be provisioned with customized Siebel process form.

Bug Number	Issue	Resolution
12542513	For a user with primary and child responsibilities, if the child responsibilities were deleted, the user status was inactive.	This issue has been resolved. For a user with primary responsibility, if the child responsibilities are deleted, the user status is ACTIVE.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.6
- Documentation-Specific Updates in Release 9.0.4.7
- Documentation-Specific Updates in Release 9.0.4.8
- Documentation-Specific Updates in Release 9.0.4.9
- Documentation-Specific Updates in Release 9.0.4.12
- Documentation-Specific Updates in Release 9.0.4.15

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.6

The following documentation-specific updates have been made in the guide from release 9.0.4.1 through 9.0.4.6:

- The external code files for Siebel 7.6, 7.7, and 7.9 have been documented in the following sections:
  - Section 1.1, "Certified Components"
- In Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning," the following fields have been added:
  - Extension
  - HomePhone
  - WorkPhone
  - MPosition
  - Title

  The Phone and PersonalTitle fields have been removed from the list.
- In Section 3.4.2, "Limited Reconciliation":
  - All occurrences of `givenname` have been replaced with `First Name`.
  - All occurrences of `sn` have been replaced with `Last Name`.
- In the "Known Issues" chapter, limitations of the target system have been separated from the known issues of the connector.
- The "Creating the Target System User Account for Connector Operations" has been added.

Documentation-Specific Updates in Release 9.0.4.7

In the "Extending the Functionality of the Connector" chapter, the "Configuring the Connector for Multiple Installations of the Target System" section has been removed. This feature is not supported by default.

Documentation-Specific Updates in Release 9.0.4.8

The following documentation-specific updates have been made in the guide for release 9.0.4.8:

- The following sections have been added:
  - Adding the Dependent (LDAP Connector) Resource Object for Provisioning
  - Additional Configuration Steps and Guidelines for the Target System
- In Section 1.2, "Certified Languages,", Arabic has been added to the list of languages that the connector supports.
- In Section 1.1, "Certified Components," changes have been made in the "Target systems" row.

Documentation-Specific Updates in Release 9.0.4.9

Major changes have been made in the structure of the guide. The objective of these changes is to improve the usability of the guide.

Documentation-Specific Updates in Release 9.0.4.10

The following documentation-specific updates have been made for release 9.0.4.10:

- The following changes have been made in Chapter 1, "About the Connector":
  - Some of the sections have been rearranged.
  - Section 1.8, "Roadmap for Deploying and Using the Connector" has been added.

Documentation-Specific Updates in Release 9.0.4.12

The following documentation-specific updates have been made for release 9.0.4.12:

- Information about the Position and Responsibility resource object fields has been removed from Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning."
- The following sections have been added:
  - Section 1.6.2, "Position Attributes for Provisioning"
  - Section 1.6.3, "Responsibility Attributes for Provisioning"

Documentation-Specific Updates in Release 9.0.4.15

The following documentation-specific updates have been made for release 9.0.4.15:

- In Section 2.2.1.2, "Configuring the IT Resource," the descriptions of some parameters have been modified.
- In Section 2.3.1.7, "Configuring Trusted Source Reconciliation," the path to locate and import xml files have been updated.
- In Section 5.1, "Running Test Cases," the xlLogger.jar file has been removed from the list.
- Section 2.2.2, "Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.*x*" has been removed as this connector is no longer certified for Oracle Identity Manager release 9.0.1 through 9.0.3.*x*.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to use Siebel Enterprise Applications either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

> **Note:** At some places in this guide, Siebel Enterprise Applications has been referred to as the **target system.**

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

> **Note:** It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.

This chapter contains the following sections:

1.1 Certified Components

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

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: - Oracle Identity Manager release 9.1.0.2 or later **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 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) **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).
Target systems	Siebel 7.5 through Siebel CRM 8.1.1
External code	For Siebel 7.5 through 7.7: SiebelJI.jar, SiebelJI_Common.jar, and SiebelJI_enu.jar For Siebel 7.8 through 8.1.1: Siebel.jar and SiebelJI_enu.jar
JDK	The JDK version can be one of the following: - For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or later in the 1.5 series. - For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

1.2 Certified Languages

This release of the connector supports the following languages:

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

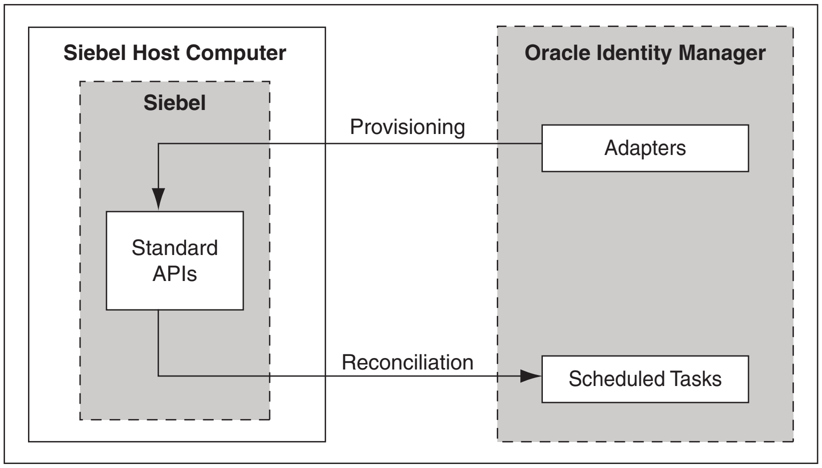
See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

1.3 Connector Architecture

Figure 1–1 shows the architecture of the connector.

> **Note:** In Oracle Identity Manager release 11.1.1, 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.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

Figure 1–1 Connector Architecture



The connector can be configured to run in one of the following modes:

- Identity reconciliation

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this form of reconciliation, OIM Users are created or updated corresponding to the creation of and updates to users on the target system.

- Account Management

  Account management is also known as target resource management. This mode of the connector enables the following operations:

  – Provisioning

    Provisioning involves creating or updating users on the target system through Oracle Identity Manager. When you allocate (or provision) a Siebel resource to an OIM User, the operation results in the creation of an account on Siebel for that user. In the Oracle Identity Manager context, the term **provisioning** is also used to mean updates made to the target system account through Oracle Identity Manager.

    During provisioning, adapters carry provisioning data submitted through the process form to the target system. Siebel APIs accept provisioning data from the adapters, carry out the required operation on Siebel, and return the response from Siebel to the adapters. The adapters return the response to Oracle Identity Manager.

  – Target resource reconciliation

In target resource reconciliation, data related to newly created and modified target system accounts can be reconciled (using scheduled tasks) and linked with existing OIM Users and provisioned resources.

1.4 Features of the Connector

The following are features of the connector:

- Section 1.4.1, "Target Resource and Trusted Source Reconciliation"
- Section 1.4.2, "Limited Reconciliation"
- Section 1.4.3, "Reconciliation Based on User Type"
- Section 1.4.4, "Reconciliation of Deleted User Records"
- Section 1.4.5, "Full and Incremental Reconciliation"
- Section 1.4.6, "Support for Transformation of Data During Reconciliation"

1.4.1 Target Resource and Trusted Source Reconciliation

You can use the connector to configure Siebel as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.4, "Configuring Reconciliation" for more information.

1.4.2 Limited Reconciliation

You can set a reconciliation filter as the value of the CustomizedReconQuery IT resource parameter while configuring the IT resource. This filter specifies the subset of added and modified target system records that must be reconciled.

See Section 3.4.2, "Limited Reconciliation" for more information.

1.4.3 Reconciliation Based on User Type

You can specify the Siebel user type (Employee, Partner User, or Customer) for which you want to reconcile records from the target system.

See Section 3.4.3, "Reconciliation Based on User Type" for more information.

1.4.4 Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records. In target resource mode, if a record is deleted on the target system, then the corresponding Siebel resource is revoked from the OIM User. In trusted source mode, if a record is deleted on the target system, then the corresponding OIM User is deleted.

See the description of the isDeleteRecon attribute in Section 3.4.4, "User Reconciliation Scheduled Task."

1.4.5 Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, change-based or incremental reconciliation is automatically enabled from the next run of the user reconciliation onward.

You can perform a full reconciliation run at any time.

See Section 3.4.1, "Performing Full Reconciliation" for more information.

1.4.6 Support for Transformation of Data During Reconciliation

You can configure transformation of data during reconciliation. For example, you can automate the look up of the field name from an external system and set the value based on the field name.

See Section 4.5, "Configuring Transformation of Data During Reconciliation" for more information.

1.5 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during reconciliation and provisioning can be divided into the following categories:

- Section 1.5.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.5.2, "Other Lookup Definitions"

1.5.1 Lookup Definitions Synchronized with the Target System

The following lookup definitions are populated with values fetched from the target system when you run the Siebel Lookup Recon scheduled task. Section 3.2, "Scheduled Task for Lookup Field Synchronization" provides information about this scheduled task.

- Lookup.Siebel.TimeZone
- Lookup.Siebel.PreferredCommunications
- Lookup.Siebel.Position
- Lookup.Siebel.EmployeeTypeCode
- Lookup.Siebel.Responsibility
- Lookup.Siebel.PersonalTitle
- Lookup.Siebel.UserType

1.5.2 Other Lookup Definitions

Table 1–2 describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–2 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.Configuration.Siebel	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.	Some of the entries in this lookup definition are preconfigured. See Section 2.3.1.6, "Setting Up the Lookup.Configuration.Siebel Lookup Definition" for information about the entries for which you can set values.
Lookup.Siebel.Constants	This lookup definition stores values that are used internally by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector.	You must not modify the entries in this lookup definition.
Lookup.Transform.Siebel	This lookup definition is used to configure transformation of attribute values fetched from the target system during reconciliation.	It is optional to enter values in this lookup definition. Section 4.5, "Configuring Transformation of Data During Reconciliation" provides information about this lookup definition.
AttrName.Map.Recon.Siebel	This lookup definition holds mappings between resource object fields and target system attributes.	This lookup definition is preconfigured. Table 1–3 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for reconciliation. Chapter 4, "Extending the Functionality of the Connector" provides more information.
AttrName.Map.Prov.Siebel	This lookup definition holds mappings between process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–3 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for provisioning. Chapter 4, "Extending the Functionality of the Connector" provides more information.

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

The following sections provide information about connector objects used during target resource reconciliation and provisioning:

> **See Also:** The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about reconciliation

- Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Position Attributes for Provisioning"
- Section 1.6.3, "Responsibility Attributes for Provisioning"
- Section 1.6.4, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.5, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.6, "Provisioning Functions"

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 provides information about user attribute mappings for target resource reconciliation and provisioning.

Table 1–3 User Attributes for Target Resource Reconciliation and Provisioning

Resource Object Field (Code Key for AttrName.Map.Recon.Siebel)	Process Form Field (Code Key for AttrName.Map.Prov.Siebel)	Siebel Enterprise Applications Attribute (Decode)	Description
UserID	UD_SIEBEL_USERID	Login Name	Login ID
LastName	UD_SIEBEL_LASTNAME	Last Name	Last name
FirstName	UD_SIEBEL_FIRSTNAME	First Name	First name
WorkPhone	UD_SIEBEL_WORKPHONE	Phone #	Phone number
Extension	UD_SIEBEL_EXTENSION	Work Phone Extension	Extension for the phone number
Fax	UD_SIEBEL_FAX	Fax #	Fax number
Email	UD_SIEBEL_EMAIL	EMail Addr	E-mail address
Alias	UD_SIEBEL_ALIAS	Alias	User alias
MiddleName	UD_SIEBEL_MIDDLENAME	Middle Name	Middle name
TimeZone	UD_SIEBEL_TIMEZONE	Time Zone Name - Translation	Time zone
EmployeeType	UD_SIEBEL_EMPLOYEETYPE	Employee Type Code	Type of employee
Title	UD_SIEBEL_TITLE	Personal Title	Title of the user
JobTitle	UD_SIEBEL_JOBTITLE	Job Title	Job title
PreferredCommunications	UD_SIEBEL_PREFERREDCOMM	Preferred Communications	Mode of communication
MPosition	UD_SIEBEL_POSITION	Position	Primary position
HomePhone	UD_SIEBEL_HOMEPHONE	Home Phone #	Home telephone number
Primary Responsibility	UD_SIEBEL_RESPONSIBILITY	Responsibility	Primary responsibility

1.6.2 Position Attributes for Provisioning

Table 1–4 provides information about position attribute mappings for provisioning.

Table 1–4 Position Attributes for Provisioning

Resource Object Field (Code Key for AttrName.Map.Recon.Siebel)	Process Form Field (Code Key for AttrName.Map.Prov.Siebel)	Siebel Enterprise Applications Attribute (Decode)	Description
Position Id	UD_SIEBEL_POSITION	Position	Position ID

1.6.3 Responsibility Attributes for Provisioning

Table 1–5 provides information about responsibility attribute mappings for provisioning.

Table 1–5 Responsibility Attributes for Provisioning

Resource Object Field (Code Key for AttrName.Map.Recon .Siebel)	Process Form Field (Code Key for AttrName.Map.Prov.Siebel)	Siebel Enterprise Applications Attribute (Decode)	Description
Responsibility	UD_SIEBEL_RESPONSIBILITY	Responsibility	Responsibility name

1.6.4 Reconciliation Rule for Target Resource Reconciliation

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

The following is the process matching rule:

Rule name: Siebel Recon Rule

Rule element: User Login Equals User ID

In this rule element:

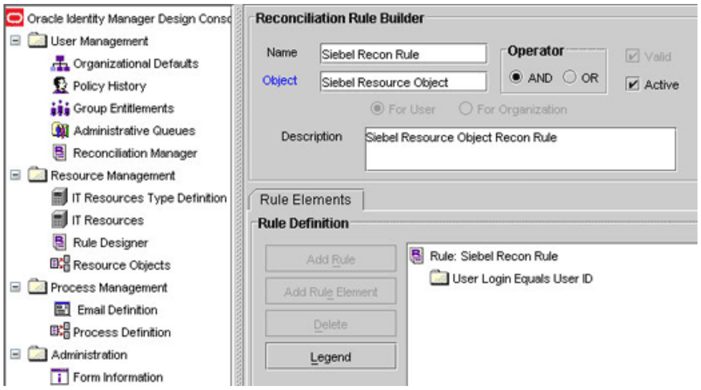
- User Login is the User ID field on the OIM User form.
- User ID is the User ID field of Siebel.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Siebel Recon Rule**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



Name: Siebel Recon Rule

Object: Siebel Resource Object

Operator: ● AND ○ OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: Siebel Resource Object Recon Rule

Rule: Siebel Recon Rule
- User Login Equals User ID

1.6.5 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–6 lists the action rules for target resource reconciliation.

Table 1–6 Action Rules for Target Resource Reconciliation

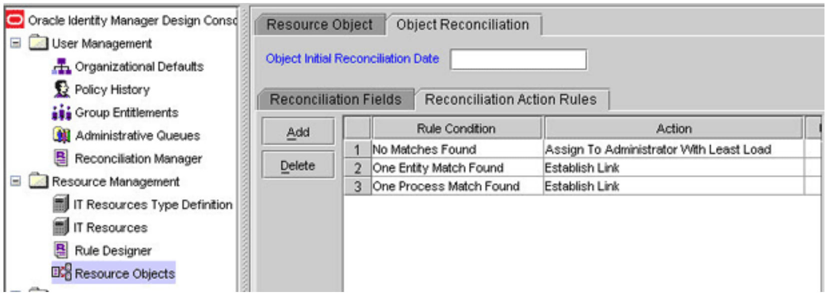
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

> **Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Siebel** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rules for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation



Object Initial Reconciliation Date

	Rule Condition	Action
1	No Matches Found	Assign To Administrator With Least Load
2	One Entity Match Found	Establish Link
3	One Process Match Found	Establish Link

1.6.6 Provisioning Functions

Table 1–7 lists the provisioning functions supported by the connector.

Table 1–7 Provisioning Functions

Function	Adapter
Create User	Siebel Create User
Delete User	Siebel Delete User
Add Position to User	Siebel Add Position

Table 1–7 (Cont.) Provisioning Functions

Function	Adapter
Add User Responsibility	Siebel Add Responsibility
Delete User Position	Siebel Remove Position
Delete User Responsibility	Siebel Remove Responsibility
Primary Position Updated	Siebel Add Primary Position
Primary Responsibility Updated	Siebel Add Primary Responsibility
Time Zone Updated	Siebel Modify User
Email Updated	Siebel Modify User
Alias Updated	Siebel Modify User
MI Updated	Siebel Modify User
Work Phone Updated	Siebel Modify User
First Name Updated	Siebel Modify User
Last Name Updated	Siebel Modify User
Title Updated	Siebel Modify User
Home Phone Updated	Siebel Modify User
Fax Updated	Siebel Modify User
Preferred Communications Updated	Siebel Modify User
Extension Updated	Siebel Modify User
Employee Type Updated	Siebel Modify User
Job Title Updated	Siebel Modify User
Add Multivalued attribute	AddMultiValueAttribute To Siebel User
Remove Multivalued attribute	RemoveMultiValueAttribute To Siebel User
Update Multivalued attribute	Siebel Update Multivalue attribute

1.7 Connector Objects Used During Trusted Source Reconciliation

The following sections provide information about connector objects used during trusted source reconciliation:

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–8 lists user attributes for trusted source reconciliation.

Table 1–8 User Attributes for Trusted Source Reconciliation

OIM User Form Field	Siebel Attribute	Description
User ID	Login Name	Login ID
First Name	First Name	First Name
Last Name	Last Name	Last name
Employee Type	NA	The default value is `Employee`.
User Type	NA	The default value is `End-User Administrator`.
Organization	NA	The default value is `Xellerate Users`.
Email	EMail Addr	The e-mail address of the employee.

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

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

The following is the process matching rule:

Rule name: Trusted Source recon Rule

Rule element: User Login Equals User ID

In this rule element:

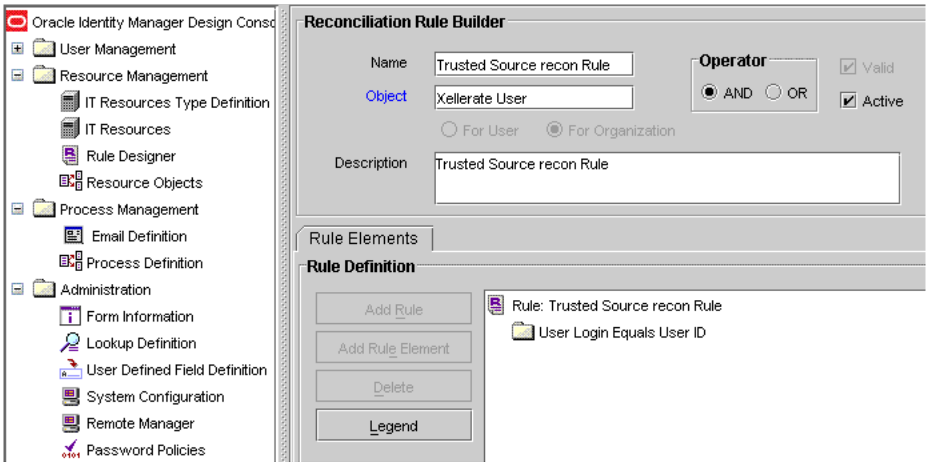
- User Login is the User ID field on the OIM User form.
- User ID is the User ID field of Siebel.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Trusted Source recon Rule**. Figure 1–4 shows the reconciliation rule for target resource reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



Name: Trusted Source recon Rule

Object: Xellerate User

Operator: ● AND ○ OR

☑ Valid

☑ Active

○ For User ● For Organization

Description: Trusted Source recon Rule

Rule: Trusted Source recon Rule

User Login Equals User ID

1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–9 lists the action rules for trusted source reconciliation.

Table 1–9 Action Rules for Trusted Source Reconciliation

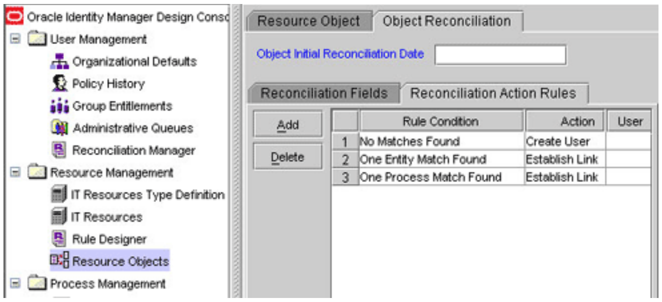
Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

> **Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view action rules by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Xellerate User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rule for target resource reconciliation.

Figure 1–5 Reconciliation Action Rules for Target Resource Reconciliation



Object Initial Reconciliation Date

	Rule Condition	Action	User
1	No Matches Found	Create User	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.8 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.
- Chapter 5, "Testing and Troubleshooting" describes the procedure to use the connector testing utility for testing the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2 Deploying the Connector

Deploying the connector involves the following steps:

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"

2.1 Preinstallation

This section is divided into the following topics:

- Section 2.1.1, "Files and Directories on the Installation Media"
- Section 2.1.2, "Determining the Release Number of the Connector"
- Section 2.1.3, "Using External Code Files"

2.1.1 Files and Directories on the Installation Media

Table 2–1 describes the files and directories on the installation media.

Table 2–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
configuration/SeibelConnector-CI.xml	This XML file contains configuration information that is used during connector installation.
lib/xlSiebel.jar	This JAR file contains the class files required for provisioning. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
lib/SiebelRecon.jar	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database

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

File in the Installation Media Directory	Description
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
Troubleshoot/TroubleShootingUtility.class	This is the testing utility.
Troubleshoot/global.properties	This file contains the connection details that are required to connect to the target system. It also contains details about the commands to be run.
Troubleshoot/log.properties	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
xml/SiebelEmpResourceObject.xml	This XML file contains definitions for the following connector components: ■ IT resource type ■ Process form ■ Process task and rule-generator adapters (along with their mappings) ■ Resource object ■ Pre-populate rules
xml/SiebelEmpXLResourceObject.xml	This file contains the configuration for the Xellerate User (OIM User). You import this file only if you plan to use the connector in trusted source reconciliation mode.
xml/SiebelConnectorRequestDatasets.xml	This file contains the request dataset for the connector. You import this file by using the Deployment Manager.

Note: The files in the Troubleshoot directory are used only to run tests on the connector.

2.1.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager release 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.1, then skip this section.

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME/xellerate/JavaTasks/xlSiebel.jar

2. Open the manifest.mf file in a text editor. The manifest.mf file is one of the files bundled inside the xlSiebel.jar file.

   In the manifest.mf file, the release number of the connector is displayed as the value of the Version property.

2.1.3 Using External Code Files

> **Note:** While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the contents of the ThirdParty directory to the corresponding directory on each node of the cluster.

If you are using Siebel 7.5, 7.6, or 7.7, then perform one of the following steps:

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

  Copy the following files from the *SIEBEL_INSTALLATION_DIRECTORY*/siebsrvr/CLASSES directory into the *OIM_HOME*/xellerate/ThirdParty directory:

  - SiebelJI.jar
  - SiebelJI_Common.jar
  - SiebelJI_enu.jar

- For Oracle Identity Manager release 11.1.1:

  Copy the following files from the *SIEBEL_INSTALLATION_DIRECTORY*/siebsrvr/CLASSES directory into the *OIM_HOME*/server/ThirdParty directory:

  - SiebelJI.jar
  - SiebelJI_Common.jar
  - SiebelJI_enu.jar

If you are using Siebel 7.8, 7.9, or 8.0, the perform one of the following steps:

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

  Copy the following files from the *SIEBEL_INSTALLATION_DIRECTORY*/siebsrvr/CLASSES directory into the *OIM_HOME*/xellerate/ThirdParty directory:

  - Siebel.jar
  - SiebelJI_enu.jar

- For Oracle Identity Manager release 11.1.1:

  Copy the following files from the *SIEBEL_INSTALLATION_DIRECTORY*/siebsrvr/CLASSES directory into the *OIM_HOME*/server/ThirdParty directory:

  - Siebel.jar

- SiebelJI_enu.jar

2.2 Installation

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in one of the following sections:

- Section 2.2.1, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"

2.2.1 Installing the Connector on Oracle Identity Manager Release 9.1.0.*x* or Release 11.1.1

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

Installing the connector on Oracle Identity Manager release 9.1.0.*x* or release 11.1.1 involves the following procedures:

- Section 2.2.1.1, "Running the Connector Installer"
- Section 2.2.1.2, "Configuring the IT Resource"

2.2.1.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

   > **Note:** In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

   - For Oracle Identity Manager release 9.1.0.*x*:
     OIM_HOME/xellerate/ConnectorDefaultDirectory
   - For Oracle Identity Manager release 11.1.1:
     OIM_HOME/server/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:

   - 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:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

3. 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*:

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

- For Oracle Identity Manager release 11.1.1:

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

4. From the Connector List list, select **Siebel Connector** ***RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

   If you have copied the installation files into a different directory, then:

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

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

   c. From the Connector List list, select **Seibel Connector** ***RELEASE_NUMBER*.**

5. Click **Load**.

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

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

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

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

   > **Note:** At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.
   >
   > There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector

> **Note:** In Oracle Identity Manager release 11.1.1, 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.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Table 2–1 for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

2.2.1.2 Configuring the IT Resource

You must specify values for the parameters of the SIEBEL IT Resource IT resource as follows:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `SIEBEL IT Resource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–2 describes the parameters that are used to generate a Siebel Internet Session Network API (SISNAPI) connection.

> **Note:** See *Siebel Object Interfaces Reference Guide* for more information about the Siebel object interface and extension events.

Table 2–2 IT Resource Parameters and Values

Parameter	Description	Sample/Default Value
EnterpriseServer	Name of the Siebel Enterprise server.	`siebel`
GatewayServer	■ For Siebel 7.5.3: Name of the computer on which the gateway server is installed. ■ For Siebel 7.7 and above: The IP address or the hostname of the Siebel server. The virtual IP address, in the case of a load-balanced server.	`STS_TESTING`

GatewayServerPort	■ For Siebel 7.5.3:
	Port number of the gateway server.
	■ For Siebel 7.7 and above:
	Port number of the computer on which the Siebel Connection Broker component (SCBroker) runs.
	Virtual port number, in the case of a load-balanced server.
		■ For Siebel 7.5.3:
		`2320`
		■ For Siebel 7.7 and above:
		`2321`

Language	Language.	You can specify any one of the following: For English: `ENU` For Brazilian Portuguese: `PTB` For French: `FRA` For German: `DEU` For Italian: `ITA` For Japanese: `JPN` For Korean: `KOR` For Simplified Chinese: `CHS` For Spanish: `ESP` For Traditional Chinese: `CHT`

Table 2–2 (Cont.) IT Resource Parameters and Values

Parameter	Description	Sample/Default Value
ObjectManager	Name of the Siebel application object manager.	The following names are examples for the Siebel Call Center application: For English: `SCCObjMgr_enu` For Brazilian Portuguese: `SCCObjMgr_ptb` For French: `SCCObjMgr_fra` For German: `SCCObjMgr_deu` For Italian: `SCCObjMgr_ita` For Japanese: `SCCObjMgr_jpn` For Korean: `SCCObjMgr_kor` For Simplified Chinese: `SCCObjMgr_chs` For Spanish: `SCCObjMgr_esp` For Traditional Chinese: `SCCObjMgr_cht`
Password	Password of the target system user account that you want to use for connector operations. See Section 2.3.2, "Creating the Target System User Account for Connector Operations" for more information.	`sadmin`
SiebelServer	Name of the target Siebel server.	`STS_TESTING`
UserName	User ID of the target system user account that you want to use for connector operations. See Section 2.3.2, "Creating the Target System User Account for Connector Operations" for more information.	`sadmin`
Encryption	Type of encryption for secure communication. **Note:** The value of this parameter is case-sensitive.	If encryption is required, then specify `RSA`. Otherwise, specify `None`.
Version	Version of the target system supported by this connector.	`7.5` or `7.8`

Table 2–2 (Cont.) IT Resource Parameters and Values

Parameter	Description	Sample/Default Value
TimeStamp	For the first reconciliation run, the time-stamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of reconciliation was completed is stored in this parameter.	The following are sample time-stamp values: For English: `Jun 01, 2006 at 10:00:00 GMT+05:30` For French: `juil. 01, 2006 at 10:00:00 GMT+05:30` For Japanese: `6 01, 2006 at 10:00:00 GMT+05:30`
CustomizedReconQuery	Query condition on which reconciliation must be based. If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can include the AND (&) and OR (|) logical operators. For more information about this parameter, see Section 3.4.2, "Limited Reconciliation."	`First Name=John&Last Name=Doe`
SSO	Enter `yes` to specify that the target system is configured to use a SSO solution for authentication. Otherwise, enter `no`.	`no`
Trusted Token	Enter the trusted token value that you specify while configuring the target system to communicate with the SSO system. If you have not configured SSO authentication, then enter `no`.	`no`
Configuration Lookup	Name of the lookup definition that holds connector configuration entries used during reconciliation and provisioning.	`Lookup.Configuration.Siebel`

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

2.3 Postinstallation

The following sections discuss postinstallation procedures:

- Section 2.3.1, "Configuring Oracle Identity Manager"
- Section 2.3.2, "Creating the Target System User Account for Connector Operations"
- Section 2.3.3, "Configuring the Target System"

2.3.1 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves performing the following procedures:

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

- Section 2.3.1.1, "Changing to the Required Input Locale"
- Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.1.3, "Enabling Logging"
- Section 2.3.1.4, "Setting Up Lookup Definitions in Oracle Identity Manager"
- Section 2.3.1.5, "Adding the Dependent (LDAP Connector) Resource Object for Provisioning"
- Section 2.3.1.6, "Setting Up the Lookup.Configuration.Siebel Lookup Definition"
- Section 2.3.1.7, "Configuring Trusted Source Reconciliation"
- Section 2.3.1.8, "Configuring Oracle Identity Manager for Request-Based Provisioning"

2.3.1.1 Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

You may require the assistance of the system administrator to change to the required input locale.

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

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/bin directory.

Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

For Oracle Identity Manager release 9.1.0.*x*:

```
OIM_HOME/xellerate/bin/SCRIPT_FILE_NAME
```

For Oracle Identity Manager release 11.1.1:

```
OIM_HOME/server/bin/SCRIPT_FILE_NAME
```

2. Enter one of the following commands:

Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *`CATEGORY_NAME`* on Microsoft Windows or `PurgeCache.sh` *`CATEGORY_NAME`* on UNIX. The *`CATEGORY_NAME`* argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

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

  On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`

  On UNIX: `PurgeCache.sh ConnectorResourceBundle`

  Note: You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

  In this command, `ConnectorResourceBundle` is one of the content categories that you can delete from the server cache. See the following file for information about the other content categories:

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

  When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

  ```
  t3://OIM_HOST_NAME:OIM_PORT_NUMBER
  ```

  In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.3.1.3 Enabling Logging

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

- Section 2.3.1.3.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"
- Section 2.3.1.3.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.3.1.3.1 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:

- **IBM WebSphere Application Server**

To enable logging:

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

   ```
   log4j.logger.XELLERATE=log_level
   log4j.logger.XL_INTG.SIEBEL=log_level
   ```

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

   For example:

   ```
   log4j.logger.XELLERATE=INFO
   log4j.logger.XL_INTG.SIEBEL=INFO
   ```

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

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

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

     ```
     <category name="XELLERATE">
        <priority value="log_level"/>
     </category>

     <category name="XL_INTG.SIEBEL">
        <priority value="log_level"/>
     </category>
     ```

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

     ```
     <category name="XELLERATE">
        <priority value="INFO"/>
     </category>

     <category name="XL_INTG.SIEBEL">
        <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 lines in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SIEBEL=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.SIEBEL=INFO
     ```

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

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

- **Oracle WebLogic Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SIEBEL=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.SIEBEL=INFO
     ```

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

2.3.1.3.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

Oracle Identity Manager release 11.1.1 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 2–3.

Table 2–3 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1

Table 2–3 (Cont.) Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
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='siebel' 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="XL_INTG.SIEBEL" level="[LOG_LEVEL]"
   useParentHandlers="false">
        <handler name="siebel"/>
        <handler name="console-handler"/>
     </logger>
   ```

   b. Replace both occurrences of **`[LOG_LEVEL]`** with the ODL message type and level combination that you require. Table 2–3 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='siebel' 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="XL_INTG.SIEBEL" level="NOTIFICATION:1"
 useParentHandlers="false">
      <handler name="siebel"/>
      <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.

2.3.1.4 Setting Up Lookup Definitions in Oracle Identity Manager

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

- Lookup.Siebel.EmployeeTypeCode

  During a provisioning operation, you use this lookup definition to set one of the following employee types for the user:

  - Contractor
  - Employee
  - Intern
- Lookup.Siebel.PreferredCommunications

  During a provisioning operation, you use this lookup definition to set one of the following communication modes for the user:

  - Email
  - Fax
  - Pager
  - Phone
  - Wireless Message
- Lookup.Siebel.UserType

  During a provisioning operation, you use this lookup definition to set one of the following user types for the user:

- Employee
- User

You must enter values in this lookup definition before you can use it during provisioning operations. To enter values in a lookup definition:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the lookup definition.
4. Enter Code Key and Decode values for each of entry.

   For each lookup definition, the Code Key and Decode values must be items from the lists given earlier in this section. The target system supports only these values.
5. Click **Save**.

2.3.1.5 Adding the Dependent (LDAP Connector) Resource Object for Provisioning

> **Note:** The connector for the LDAP solution must be installed before you can perform this procedure.

Add the dependent (LDAP connector) resource object for provisioning as follows:

1. Log in to the Design Console.
2. Expand the **Resource Management** folder, and double-click **Resource Objects**.
3. Search for and open the **Siebel** resource object.
4. On the Depends On tab, click **Assign**.
5. In the dialog box that is displayed, select the resource object for the LDAP connector and use the right arrow icon to move it from the Unassigned Objects list to the list on the right. Then, click OK.
6. Click the Save icon, and then close the dialog box.
7. Click the Save icon on the Siebel resource object.

2.3.1.6 Setting Up the Lookup.Configuration.Siebel Lookup Definition

The Lookup.Configuration.Siebel lookup definition is created when you deploy the connector. You must set values for some of the entries in this lookup definition. To set values for these entries:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.Configuration.Siebel** lookup definition.
3. Set values for the entries specified in Table 2–4.

> **Note:** You must not change any of the Code Key values of this lookup definition.

Table 2–4 Entries in the Lookup.Configuration.Siebel Lookup Definition

Code Key	Decode Description
BusinessCompOfMultiValueGroups	This entry holds the names of business components of multivalued group attributes. If you add a multivalued group attribute by performing the procedure described in Chapter 4, "Extending the Functionality of the Connector", then you must append the name of the business component to the default value of the BusinessCompOfMultiValueGroups entry. Use the comma (,) as the delimiter when you append a value. Default value: `Position,Responsibility`
Constants Lookup	This entry holds the name of the constants lookup definition. Default value: `Lookup.Siebel.Constants`
MultiValueAttributesDelimiter	This entry holds the name of the delimiter that you want to use to separate values in the BusinessCompOfMultiValueGroups, MultiValueAttributesFields, and MultiValueAttrsOnProcessForm entries. Default value: , (the comma character)
MultiValueAttributesFields	This entry holds the names of multivalued attributes that are reconciled and provisioned. If you add a multivalued attribute by performing the procedure described in Chapter 4, "Extending the Functionality of the Connector", then you must append the name of the attribute to the default value of the MultiValueAttributesFields entry. Use the comma (,) as the delimiter when you append a value. Default value: `Position Id,Name`
MultiValueAttrsOnProcessForm	This entry holds the list of multivalued attributes on the process form. Default value: `Position,Responsibility`
Provisioning Attribute Map	This entry holds the name of the lookup definition that stores attribute mappings for provisioning. Default value: `AttrName.Map.Prov.Siebel`
Reconciliation Attribute Map	This entry holds the name of the lookup definition that stores attribute mappings for reconciliation. Default value: `AttrName.Map.Recon.Siebel`
TargetDateFormat	Enter the date format supported by the target system. This date format is used by the connector during reconciliation to parse date values fetched from the target system. Default value: `MM/dd/yyyy HH:mm:ss`

2.3.1.7 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a 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.

If you designate the target system as a **target resource**, then during a 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.

> **Note:** Skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, SiebelEmpXLResourceObject.xml, by using the Deployment Manager. This section describes the procedure to import the XML file.
2. Set the IsTrusted scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation pane.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
4. Locate and open the SiebelEmpXLResourceObject.xml file, which is located in the directory.
   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel_9.0.4.15.0/xml
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory/Siebel_9.0.4.15.0/xml

   Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

After you import the XML file for trusted source reconciliation, you must set the value of the IsTrusted reconciliation scheduled task attribute to `True`. This procedure is described in Section 3.4.4, "User Reconciliation Scheduled Task."

2.3.1.8 Configuring Oracle Identity Manager for Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

> **Note:** Direct provisioning allows the provisioning of multiple target system accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Section 2.3.1.8.1, "Importing Request Datasets Using Deployment Manager"
- Section 2.3.1.8.2, "Copying Predefined Request Datasets"
- Section 2.3.1.8.3, "Importing Request Datasets into MDS"
- Section 2.3.1.8.4, "Enabling the Auto Save Form Feature"
- Section 2.3.1.8.5, "Running the PurgeCache Utility"

2.3.1.8.1 Importing Request Datasets Using Deployment Manager

> **Note:**
>
> - You can perform this procedure instead of the procedures described in Section 2.3.1.8.2, "Copying Predefined Request Datasets" and Section 2.3.1.8.3, "Importing Request Datasets into MDS".
> - See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about importing objects from an XML file using the Deployment Manager.

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

To import a request dataset XML file by using the Deployment Manager:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management.

   A dialog box for opening files is displayed.
4. Locate and open the request dataset XML file, SiebelConnectorRequestDatasets.xml, which is in the xml directory of the installation media.

   Details of this XML file are shown on the **File Preview** page.
5. Click **Add File**.

The Substitutions page is displayed.

6. Click **Next**.

   The Confirmation page is displayed.

7. Click **Import**.

8. Close the Deployment Manager dialog box.

   The request dataset is imported into Oracle Identity Manager.

2.3.1.8.2 Copying Predefined Request Datasets

Predefined request datasets are shipped with this connector. The following are the predefined request dataset available in the DataSets directory on the installation media:

- ProvisionResourceSiebel Resource Object.xml
- ModifyResourceSiebel Resource Object.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\SiebelStd

> **Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide* for Oracle Identity Manager for information on modifying request datasets.

2.3.1.8.3 Importing Request Datasets into MDS

You can configure request-based provisioning by importing the request datasets into into the metadata store (MDS) by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

> **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.3.1.8.2, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\SiebelStd directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

2. In a command window, change to the *OIM_HOME*\server\bin directory.
3. Run one of the following commands:
   - On Microsoft Windows

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX

     ```
     weblogicImportMetadata.sh
     ```

4. When prompted, enter the following values:
   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

     Enter the password used to log in to the WebLogic server.

   - `Please enter your server URL [t3://localhost:7001]`

     Enter the URL of the application server in the following format:

     `t3://`*`HOST_NAME_IP_ADDRESS`*`:`*`PORT`*

     In this format, replace:

     – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

     – *PORT* with the port on which Oracle Identity Manager is listening.

   The request dataset is imported into MDS.

2.3.1.8.4 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **Siebel Process** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.3.1.8.5 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

2.3.2 Creating the Target System User Account for Connector Operations

Oracle Identity Manager uses a target system user account to provision to and reconcile data from the target system. To create this target system user account with the permissions required for performing connector operations:

> **Note:** The target system user account that you create for connector operations must also be created in the LDAP repository. As a security precaution, you must ensure that this account does not have access to areas protected by Oracle Access Manager.

1. Create the user account on Siebel as follows:

   a. Log in to Siebel.

   b. Click the Site Map icon.

   c. Click **Administration – User**.

   d. Click **Employees**.

   e. Click **New**.

   f. Enter the following details for the account that you are creating:

      – Last Name

      – First Name

      – Job Title

      – User ID

      – Responsibility: Select **Siebel Administrator**.

      – Position: Select **Siebel Administrator**.

      – Organization: Select **Default Organization**.

      – Employee Type

2. Create the user account on the Siebel database as follows:

   a. Open the Siebel home directory.

   b. Open the dbsrvr directory.

   c. Open one of the following directories:

      For IBM DB2 UDB: DB2

      For Microsoft SQL Server: MSSQL

      For Oracle Database: Oracle

   d. Open one of the following files in a text editor:

      For IBM DB2 UDB: grantusrdb2.sql

      For Microsoft SQL Server: addusrmsql.sql

For Oracle Database: grantusroracle.sql

e. In the file that you open:

Specify the user ID of the user that you create in Step 1.

Set a password for the user.

Provide other required details.

f. Run the script.

Additional Configuration Steps and Guidelines for the Target System

Siebel can be configured to use either a database or an LDAP repository to store user information. If an LDAP repository is used, then you must ensure that the following prerequisites are addressed:

- If Microsoft Active Directory is used as the LDAP repository, then use the ADSI Security Adapter. Ensure that the Propagate Change attribute of the ADSI Security Adapter is set to False on Siebel.
- If any other LDAP repository is used, then use the LDAP Security Adapter.

> **Note:** Only LDAP solutions for which there are predefined Oracle Identity Manager connectors are supported.

- Users must first be created in the LDAP repository and then created on the target system. This also means that users created through provisioning operations performed on Oracle Identity Manager must first be created in the LDAP repository and then created on the target system.
- Ensure that the credential attribute is correctly set for users created in the LDAP repository. For example, on Microsoft Active Directory the credential attribute is the Office attribute. The format for Office attribute values is as follows:

```
username=USER_ID_OF_SIEBEL_ACCOUNT password=PASSWORD_OF_SIEBEL_ACCOUNT
```

  The following is a sample value:

```
username=jdoe password=Ke42r0s
```

2.3.3 Configuring the Target System

> **Note:** Perform this procedure only if you want to use RSA encryption on the target system.

You can configure encryption to secure communication between the target system server and Oracle Identity Manager. This section discusses the following topics related to configuring encryption:

- Section 2.3.3.1, "Enabling RSA Encryption on Siebel"
- Section 2.3.3.2, "Configuring the Siebel Web Server Extension for RSA Encryption"
- Section 2.3.3.3, "Enabling RSA Encryption for the Siebel Call Center Application"
- Section 2.3.3.4, "Starting the Siebel Software Configuration Wizard"

2.3.3.1 Enabling RSA Encryption on Siebel

This section describes how to configure the target system to use RSA encryption for Siebel Internet Session API (SISNAPI) communication between the target system server and Oracle Identity Manager.

To enable RSA encryption on Siebel:

1. Start the Siebel Software Configuration Wizard.

   This wizard is started automatically when you install the target system. If required, you can start it manually by following instructions given in Section 2.3.3.4, "Starting the Siebel Software Configuration Wizard."

2. On the Encryption Type page of the wizard, select the **RSA** option to specify that you want to use the RSA Security Systems 128-bit strong encryption feature for the target system components.

3. Review the settings, and exit the wizard.

4. Restart the server.

2.3.3.2 Configuring the Siebel Web Server Extension for RSA Encryption

After you configure the target system for RSA encryption, perform the same procedure to configure the Siebel Web Server Extension for RSA encryption.

2.3.3.3 Enabling RSA Encryption for the Siebel Call Center Application

To enable RSA encryption for the Siebel Call Center Application:

1. Start the Siebel Call Center Application.

2. Navigate to **Sitemap, Server Administration, Components,** and **Component Parameters.**

3. Query for **Call Center Object Manager (ENU)** in the Server Component-Parameter List applet.

4. In the applet, select the **Encryption Type** parameter and select **RSA**. If RSA encryption is not required, then select **None** instead of **RSA**.

2.3.3.4 Starting the Siebel Software Configuration Wizard

This section provides information about starting the Siebel Software Configuration Wizard.

The Siebel Software Configuration Wizard opens automatically after the installation of most server components. If required, you can use one of the following methods to manually start the wizard on a Microsoft Windows computer:

- From the Microsoft Windows desktop:

   1. Click **Start.**

   2. Select **Programs, Siebel Servers 7.0,** and **Configure** ***SERVER_TYPE***, where ***SERVER_TYPE*** is the server you want to configure. For example, ***SERVER_TYPE*** can be Siebel Gateway.

- From a command window:

   1. In a command window, navigate to the bin subdirectory component to configure components in the SIEBEL_ROOT directory. For example, D://sea700/siebsrvr/bin.

2. Depending on the component that you want to configure, enter one of the following commands:

   – To configure the Siebel Database Server, enter the following command:

     ```
     ssincfgw -l LANGUAGE -v y
     ```

   – To configure any component except the Siebel Database Server, enter the following command:

     ```
     ssincfgw -l LANGUAGE
     ```

   In these commands, replace *LANGUAGE* with the language in which the Siebel Software Configuration Wizard must run. For example, replace *LANGUAGE* with ENU for U.S. English or DEU for German. When you run any one of these commands, a menu of configuration modules for each installed component is displayed.

3 Using the Connector

This chapter provides information about the following topics:

3.1 Performing First-Time Reconciliation

First-time recon involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing user records from the target system are brought into Oracle Identity Manager.

The following is the sequence of steps involved in reconciling all existing user records:

> **Note:** In Oracle Identity Manager release 11.1.1, 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.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

1. Perform lookup field synchronization by running the scheduled tasks provided for this operation.

   See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about the attributes of the scheduled tasks for lookup field synchronization.

   See Section 3.5, "Configuring Scheduled Tasks" for information about running scheduled tasks.

2. Perform user reconciliation by running the scheduled task for user reconciliation.

   See Section 3.4.4, "User Reconciliation Scheduled Task" for information about the attributes of this scheduled task.

   See Section 3.5, "Configuring Scheduled Tasks" for information about running scheduled tasks.

After first-time reconciliation, depending on the mode in which you configure the connector, the TimeStamp parameter of the SIEBEL IT Resource IT resource is automatically set to the time stamp at which the reconciliation run began.

> **See Also:** Section 2.2.1.2, "Configuring the IT Resource" for information about the parameters of the IT resource

From the next reconciliation run onward, only target system user records that are added or modified after the time stamp stored in the IT resource are considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the user reconciliation scheduled task.

3.2 Scheduled Task for Lookup Field Synchronization

The Siebel LookupRecon scheduled task is used for lookup field synchronization. Table 3–1 describes the attributes of this scheduled task. See Section 3.5, "Configuring Scheduled Tasks" for information about configuring scheduled tasks.

> **Note:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Table 3–1 Attributes of the Siebel LookupRecon Scheduled Task

Attribute	Description
`ITResource`	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SIEBEL IT Resource`

3.3 Guidelines on Performing Provisioning

The following is a guideline on performing provisioning:

Activating and Deactivating Employee Accounts

To activate an employee account on the target system, assign any responsibility from Oracle Identity Manager.

To deactivate an employee account on the target system, delete all responsibilities of the employee from Oracle Identity Manager.

Note: To perform a provisioning operation for users of type User, customize the Siebel process form and make the Position field optional.

3.4 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Section 3.4.1, "Performing Full Reconciliation"
- Section 3.4.2, "Limited Reconciliation"
- Section 3.4.3, "Reconciliation Based on User Type"
- Section 3.4.4, "User Reconciliation Scheduled Task"

3.4.1 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

To perform a full reconciliation run, set the TimeStamp parameter of the SIEBEL IT resource to `0`. At the end of the reconciliation run, the TimeStamp parameter of the SIEBEL IT resource is automatically set to the time stamp at which the run started. From the next run onward, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

3.4.2 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

For this connector, you create a filter by specifying values for the CustomizedReconQuery IT resource parameter while configuring the IT resource.

The following table lists the target system attributes, and the corresponding Oracle Identity Manager attributes, that you can use to build the query condition. You specify this query condition as the value of the CustomizedReconQuery parameter.

Oracle Identity Manager Attribute	Target System Attribute
User ID	Login Name
First Name	First Name
Last Name	Last Name
Email	EMail Addr
Job Title	Job Title

Oracle Identity Manager Attribute	Target System Attribute
Middle Name	Middle Name
Organization	Organization
Responsibility	Responsibility
Position	Position
Employee Type	Employee Type
Alias	Alias

The following are sample query conditions:

- `First Name=John&Last Name=Doe`

  With this query condition, records of users whose first name is `John` and last name is `Doe` are reconciled.

- `First Name=John&Last Name=Doe|group=contractors`

  With this query condition, records of users who meet either of the following conditions are reconciled:

  – The user's first name is `John` or last name is `Doe`.

  – The user belongs to the `contractors` group.

If you do not specify values for the `CustomizedReconQuery` parameter, then all the records in the target system are compared with existing Oracle Identity Manager records during reconciliation.

The following are guidelines to be followed while specifying a value for the `CustomizedReconQuery` parameter:

- For the target system attributes, you must use the same case (uppercase or lowercase) as given in the table shown earlier in this section. This is because the attribute names are case-sensitive.

- You must not include unnecessary blank spaces between operators and values in the query condition.

  A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

  ```
  First Name=John&Last Name=Doe
  ```

  ```
  First Name= John&Last Name= Doe
  ```

  In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

  Note: An exception is thrown if you include special characters other than the equal sign (=), ampersand (&), and vertical bar (|).

- The query condition must be an expression without any braces.

- Searching users based on multiple value roles and groups are not supported. Only one value for roles and profiles can be queried at a time. For example, if the query condition is `Usergroup=a,b,c`, then the query generates an error.
- Searching users based on more than three user attributes are not supported. For example, if the query condition is `userid=JOHN&firstname=John&lastname=Doe&country=US`, then the query generates an error.

You specify a value for the `CustomizedReconQuery` parameter while configuring the IT resource.

3.4.3 Reconciliation Based on User Type

> **Note:** This section discusses the UserType attribute of the scheduled task.

Siebel supports the definition of the following user types:

- Employee
- Partner User
- Customer
- User

You can specify the user type for which reconciliation must be performed.

To specify the user type for which reconciliation must be performed, you use the UserType scheduled task attribute. This attribute is discussed in Section 3.4.4, "User Reconciliation Scheduled Task."

3.4.4 User Reconciliation Scheduled Task

When you run the Connector Installer or import the connector XML file, the Siebel Recon scheduled task is automatically created in Oracle Identity Manager. This scheduled task is used to reconcile user data from the target system.

You must specify values for the following attributes of the Siebel Recon scheduled task. Table 3–2 describes the attributes of this scheduled task.

Table 3–2 Attributes of the User Reconciliation Scheduled Task

Attribute	Description
Organization	Oracle Identity Manager users Enter the name of the Oracle Identity Manager organization in which reconciled users must be created. Default value: `Xellerate Users`
Configuration Lookup	This attribute contains the name of the lookup definition that stores configuration information used during connector operations. Default value: `Lookup.Configuration.Siebel` **Note:** You must not change the value of this attribute.
MultiValueAttributes	If you perform the procedure described in Section 4.4, "Adding New Multivalued Attributes for Provisioning," then append the multivalued attribute to the default value of the MultiValueAttributes attribute. Step 4 of that section describes the procedure. Default value: `Position,MPosition,Position Id&Responsibility,Primary Responsibility,Responsibility` **Note:** You must not delete this default value. You can only append to it.
TransformLookupName	This attribute holds the name of the lookup definition that is used to configure transformation of attribute values fetched from the target system during reconciliation. Default value: `Lookup.Transform.Siebel`
Use Transform Mapping	Enter `yes` if you want to configure transformation of attribute values fetched from the target system during reconciliation. Otherwise, enter `no`. See Section 4.5, "Configuring Transformation of Data During Reconciliation" for more information about this feature. Default value: `no`
Xellerate Type	Enter the role that must be set for OIM Users created through reconciliation. You can enter one of the following values: ■ `End-User` ■ `End-User Administrator` Default value: `End-User Administrator` **Note:** If you are configuring the connector for trusted source reconciliation, then you need not set a value for this attribute.
Role	Enter the employee type that must be set for OIM Users created through reconciliation. You can enter one of the following values: ■ `Full-Time Employee` ■ `Part-Time Employee` ■ `Temp` ■ `Intern` ■ `Consultant` Default value: `Consultant`
ITResource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `SIEBEL IT Resource`
ResourceObject	Enter the name of the resource object that is used in reconciliation. Default value: `SIEBEL Resource Object`

Table 3–2 (Cont.) Attributes of the User Reconciliation Scheduled Task

Attribute	Description
IsTrusted	Enter `True` if you want to configure the connector for trusted source reconciliation. Enter `False` if you want to configure the connector for target resource reconciliation. Default value: `False`
isDeleteRecon	Enter `True` if you want to perform reconciliation of deleted user records. During reconciliation of deleted users: ■ In target resource mode, if a record is deleted on the target system, then the corresponding Siebel resource is revoked from the OIM User. ■ In trusted source mode, if a record is deleted on the target system, then the corresponding OIM User is deleted. Enter `False` if you want to run user reconciliation. Default value: `False`
UserType	Specify the type of user that must be reconciled from the target system. You can specify one of the following Siebel user types: ■ `Employee`: This user is an internal employee and user who is associated with a position in a division within your company. ■ `Partner User`: This user is an employee at a partner company (external organization) and is associated with a position in a division within that company. Therefore, a `Partner User` is also an `Employee`, but not an internal one. ■ `Customer`: This user is a self-registered partner having no position in your company. However, this user has a responsibility that specifies the application views the user can access. Default value: `Employee` **Note:** To run a target system reconciliation of a user of type User, customize the Siebel process form and make the Position field optional.
SiebelServerTimeZone	Specifies the time zone of the target system database The connector uses this information to identify records that must be reconciled during incremental reconciliation. Default value: `GMT+10:00`
DayLightSaving	Enter the time (in minutes) that must be added to the time stamp Sample value: `60` With this sample value, 60 minutes are added to the time stamp stored in the TimeStamp parameter, and the new time stamp is used to identify records that have been created or modified after the last reconciliation run. Defaul value: `0`

3.5 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–3 lists the scheduled tasks that you must configure.

Table 3–3 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
Siebel LookupRecon	This scheduled task is used for lookup field synchronization. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about this scheduled task.
Siebel Recon	This scheduled task is used for user reconciliation. See Section 3.4.4, "User Reconciliation Scheduled Task" for information about this scheduled task.

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in one of the following sections:

- Section 3.5.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"

3.5.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Perform one of the following:

   a. If you are using Oracle Identity Manager release release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**

   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.

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

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

     a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

     b. In the search results table, click the edit icon in the Edit column for the scheduled task.

     c. On the Scheduled Task Details page where the details of the scheduled task that you selected is displayed, click **Edit**.

   - If you are using Oracle Identity Manager release 11.1.1, then:

     a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

     b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

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

4. Modify the details of the scheduled task. To do so:

   a. If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

- **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
- **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.
- **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
- **Frequency:** Specify the frequency at which you want the task to run.

b. If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, you can modify the following parameters:

- **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
- **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

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

5. Specify values for the attributes of the scheduled task. To do so:

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
- Attributes of the scheduled task are discussed in Section 3.4.4, "User Reconciliation Scheduled Task."

- If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.
- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

6. After specifying the attributes, perform one of the following:

- If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

> **Note:** The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

- If you are using Oracle Identity Manager release 11.1.1, then click **Apply** to save the changes.

> **Note:** The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.6 Performing Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.7, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

> **See Also:** *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- Section 3.6.1, "Direct Provisioning"
- Section 3.6.2, "Request-Based Provisioning"

3.6.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.

   b. On the Create User page, enter values for the OIM User fields and then click **Create User**.

- If you are using Oracle Identity Manager release 11.1.1, then:

   a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.

   b. On the Create User page, enter values for the OIM User fields, and then click **Save**.

3. If you want to provision a target system account to an existing OIM User, then:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

      a. From the Users menu, select **Manage**.

      b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.

   - If you are using Oracle Identity Manager release 11.1.1, then:

      a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.

      b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.

4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

      a. On the User Detail page, select **Resource Profile** from the list at the top of the page.

      b. On the Resource Profile page, click **Provision New Resource**.

   - If you are using Oracle Identity Manager release 11.1.1, then:

      a. On the user details page, click the **Resources** tab.

      b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **Siebel Resource Object** from the list and then click **Continue**.

6. On the Step 2: Verify Resource Selection page, click **Continue**.

7. On the Step 5: Provide Process Data for Siebel User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.

8. On the Step 5: Provide Process Data for Siebel Responsibility Form page, search for and select a group for the user on the target system and then click **Continue**.

9. On the Step 5: Provide Process Data for Siebel Position Form page, search for and select a group for the user on the target system and then click **Continue**.

10. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.

11. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:

- If you are using Oracle Identity Manager release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
- If you are using Oracle Identity Manager release 11.1.1, then:

  a. Close the window displaying the "Provisioning has been initiated" message.

  b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.6.2 Request-Based Provisioning

> **Note:** The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

> **Note:** The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- Section 3.6.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.6.2.2, "Approver's Role in Request-Based Provisioning"

3.6.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

> **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account..

If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.

8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **Siebel Resource Object**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.6.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

    A message confirming that the task was approved is displayed.

3.7 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

> **Note:** It is assumed that you have performed the procedure described in Section 2.3.1.8, "Configuring Oracle Identity Manager for Request-Based Provisioning"

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.

2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **Siebel Process** process definition.
   c. Deselect the **Auto Save Form** check box.
   d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **Siebel Resource Object** resource object.
   c. Deselect the **Self Request Allowed** check box.
   d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **Siebel Process** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **Siebel Resource Object** resource object.
   c. Select the **Self Request Allowed** check box.
   d. Click the Save icon.

4 Extending the Functionality of the Connector

After you deploy the connector, you can configure it to meet your requirements. This chapter discusses the following optional configuration procedures:

- Section 4.1, "Adding New Attributes for Target Resource Reconciliation"
- Section 4.2, "Adding New Attributes for Provisioning"
- Section 4.3, "Adding New Multivalued Attributes for Target Resource Reconciliation"
- Section 4.4, "Adding New Multivalued Attributes for Provisioning"
- Section 4.5, "Configuring Transformation of Data During Reconciliation"

4.1 Adding New Attributes for Target Resource Reconciliation

Note:

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

You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in Table 1–3, " User Attributes for Target Resource Reconciliation and Provisioning" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

To add a new attribute for target resource reconciliation, perform the following procedure:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Search for and open the **Siebel** process form.
   d. Click **Create New Version**.
   e. In the **Label** field, enter the version name. For example, `version#1`.

f. Click the **Save** icon.

g. Select the current version created in Step e from the **Current Version** list.

h. Click **Add** to create a new attribute, and provide the values for that attribute.

For example, if you are adding the organization attribute, then enter the following values in the **Additional Columns** tab:

Field	Value
Name	organization
Variant Type	String
Length	100
Field Label	organization
Order	20

The following screenshot shows this form:

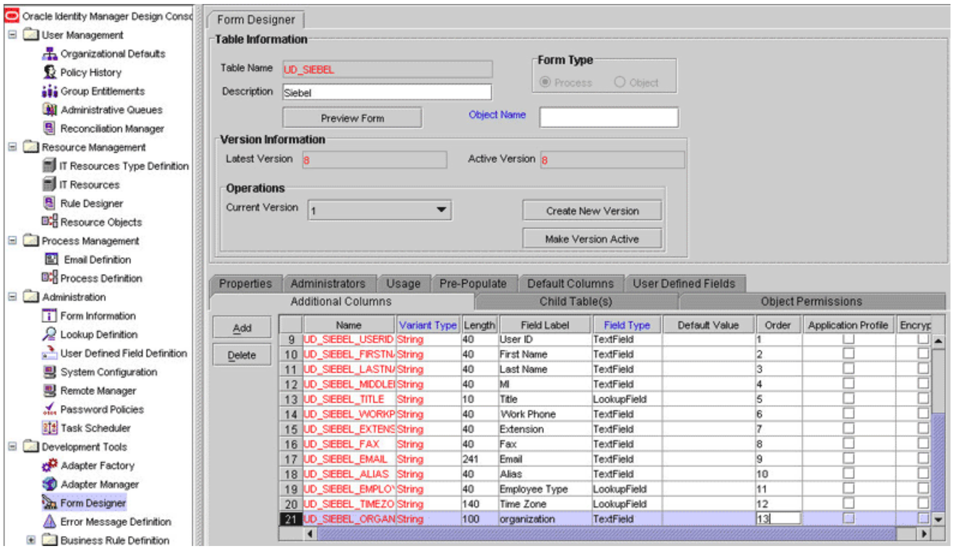


Table Information

Table Name: UD_SIEBEL

Description: Siebel

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 8

Active Version: 8

Operations

Current Version: 1

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encryp
9	UD_SIEBEL_USERID	String	40	User ID	TextField		1	□	□
10	UD_SIEBEL_FIRSTN/	String	40	First Name	TextField		2	□	□
11	UD_SIEBEL_LASTN/	String	40	Last Name	TextField		3	□	□
12	UD_SIEBEL_MIDDLEI	String	40	MI	TextField		4	□	□
13	UD_SIEBEL_TITLE	String	10	Title	LookupField		5	□	□
14	UD_SIEBEL_WORKP	String	40	Work Phone	TextField		6	□	□
15	UD_SIEBEL_EXTENS	String	40	Extension	TextField		7	□	□
16	UD_SIEBEL_FAX	String	40	Fax	TextField		8	□	□
17	UD_SIEBEL_EMAIL	String	241	Email	TextField		9	□	□
18	UD_SIEBEL_ALIAS	String	40	Alias	TextField		10	□	□
19	UD_SIEBEL_EMPLO'	String	40	Employee Type	LookupField		11	□	□
20	UD_SIEBEL_TIMEZO	String	140	Time Zone	LookupField		12	□	□
21	UD_SIEBEL_ORGAN	String	100	organization	TextField		13	□	□

i. Click the **Save** icon.

j. Click **Make Version Active**.

3. Add the new attribute to the list of reconciliation fields in the resource object as follows:

a. Expand **Resource Management.**

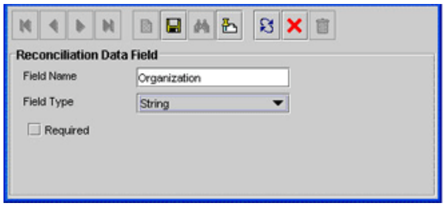
b. Double-click **Resource Objects**.

c. Search for and open the **Siebel** resource object.

d. On the **Object Reconciliation** tab, click **Add Field**, and then enter the following values:

Field Name: `Organization`

Field Type: `String`



Reconciliation Data Field

Field Name: Organization

Field Type: String

□ Required

   e. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

   f. Click the **Save** icon.

4. Create a reconciliation field mapping for the new attribute in the process definition form as follows:

   a. Expand **Process Management.**

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

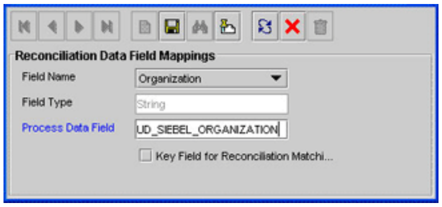
   c. Search for and open the **Siebel** process definition.

   d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then select the following values:

   Field Name: `Organization`

   Field Type: `String`

   Process Data Field: `Organization`



Reconciliation Data Field Mappings

Field Name: Organization

Field Type: String

Process Data Field: UD_SIEBEL_ORGANIZATION

□ Key Field for Reconciliation Matchi...

   e. Click the **Save** icon.

5. Create an entry for the attribute in the lookup definition for reconciliation as follows:

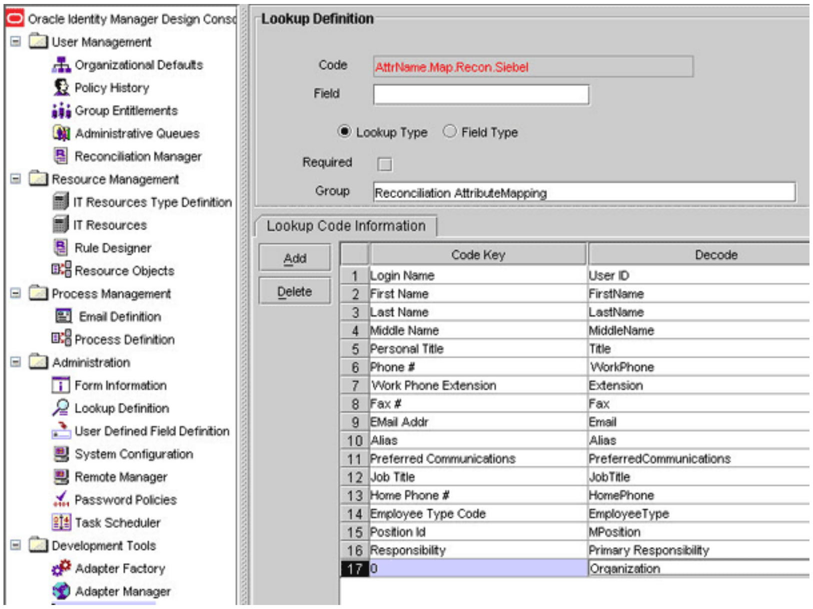
   a. Expand **Administration**.

   b. Double-click **Lookup Definition**.

   c. Search for and open the **AttrName.Map.Recon.Siebel** lookup definition.

   d. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute on the target system. The Decode value is the name of the attribute in the target system.

   For example, enter `o` in the **Code Key** field and then enter `Organization` in the **Decode** field.



Lookup Definition

Code: AttrName.Map.Recon.Siebel

Field:

● Lookup Type ○ Field Type

Required □

Group: Reconciliation AttributeMapping

	Code Key	Decode
1	Login Name	User ID
2	First Name	FirstName
3	Last Name	LastName
4	Middle Name	MiddleName
5	Personal Title	Title
6	Phone #	WorkPhone
7	Work Phone Extension	Extension
8	Fax #	Fax
9	EMail Addr	Email
10	Alias	Alias
11	Preferred Communications	PreferredCommunications
12	Job Title	JobTitle
13	Home Phone #	HomePhone
14	Employee Type Code	EmployeeType
15	Position Id	MPosition
16	Responsibility	Primary Responsibility
17	0	Organization

e. Click the **Save** icon.

4.2 Adding New Attributes for Provisioning

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

By default, the attributes listed in Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning users:

Note: You need not perform steps that you have already performed as part of the procedure described in Section 4.1, "Adding New Attributes for Target Resource Reconciliation."

1. Log in to Oracle Identity Manager Design Console.
2. Add the new attribute on the process form.

   If you have added the attribute on the process form by performing Step 2 of Section 4.1, "Adding New Attributes for Target Resource Reconciliation," then you need not add the attribute again. If you have not added the attribute, then:

   a. Expand **Development Tools**.

   b. Double-click **Form Designer**.

   c. Search for and open the **Siebel** process form.

   d. Click **Create New Version**.

   e. In the **Label** field, enter the version name. For example, `version#1`.

f. Click the **Save** icon.

g. Select the current version created in Step e from the **Current Version** list.

h. Click **Add** to create a new attribute, and provide the values for that attribute.

For example, if you are adding the organization attribute, then enter the following values in the **Additional Columns** tab:

Field	Value
Name	organization
Variant Type	String
Length	100
Field Label	organization
Order	20

The following screenshot shows this form:

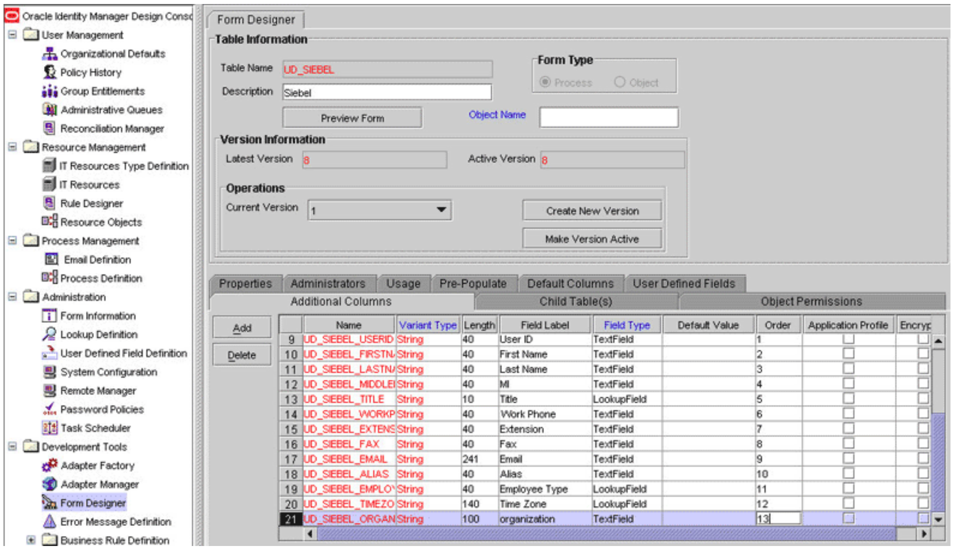


Table Information

Table Name: UD_SIEBEL

Description: Siebel

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 8

Active Version: 8

Operations

Current Version: 1

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encryp
9	UD_SIEBEL_USERID	String	40	User ID	TextField		1	□	□
10	UD_SIEBEL_FIRSTN/	String	40	First Name	TextField		2	□	□
11	UD_SIEBEL_LASTN/	String	40	Last Name	TextField		3	□	□
12	UD_SIEBEL_MIDDLEI	String	40	MI	TextField		4	□	□
13	UD_SIEBEL_TITLE	String	10	Title	LookupField		5	□	□
14	UD_SIEBEL_WORKP	String	40	Work Phone	TextField		6	□	□
15	UD_SIEBEL_EXTENS	String	40	Extension	TextField		7	□	□
16	UD_SIEBEL_FAX	String	40	Fax	TextField		8	□	□
17	UD_SIEBEL_EMAIL	String	241	Email	TextField		9	□	□
18	UD_SIEBEL_ALIAS	String	40	Alias	TextField		10	□	□
19	UD_SIEBEL_EMPLOY	String	40	Employee Type	LookupField		11	□	□
20	UD_SIEBEL_TIMEZO	String	140	Time Zone	LookupField		12	□	□
21	UD_SIEBEL_ORGAN	String	100	organization	TextField		13	□	□

i. Click the **Save** icon.

j. Click **Make Version Active**.

3. Create an entry for the attribute in the lookup definition for provisioning as follows:

a. Expand **Administration.**

b. Double-click **Lookup Definition.**

c. Search for and open the **AttrName.Prov.Map.Siebel** lookup definition.

d. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute given in the process form. The Decode value is the name of the attribute in the target system.

For example, enter `UD_SIEBEL_CELLPHONE` in the **Code Key** field and then enter `CellPhone #` in the Decode field.

e. Click the Save icon.

Note: Perform steps 4 through 6 only if you want to perform request-based provisioning.

4. Update the request dataset.

   When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

   a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

   b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

      See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

      For example, while performing Step 2 of this procedure, if you added organization as an attribute on the process form, then enter the following line:

      ```
      <AttributeReference
      name = "organization"
      attr-ref = "organization"
      type = "String"
      widget = "text"
      length = "50"
      available-in-bulk = "false"/>
      ```

      In this AttributeReference element:

      – For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

        For example, if UD_SIEBEL_ORGANIZATION is the value in the Name column of the process form, then you must specify `organization` as the value of the name attribute in the AttributeReference element.

      – For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 2.

      – For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 2.

      – For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 2.

      – For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 2.

      – For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

      While performing Step 2, if you added more than one attribute on the process form, then repeat this step for each attribute added.

   c. Save and close the XML file.

5. Run the PurgeCache utility to clear content related to request datasets from the server cache.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

6. Import into MDS the request dataset definitions in XML format.

   See Section 2.3.1.8.3, "Importing Request Datasets into MDS" for detailed information about the procedure.

7. To enable the update of a new attribute for provisioning a user:

   a. Expand **Process Management.**

   b. Double-click **Process Definition** and open the **Siebel** process definition.

   c. In the process definition, add a new task for updating the field as follows:

      – Click **Add** and enter the task name, for example, `CellPhone Updated`, and the task description.

      – In the Task Properties section, select the following fields:

        Conditional

        Required for Completion

        Allow Cancellation while Pending

        Allow Multiple Instances

      – Click on the Save icon.

   d. On the Integration tab, click **Add,** and then click **Adapter.**

   e. Select the **adpSIEBELMODIFYUSER** adapter, click **Save,** and then click **OK** in the message that is displayed.

   f. To map the adapter variables listed in this table, select the adapter, click **Map,** and then specify the data given in the following table:

Note: Some of the values in this table are specific to Organization (`o` value in Siebel). These values must be replaced with values relevant to the attributes that you require.

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
Adapter return value	Object	Response code	NA	NA	NA
auserid	String	Process Data	User ID	NA	NA
afieldvalue	String	Process Data	CellPhone **Note:** This is the name of the newly added field on the process form.	NA	NA
afieldname	String	Process data	CellPhone #	NA	NA
ITResource	IT Resource (Siebel IT resource definition)	Process data	IT Resource Type	NA	NA
iProcessInstKey	Long	Process data	processinstance	NA	NA

g. Click the Save icon and then close the dialog box.

4.3 Adding New Multivalued Attributes for Target Resource Reconciliation

---

Note:

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

You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, only the UserGroup and UserRole multivalued attributes are mapped for user reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for target system reconciliation.

By default, no multivalued attributes are mapped for reconciliation between Oracle Identity Manager and the target system for groups and roles. If required, you can add new multivalued attributes for reconciliation of groups or roles.

To add a new multivalued attribute for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued attribute as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Create a form by specifying a table name and description, and then click **Save**.
   d. Click **Add** and enter the details of the attribute.

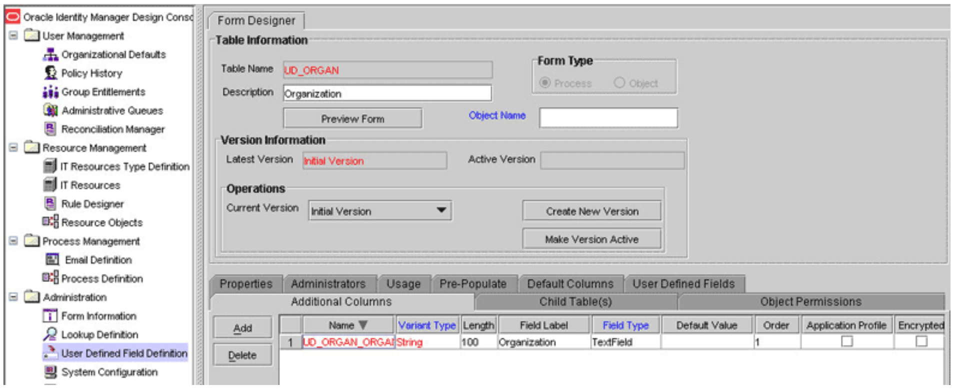


Table Information

Table Name: UD_ORGAN

Description: Organization

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: Initial Version

Active Version:

Operations

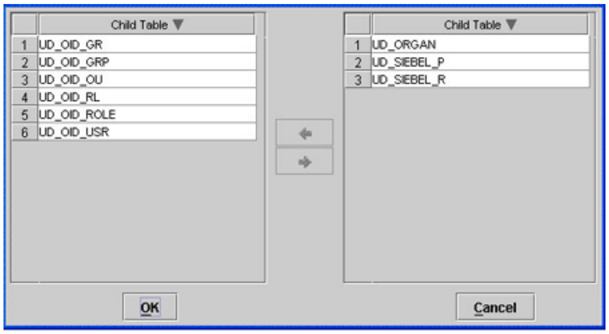
Current Version: Initial Version

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
1	UD_ORGAN_ORGA	String	100	Organization	TextField		1	□	□

   e. Click **Save** and then click **Make Version Active.**
3. Add the form created for the multivalued attribute as a child form of the process form as follows:
   a. Search for and open the **UD_SIEBEL** process form.
   b. Click **Create New Version**.
   c. Click the **Child Table(s)** tab.

d. Click **Assign**.

e. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.



	Child Table
1	UD_OID_GR
2	UD_OID_GRP
3	UD_OID_OU
4	UD_OID_RL
5	UD_OID_ROLE
6	UD_OID_USR

	Child Table
1	UD_ORGAN
2	UD_SIEBEL_P
3	UD_SIEBEL_R

f. Click **Save** and then click **Make Version Active.**

4. Add the new attribute to the list of reconciliation fields in the resource object as follows:

a. Expand **Resource Management**.

b. Double-click **Resource Objects**.

c. Search for and open the **Siebel User** resource object.

d. On the Object Reconciliation tab, click **Add Field**.

e. In the Add Reconciliation Fields dialog box, enter the details of the attribute.

For example, enter `Organization` in the **Field Name** field and select **Multi Valued Attribute** from the Field Type list.

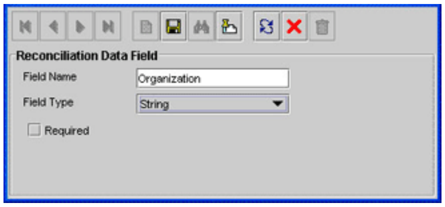
f. Click **Save** and then close the dialog box.

g. Right-click the newly created attribute.

h. Select **Define Property Fields**.

i. In the Add Reconciliation Fields dialog box, enter the details of the newly created field.

For example, enter `Organization` in the Field Name field and select **String** from the Field Type list.



Reconciliation Data Field

Field Name: Organization

Field Type: String

□ Required

j. Click **Save**, and then close the dialog box.

k. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

5. Create a reconciliation field mapping for the new attribute as follows:

a. Expand **Process Management**.

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

c. Search for and open the **Siebel User** process form.

d. On the Reconciliation Field Mappings tab of the process definition, click **Add Table Map**.

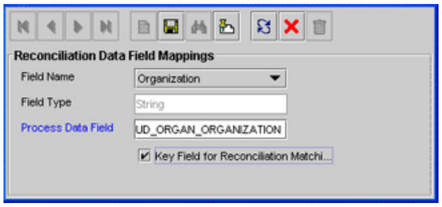
e. In the Add Reconciliation Table Mapping dialog box, select the field name and table name from the list, click **Save**, and then close the dialog box.

f. Right-click the newly created field, and select **Define Property Field Map**.

g. In the **Field Name** field, select the value for the field that you want to add.

h. Double-click the **Process Data Field** field, and then select the required data field.

i. Select the **Key Field for Reconciliation Mapping** check box, and then click **Save**.



Reconciliation Data Field Mappings

Field Name: Organization

Field Type: String

Process Data Field: UD_ORGAN_ORGANIZATION

☑ Key Field for Reconciliation Matchi...

6. Create an entry for the attribute in the lookup definition for reconciliation as follows:

   a. Expand **Administration**.

   b. Double-click **Lookup Definition.**

   c. Search for and open the **AttrName.Map.Recon.Siebel** lookup definition.

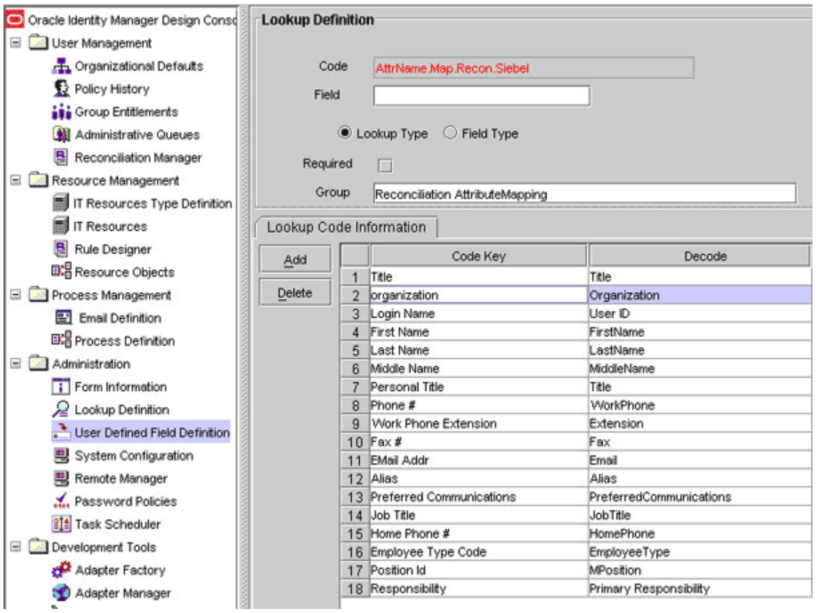
   d. Add the Code Key and Decode of the multivalued attribute in the lookup definition. The Code Key value must be the name of the attribute on the target system. The Decode value must be the name of the field on the process form.

      For example:

      Code Key: `homeaddress`

      Decode: `Address`

Note: You must append the Decode value of newly added multivalued attributes to the value of the MultiValueAttributes attribute. See Section 3.4.4, "User Reconciliation Scheduled Task" for information about this attribute.



Lookup Definition

Code: AttrName.Map.Recon.Siebel

Field:

● Lookup Type ○ Field Type

Required □

Group: Reconciliation AttributeMapping

Lookup Code Information

	Code Key	Decode
1	Title	Title
2	organization	Organization
3	Login Name	User ID
4	First Name	FirstName
5	Last Name	LastName
6	Middle Name	MiddleName
7	Personal Title	Title
8	Phone #	WorkPhone
9	Work Phone Extension	Extension
10	Fax #	Fax
11	EMail Addr	Email
12	Alias	Alias
13	Preferred Communications	PreferredCommunications
14	Job Title	JobTitle
15	Home Phone #	HomePhone
16	Employee Type Code	EmployeeType
17	Position Id	MPosition
18	Responsibility	Primary Responsibility

7. Append details of the multivalued attribute to the existing value of the Siebel Recon user reconciliation scheduled task.

   > **See Also:** Section Section 3.4.4, "User Reconciliation Scheduled Task" for more information about this attribute

   The following is the format of a single entry in the list:

   ```
   OIM_TABLE_NAME,OIM_ATTRIBUTE_NAME_IN_TABLE,SIEBEL_ATTRIBUTE_NAME
   ```

   In this format:

   - *OIM_TABLE_NAME* is the name of the child table in Oracle Identity Manager.
   - *OIM_ATTRIBUTE_NAME* is the name of the attribute in the child table.
   - *SIEBEL_ATTRIBUTE_NAME* is the name of the attribute on the target system.

   For multiple entries, use the ampersand (&) as the delimiting character. This is illustrated by the default value of the multivalued attribute:

   ```
   Position,MPosition,Position Id&Responsibility,Primary
   Responsibility,Responsibility
   ```

If you have added new multivalued for groups or roles, then you must specify the decode key values of the newly added attributes as a value of the MultiValueAttributes attribute that is described in Section 3.4.4, "User Reconciliation Scheduled Task."

4.4 Adding New Multivalued Attributes for Provisioning

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for provisioning.

By default, only the Siebel Position form and Siebel Responsibility form attributes are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for target system reconciliation.

By default, no multivalued attributes are mapped for provisioning between Oracle Identity Manager and the target system for groups and roles. If required, you can add new multivalued attributes for reconciliation and provisioning of groups or roles.

To add a new multivalued attribute for provisioning:

> **Note:** You need not perform steps that you have already performed as part of the procedure described in Section 4.3, "Adding New Multivalued Attributes for Target Resource Reconciliation."

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued attribute as follows:
   - **a.** Expand **Development Tools**.
   - **b.** Double-click **Form Designer**.
   - **c.** Create a form by specifying a table name and description, and then click **Save**.
   - **d.** Click **Add** and enter the details of the attribute.

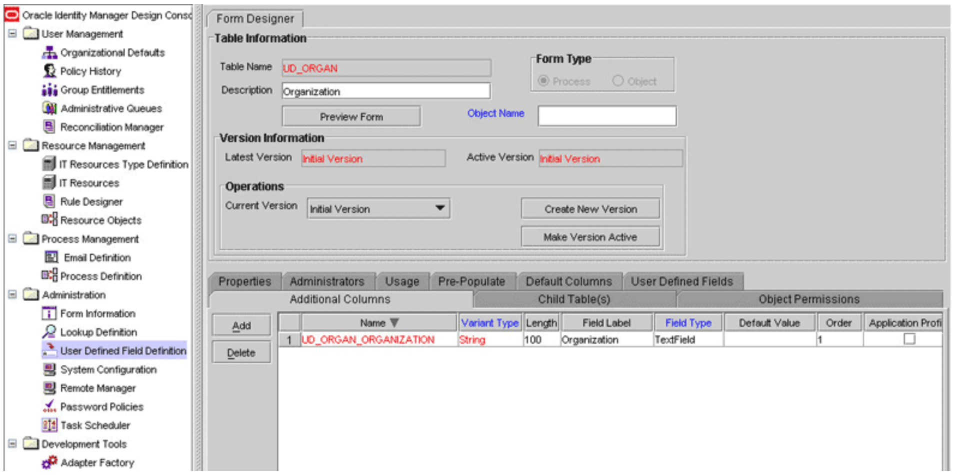


Table Information

Table Name: UD_ORGAN

Description: Organization

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: Initial Version

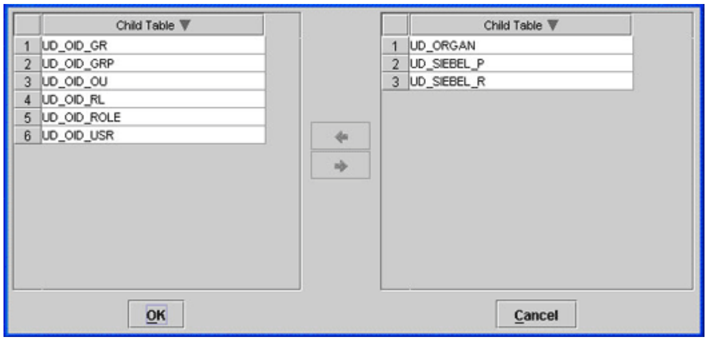
Active Version: Initial Version

Operations

Current Version: Initial Version

	Name ▼	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profi
1	UD_ORGAN_ORGANIZATION	String	100	Organization	TextField		1	□

   - **e.** Click **Save** and then click **Make Version Active.**
3. Add the form created for the multivalued attribute as a child form of the process form as follows:
   - **a.** Search for and open the **UD_SIEBEL** process form.
   - **b.** Click **Create New Version**.
   - **c.** Click the **Child Table(s)** tab.
   - **d.** Click **Assign**.
   - **e.** In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.



	Child Table
1	UD_OID_GR
2	UD_OID_GRP
3	UD_OID_OU
4	UD_OID_RL
5	UD_OID_ROLE
6	UD_OID_USR

	Child Table
1	UD_ORGAN
2	UD_SIEBEL_P
3	UD_SIEBEL_R

f. Click **Save** and then click **Make Version Active.**

4. Append details of the multivalued attribute to the existing value of the Siebel Recon user reconciliation scheduled task.

> **See Also:** Section Section 3.4.4, "User Reconciliation Scheduled Task" for more information about this attribute

The following is the format of a single entry in the list:

OIM_TABLE_NAME,*OIM_ATTRIBUTE_NAME_IN_TABLE*,*SIEBEL_ATTRIBUTE_NAME*

In this format:

- *OIM_TABLE_NAME* is the name of the child table in Oracle Identity Manager.
- *OIM_ATTRIBUTE_NAME* is the name of the attribute in the child table.
- *SIEBEL_ATTRIBUTE_NAME* is the name of the attribute on the target system.

For multiple entries, use the ampersand (&) as the delimiting character. This is illustrated by the default value of the multivalued attribute:

```
Position,MPosition,Position Id&Responsibility,Primary
Responsibility,Responsibility
```

5. To enable the update of a new multivalued attribute for provisioning:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

a. Log in to the Oracle Identity Manager Design Console.

b. Expand **Process Management**.

c. Double-click **Process Definition**, and then open the **Siebel** process definition.

d. In the process definition, add a task for setting a value for the attribute:

– Click **Add**, enter the name of the task for adding multivalued attributes, and enter the task description.

– In the Task Properties section, select the following fields:

Conditional

Required for Completion

Allow Cancellation while Pending

Allow Multiple Instances

Select the child table from the list.

For the example described earlier, select **Mailing Address** from the list.

Select **Insert** as the trigger type for adding multivalued data. Alternatively, select **Delete** as the trigger type for removing multivalued data.

- On the **Integration** tab, click **Add**, and then click **Adapter**.
- Select the **adpADDMULTIVALUEATTRIBUTETOSIEBELUSER** adapter, click **Save**, and then click **OK** in the message.
- To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

Note: Some of the values in this table are specific to the Mailing Address/Postal Address example. These values must be replaced with values relevant to the multivalued attributes that you require.

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
Adapter return value	Object	Response code	NA	NA	NA
UserID	String	Process Data	User ID	NA	NA
businessobject	Literal Value: Employee Business value of the multivalued attribute	NA	NA	NA	NA
Businesscomponent	Literal value: employee Business component of the multivalued attribute	NA	NA	NA	NA
MVGBusComp	Literal value: employee Name of the multivalued attribute on the target system	NA	NA	NA	NA
Attributename	String	Literal	String	homePostalAddress **Note:** This is a sample (literal) value.	NA
attributevalue	String	**Data** and then select (for example) **OID** User Role	Address **Note:** This is a sample value	NA	NA
ITResource	IT Resource (Siebel IT resource definition)	Process data	IT Resource Type	NA	NA

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
iProcessInstKey	Long	Process data	processinstance	NA	NA

– Click the Save icon and then close the dialog box.

e. In the process definition, add a task for removing the value of the attribute by performing Step d. While performing Step d.–, select the **adpREMOVEMULTIVALUEATTRIBUTETOSIEBELUSER** adapter.

f. In the process definition, add a task for updating the value of the attribute by performing Step d.

While performing Step d.– select the **adpUPDATEMULTIVALUEATTRIBUTETOSIEBELUSER** adapter. Map the Adapter return Value attribute for this update task by providing the values described in the preceding table.

Note: Perform steps 6 through 8 only if you want to perform request-based provisioning.

6. Update the request dataset.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

For example, if you added Organization as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Organization"
attr-ref = "Organization"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

In this AttributeReference element:

– For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if UD_SIEBEL_ORGANIZATION is the value in the Name column of the process form, then you must specify `Organization` as the value of the name attribute in the AttributeReference element.

– For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form.

- For the type attribute, enter the value that you entered in the Variant Type column of the process form.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form.
- For the length attribute, enter the value that you entered in the Length column of the process form.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

7. Run the PurgeCache utility to clear content related to request datasets from the server cache.

   See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

8. Import into MDS the request dataset definitions in XML format.

   See Section 2.3.1.8.3, "Importing Request Datasets into MDS" for detailed information about the procedure.

4.5 Configuring Transformation of Data During Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to configure transformation of data during reconciliation.

You can configure transformation of reconciled data according to your requirements. For example, you can automate the look up of the field name from an external system and set the value based on the field name.

To configure transformation of data:

1. Incorporate the required logic in a Java class.

   This transformation class must implement the com.thortech.xl.schedule.tasks.AttributeTransformer interface and the transform method.

   The following is one such sample class:

```
package com.thortech.xl.schedule.tasks;
public class AppendTransformer implements AttributeTransformer {
/**
* @param inValue: This is the input string to be transformed.
* @return String: This is the string that is returned.
*/
public String transform(String value) {
   return value;

}
```

2. Compile the class and place the JAR file in the JavaTasks directory.

3. Add an entry in the Lookup.Transform.Siebel lookup definition.

   Code Key: Enter the name of the attribute on which you want to apply the transformation. For example: `FirstName`

   Decode: Enter the name of the class file. For example: `com.thortech.xl.schedule.tasks.AppendTransformer`

4. Enter `yes` as the value of the Use Transform Mapping attribute of the Siebel Recon scheduled task. See Section 3.4.4, "User Reconciliation Scheduled Task" for more information.

5 Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- Section 5.1, "Running Test Cases"
- Section 5.2, "Troubleshooting"

5.1 Running Test Cases

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

To use the testing utility:

1. Copy the contents of the Troubleshoot directory on the installation media, to the one of the following directories:
   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troubleshoot
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory/Siebel/Troubleshoot
2. Specify the required values in the global.properties file.

   This file is present in the following directory:
   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troubleshoot
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory/Siebel/Troubleshoot

   The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
Siebel Server Parameters	Parameters required to connect to the target system These parameters are the same as the parameters of the IT resource.
Create User Parameters	Values required to create a user
Modify User Parameters	Values required to modify a user
Delete User Parameters	User ID of the user to be deleted

Section	Information
Recon Parameters	Date from which modified data is to be reconciled The To Date value is taken as the current date and time.

3. Depending on the Oracle Identity Manager version you are using, add one of the following to the CLASSPATH environment variable:

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

     OIM_HOME/xellerate/lib/xlUtils.jar

     OIM_HOME/xellerate/JavaTasks/xlSiebel.jar

     OIM_HOME/xellerate/ScheduleTask/SiebelRecon.jar

     OIM_HOME/xellerate/lib/xlLogger.jar

     OIM_HOME/xellerate/ext/log4j-1.2.8.jar

     In addition to the preceding list, add the following files:

     – For Siebel 7.5:

       The following files from the *OIM_HOME*/xellerate/ThirdParty directory:

       SiebelJI_enu.jar

       SiebelJI_Common.jar

       SiebelJI.jar

     – For Siebel 7.8:

       The following files from the *OIM_HOME*/xellerate/ThirdParty directory:

       Siebel.jar

       SiebelJI_enu.jar

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/lib/xlUtils.jar

     OIM_HOME/server/JavaTasks/xlSiebel.jar

     OIM_HOME/server/ScheduleTask/SiebelRecon.jar

     OIM_HOME/server/ext/log4j-1.2.8.jar

     In addition to the preceding list, add the following files:

     – For Siebel 7.5:

       The following files from the *OIM_HOME*/server/ThirdParty directory:

       SiebelJI_enu.jar

       SiebelJI_Common.jar

       SiebelJI.jar

     – For Siebel 7.8:

       The following files from the *OIM_HOME*/server/ThirdParty directory:

       Siebel.jar

       SiebelJI_enu.jar

4. Create an ASCII-format copy of the global.properties file as follows:

Note: You must perform this procedure every time you make a change in the contents of the global.properties file.

a. In a command window, change to the following directory:

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

     OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troubleshoot

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory/Siebel/Troubleshoot

b. Enter the following command:

   ```
   native2ascii global.properties troubleshoot.properties
   ```

   The troubleshoot.properties is created when you run the `native2ascii` command. The contents of this file are an ASCII-format copy of the contents of the global.properties file.

5. Perform the following tests:

   - Enter the following command to create a user:

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

       ```
       java
       -DTproperties=OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troub
       leshoot/troubleshoot.properties
       -Dlog4j.configuration=file:/OIM_HOME/xellerate/ConnectorDefaultDirector
       y/Siebel/Troubleshoot/log.properties TroubleShootingUtility C
       ```

     - For Oracle Identity Manager release 11.1.1:

       ```
       java
       -DTproperties=OIM_HOME/server/ConnectorDefaultDirectory/Siebel/Troubles
       hoot/troubleshoot.properties
       -Dlog4j.configuration=file:/OIM_HOME/server/ConnectorDefaultDirectory/S
       iebel/Troubleshoot/log.properties TroubleShootingUtility C
       ```

   - Enter the following command to modify a user:

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

       ```
       java
       -DTproperties=OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troub
       leshoot/troubleshoot.properties
       -Dlog4j.configuration=file:/OIM_HOME/xellerate/ConnectorDefaultDirector
       y/Siebel/Troubleshoot/log.properties TroubleShootingUtility M
       ```

     - For Oracle Identity Manager release 11.1.1:

       ```
       java
       -DTproperties=OIM_HOME/server/Siebel/Troubleshoot/troubleshoot.properti
       es
       -Dlog4j.configuration=file:/OIM_HOME/xellerate/server/Troubleshoot/log.
       properties TroubleShootingUtility M
       ```

   - Enter the following command to delete a user:

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

       ```
       java
       ```

```
-DTproperties=OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troub
leshoot/troubleshoot.properties
-Dlog4j.configuration=file:/OIM_HOME/xellerate/ConnectorDefaultDirector
y/Siebel/Troubleshoot/log.properties TroubleShootingUtility D
```

  - For Oracle Identity Manager release 11.1.1:

    ```
    java
    -DTproperties=OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troub
    leshoot/troubleshoot.properties
    -Dlog4j.configuration=file:/OIM_HOME/xellerate/ConnectorDefaultDirector
    y/Siebel/Troubleshoot/log.properties TroubleShootingUtility D
    ```

- Enter the following command to reconcile user information:
  - For Oracle Identity Manager release 9.1.0.*x*:

    ```
    java
    -DTproperties=OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troub
    leshoot/troubleshoot.properties
    -Dlog4j.configuration=file:/OIM_HOME/xellerate/ConnectorDefaultDirector
    y/Siebel/Troubleshoot/log.properties TroubleShootingUtility R
    ```

  - For Oracle Identity Manager release 11.1.1:

    ```
    java
    -DTproperties=OIM_HOME/xellerate/ConnectorDefaultDirectory/Siebel/Troub
    leshoot/troubleshoot.properties
    -Dlog4j.configuration=file:/OIM_HOME/xellerate/ConnectorDefaultDirector
    y/Siebel/Troubleshoot/log.properties TroubleShootingUtility R
    ```

Testing Partial Reconciliation

To test query-based reconciliation, you can specify the following types of query conditions as values for the CustomizedReconQuery parameter:

- Simple query with user attributes, for example:
  - Value assigned to the CustomizedReconQuery parameter: `First Name=John`

    Users with first name `John` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `Login Name=JOHN`

    Users with login name `JOHN` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `First Name=John|First Name=Jane`

    Users with first name `John` and `Jane` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `First Name=John&Last Name=Doe`

    Users with the first name `John` and last name `Doe` are reconciled.
- Query based on positions and responsibilities, for example:
  - Value assigned to the CustomizedReconQuery parameter: `Position=Proxy Employee|Position=ERM AnonUser`

    All users having positions as `Proxy Employee` or `ERM AnonUser` are reconciled.

  - Value assigned to the CustomizedReconQuery parameter: `Responsibility=CEO&Responsibility=Consultant`

    All users having responsibilities as `CEO` and `Consultant` are reconciled.

  - Value assigned to the CustomizedReconQuery parameter: `Responsibility=CEO& Position=ERM AnonUser`

    All users having responsibility `CEO` and position as `ERM AnonUser` are reconciled.

- Complex queries, for example:

  - Value assigned to the CustomizedReconQuery parameter: `First Name=John&Position=Proxy Employee|Position=ERM AnonUser`

    All users having first name as `John` and position as `Proxy Employee`, as well as all users with position as `ERM AnonUser` are reconciled.

  - Value assigned to the CustomizedReconQuery parameter: `Last Name=Doe|Position=Proxy Employee&Responsibility=CEO`

    All users having last name as `Doe` plus all users having both Position as `Proxy Employee` and Responsibility as `CEO` are reconciled.

> **Note:** For queries with a combination of & and `|`, the name value pairs adjacent to the & operator are taken as if they are in parenthesis by Siebel.

Testing Reconciliation Based on User Type

You can test reconciliation based on the type of user by specifying the following values for the UserType scheduled task attribute:

> **Note:** To run a target system reconciliation of a user of type User, customize the Siebel process form and make the Position field optional.

- `Employee`

  All information about users belonging to the `Employee` type is reconciled.

- `Partner User`

  All information about users belonging to the `Partner User` type is reconciled.

- `Customer`

  All information about users belonging to the `Customer` type is reconciled. These users belonging to the `Customer` type have `NONE` as the value for the Position field.

5.2 Troubleshooting

The following sections list solutions to some commonly encountered errors of the following types:

- Section 5.2.1, "Connection Errors"
- Section 5.2.2, "Create User Errors"

- Section 5.2.3, "Delete User Errors"
- Section 5.2.4, "Edit User Errors"

5.2.1 Connection Errors

The following table lists the solution to a commonly encountered connection error.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the target system. **Returned Error Message:** SIEBEL connection exception	■ Ensure that the target system is running. ■ Ensure that Oracle Identity Manager is working (that is, the database is running). ■ Ensure that all the adapters have been compiled. ■ Examine the Oracle Identity Manager record (from the IT Resources form). Ensure that values for all the IT resource parameters have been correctly specified.

5.2.2 Create User Errors

The following table lists the solution to a commonly encountered Create User error.

Problem Description	Solution
Oracle Identity Manager cannot create a user. **Returned Error Message:** User already exists **Returned Error Code:** `SIEBEL.USER_ALREADY_EXIST`	A user with the assigned ID already exists in the target system.

5.2.3 Delete User Errors

The following table lists the solution to a commonly encountered Delete User error.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist in target system **Returned Error Code:** `SIEBEL.USER_DOES_NOT_EXIST`	The specified user does not exist in the target system.

5.2.4 Edit User Errors

The following table lists the solution to a commonly encountered Edit User error.

Problem Description	Solution
Oracle Identity Manager cannot update a user. **Returned Error Message:** User does not exist in target system **Returned Error Code:** `SIEBEL.USER_DOES_NOT_EXIST`	Review the log for more details.

6

Known Issues

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

- **Bug 7703095**

  During provisioning, if you set a secondary responsibility but do not select a value from the PrimaryResponsibility lookup field, then the secondary responsibility becomes the primary responsibility on the target system.

  During provisioning, if you set the primary responsibility on the process form, then the responsibility is propagated to the child form. However, if you delete the responsibility from the child form, the change is not propagated to the process form. This change is propagated to the process form only after the next reconciliation run with the target system.

- **Bug 7207232**

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

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

- **Bug 8722540**

  The connector does not support the failover feature in which multiple Siebel installations are used to ensure uninterrupted service to users.

- **Bug 12543085**

  If you run a target system reconciliation for users of type **User**, the target system reconciliation task fails.

  As a workaround, customize the process form and make the Position field optional.

The following are limitations of the target system:

- During provisioning, the Set/Reset Password function cannot be run because the target system does not support JDB APIs.

- During reconciliation, a user's password cannot be fetched because the target system does not support JDB APIs.

- The batched reconciliation feature has not been implemented for this connector because the target system does not support JDB APIs.

- During provisioning, the primary position assigned to a user in the target system cannot be removed through Oracle Identity Manager.
- The Lock/Unlock and Disable/Enable functions cannot be run because the target system does not support these functions.
- On the target system, if you delete a position or responsibility assigned to a user, then this change is not fetched into Oracle Identity Manager during the next incremental reconciliation run. This is because the time stamp of the user record is not updated in response to these events.

Index