Oracle® Identity Manager

Connector Guide for Siebel User Management

11.1.1
E20467-26

ORACLE

Oracle Identity Manager Connector Guide for Siebel User Management, 11.1.1

E20467-26

Primary Author: Christina Sekar

Contents

2 Deploying the Connector

3 Using the Connector

List of Figures

List of Tables

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

Related Documents

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

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

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

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

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://download.oracle.com/docs/cd/E22999_01/index.htm

Conventions

The following text conventions are used in this document:

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

What's New in 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 11.1.1.6.0.

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 11.1.1.6.0
- Software Updates in Release 11.1.1.5.0

Software Updates in Release 11.1.1.6.0

The following are issues resolved in this release of the connector:

Bug Number	Issue
16482094	Entitlement, IT resource, Account Name, and Account ID tagging were missing in the process form fields in Oracle Identity Manager 11.1.2.
16483473	When an access policy was created with DNLA flags for the connector, the policy did not work as expected.

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager Connector for Siebel User Management based on Identity Connector Framework (ICF). The following are the software updates in release 11.1.1.5.0:

- Support for Identity Connector Framework
- Support for Deployment Using Connector Server
- Support for Dependent Lookup Fields
- Transformation and Validation of Account Data
- Reconciliation of Deleted User Records

- Independent Scheduled Jobs for User Records and Deleted User Records Reconciliation
- Support for Adding New Siebel Business Objects and Business Components
- Support for Configuring the Connector for Multiple Target System Versions

Support for Identity Connector Framework

The Oracle Identity Manager Connector for Siebel User Management is an ICF-based connector.

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager and Oracle Waveset connectors require. The ICF also uses classpath isolation, which allows the Siebel User Management connector to co-exist with legacy versions of the connector.

See Connector Architecture for more information.

Support for Deployment Using Connector Server

In the earlier releases, the Siebel User Management connector could be deployed in the machine on which Oracle Identity Manager was running. This release onward, you can deploy this connector either locally in Oracle Identity Manager or remotely in the Connector Server.

See the following sections for more information:

- Installing and Configuring the Connector Server
- Running the Connector Server

Support for Dependent Lookup Fields

In earlier releases, if you had multiple installations of the target system, then entries in a lookup definition were not linked with the target system installation from which the entries were copied. During a provisioning operation, you could not select lookup field values that were specific to the target system installation on which the provisioning operation was to be performed.

From this release onward, entries in lookup definitions are linked to the target system installation from which they are copied.

See Lookup Definitions Synchronized with the Target System for more information.

Transformation and Validation of Account Data

You can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. In addition, you can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. See the following sections for more information:

- Configuring Transformation of Data During User Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning

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 Scheduled Job for Reconciliation of Deleted Users Records for more information about scheduled jobs used for reconciling deleted user records.

Independent Scheduled Jobs for User Records and Deleted User Records Reconciliation

In the earlier releases, you had one scheduled task for configuring your connector for user record and deleted user record reconciliation in both the target resource and trusted source mode.

From this release onward, you have independent scheduled jobs as follows:

- Siebel Target User Recon
- Siebel Trusted User Reconciliation
- Siebel Target Resource User Delete Reconciliation
- Siebel Trusted User Delete Reconciliation

See Reconciliation Scheduled Jobs for more information about each of the scheduled jobs.

Support for Adding New Siebel Business Objects and Business Components

Depending upon the requirement in your environment, you can add new Siebel Business Objects and Business Components for reconciliation and provisioning. See the following sections for more information:

- Adding New Siebel Business Objects and Business Components for Reconciliation
- Adding New Siebel Business Objects and Business Components for Provisioning

Support for Configuring the Connector for Multiple Target System Versions

From this release onward, you can configure the connector for target system installations of different versions. See Configuring the Connector for Multiple Versions of the Target System for more information.

Documentation-Specific Updates

The following section discusses documentation-specific updates:

- Documentation-Specific Updates in Release 11.1.1.6.0
- Documentation-Specific Updates in Release 11.1.1.5.0

Documentation-Specific Updates in Release 11.1.1.6.0

The following documentation-specific updates have been made in revision "24" of this guide:

- Incremental Reconciliation Might Fail With Siebel Target System Version 20.*x* has been added to the list of known issues.
- The "Target systems", "Connector Server JDK and JRE", and "External code" row of Table 1-1 and Understanding the JDK Requirement for Siebel IP 2017, Siebel IP 2018, Siebel 19.*x*, or Siebel 20.*x* have been updated to include support for Siebel 20.*x*.

The following documentation-specific update has been made in revision "23" of this guide:

Few editorial changes and minor updates to the document structure have been made for better readability.

The following documentation-specific updates have been made in revision "22" of this guide:

- The "Target systems", "Connector Server JDK and JRE", and "External code" row of Table 1-1 and Understanding the JDK Requirement for Siebel IP 2017, Siebel IP 2018, Siebel 19.*x*, or Siebel 20.*x* have been updated to include support for Siebel 19.*x*.
- The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance 12c (12.2.1.4.0).

The following documentation-specific updates have been made in revision "21" of this guide:

- The "Target systems" row of Table 1-1 has been updated to include support for Siebel Innovation Pack 2017 and 2018.
- A "Note" has been added to the "Connector Server JDK and JRE" row of Table 1-1.
- Understanding the JDK Requirement for Siebel IP 2017, Siebel IP 2018, Siebel 19.*x*, or Siebel 20.*x* has been added.
- Siebel Innovation Pack 2017 and 2018 have been added throughout the document as Siebel target systems along with 2015 and 2016.

The following documentation-specific update has been made in revision "20" of this guide:

The "Oracle Identity Manager" row of Table 1-1 has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12*c* (12.2.1.3.0) certification.

The following documentation-specific updates have been made in revision "19" of this guide:

- The "Target systems" and "External code" rows of Table 1-1 have been updated to include support for Siebel Innovation Pack 2016.
- Updated the support for Siebel Innovation Pack 2016 throughout the document.

The following documentation-specific updates have been made in revision "18" of this guide:

- The "Target systems" and "External code" rows of Table 1-1 have been updated to include support for Siebel Innovation Pack 2015.
- Information regarding Siebel Innovation Pack 2015 has been added to the following sections:
  - Using External Code Files
  - Configuring the Connector for Multiple Versions of the Target System
  - Testing Provisioning Operations

The following documentation-specific updates have been made in revision "17" of this guide:

- The "Connector Server" row has been added to Table 1-1.
- The "JDK and JRE" row of Table 1-1 has been renamed to "Connector Server JDK and JRE".

The following documentation-specific update has been made in revision "16" of this guide:

A "Note" regarding trusted source IT resource has been added at the beginning of Configuring the IT Resource for the Target System.

The following documentation-specific update has been made in revision "15" of this guide:

Postcloning Steps has been added.

The following documentation-specific updates have been made in revision "14" of this guide:

- The "Oracle Identity Manager" row of Table 1-1 has been updated.
- Information specific to Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) has been added to Usage Recommendation.

The following documentation-specific update has been made in revision "13" of this guide:

A "Note" has been added at the beginning of Extending the Functionality of the Connector.

The following documentation-specific update has been made in revision "12" of this guide:

Configuring the Connector to Remove Old Primary Position or Responsibility has been added.

The following documentation-specific updates have been made in revision "11" of this guide:

- Creating and Populating a New Lookup Definition has been added.
- The following sections have been updated:
  - Adding New Attributes for Reconciliation
  - Adding New Attributes for Provisioning
  - Adding New Multivalued Attributes for Reconciliation
  - Adding New Multivalued Attributes for Provisioning

The following documentation-specific updates have been made upto revision "10" of this guide:

- The "Oracle Identity Manager" row in Table 1-1 has been modified.
- A note has been added in the "xml/SiebelConnectorRequestDatasets.xml" row of Table A-1.
- The following sections have been added:
  - Configuring Oracle Identity Manager 11.1.2 or Later
  - Localizing Field Labels in UI Forms
  - Upgrading the Connector from Release 11.1.1.5.0 to 11.1.1.6.0
  - Upgrading the Connector from Release 9.0.4.x to 11.1.1.6.0
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Configuring the IT Resource for the Target System
  - Creating the IT Resource for the Connector Server
  - Configuring Scheduled Jobs
- Known Issues and Workarounds has been revised to include workarounds for some known issues.

Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific updates have been made in the revision "8" of this guide:

- In Certified Components, the certified target system has been updated to Siebel CRM 8.2.2.
- In Known Issues and Workarounds the bug 14756265 has been added.

The following documentation-specific update has been made in the revision "7" of this guide:

In Adding New Siebel Business Objects and Business Components for Reconciliation, and Adding New Siebel Business Objects and Business Components for Provisioning, a note has been included on the support of non-account Siebel object in the connector guide.

The following documentation-specific update has been made in the revision "6" of this guide:

Installation includes connector installation scenarios depending on where you want to run the connector code (bundle), either locally in Oracle Identity Manager or remotely in a Connector Server.

The following documentation-specific updates have been made in the revision "5" of this guide:

- In Configuring the IT Resource for the Target System, the Connector Server Name parameter has been added to Table 2-1.
- The name of the "Known Issues" chapter has been changed to "Known Issues and Limitations." In addition, Known Issues and Workarounds has been restructured.
- In Table 2-1 of Configuring the IT Resource for the Target System, the values that you can set for the "ssoFlag" parameter have been changed to `True/False` from `Yes/No`.
- In Enabling Logging, the logger name has been changed from "OIMCP.SIEBEL" to "ORG.IDENTITYCONNECTORS.SIEBEL."

1

About the Connector

This chapter introduces the Siebel User Management 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 as a managed (target) resource 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.

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 Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) • Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) and any later BP in this release track • Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) and any later BP in this release track
Target systems	The target system can be any one of the following: • Siebel 7.5 through Siebel CRM 8.2.2 • Siebel Innovation Pack 2015 • Siebel Innovation Pack 2016 • Siebel Innovation Pack 2017 • Siebel Innovation Pack 2018 • Siebel 19.*x*, 20.*x*21.*x*, 22.*x*, 23.*x*, 24.*x* **Note:** Siebel Connector needs JDK 1.8 or later as a minimum version to work with Siebel IP 2017, IP 2018, Siebel 19.*x*, and 20.*x* 23.*x*, 24.*x* target systems.
Connector Server	11.1.2.1.0
Connector Server JDK and JRE	This requirement must be as follows: • For deploying the connector: JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later • For deploying the connector server: JDK or JRE 1.5 or later **Note:** If you are using Siebel Innovation Pack 2017, 2018, Siebel 19.*x*, or 20.*x* see Understanding the JDK Requirement for Siebel IP 2017, Siebel IP 2018, Siebel 19.*x*, or Siebel 20.*x* for information related to JDK requirement.
External code	Depending on the target system that you use, obtain one of the following dependent libraries from the target system: • For Siebel 7.5 through 7.7: SiebelJI_Common.jar, SiebelJI_enu.jar, and SiebelJI.jar • For Siebel 7.8 through 8.2.2 and Siebel Innovation Pack 2015, 2016, 2017, 2018, Siebel 19.*x*, and 20.*x*: Siebel.jar and SiebelJI_enu.jar

1.2 Usage Recommendation

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

- If you are using an Oracle Identity Manager release 9.1.0.2 or later and earlier than Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0), then you must use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) or later, Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) or later, or Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.*x* version of this connector.

1.3 Certified Languages

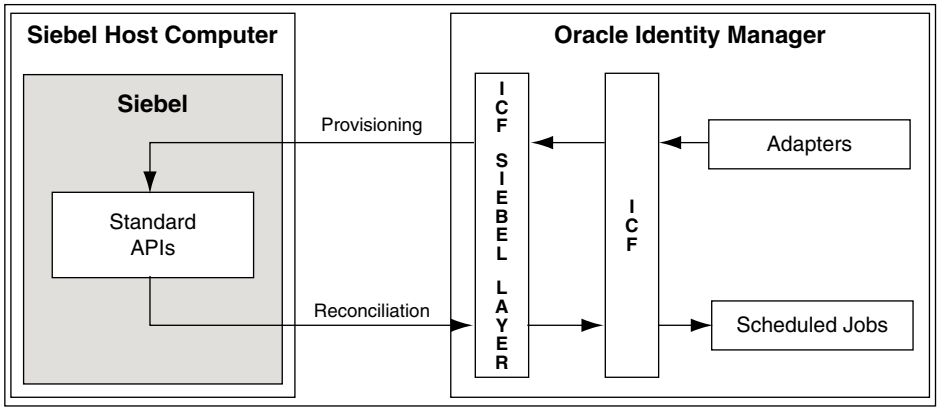
This release of the connector supports the following languages:

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

1.4 Connector Architecture

Figure 1-1 shows the architecture of the connector.

Figure 1-1 Connector Architecture



The Siebel User Management connector is implemented by using the Identity Connector Framework (ICF). The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped along with Oracle Identity Manager. Therefore, you need not configure or modify the ICF.

See Also:

Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about the ICF

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, the target system is used as the trusted source and users are directly created and modified on it.

  During reconciliation, a scheduled job (an instance of the scheduled task) establishes a connection with the target system and sends reconciliation criteria to the APIs. The APIs extract user records that match the reconciliation criteria and hand them over to the scheduled job, which brings the records to Oracle Identity Manager. The next step depends on the mode of connector configuration.

  Each record fetched from the target system is compared with existing OIM Users. If a match is found, then the update made to the record on the target system is copied to the OIM User attributes. If no match is found, then the target system record is used to create an OIM User.

- Account Management

  Account management is also known as target resource management. In the account management mode, the target system is used as a target resource. 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 jobs) and linked with existing OIM Users and provisioned resources.

1.5 Features of the Connector

The following are features of the connector:

- Dependent Lookup Fields
- Full and Incremental Reconciliation
- Limited Reconciliation
- Reconciliation Based on User Type
- Reconciliation of Deleted User Records
- Transformation and Validation of Account Data
- Support for Connector Server
- Connection Pooling
- Support for Enabling and Disabling Accounts

1.5.1 Dependent Lookup Fields

If you have multiple installations of the target system, the entries in lookup definitions (used as an input source for lookup fields during provisioning) can be linked to the target system installation from which they are copied. Therefore, during a provisioning operation, you can select lookup field values that are specific to the target system installation on which the provisioning operation is being performed.

See Lookup Definitions Synchronized with the Target System for more information about the format in which data is stored in dependent lookup definitions.

1.5.2 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, incremental reconciliation is automatically enabled. In incremental reconciliation, user accounts that have been added, modified, or deleted since the last reconciliation run are fetched into Oracle Identity Manager.

You can perform a full reconciliation run at any time.

See Performing Full Reconciliation for more information.

1.5.3 Limited Reconciliation

You can set a reconciliation filter as the value of the Custom Recon Query attribute of the user reconciliation scheduled job. This filter specifies the subset of added and modified target system records that must be reconciled.

See Performing Limited Reconciliation for more information.

1.5.4 Reconciliation Based on User Type

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

See Reconciliation Based on User Type for more information.

1.5.5 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 Scheduled Job for Reconciliation of Deleted Users Records for more information about scheduled jobs used for reconciling deleted user records.

1.5.6 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

- Configuring Transformation of Data During User Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning

1.5.7 Support for Connector Server

Connector Server is a component provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles. In other words, a connector server enables remote execution of an Oracle Identity Manager connector.

A Java connector server is useful when you do not wish to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements.

1.5.8 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

Setting up the Lookup.Configuration.Siebel Lookup Definition for Connection Pooling provides information about connection pooling.

1.5.9 Support for Enabling and Disabling Accounts

Enabling User accounts from Oracle Identity Governance makes the Console and Programmatic Access active in the target system if the `enableProgrammaticAccess` configuration parameter is set to true. Only the Console access is active if the configuration parameter is set to false.

Disabling user accounts from Oracle Identity Governance makes the Console access and Programmatic Access deactivated in the target system irrespective of the `enableProgrammaticAccess` configuration parameter value. This disables user accounts in Oracle Identity Governance thereby prohibiting them from performing any operation.

Enabling and disabling Oracle Identity Governance account status during reconciliation operation:

Oracle Identity Governance account status is disabled if both the Console access and Programmatic access are deactivated in the target. If either Console access or Programmatic access is activated, Oracle Identity Governance account status is enabled.

1.6 Lookup Definitions Used During Reconciliation and Provisioning

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

- Lookup Definitions Synchronized with the Target System
- Preconfigured Lookup Definitions

1.6.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Responsibility lookup field to select a responsibility to be assigned to the user from the list of available responsibilities. When you deploy the connector, lookup definitions (with no lookup entries) corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

The following lookup definitions are populated with values fetched from the target system by the scheduled jobs for lookup field synchronization:

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

The Siebel Lookup Recon scheduled job is used to synchronize values of these lookup definitions with the target system. While configuring the Siebel Lookup Recon scheduled job, you specify the name of the lookup definition that you want to synchronize as the value of the Lookup Definition Name attribute. See Scheduled Job for Lookup Field Synchronization for more information about this scheduled job.

After lookup definition synchronization, data is stored in the following format:

- Code Key format: *IT_RESOURCE_KEY~LOOKUP_FIELD_ID_OR_NAME*

  In this format:

  – *IT_RESOURCE_KEY* is the numeric code assigned to the IT resource in Oracle Identity Manager.

  – *LOOKUP_FIELD_ID_OR_NAME* is the target system code or name assigned to the lookup field entry.

  Sample value: `1~AHA CEO`

- Decode format: *IT_RESOURCE_NAME~LOOKUP_FIELD_ENTRY*

  In this format:

  – *IT_RESOURCE_NAME* is the name of the IT resource in Oracle Identity Manager.

– *LOOKUP_FIELD_ENTRY* is the value or description of the lookup field entry on the target system.

Sample value: `SIEBEL IT Resource~AHA Headquarter`

While performing a provisioning operation on the Administrative and User Console, you select the IT resource for the target system on which you want to perform the operation. When you perform this action, the lookup definitions on the page are automatically populated with values corresponding to the IT resource (target system installation) that you select. If your environment has multiple installations of the target system then only values that correspond to the IT resource that you select are displayed. During lookup field synchronization, new entries are appended to the existing set of entries in the lookup definitions. You can switch between multiple installations of the same target system. Because the IT resource key is part of each entry created in each lookup definition, only lookup field entries that are specific to the IT resource you select during a provisioning operation are displayed.

1.6.2 Preconfigured Lookup Definitions

This section discusses 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. The other lookup definitions are as follows:

- Lookup.Configuration.Siebel
- Lookup.Siebel.UM.Configuration
- Lookup.Siebel.UM.ReconAttrMap
- Lookup.Siebel.UM.ProvAttrMap

1.6.2.1 Lookup.Configuration.Siebel

The Lookup.Configuration.Siebel lookup definition holds connector configuration entries that are used during reconciliation and provisioning operations.

Table 1-2 lists the default entries in this lookup definition.

Table 1-2 Entries in the Lookup.Configuration.Siebel Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.siebel	This entry holds the name of the connector bundle package. Do not modify this entry.
Bundle Version	1.0.1	This entry holds the version of the connector bundle class. Do not modify this entry.
Connector Name	org.identityconnectors.siebel.SiebelConnector	This entry holds the name of the connector class. Do not modify this entry.
User Configuration Lookup	Lookup.Siebel.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do not modify this entry.

1.6.2.2 Lookup.Siebel.UM.Configuration

As discussed earlier, the Lookup.Siebel.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations.

Table 1-3 lists the default entries in this lookup definition.

Table 1-3 Entries in the Lookup.Siebel.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.Siebel.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.Siebel.UM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.Siebel.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.Siebel.UM.ReconAttrMap for more information about this lookup definition.
Provisioning Validation Lookup	Lookup.Siebel.UM.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.
Recon Validation Lookup	Lookup.Siebel.UM.ReconValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.
Recon Transformation Lookup	Lookup.Siebel.UM.ReconTransformation	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During User Reconciliation for more information about adding entries in this lookup definition.

1.6.2.3 Lookup.Siebel.UM.ReconAttrMap

The Lookup.Siebel.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definitions is used during reconciliation. This lookup definition is preconfigured. Table 1-4 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Connector for more information.

1.6.2.4 Lookup.Siebel.UM.ProvAttrMap

The Lookup.Siebel.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definitions is used during provisioning. This lookup definition is preconfigured. #unique_96/unique_96_Connect_42_CEGBCDDJ lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Connector for more information.

1.7 Connector Objects Used During Target Resource Reconciliation

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for conceptual information about reconciliation

This section discusses the following topics:

- User Attributes for Reconciliation
- Reconciliation Rule for Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation

1.7.1 User Attributes for Reconciliation

The Lookup.Siebel.UM.ReconAttrMap lookup definition maps resource object fields and target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, the Code Key contains the reconciliation attribute of the resource object.

The following is the format of the Code Key and Decode values in this lookup definition:

For single-valued attributes:

- **Code Key:** Reconciliation attribute of the resource object
- **Decode:** *ATTRIBUTE_TYPE*;*ATTRIBUTE_NAME*

  In this format:

  – *ATTRIBUTE_TYPE* specifies the type of attribute being reconciled. This connector supports reconciliation of both user and employee attributes. Therefore, the value of *ATTRIBUTE_TYPE* can be `Employee`, `User`, or `common`. Here, `common` specifies that the attribute being reconciled is both a user and employee attribute.

  – *ATTRIBUTE_NAME* specifies the name of the target system attribute.

For multivalued attributes (position and responsibility):

- **Code Key:** *RO_ATTR_NAME~CHILD_RO_ATTR_NAME*

  In this format, *RO_ ATTR_NAME* specifies the reconciliation field of the parent resource object. *CHILD_RO_ATTR_NAME* specifies the reconciliation field on the child resource object.

- **Decode:** Combination of the following elements separated by semicolon (;):

  ATTRIBUTE_TYPE;*OBJECT_CLASS*;*ATTRIBUTE_NAME*;*TRUE_OR_FALSE*

  In this format:

  – *ATTRIBUTE_TYPE* specifies the type of attribute being reconciled. This connector supports reconciliation of both user and employee attributes. Therefore, the value of

ATTRIBUTE_TYPE can be `Employee`, `User`, or `common`. Here, `common` specifies that the attribute being reconciled is both a user and employee attribute.

- *OBJECT_CLASS* is the name of the object class in which the attribute is stored. In other words, it is the business component name.
- *ATTRIBUTE_NAME* is the name of the attribute.
- *TRUE_OR_FALSE* is used to indicate whether the attribute is primary or secondary. For example, a value of `true` indicates that the attribute is a primary attribute. A value of `False` indicates that the attribute is a secondary attribute.

Table 1-4 lists the entries in this lookup definition.

Table 1-4 Entries in the Lookup.Siebel.UM.ReconAttrMap Lookup Definition

Resource Object Field (Code Key)	Target System Attribute (Decode)
Single-Valued Fields	
Alias	common;Alias
Email	common;EMail Addr
EmployeeType[Lookup]	Employee;Employee Type Code
Extension	Employee;Work Phone Extension
Fax	common;Fax #
FirstName	common;First Name
HomePhone	common;Home Phone #
JobTitle	common;Job Title
LastName	common;Last Name
MiddleName	common;Middle Name
MPosition[Lookup]	Employee; Position;Name;true
PreferredCommunications[Lookup]	common;Preferred Communications
Primary Responsibility[Lookup]	common;Responsibility;Name;true
Status[WRITEBACK]	common;Responsibility;Name;true[WRITEBACK]
Title[Lookup]	common;Personal Title
User ID	common;Login Name
WorkPhone	common;Phone #
Multivalued Fields	
Position~Position[Lookup]	Employee; Position;Name;false
Responsibility~Responsibility[Lookup]	common;Responsibility;Name;false

1.7.2 Reconciliation Rule for Target Resource Reconciliation

Learn about the reconciliation rule for this connector and how to view it.

- Target Resource Reconciliation Rule
- Viewing Target Resource Reconciliation Rules in the Design Console

> **See Also:**
>
> Reconciliation Engine in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for generic information about reconciliation matching and action rules

1.7.2.1 Target Resource Reconciliation Rule

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.

1.7.2.2 Viewing Target Resource Reconciliation Rules in the Design Console

You can view the reconciliation rule for 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**.

1.7.3 Reconciliation Action Rules for Target Resource Reconciliation

Learn about the reconciliation action rules for this connector and how to view them.

> **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
>
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using Java)
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using .net)
>
> in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about setting a reconciliation action rule.

- Target Resource Reconciliation Action Rules
- Viewing Target Resource Reconciliation Action Rules in the Design Console

1.7.3.1 Target Resource Reconciliation Action Rules

Table 1-5 lists the action rules for Target Resource reconciliation.

Table 1-5 Action Rules for Target Resource Reconciliation

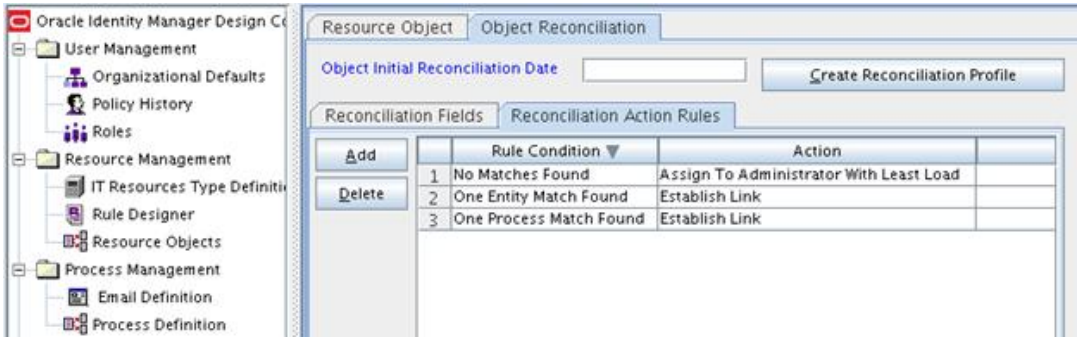
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.7.3.2 Viewing Target Resource Reconciliation Action Rules in the Design Console

You can view the reconciliation rule for reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects.**
3. If you want to view the reconciliation action rules for reconciliation, then search for and open the **Siebel Resource Object** resource object.
4. 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 1-2 shows the reconciliation action rules for target resource reconciliation.

Figure 1-2 Target Resource Reconciliation Action Rules



1.8 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

This section discusses the following topics:

- Provisioning Functions
- User Attributes for Provisioning

> **See Also:**
>
> Managing Provisioning Tasks in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for conceptual information about provisioning

1.8.1 Provisioning Functions

These are the provisioning functions that the connector supports.

Table 1-6 Provisioning Functions

Function	Adapter
Create User	Siebel Create
Delete User	Siebel Delete
Add User Position	Siebel Update Child Table
Add User Responsibility	Siebel Update Child Table
Delete User Position	Siebel Update Child Table
Delete User Responsibility	Siebel Update Child Table
Primary Position Updated	Siebel Update
Primary Responsibility Updated	Siebel Update
Time Zone Updated	Siebel Update
Email Updated	Siebel Update
Alias Updated	Siebel Update
MI Updated	Siebel Update
Work Phone Updated	Siebel Update
First Name Updated	Siebel Update
Last Name Updated	Siebel Update
Title Updated	Siebel Update
Home Phone Updated	Siebel Update
Fax Updated	Siebel Update
Preferred Communications Updated	Siebel Update
Extension Updated	Siebel Update
Employee Type Updated	Siebel Update
Job Title Updated	Siebel Update
User ID Updated	Siebel Update
Child Position Updated	Siebel Update Child Table
Child Responsibility Updated	Siebel Update Child Table

1.8.2 User Attributes for Provisioning

The Lookup.Siebel.UM.ProvAttrMap lookup definition maps process form fields with target system attributes. This lookup definition is used for performing provisioning operations.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code Key:** Name of the field on the OIM User form in the Administrative and User Console. In other words, the process form field name.
- **Decode:** *ATTRIBUTE_TYPE*;*ATTRIBUTE_NAME*

  In this format:

  – *ATTRIBUTE_TYPE* specifies the type of attribute being reconciled. This connector supports reconciliation of both user and employee attributes. Therefore, the value of *ATTRIBUTE_TYPE* can be `Employee`, `User`, or `common`. Here, `common` specifies that the attribute being reconciled is both a user and employee attribute.

  – *ATTRIBUTE_NAME* specifies the name of the target system attribute.

For entries corresponding to process form fields on child forms, the following is the format of the Code Key and Decode values:

- **Code Key:** *CHILD_FORM_NAME~FIELD_NAME*

  In this format, *CHILD_FORM_NAME* specifies the name of the child form. *FIELD_NAME* specifies the name of the field on the OIM User child form in the Administrative and User Console.

- **Decode:** Combination of the following elements separated by semicolon (;):

  ATTRIBUTE_TYPE;*OBJECT_CLASS*;*ATTRIBUTE_NAME*;*TRUE_OR_FALSE*

  In this format:

  – *ATTRIBUTE_TYPE* specifies the type of attribute being reconciled. This connector supports reconciliation of both user and employee attributes. Therefore, the value of *ATTRIBUTE_TYPE* can be `Employee`, `User`, or `common`. Here, `common` specifies that the attribute being reconciled is both a user and employee attribute.

  – *OBJECT_CLASS* is the name of the object class in which the attribute is stored. In other words, it is the business component name.

  – *ATTRIBUTE_NAME* is the name of the attribute.

  – *TRUE_OR_FALSE* is used to indicate whether the attribute is primary or secondary. For example, a value of `true` indicates that the attribute is a primary attribute. A value of `False` indicates that the attribute is a secondary attribute.

1.9 Connector Objects Used During Trusted Source Reconciliation

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

- User Attributes for Trusted Source Reconciliation
- Reconciliation Rule for Trusted Source Reconciliation
- Reconciliation Action Rules for Trusted Source Reconciliation

1.9.1 User Attributes for Trusted Source Reconciliation

Table 1-7 lists user attributes for trusted source reconciliation.

Table 1-7 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.

1.9.2 Reconciliation Rule for Trusted Source Reconciliation

Learn about the reconciliation rule for trusted source reconciliation and how to view it.

- Trusted Source Reconciliation Rule
- Viewing Trusted Source Reconciliation Rule

1.9.2.1 Trusted Source Reconciliation Rule

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.

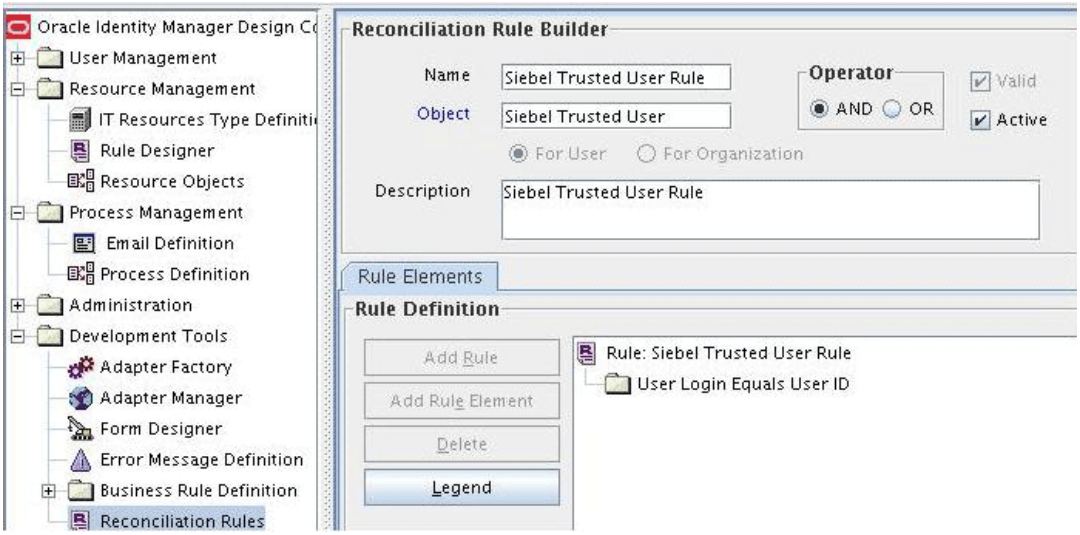
1.9.2.2 Viewing Trusted Source Reconciliation Rule

You can view the reconciliation rule for trusted 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 Trusted User Rule**. Figure 1-3 shows the reconciliation rule for trusted source reconciliation.

Figure 1-3 Reconciliation Rule for Trusted Source Reconciliation



1.9.3 Reconciliation Action Rules for Trusted Source Reconciliation

Learn about the reconciliation action rules for trusted source reconciliation and how to view them.

- Trusted Source Reconciliation Action Rules
- Viewing Trusted Source Reconciliation Action Rules

1.9.3.1 Trusted Source Reconciliation Action Rules

Table 1-8 lists the action rules for trusted source reconciliation.

Table 1-8 Action Rules for Trusted Source Reconciliation

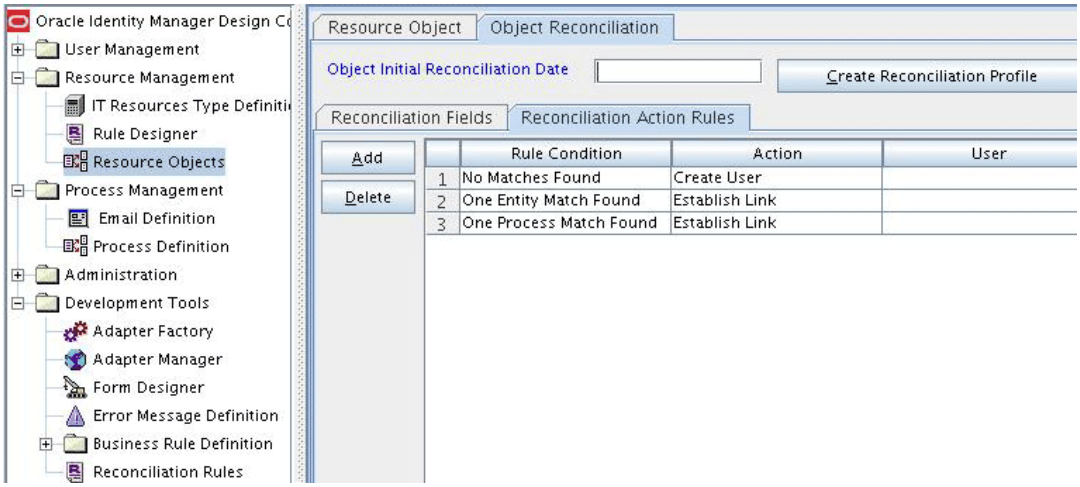
Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.9.3.2 Viewing Trusted Source 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 **Siebel Trusted 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 1-4 shows the reconciliation action rule for trusted source reconciliation.

Figure 1-4 Reconciliation Action Rules for Trusted Source Reconciliation



2
Deploying the Connector

The procedure to deploy the connector can be divided into these stages.

- Preinstallation
- Installation
- Postinstallation
- Upgrading the Connector
- Postcloning Steps

2.1 Preinstallation

Preinstallation involves performing procedures such as copying external code files on Oracle Identity Manager, creating a target system user account for performing connector operations, installing and running the Connector Server, and so on.

- Prerequisites to be done in Siebel Target to Use the Enable/Disable Feature in the Connector
- Using External Code Files
- Understanding the JDK Requirement for Siebel IP 2017, Siebel IP 2018, Siebel 19.*x*, or Siebel 20.*x*
- Creating the Target System User Account for Connector Operations
- Additional Configuration Steps and Guidelines for the Target System
- Installing and Configuring the Connector Server
- Running the Connector Server

2.1.1 Prerequisites to be done in Siebel Target to Use the Enable/Disable Feature in the Connector

You can add the **User Status** attribute in target by following either of the following steps:

- Manually Making Configuration Changes
- Importing SIF File

2.1.1.1 Manually Making Configuration Changes

Perform the followings tasks to manually make the configuration changes:

1. Login to Siebel Web Tools.
2. Create Workspace.
   a. Click Workspace dashboard button next to the option **Main**.
   b. Click **Create** button on top.

c. Enter the name for your Workspace and provide comments and create the workspace. The workspace is now available under **Main**.

3. Close the window.
4. Open the newly created workspace and locate the **Employee BusComp** as follows.
   a. Under **Type**, select **Expand Business Component**, and click **Field**.
   b. In the **Business Component** drop-down, select **Name** and search for the employee.
   c. In the **Fields** option, add a new field with the following attributes:

Attribute	Value
Name	User Status
Join	S_USER
Column	STATUS_CD
Picklist	User Status Picklist
Text Length	30
Type	DTYPE_TEXT

5. Create a child Pick Map for this field as follows:
   a. Expand the option **Field** under **Business component** and select **Pick Map**
   b. Add the following attributes under **Pick Map**.

Attribute	Value
Field	User Status
Picklist Field	Value

6. Navigate to the Employee List Applet as follows.
   a. Expand Applet, and select **List**.
   b. Under **Applet** drop-down list, select **Name** and search for Employee List.
7. Go to **List Column** under List and add a new list column with the following attributes:

Attribute	Value
Name	User Status
Field	User Status
Available	TRUE
Display Name – String Reference	SBL_USER_STATUS-1004233658-7EI
Display Name	User Status
HTML Display Mode	EncodeData
HTML List Edit	TRUE
HTML Row Sensitive	TRUE
HTML Type	Field
Runtime	TRUE
Text Alignment	Left
Show in List	TRUE
Text Alignment-Label	Left

8. For the same applet, choose the **Edit List Applet Web Template** to add the newly created list column to any empty placeholder in the list as follows:

a. Expand Applet and select **Applet Web Template**.

b. Under **Applet Web Template**, choose an empty place holder in **Edit List** and select Edit.

c. Click **Controls/Columns**, and deselect the option *show unmapped controls only* and select **User Status**

9. Unit test the changes:

a. Open the Siebel Call Center to **Open** and **Inspect** the workspace for ensuring that the newly added column **User Status** appears in the user interface to change from **Active** to **Inactive** and oppositely.

b. Change the status to **Inactive** for different known users.

c. Log out.

d. Try to log in as other user.

> **Note:**
>
> This test should fail.

10. Deliver the workspace.

a. Login to Siebel Web Tools.

b. Click Workspace dashboard button and select your workspace and then click **Open**.

c. Click **Version** to provide the comments and create the version.

d. Click **Submit** and submit the delivery in the pop-up window.

e. Click **Deliver** to provide the comments and deliver the workspace.

2.1.1.2 Importing SIF File

This approach allows a customer developer to make the changes (without the manual modifications described above) through the import of an archive file (SIF) containing the repository changes.

Perform the following steps:

1. In Siebel Web Tools, create a **Developer Workspace** under a upcoming release branch (Integration Workspace).

a. Click Workspace dashboard option next to **Main**.

b. Click **Create.**

c. Enter the name of your Workspace and provide comments to create the workspace. The workspace is now visible under Main.

d. Open the newly created workspace.

2. Select **Archive** > **Import from Archive** menu item.

3. Follow the wizard to import the file.

4. Checkpoint and submit the workspace for delivery, rebasing if necessary.

5. Deliver the workspace as follows:

a. Click the Workspace dashboard option and select your workspace then click **Open**.

b. Click **Version** to provide your comments and create the version.

c. Click **Submit** and submit for delivery in the pop-up window.

d. Click **Deliver** to provide the comments and deliver the workspace.

6. Test the changes as follows:

a. Open the Siebel Call Center and click **Open** to inspect the workspace for ensuring that the newly added column is visible under **User Status** in the user interface and can be changed from **Active** to **Inactive** and the opposite.

b. Change the status to **Inactive** for different known users.

c. Log out.

d. Try to log in as other user.

> **Note:**
>
> This test should fail.

2.1.2 Using External Code Files

Depending on the target system version that you are using, copy these external code files.

> **Note:**
>
> If a particular directory does not exist on the Oracle Identity Manager host computer, then create it.

- For Siebel 7.5 through 7.7

  Copy the following files from the *SIEBEL_INSTALLATION_DIRECTORY*/siebsrvr/CLASSES directory into the *OIM_HOME*/ConnectorDefaultDirectory/targetsystems-lib/siebel-***RELEASE_NUMBER*** directory:

  – SiebelJI.jar

  – SiebelJI_Common.jar

  – SiebelJI_enu.jar

- For Siebel 7.8 through 8.2.2 and Siebel Innovation Pack 2015, 2016, 2017, 2018, and Siebel 19.*x*

  Copy the following files from the *SIEBEL_INSTALLATION_DIRECTORY*/siebsrvr/CLASSES directory into the *OIM_HOME*/ConnectorDefaultDirectory/targetsystems-lib/siebel-***RELEASE_NUMBER*** directory:

  – Siebel.jar

  – SiebelJI_enu.jar

2.1.3 Understanding the JDK Requirement for Siebel IP 2017, Siebel IP 2018, Siebel 19.*x*, or Siebel 20.*x*

If you are using Siebel IP 2017, Siebel IP 2018, Siebel 19.*x*, or 20.*x* then the following is the JDK requirement:

- If you are already using a Connector Server, then it is mandatory to use JDK 1.8 as the minimum version in the Connector Server.
- If the you are not using a Connector Server and Oracle Identity Manager is not using JDK 1.8, then follow one of the following steps:
  - Refer the Oracle Identity Manager certification matrix and upgrade the JDK version used by Oracle Identity Manager to JDK 1.8 if it is supported.
  - If JDK 1.8 is not supported for Oracle Identity Manager, then it is mandatory to use a Connector Server with JDK 1.8 as a minimum. In addition, enter the name of this Connector Server as the value of the Connector Server name parameter of the IT resource.

2.1.4 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.

2.1.5 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
```

2.1.6 Installing and Configuring the Connector Server

You can deploy the Siebel User Management connector either locally in Oracle Identity Manager or remotely in the Connector Server. A *connector server* is a Microsoft Windows application that enables remote execution of an Identity Connector, such as the Microsoft Active Directory User Management connector.

Connector servers are available in two implementations:

- As a .Net implementation that is used by Identity Connectors implemented in .Net
- As a Java Connector Server implementation that is used by Java-based Identity Connectors

The Siebel User Management connector is implemented in Java, so you can deploy this connector to a Java Connector Server.

Use the following steps to install and configure the Java Connector Server:

> **Note:**
>
> Before you deploy the Java Connector Server, ensure that you install the JDK or JRE on the same computer where you are installing the Java Connector Server and that your *JAVA_HOME* or *JRE_HOME* environment variable points to this installation.

1. Create a new directory on the computer where you want to install the Java Connector Server.

   > **Note:**
   >
   > In this guide, *CONNECTOR_SERVER_HOME* represents this directory.

2. Unzip the Java Connector Server package in the new directory created in Step 1. You can download the Java Connector Server package from the Oracle Technology Network.
3. Open the ConnectorServer.properties file located in the `conf` directory. In the ConnectorServer.properties file, set the following properties, as required by your deployment.

Property	Description
connectorserver.port	Port on which the Java Connector Server listens for requests. Default is `8759`.
connectorserver.bundleDir	Directory where the connector bundles are deployed. Default is `bundles`.
connectorserver.libDir	Directory in which to place dependent libraries. Default is `lib`.

Property	Description
connectorserver.usessl	If set to **`true`**, the Java Connector Server uses SSL for secure communication. Default is `false`. If you specify **`true`**, use the following options on the command line when you start the Java Connector Server: • `-Djavax.net.ssl.keyStore` • `-Djavax.net.ssl.keyStoreType` (*optional*) • `-Djavax.net.ssl.keyStorePassword`
connectorserver.ifaddress	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the computer.
connectorserver.key	Java Connector Server key.

4. Set the properties in the ConnectorServer.properties file, as follows:
   - To set the connectorserver.key, run the Java Connector Server with the `/setKey` option.

     > **Note:**
     >
     > For more information, see Running the Connector Server.

   - For all other properties, edit the ConnectorServer.properties file manually.
5. The conf directory also contains the logging.properties file, which you can edit if required by your deployment.

> **Note:**
>
> Oracle Identity Manager has no built-in support for connector servers, so you cannot test your configuration.

2.1.7 Running the Connector Server

To run the Java Connector Server, use the ConnectorServer.bat script as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Installing and Configuring the Connector Server.
2. Change to the *CONNECTOR_SERVER_HOME*\bin directory and find the ConnectorServer.bat script.

   The ConnectorServer.bat supports the following options:

Option	Description
`/install [`*`serviceName`*`]` `["-J `*`java-option`*`"]`	Installs the Java Connector Server as a Windows service. Optionally, you can specify a service name and Java options. If you do not specify a service name, the default name is `ConnectorServerJava`.

Option	Description
`/run ["-J java-option"]`	Runs the Java Connector Server from the console. Optionally, you can specify Java options. For example, to run the Java Connector Server with SSL: `ConnectorServer.bat /run "-J-Djavax.net.ssl.keyStore=mykeystore.jks" "-J-Djavax.net.ssl.keyStorePassword=password"`
`/setKey [key]`	Sets the Java Connector Server key. The `ConnectorServer.bat` script stores the hashed value of the key in the `connectorserver.key` property in the `ConnectorServer.properties` file.
`/uninstall [serviceName]`	Uninstalls the Java Connector Server. If you do not specify a service name, the script uninstalls the `ConnectorServerJava` service.

3. If you need to stop the Java Connector Server, stop the respective Windows service.

2.2 Installation

Depending on where you want to run the connector code (bundle), the connector provides these installation options.

- Run the connector code locally in Oracle Identity Manager.

  In this scenario, you deploy the connector in Oracle Identity Manager.

- Run the connector code remotely in a Connector Server.

  In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing, configuring, and running the Connector Server.

To deploy the connector in Oracle Identity Manager, perform the following procedures:

- Running the Connector Installer
- Configuring the IT Resource for the Target System

2.2.1 Running the Connector Installer

When you run the Connector Installer, it automatically copies the connector files to directories in Oracle Identity Manager, imports connector XML files, and compiles adapters used for provisioning.

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

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.

OIM_HOME/server/ConnectorDefaultDirectory

2. If you are using Oracle Identity Manager release 11.1.1, then:
   a. Log in to the Administrative and User Console.
   b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector.**
3. If you are using Oracle Identity Manager release 11.1.2.*x*, then:
   a. Log in to Oracle Identity System Administration.
   b. In the left pane, under System Management, click **Manage Connector.**
4. In the Manage Connector page, click **Install.**
5. 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 **Siebel Connector *RELEASE_NUMBER.***
6. Click **Load**.
7. 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.
8. 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 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

   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 A-1.

2.2.2 Configuring the IT Resource for the Target System

> **Note:**
>
> If you have configured your target system as a trusted source, then create an IT resource of type **Siebel.** For example, Siebel Trusted. The parameters of this IT resource are the same as the parameters of the IT resources described in Table 2-1 of this section. See Creating IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about creating an IT resource.

The IT resource for the target system is created during connector installation. This IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

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

1. If you are using Oracle Identity Manager release 11.1.1, then:
   a. Log in to the Administrative and User Console
   b. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
2. If you are using Oracle Identity Manager release 11.1.2.*x,* then Log in to Oracle Identity System Administration, and then in the left pane under Configuration, click **IT Resource.**
3. In the IT Resource Name field on the Manage IT Resource page, enter `SIEBEL IT Resource` and then click **Search**.
4. Click the edit icon for the IT resource.

5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource. Table 2-1 describes each parameter.

Table 2-1 Parameters of the IT Resource for the Target System

Parameter	Description
Configuration Lookup	Name of the lookup definition that holds connector configuration entries used during reconciliation and provisioning If you have configured your target system as a target resource, then the default value is `Lookup.Configuration.Siebel`. If you have configured your target system as a trusted source, then the default value is `Lookup.Configuration.Siebel.Trusted`.
Connector Server Name	Name of the IT resource of the type "Connector Server." You create an IT resource for the Connector Server in Creating the IT Resource for the Connector Server. **Note:** Enter a value for this parameter *only* if you have deployed the Siebel User Management connector in the Connector Server.
enterpriseServer	Name of the Enterprise server An Enterprise is a logical collection of Siebel servers that access a single database server and file system. Sample value: `siebel`
gatewayServer	Name of the Gateway server A Gateway server is a Windows service or UNIX daemon process that stores component definitions and assignments, operational parameters, and connectivity information. Sample value: `SBA_SIEBEL`
gatewayServerPort	Listening port number for Siebel Connection Broker (SCBroker). Sample value : `2321`
Language	Language in which the text on UI is displayed 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 2-1 (Cont.) Parameters of the IT Resource for the Target System

Parameter	Description
objectManager	Name of the object manager You can specify any one of the following: 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 Sample value: `sadmin` See Creating the Target System User Account for Connector Operations for more information.
siebelServer	Name of the target system server Sample value: `SBA_SIEBEL`
userName	User ID of the target system user account that you want to use for connector operations Sample value: `SADMIN` See Creating the Target System User Account for Connector Operations for more information.
encryption	Type of encryption for secure communication If encryption is required, then specify `RSA`. Otherwise, specify `None`. **Note:** The value of this parameter is case-sensitive. Default value: `None`
version	Version of the target system supported by this connector Sample value: `15.5` **Note:** If the target system version that you are using is Siebel 7.5.*x* or 7.5.*x*.*x* then enter `7.5` only as the value of this parameter. For example, if you are using Siebel 7.5.3.7 as the target system, then enter `7.5`.
ssoFlag	Enter `True` to specify that the target system is configured to use a SSO solution for authentication. Otherwise, enter `False`. Default value: `False`
employeeBusObj	Business Object of Employee userType Default value: `Employee`
employeeBusComp	Business Component of Employee userType Default value: `Employee`
userBusObj	Business Object of the 'User' userType Default value: `Users`

Table 2-1 (Cont.) Parameters of the IT Resource for the Target System

Parameter	Description
userBusComp	Business Component of 'User' userType Default value: `User`
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`.
keyFieldName	Enter the search attribute in the Siebel Business Component that must be treated as the unique identifier for an account. The format of this parameter is as follows: *ATTRIBUTE_TYPE*;*ATTRIBUTE_NAME* Default Value: `common;Login Name`

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

2.3 Postinstallation

Postinstallation involves performing certain procedures such as configuring Oracle Identity Manager, creating the IT resource for the Connector Server, enabling logging, localizing field labels, and so on.

The following sections discuss postinstallation procedures:

- Configuring Oracle Identity Manager 11.1.2 or Later
- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Managing Logging
- Adding the Dependent (LDAP Connector) Resource Object for Provisioning
- Configuring Oracle Identity Manager for Request-Based Provisioning
- Setting up the Lookup.Configuration.Siebel Lookup Definition for Connection Pooling
- Configuring the Target System
- Creating the IT Resource for the Connector Server
- Localizing Field Labels in UI Forms

2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

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

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

2.3.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes.** The Manage Sandboxes page is displayed.
2. On the toolbar, click **Create Sandbox.** The Create Sandbox dialog box is displayed.
3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.
5. Click **Save and Close.** A message is displayed with the sandbox name and creation label.
6. Click **OK.** The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. Select the sandbox that you created.
8. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
9. On the toolbar, click **Activate Sandbox.**

   The sandbox is activated.

2.3.1.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see Managing Forms in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer.**
2. Under Search Results, click **Create.**
3. Select the resource type for which you want to create the form, for example, `Siebel UM`.
4. Enter a form name and click **Create.**

2.3.1.3 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see Managing Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances.**
2. Under Search Results, click **Create.**
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save.**
4. In the Form drop-down list, select the newly created form and click **Apply.**
5. Publish the application instance for a particular organization.

2.3.1.4 Publishing a Sandbox

To publish the sandbox that you created in Creating and Activating a Sandbox:

1. Close all the open tabs and pages.

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

2.3.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Job for Lookup Field Synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.3.1.6 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in Creating and Activating a Sandbox.
2. Create a new UI form for the resource as described in Creating a New UI Form.
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in Publishing a Sandbox.

2.3.2 Changing to the Required Input Locale

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

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.

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. 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, 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:
>
> *OIM_HOME*/server/bin/*SCRIPT_FILE_NAME*

2. Enter the following command:

> **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
> ```

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.

2.3.4 Managing Logging

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

2.3.4.1 Understanding Log Levels

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

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

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

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

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

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

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

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

2.3.4.2 Enabling Logging

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="ORG.IDENTITYCONNECTORS.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 2-2 lists the supported message type and level combinations.

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

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

```
<log_handler name='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\oim_ser
ver1\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="ORG.IDENTITYCONNECTORS.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.

2.3.5 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.

2.3.6 Configuring Oracle Identity Manager for 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.

> **Note:**
>
> Perform this procedure only if you are using Oracle Identity Manager release prior to 11.1.2. The direct provisioning feature of the connector is automatically disabled when you enable request-based provisioning. Therefore, do not enable request-based provisioning if you want to use the direct provisioning.

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

- Copying Predefined Request Datasets
- Importing Request Datasets
- Enabling the Auto Save Form Feature
- Running the PurgeCache Utility

2.3.6.1 Copying Predefined Request Datasets

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

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\Siebel

> **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.

2.3.6.2 Importing Request Datasets

There are two ways of importing request datasets:

- Importing Request Datasets Using MDS Import Utility
- Importing Request Datasets Using Deployment Manager

> **Note:**
>
> Request Datasets imported either into MDS or by using Deployment Manager are same.

2.3.6.2.1 Importing Request Datasets Using MDS Import Utility

All request datasets must be imported into the metadata store (MDS), which can be done 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.

   > **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 Copying Predefined Request Datasets, if you copy the files to the E:\MyDatasets\custom\connector\RACFStd 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 at the following location:

/custom/connector/*RESOURCE_NAME*

2.3.6.2.2 Importing Request Datasets Using Deployment Manager

The request datasets (predefined or generated) can also be imported by using the Deployment Manager (DM). The predefined request datasets are stored in the xml/SiebelConnectorRequestDatasets.xml on the installation media.

To import a request dataset definition by using the Deployment Manager:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. 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 SiebelConnectorRequestDatasets.xml file, which is located 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. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

The request datasets are imported into MDS.

2.3.6.3 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.

2.3.6.4 Running the PurgeCache Utility

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

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

2.3.7 Setting up the Lookup.Configuration.Siebel Lookup Definition for Connection Pooling

By default, this connector uses the ICF connection pooling. Table 2-3 lists the connection pooling properties, their description, and default values set in ICF:

Table 2-3 Connection Pooling Properties

Property	Description
Pool Max Idle	Maximum number of idle objects in a pool. Default value: `10`
Pool Max Size	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min Evict Idle Time	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	Minimum number of idle objects in a pool. Default value: `1`

If you want to modify the connection pooling properties to use values that suit requirements in your environment, then:

1. Log in to the Design Console.
2. Expand **Administration,** and then double-click **Lookup Definition.**
3. Search for and open the **Lookup.Configuration.Siebel** lookup definition.
4. On the Lookup Code Information tab, click **Add.**

   A new row is added.
5. In the **Code Key** column of the new row, enter `Pool Max Idle`.
6. In the **Decode** column of the new row, enter a value corresponding to the Pool Max Idle property.
7. Repeat Steps 4 through 6 for adding each of the connection pooling properties listed in Table 2-3.
8. Click the Save icon.

2.3.8 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:

- Enabling RSA Encryption on Siebel
- Configuring the Siebel Web Server Extension for RSA Encryption
- Enabling RSA Encryption for the Siebel Call Center Application
- Starting the Siebel Software Configuration Wizard

2.3.8.1 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 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.

2.3.8.2 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.

2.3.8.3 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**.

2.3.8.4 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.

2.3.9 Creating the IT Resource for the Connector Server

Perform the procedure described in this section only if you have deployed the connector bundle remotely in a Connector Server.

> **Note:**
>
> Before you deploy the connector bundle remotely in a Connector Server, you must deploy the connector in Oracle Identity Manager by performing the procedures described in Installation.

To create the IT resource for the Connector Server:

1. If you are using Oracle Identity Manager release 11.1.1, then:
   a. Log in to the Administrative and User Console
   b. On the Welcome page, click **Advanced** in the upper-right corner of the page.

c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Create IT Resource**.

2. If you are using Oracle Identity Manager release 11.1.2.*x*, then:

   a. Log in to Oracle Identity System Administration

   b. In the left pane under Configuration, click **IT Resource.**

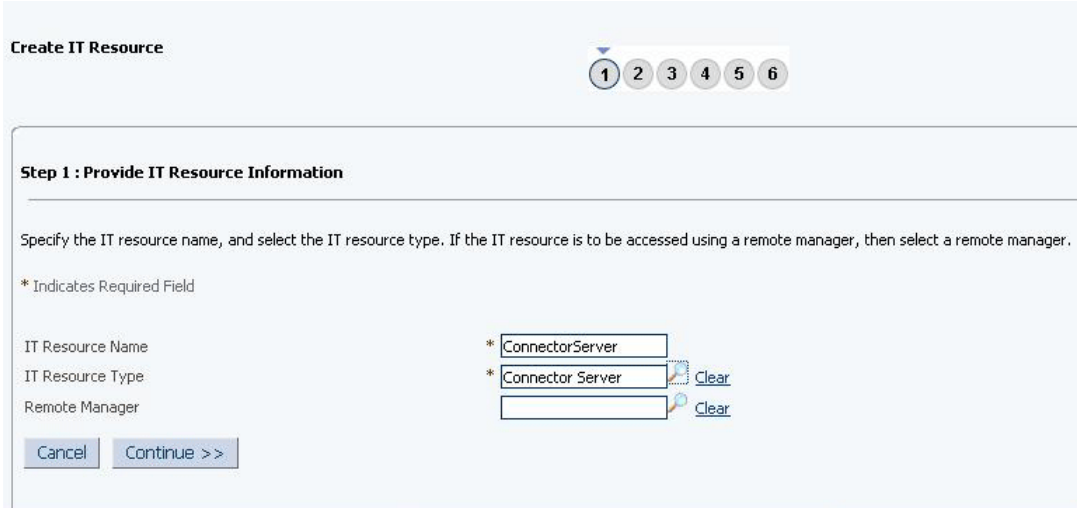
   c. In the Manage IT Resource page, click **Create IT Resource.**

3. On the Step 1: Provide IT Resource Information page, perform the following steps:

   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select **Connector Server** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.

4. Click **Continue**. Figure 2-1 shows the IT resource values added on the Create IT Resource page.

Figure 2-1 Step 1: Provide IT Resource Information



5. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Figure 2-2 shows the Step 2: Specify IT Resource Parameter Values page.

Figure 2-2 Step 2: Specify IT Resource Parameter Values

Table 2-4 provides information about the parameters of the IT resource.

Table 2-4 Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `RManager`
Key	Enter the key for the Java connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: `8759`
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: `300`
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false`. Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, run the connector server by using the /setKey [*key*] option. The value of this key must be specified as the value of the Key IT resource parameter of the connector server.

6. On the Step 3: Set Access Permission to IT Resource page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

> **Note:**
>
> This step is optional.

If you want to assign groups to the IT resource and set access permissions for the groups, then:

a. Click **Assign Group**.

b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

c. Click **Assign**.

7. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

> **Note:**
>
> - This step is optional.
> - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

a. Click **Update Permissions**.

b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

c. Click **Update**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

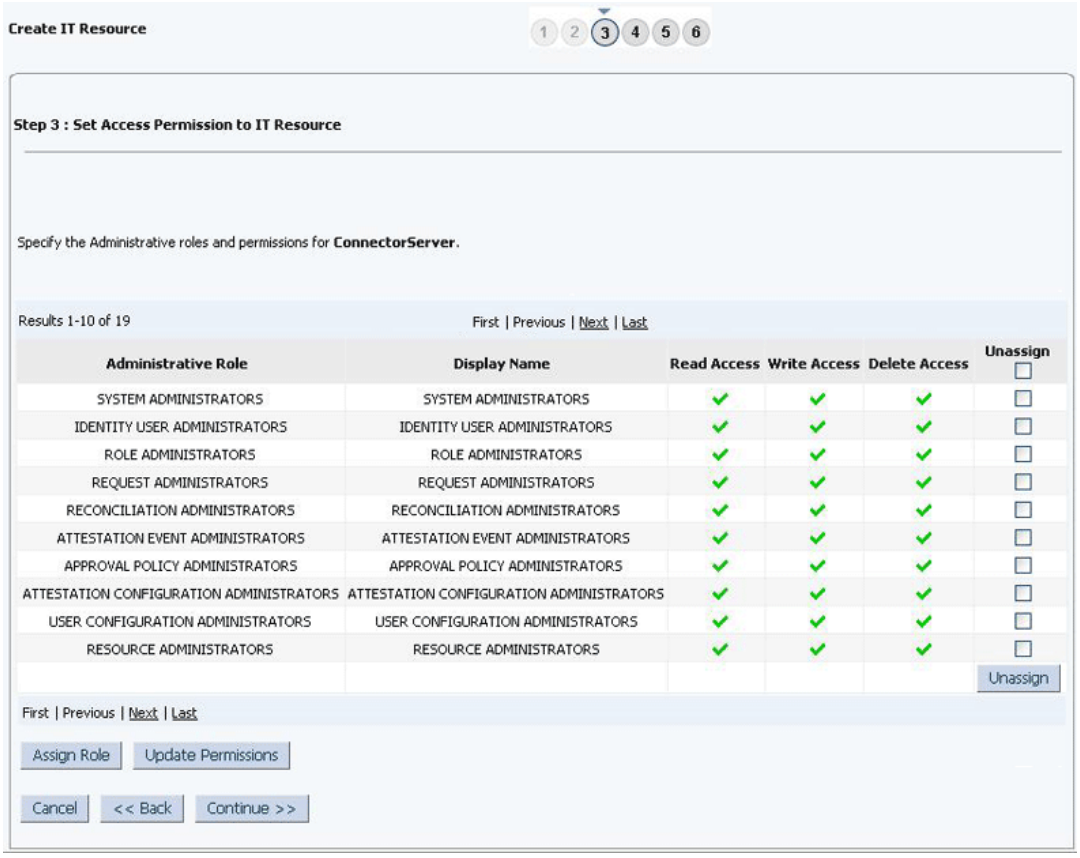
> **Note:**
>
> - This step is optional.
> - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

a. Select the **Unassign** check box for the group that you want to unassign.

b. Click **Unassign**.

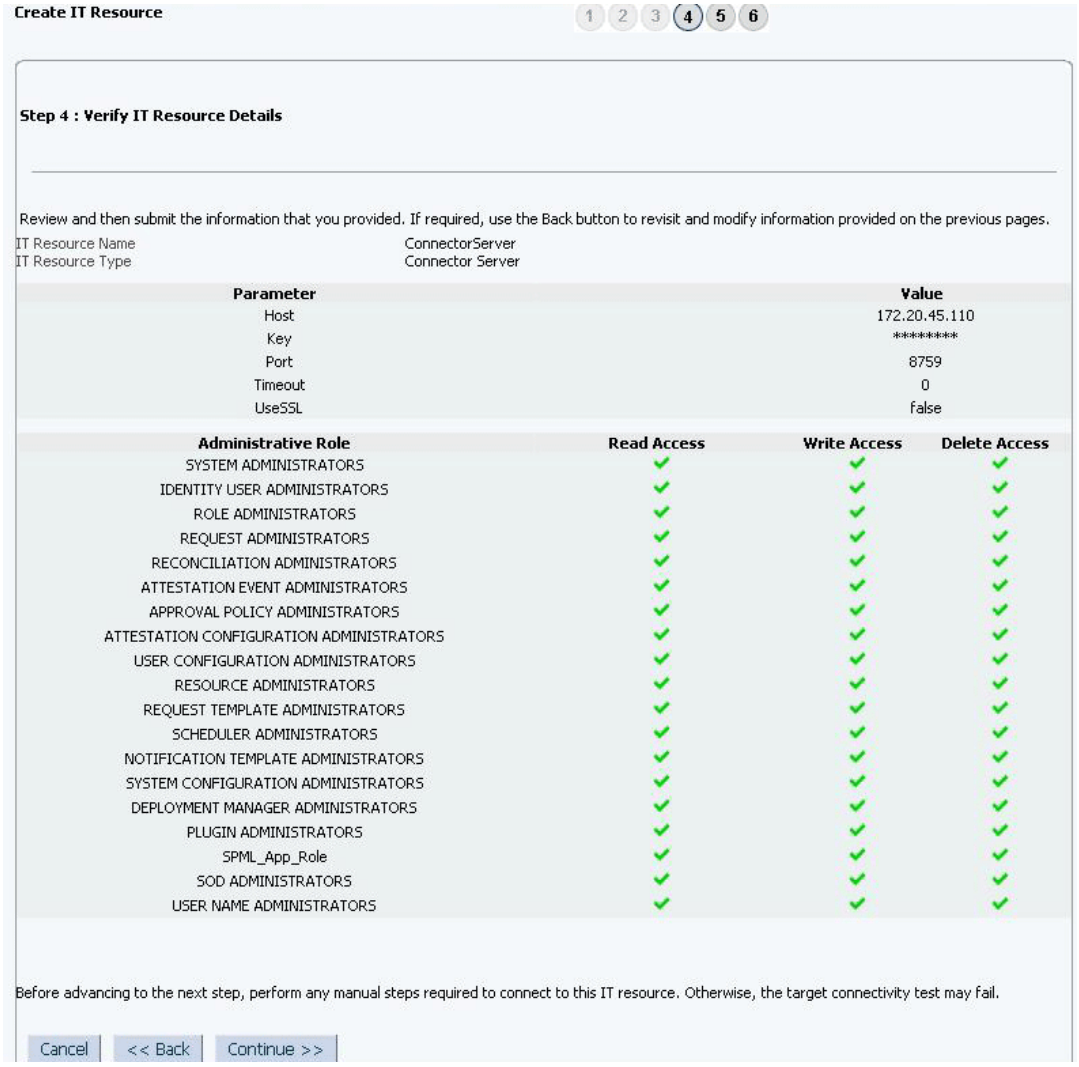
9. Click **Continue**. Figure 2-3 shows the Step 3: Set Access Permission to IT Resource page.

Figure 2-3 Step 3: Set Access Permission to IT Resource



10. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.
11. To proceed with the creation of the IT resource, click **Continue**. Figure 2-4 shows Step 4: Verify IT Resource Details page.

Figure 2-4 Step 4: Verify IT Resource Details

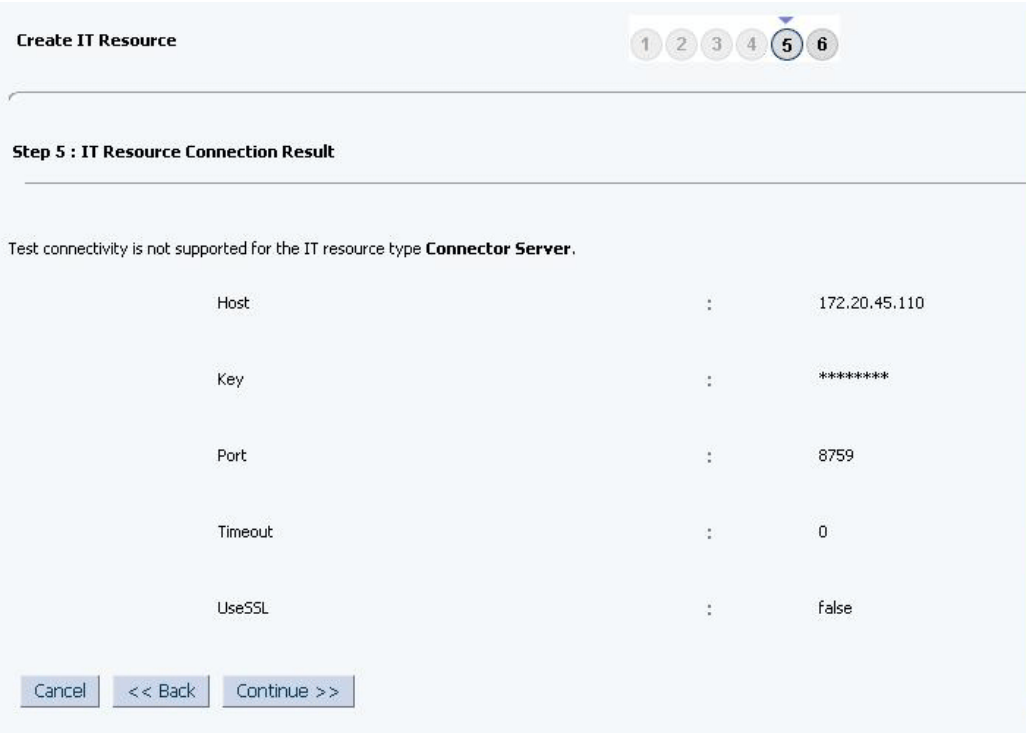


12. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:

    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.

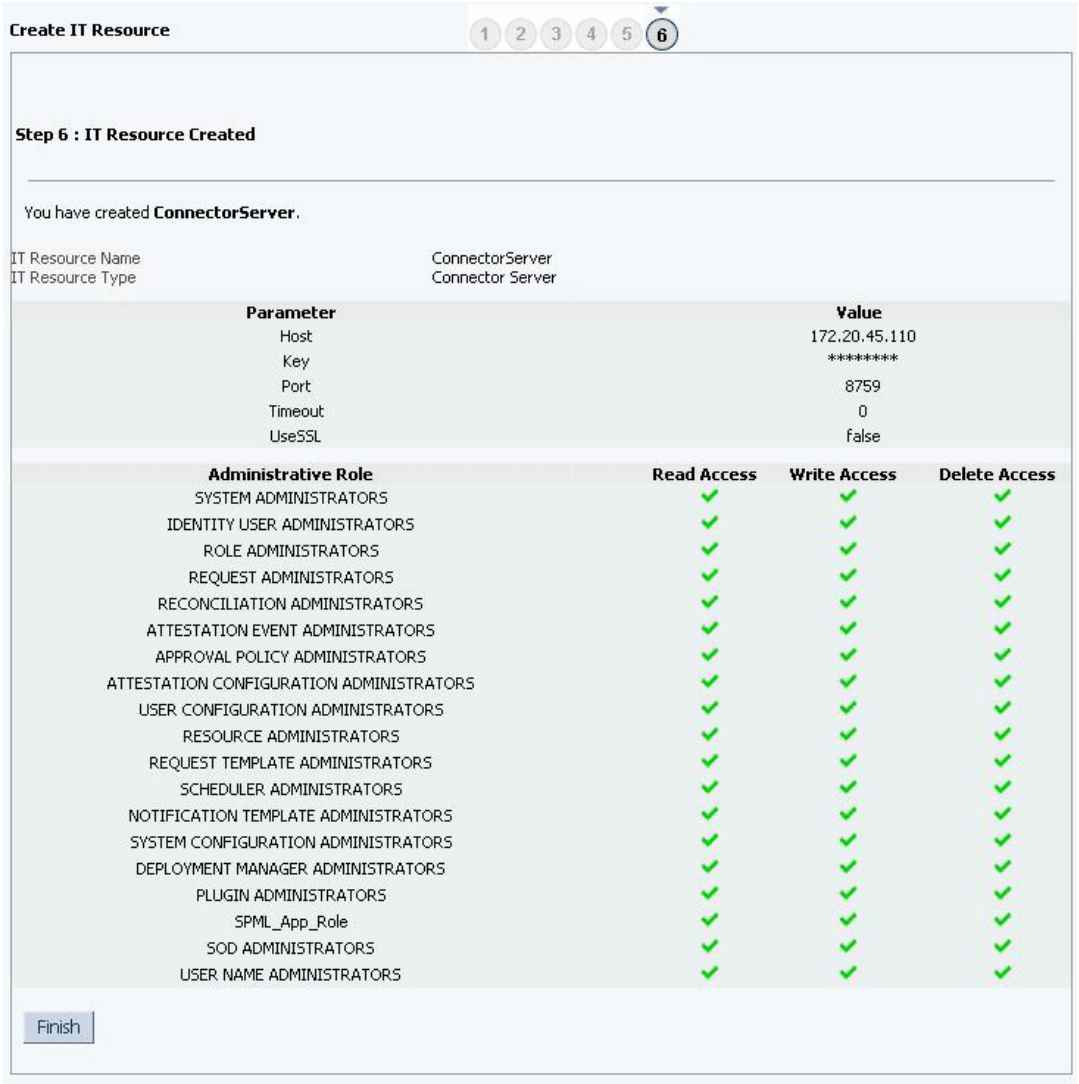
    Figure 2-5 shows the Step 5: IT Resource Connection Result page.

Figure 2-5 Step 5: IT Resource Connection Result



13. Click **Finish**. Figure 2-6 shows the IT Resource Created Page.

Figure 2-6 Step 6: IT Resource Created



2.3.10 Localizing Field Labels in UI Forms

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

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

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

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**

3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:
   - For Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and later:

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
   - For releases prior to Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0):

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

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

   b. Replace with the following text:

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

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

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

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

      ```
      <trans-unit id="$
      {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_SIEBE
      L_ALIAS__c_description']}">
      <source>Alias</source>
      </target>
      </trans-unit>
      <trans-unit
      id="sessiondef.oracle.iam.ui.runtime.form.model.SIEBEL.entity.SIEBELEO.UD_SIEBEL_
      ALIAS__c_LABEL">
      <source>Alias</source>
      </target>
      </trans-unit>
      ```

   d. Open the resource file from the connector package, for example Siebel_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_SIEBEL_ALIAS=\u5225\u540D.

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

      ```
      <trans-unit id="$
      {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_SIEBE
      L_ALIAS__c_description']}">
      <source>Alias</source>
      <target>\u5225\u540D</target>
      </trans-unit>
      <trans-unit
      ```

```
id="sessiondef.oracle.iam.ui.runtime.form.model.SIEBEL.entity.SIEBELEO.UD_SIEBEL_
ALIAS__c_LABEL">
<source>Alias</source>
<target>\u5225\u540D</target>
</trans-unit>
```

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

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

   Sample file name: BizEditorBundle_ja.xlf.

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

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

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

2.4 Upgrading the Connector

If you have already deployed an earlier release of this connector, then upgrade the connector to the current release 11.1.1.6.0 by performing one of the following procedures:

> **Note:**
>
> - Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
> - As a best practice, first perform the upgrade procedure in a test environment.

> **See Also:**
>
> Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information of these steps

This section contains the following topics:

2.4.1 Upgrading the Connector from Release 11.1.1.5.0 to 11.1.1.6.0

To upgrade the Siebel User Management connector from release 11.1.1.5.0 to this release of the connector, perform the following steps:

1. Set entitlement tagging for Siebel Responsibility form (UD_SIEBEL_R) and Siebel Position form (UD_SIEBEL_P) as follows:
   a. Log in to the Oracle Identity Manager Design Console.
   b. Expand **Development Tools** and then double-click **Form Designer.**
   c. Enter the name of the Siebel Responsibility form, `UD_SIEBEL_R`, in the Table Name field and click the **Query for records** button.
   d. Click **Create New Version.**
   e. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.
   f. From the **Current Version** list, select the newly created version.
   g. Click the **Properties** tab.
   h. Select the Responsibility field, and click **Add Property.**
   i. From the Property Name list, select **Entitlement.**
   j. In the Property Value field, enter `true`.
   k. Click **Make Version Active.**
   l. In the Form Designer, enter the name of the Siebel Position form, `UD_SIEBEL_P`, in the Table Name field and click the **Query for records** button.
   m. Click **Create New Version.**
   n. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.
   o. From the **Current Version** list, select the newly created version.
   p. Click the **Properties** tab.
   q. Select the Position field, and click **Add Property.**
   r. From the Property Name list, select **Entitlement.**
   s. In the Property Value field, enter `true`.
   t. Click **Make Version Active.**
2. Set IT resource, Account ID, and Account Name tagging in the Siebel parent form (UD_SIEBEL) as follows:
   a. In the Oracle Identity Manager Design Console, expand **Development Tools** and then double-click **Form Designer.**
   b. Enter the name of the Siebel parent form, `UD_SIEBEL`, in the Table Name field and click the **Query for records** button.
   c. Click **Create New Version.**
   d. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.
   e. From the **Current Version** list, select the newly created version.
   f. Click the **Properties** tab.
   g. Select the IT Resource Type field, and click **Add Property.**
   h. From the Property Name list, select **ITResource.**
   i. In the Property Value field, enter `true`.

j. Select the User ID field, and click **Add Property.**

k. From the Property Name list, select **AccountName.**

l. In the Property Value field, enter `true`.

m. Select the Unique ID field, and click **Add Property.**

n. From the Property Name list, select **AccountID.**

o. In the Property Value field, enter `true`.

p. Update the parent form to add the child form created in Step 1.

q. Click **Make Version Active.**

r. Recreate the form in the user interface (UI) and update the application instance with the new form as described in Updating an Existing Application Instance with a New Form .

3. Set the status of Task to Object Status Mapping of the Child Update process task to None as follows:

   a. In the Oracle Identity Manager Design Console, expand **Process Management** and then double-click **Process definition.**

   b. In the Name field, enter `Siebel Process` and then click the **Query for records** button.

   c. Under Tasks, open the **Add User Position** task.

   d. In the Task to Object Status Mapping tab, change the Object Status of status C from Provisioned to `None`.

   e. Repeat Step 3.c and 3.d for the Delete User Position, Add User Responsibility, and Delete User Responsibility tasks.

4. Update the bundle in the Oracle Identity Manager database with the latest bundle JAR from this release as follows:

   a. Update the latest connector bundle JAR with the third-party JAR files as described in Using External Code Files.

   b. Run the UploadJars utility to upload the updated connector JAR to Oracle Identity Manager database.

   c. Purge the cache to get the changes reflected in Oracle Identity Manager.

2.4.2 Upgrading the Connector from Release 9.0.4.x to 11.1.1.6.0

To upgrade the Siebel User Management connector from release 9.0.4.*x* to this release of the connector, perform the following steps:

1. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector.

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

   - Staging Environment

     Perform the upgrade procedure by using the wizard mode.

   - Production Environment

     Perform the upgrade procedure by using the silent mode.

3. Perform the postupgrade steps.

4. If you are using Oracle Identity Manager release 11.1.2.*x* or later, you must create a new UI form and attach it to an existing application instance to view the user-defined fields (UDFs or custom attributes).

   For more information about UDFs, see Configuring Custom Attributes in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

5. Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so:

   a. In a text editor, open the fvc.properties file located in the *OIM_DC_HOME* directory and include the entries as specified in the following example:

   ```
   ResourceObject;Siebel Resource Object
   FormName;UD_SIEBEL
   FromVersion;Enter the active form version before upgrade
   ToVersion;v_11.1.1.6.0
   ParentParent;UD_SIEBEL_USERID;UD_SIEBEL_UNIQUE_ID
   ```

   b. Run the FVC utility. This utility is copied into the following directory when you install the design console:

   For Microsoft Windows:

   OIM_DC_HOME/fvcutil.bat

   For UNIX:

   OIM_DC_HOME/fvcutil.sh

   When you run this utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, and the logger level and log file location.

> **See Also:**
>
> For detailed information about the FVC utility, see Using the Form Version Control Utility of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*

2.5 Postcloning Steps

You can clone the Siebel connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

> **See Also:**
>
> Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about cloning connectors and the steps mentioned in this section

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the

following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- Lookup Definition

  If the lookup definition contains the old lookup definition details, then you must modify it to provide the new cloned lookup definition names. If the Code Key and Decode values are referring the base connector attribute references, then replace these with new cloned attributes.

  For example, consider Lookup.Siebel.UM.ProvAttrMap1 and UD_SIEBEL_P1 to be the cloned versions of the Lookup.Siebel.UM.ProvAttrMap lookup definition and UD_SIEBEL_P child form, respectively.

  After cloning, the Lookup.Siebel.UM.ProvAttrMap1 lookup definition contains Code Key entries that correspond to the fields of the old child form UD_SIEBEL_P. To ensure that the Code Key entries point to the fields of the cloned child form (UD_SIEBEL_P1), specify UD_SIEBEL_P1~Position[Lookup] in the corresponding Code Key column.

- Scheduled Task

  You must replace the base connector resource object name in the scheduled task with the cloned resource object name. If the scheduled task parameter has any data referring to the base connector artifacts or attributes, then these must be replaced with the new cloned connector artifacts or attributes.

- Localization Properties

  You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

- IT Resource

  The cloned connector has its own set of IT resources. You must configure both the cloned IT resources, Active Directory and Connector Server, and provide the reference of the cloned Connector Server IT Resource in the cloned Siebel IT resource. Ensure you use the configuration lookup definition of the cloned connector.

- Child Table

  As a result of a change in the name of the child table, you must modify the corresponding mappings for the child table operations to work successfully.

  To update the corresponding mappings, perform the following procedure:

  1. Log in to Design Console.
  2. Expand **Process Management,** and then double-click **Process Definition.**
  3. Search for and open the **Siebel User1** process form.
  4. Double-click the child table process task for the insert functionality. For example: **UD_SIEBEL_P1 Insert**

     The Editing Task window is displayed.
  5. On the Integration tab, select the row corresponding to the name of the child table, and then click **Map.**
  6. The Data Mapping for Variable window is displayed.
  7. Change the value in the Literal Value field to the cloned table name. For example, `UD_SIEBEL_P1`.
  8. Click **Save** and close the window.

9. To change the mappings for the delete functionality, perform Steps 1 through 8 of this procedure with the following difference:

   While performing Step 4 of this procedure, instead of selecting the child table process task for the insert functionality, double-click the child table process task for the delete functionality.

10. To change the mappings for the update functionality, perform Steps 1 through 8 with the following difference:

    While performing Step 4 of this procedure, instead of selecting the child table process task for the insert functionality, double-click the child table process task for the update functionality.

3
Using the Connector

You can use the Siebel User Management connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.
This chapter provides information about the following topics:

3.1 Guidelines to Apply While Using the Connector

Apply the following guidelines while using the connector:

- While creating an account for a user of type 'User' in the target system, the Position field is optional. Suppose you create a target system user account (of the type 'User') without specifying a value for the Position attribute. After you run the scheduled job for user reconciliation, the details of this newly created target system account are reconciled into Oracle Identity Manager.

  In the Administrative and User Console, when you update the attributes of the OIM User (corresponding to the newly created target system user account), this update provisioning operation fails. This is because Position is a mandatory field on the OIM User process form.

  As a workaround, log in to the Design Console, mark the Position field as optional on the process form, and then run reconciliation for users of type 'Users'.
- The following is a guildeline on performing provisioning:

  To activate a user or an employee account in Oracle Identity Manager, assign a responsibility.

  To deactivate a user or an employee account in Oracle Identity Manager, delete all responsibilities assigned to the corresponding user or employee in the target system, and then run reconciliation.

3.2 Performing First-Time Reconciliation

First-time reconciliation 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:

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

   See Scheduled Job for Lookup Field Synchronization for information about the attributes of the scheduled jobs for lookup field synchronization.

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

   See Scheduled Jobs for Reconciliation of User Records for information about the attributes of this scheduled job.

After first-time reconciliation, the Latest Token attribute of the Siebel Target User Recon scheduled job is automatically set to the time stamp at which the reconciliation run ended.

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

3.3 Scheduled Job for Lookup Field Synchronization

The following scheduled jobs are used for lookup fields synchronization:

- Siebel Lookup Recon for Employee Type Code
- Siebel Lookup Recon for Personal Title
- Siebel Lookup Recon for Position
- Siebel Lookup Recon for Preferred Communications
- Siebel Lookup Recon for Responsibility
- Siebel Lookup Recon for TimeZone

You must specify values for the attributes of these scheduled jobs. Table 3-1 describes the attributes of these scheduled jobs. Configuring Scheduled Jobs describes the procedure to configure scheduled jobs.

> **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 Scheduled Jobs for Lookup Field Synchronization

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`

Table 3-1 (Cont.) Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Object Type	Enter the type of object you want to reconcile. Depending on the scheduled job that you are running, the default value is one of the following: • For Siebel Lookup Recon for Employee Type Code: `Employee;Employee;Employee Type Code;Value;Description` • For Siebel Lookup Recon for Personal Title: `Employee;Employee;Personal Title;Value;Description` • For Siebel Lookup Recon for Position: `Position;Position;Position Id;Name` • For Siebel Lookup Recon for Preferred Communications: `Employee;Employee;PreferredCommunications;Value;Description` • For Siebel Lookup Recon for Responsibility: `Responsibility;Responsibility;Name;Description` • For Siebel Lookup Recon for TimeZone: `Employee;Employee;Time Zone Name - Translation;Name;Standard Abbreviation`
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Depending on the scheduled job that you are using, the default values are as follows: • For Siebel Lookup Recon for Employee Type Code: `Lookup.Siebel.EmployeeTypeCode` • For Siebel Lookup Recon for Personal Title: `Lookup.Siebel.PersonalTitle` • For Siebel Lookup Recon for Position: `Lookup.Siebel.Position` • For Siebel Lookup Recon for Preferred Communications: `Lookup.Siebel.PreferredCommunications` • For Siebel Lookup Recon for Responsibility: `Lookup.Siebel.Responsibility` • For Siebel Lookup Recon for TimeZone: `Lookup.Siebel.TimeZone`
Code Key Attribute	Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job that you are using, the default values are as follows: • For Siebel Lookup Recon for Employee Type Code: `Value` • For Siebel Lookup Recon for Personal Title: `Value` • For Siebel Lookup Recon for Position: `Position Id` • For Siebel Lookup Recon for Preferred Communications: `Value` • For Siebel Lookup Recon for Responsibility: `Name` • For Siebel Lookup Recon for TimeZone: `Name`
Decode Attribute	Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Depending on the scheduled job that you are using, the default values are as follows: • For Siebel Lookup Recon for Employee Type Code: `Description` • For Siebel Lookup Recon for Personal Title: `Description` • For Siebel Lookup Recon for Position: `Name` • For Siebel Lookup Recon for Preferred Communications: `Description` • For Siebel Lookup Recon for Responsibility: `Description` • For Siebel Lookup Recon for TimeZone: `Abbreviation`

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:

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, ensure that no values are specified for the Latest Token and Custom Recon Query attributes of the scheduled jobs for reconciling user records.

At the end of the reconciliation run, the Latest Token attribute of the scheduled job for user record reconciliation is automatically set to the time stamp at which the run ended. 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 Performing 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 Custom Recon Query attribute of the scheduled job for reconciliation of user records.

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|First Name=Jane`

  With this query condition, record of Users with first name John and Jane are reconciled.

If you do not specify values for the Custom Recon Query attribute, 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 Custom Recon Query attribute:

- 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 Custom Recon Query attribute while configuring the scheduled job user record reconciliation.

Sample Query Conditions

You can specify the following types of query conditions as values for the Custom Recon Query attribute and run the scheduled job for user record reconciliation:

- Simple query with user attributes, for example:
  - Value assigned to the Custom Recon Query attribute: `First Name=John`

    Users with first name `John` is reconciled.
  - Value assigned to the Custom Recon Query attribute: `Login Name=JOHN`

    Users with login name `JOHN` are reconciled.
  - Value assigned to the Custom Recon Query attribute: `First Name=John|First Name=Jane`

    Users with first name `John` and `Jane` are reconciled.
  - Value assigned to the Custom Recon Query attribute: `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 Custom Recon Query attribute: `Position=Proxy Employee|Position=ERM AnonUser`

    All users having positions as `Proxy Employee` or `ERM AnonUser` are reconciled.
  - Value assigned to the Custom Recon Query attribute: `Responsibility=CEO&Responsibility=Consultant`

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

  - Value assigned to the Custom Recon Query attribute: `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 Custom Recon Query attribute: `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 Custom Recon Query attribute: `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.

3.4.3 Reconciliation Based on User Type

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

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 job attribute. This attribute is discussed in Scheduled Jobs for Reconciliation of User Records.

3.4.4 Reconciliation Scheduled Jobs

When you run the Connector Installer, the scheduled tasks corresponding to the following scheduled jobs are automatically created in Oracle Identity Manager:

- Scheduled Jobs for Reconciliation of User Records
- Scheduled Job for Reconciliation of Deleted Users Records

3.4.4.1 Scheduled Jobs for Reconciliation of User Records

Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled jobs:

- Siebel Target User Recon

  This scheduled job is used to reconcile user data in the target resource (account management) mode of the connector

- Siebel Trusted User Reconciliation

  This scheduled job is used to reconcile user data in the trusted source (identity management) mode of the connector

Table 3-2 describes the attributes of both scheduled jobs.

Table 3-2 Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description
Scheduled Task Name	Name of the scheduled task used for reconciliation. The default value of this attribute in the Siebel Target User Recon scheduled job is `Siebel Target User Recon.` The default value of this attribute in the Siebel Trusted User Reconciliation scheduled job is `Siebel Trusted User Reconciliation.`
ITResource Name	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`
Resource Object Name	Name of the resource object that is used for reconciliation. The default value of this attribute in the Siebel Target User Recon scheduled job is `Siebel Resource Object.` The default value of this attribute in the Siebel Trusted User Reconciliation scheduled job is `Siebel Trusted User.`
Time Zone	Enter the time zone of the target system database. Default value: `GMT-08:00`
Day Light Saving	Enter the time, in minutes, that must be added to the time-stamp value stored in the LastExecution Timestamp attribute. Default value: `0`
Custom Recon Query	Provide a value for this attribute if you want to reconcile the subset of added or modified target system records See Performing Limited Reconciliation for more information.

Table 3-2 (Cont.) Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description
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. • `User`: This user is also 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`
Latest Token	This attribute holds the time stamp at which the last reconciliation run started. The reconciliation engine automatically enters a value in this attribute. Sample value: `23 May 2011 04:30:41 -0700`
Incremental Recon Date Attribute	This attribute holds the name of the target system that maintains the time stamp of target system records. Default value: `Updated`

3.4.4.2 Scheduled Job for Reconciliation of Deleted Users Records

Depending on whether you want to implement trusted source or target resource delete reconciliation, you must specify values for the attributes of one of the following scheduled jobs:

- Siebel Target Resource User Delete Reconciliation

  This scheduled job is used to reconcile data about deleted users in the target resource (account management) mode of the connector. During a reconciliation run, for each deleted user account on the target system, the Siebel resource is revoked for the corresponding OIM User.

- Siebel Trusted User Delete Reconciliation

  This scheduled job is used to reconcile data about deleted users in the trusted source (identity management) mode of the connector. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted.

Table 3-3 describes the attributes of both scheduled jobs.

Table 3-3 Attributes of the Siebel Target Resource User Delete Reconciliation Scheduled Job

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile data about deleted user records. Default is: `SIEBEL IT Resource`

Table 3-3 (Cont.) Attributes of the Siebel Target Resource User Delete Reconciliation Scheduled Job

Attribute	Description
Resource Object Name	Name of the resource object that is used for reconciliation. The default value of this attribute in the Siebel Target User Recon scheduled job is `Siebel Resource Object.` The default value of this attribute in the Siebel Trusted User Reconciliation scheduled job is `Siebel Trusted User.`
Object Type	Enter the type of object you want to reconcile. Default is: `Employee`

3.5 Configuring Scheduled Jobs

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

You can apply this procedure to configure the scheduled jobs for lookup field synchronization and reconciliation.

See Scheduled Jobs for Lookup Field Synchronization and Reconciliation for the list of scheduled jobs that you can configure.

To configure a scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1.*x*, then:
   a. Log in to the Administrative and User Console.
   b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
2. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   a. Log in to Oracle Identity System Administration.
   b. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Managing Sandboxes of *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
   c. In the left pane, under System Management, click **Scheduler.**
3. Search for and open the scheduled job as follows:
   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the 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.

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

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

> **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 job are discussed in Scheduled Jobs for Reconciliation of User Records.

6. 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 Configuring Provisioning in Oracle Identity Manager Release 11.1.1

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 Switching Between Request-Based Provisioning and Direct Provisioning.

The following are types of provisioning operations:

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

> **See Also:**
>
> Manually Completing a Task in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for information about the types of provisioning

This section discusses the following topics:

- Direct Provisioning
- Request-Based Provisioning
- Switching Between Request-Based Provisioning and Direct 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:
   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:
   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. On the user details page, click the **Resources** tab.
5. 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.
6. On the Step 1: Select a Resource page, select **Siebel Resource Object** from the list and then click **Continue**.
7. On the Step 2: Verify Resource Selection page, click **Continue**.
8. 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**.
9. 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**.
10. 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**.
11. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
12. The "Provisioning has been initiated" message is displayed. Close the window displaying this message.
13. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.6.2 Request-Based Provisioning

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.

- End User's Role in Request-Based Provisioning
- 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:

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.

3.6.3 Switching Between Request-Based Provisioning and Direct Provisioning

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

If you have configured the connector for request-based provisioning, you can always switch to direct provisioning. Similarly, you can always switch back to request-based provisioning any time. This section discusses the following topics:

- Switching From Request-Based Provisioning to Direct Provisioning
- Switching From Direct Provisioning to Request-Based Provisioning

3.6.3.1 Switching From Request-Based Provisioning to Direct Provisioning

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.

3.6.3.2 Switching From Direct Provisioning to Request-Based Provisioning

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.

3.7 Configuring Provisioning in Oracle Identity Manager Release 11.1.2

To configure provisioning operations in Oracle Identity Manager release 11.1.2.*x:*

> **Note:**
>
> The time required to complete a provisioning operation that you perform the first time by using this connector takes longer than usual.

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See Managing Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance, and then click **Checkout.**
5. Specify value for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**

7. If you want to provision entitlements, then:
   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

3.8 Uninstalling the Connector

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the Connector

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

> **Note:**
>
> From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* guide for information about managing lookups by using the Form Designer in the Oracle Identity Manager System Administration console.

4.1 Creating and Populating a New Lookup Definition

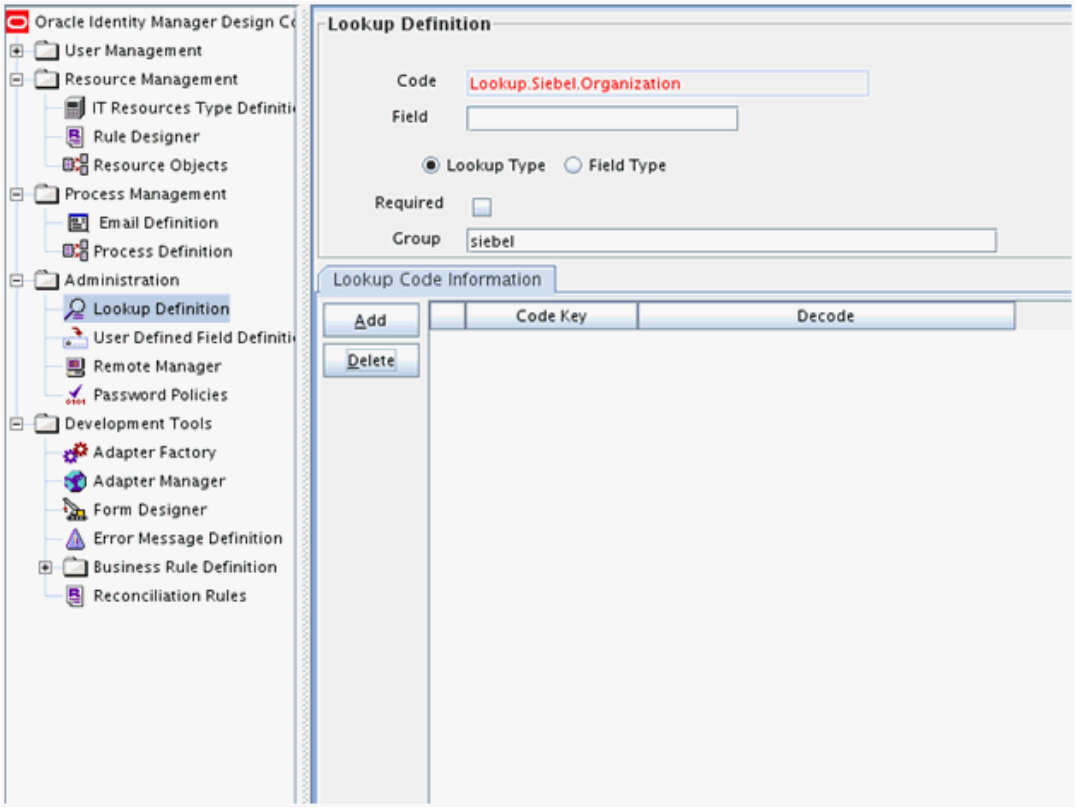
Perform this procedure if you want to add a new lookup-based attribute for reconciliation or provisioning. First, you must create a new lookup definition for storing the values of the Organization attribute of Siebel User Profile. Then, create a new scheduled job to fetch all the Organizations from the Siebel target system and populate the newly created lookup definition.

4.1.1 Creating a New Lookup Definition

To create a new lookup definition:

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

2. Expand **Administration.**
3. Double-click **Lookup Definition.**
4. In the **Code** field, enter `Lookup.Siebel.Organization` and in the **Group** field, enter `siebel`.



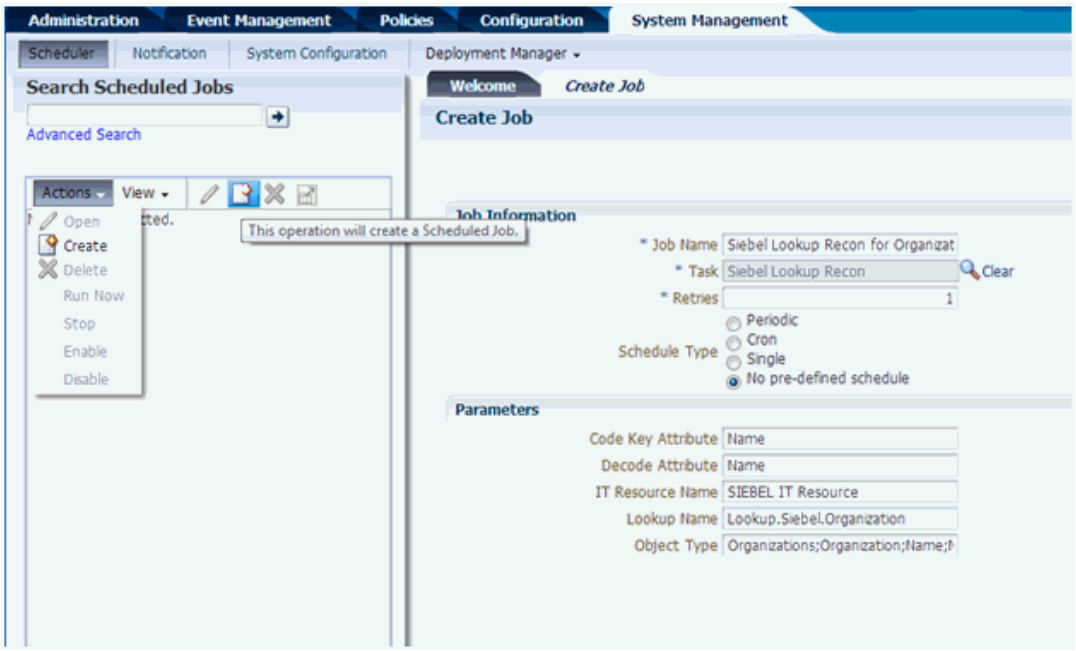
5. Click **Save.**

4.1.2 Creating a New Scheduled Job

To create a new scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1.*x*, then:
   a. Log in to the Administrative and User Console.
   b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs.**
2. If you are using Oracle Identity Manager release 11.1.2.*x*, then:
   a. Log in to Oracle Identity System Administration.
   b. In the left pane, under System Management, click **Scheduler.**
3. From the Scheduled Jobs Display pane, under Actions select Create, or directly click the **Create Scheduled Job** icon.
4. Enter the following values:

- Job Name: `Siebel Lookup Recon for Organization`
- Task: `Siebel Lookup Recon`
- Retries: `1`
- Schedule Type: `No pre-defined schedule`
- Code Key Attribute: `Name`
- Decode Attribute: `Name`
- IT Resource Name: `SIEBEL IT Resource`
- Lookup Name: `Lookup.Siebel.Organization`
- Object Type: `Organizations;Organization;Name;Name`



5. Click **Apply** to save or click **Save and Run Now** to save and run the scheduled job to populate the lookup definition with all Organizations from the Siebel target system.

4.2 Adding New Attributes for Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to add new attributes for target resource reconciliation.
>
> The new attributes you add for reconciliation must contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in User Attributes for Reconciliation 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. Perform the procedure described in Creating and Populating a New Lookup Definition.

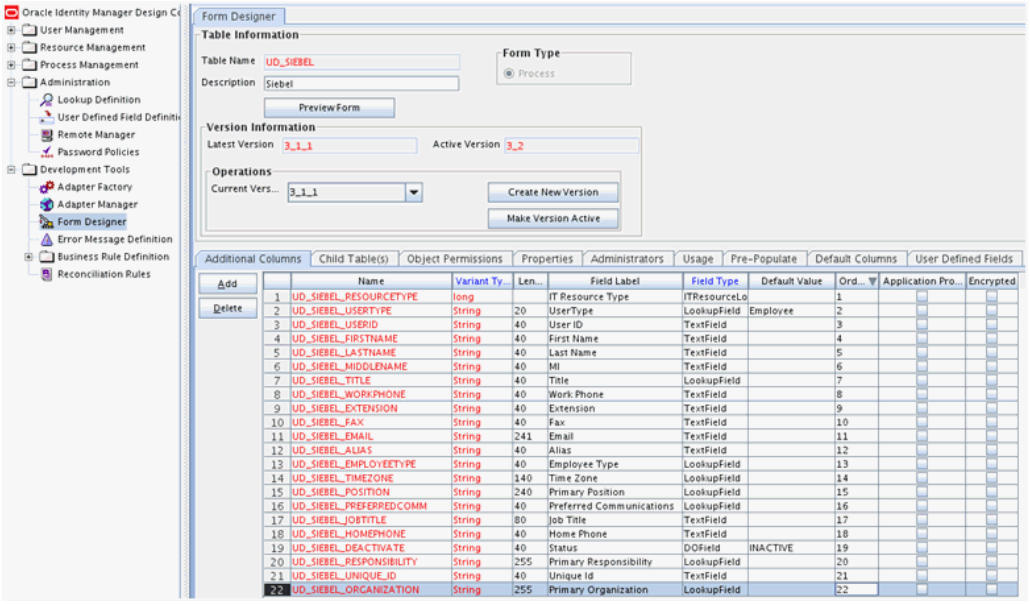
> **Note:**
>
> You can skip this step if you are not adding a lookup-based attribute or if you have created and populated a new lookup definition earlier.

2. In the Oracle Identity Manager Design Console, 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	255
Field Label	Primary Organization
Field Type	LookupField
Order	22

The following screenshot shows this form:

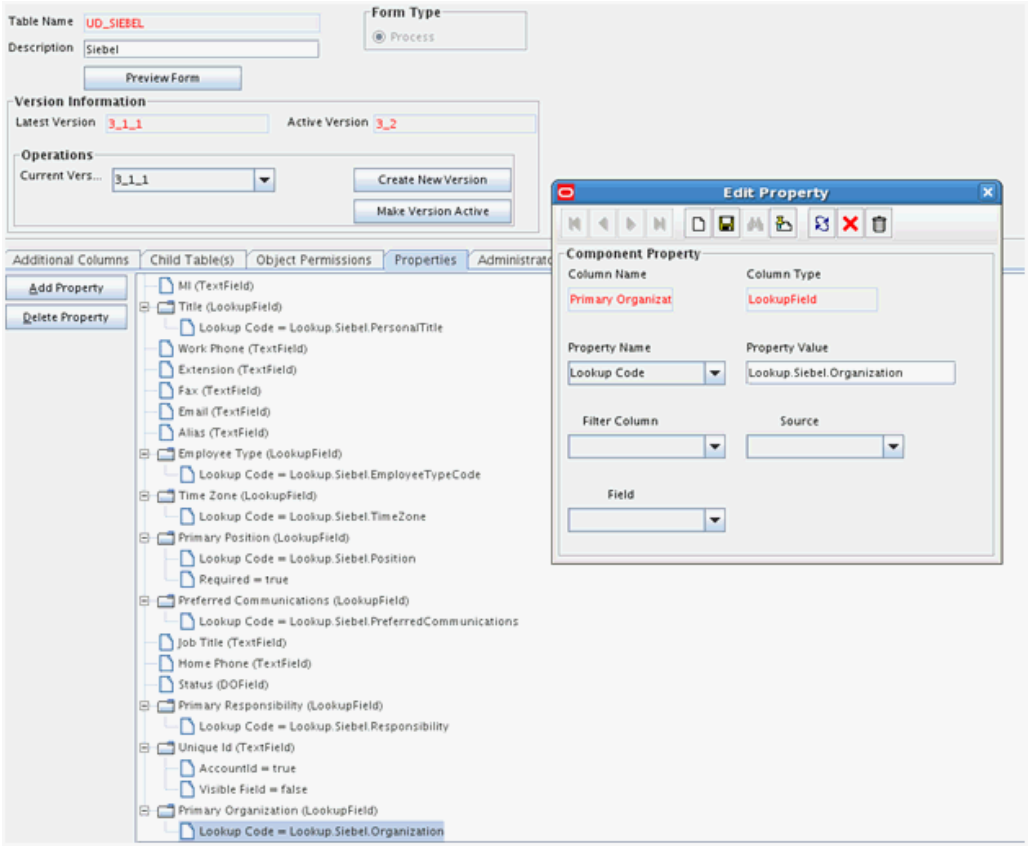


i. Click the **Save** icon.

j. Go to **Properties** tab and add a property to the newly added attribute Primary Organization with the following values:

Property Name: `Lookup Code`

Property Value: `Lookup.Siebel.Organization`



Click the **Save** icon.

k. 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.**

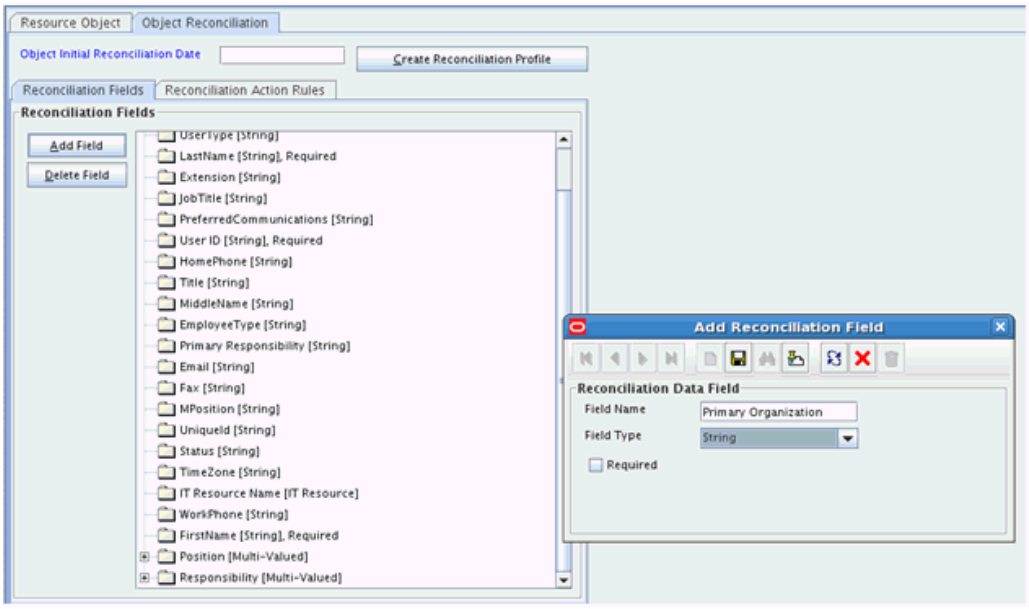
   b. Double-click **Resource Objects**.

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

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

      Field Name: `Primary Organization`

      Field Type: `String`



   e. 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**.

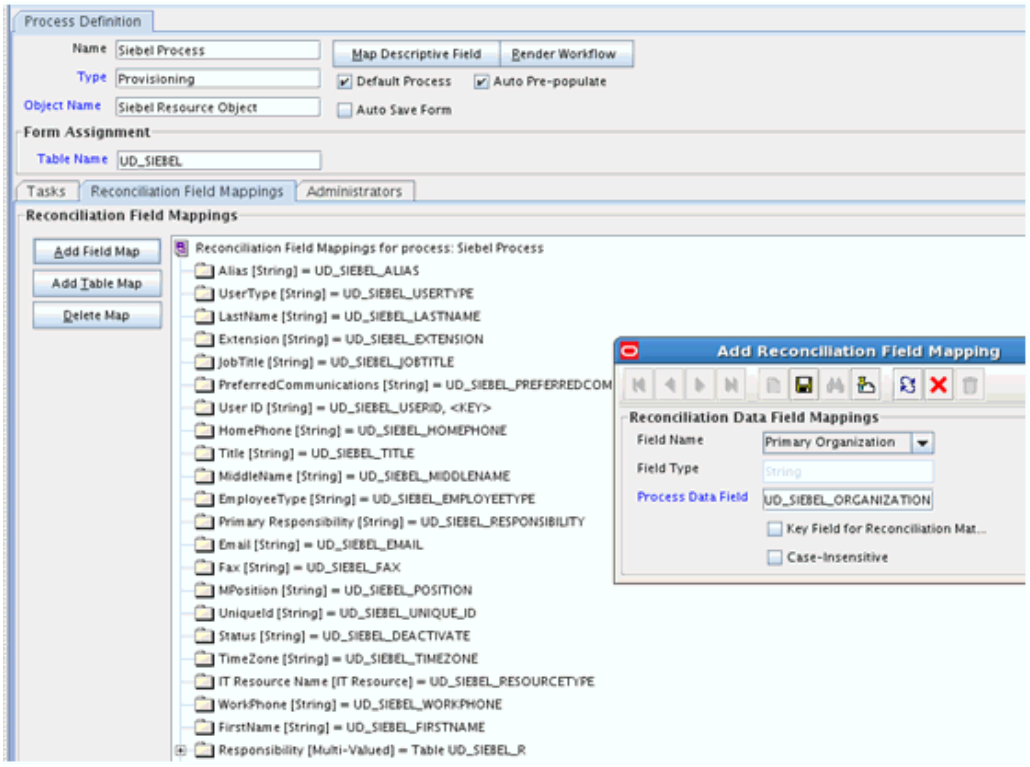
   c. Search for and open the **Siebel** process definition.

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

      Field Name: `Primary Organization`

      Field Type: `String`

      Process Data Field: `UD_SIEBEL_ORGANIZATION`



e. Click the **Save** icon.

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

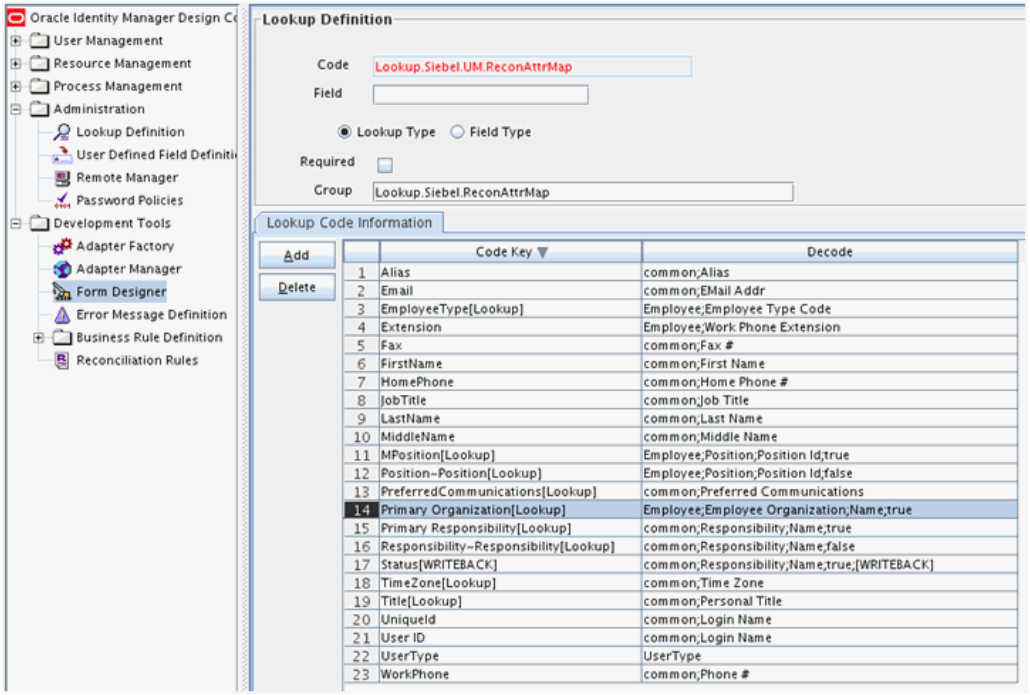
   a. Expand **Administration**.

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

   c. Search for and open the **Lookup.Siebel.UM.ReconAttrMap** 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 resource object field. The Decode value is the name of the attribute in the target system.

      For example, enter `Primary Organization[Lookup]` in the **Code Key** field and then enter `Employee;Employee Organization;Name;true` in the **Decode** field.



e. Click the **Save** icon.

6. Define the connector. If you are planning to perform any of the other procedures described in this chapter, perform those procedures and then define the connector. See Defining the Connector for more information.

7. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for the procedures.

4.3 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 User Attributes for Reconciliation 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:

1. Perform the procedure described in Creating and Populating a New Lookup Definition.

> **Note:**
>
> You can skip this step if you are not adding a lookup-based attribute or if you have created and populated a new lookup definition earlier.

2. In the Oracle Identity Manager Design Console, add the new attribute on the process form by performing Step 2 of Adding New Attributes for Reconciliation.

   If you have already added the new attribute, then you need not add it again.

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

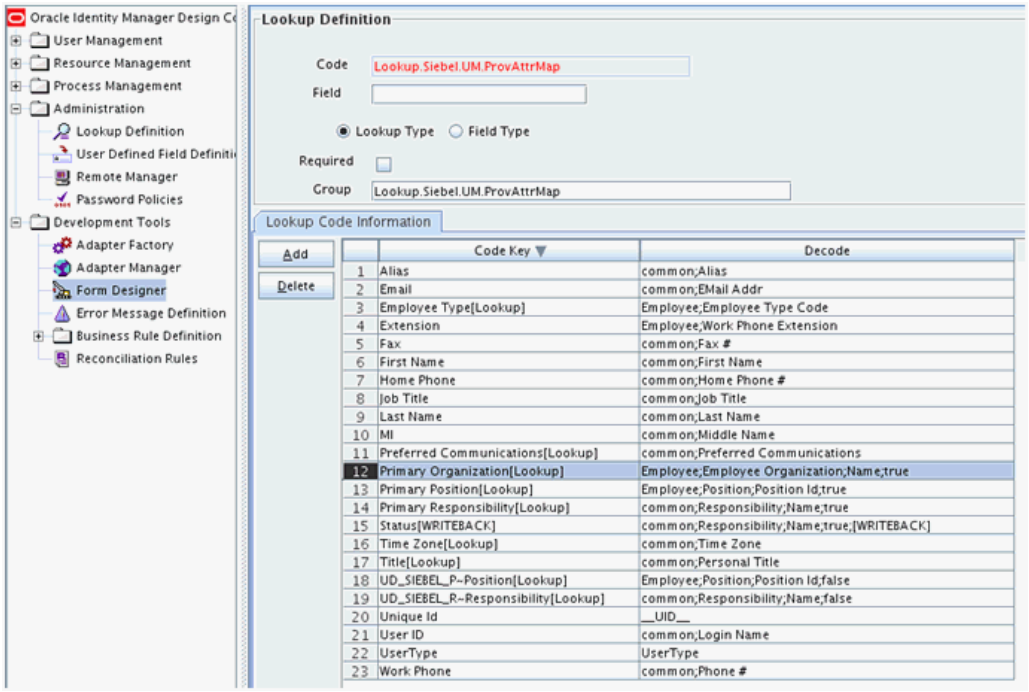
   a. Expand **Administration.**

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

   c. Search for and open the **Lookup.Siebel.UM.ProvAttrMap** lookup definition.

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

      For example, enter `Primary Organization[Lookup]` in the **Code Key** field and then enter `Employee;Employee Organization;Name;true` 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.

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 = "Primary Organization"
type = "String"
widget = "lookup"
length = "255"
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 Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

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

See Importing Request Datasets 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 by clicking **Add** and then entering the task name, for example, `Primary Organization Updated`, and the

task description. Then, in the Task Properties section, select the **Conditional, Required for Completion, Allow Cancellation while Pending,** and **Allow Multiple Instances** fields, and click on the Save icon.

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

e. Select the **adpSIEBELUPDATE** 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 (○ value in Siebel). These values must be replaced with values relevant to the attributes that you require.

Variable Name	Data Type	Map To	Qualifier	Literal Value
Adapter return value	Object	Response code	NA	NA
objectType	String	Literal	String	User
itResourceFieldName	String	Literal	String	UD_SIEBEL_RESOURCETYPE
label	String	Literal	String	Primary Organization
iProcessInstKey	Long	Process data	processinstance	NA

g. On the Responses tab, click **Add** to add the following response codes:

Code Name	Description	Status
UNKNOWN_UID	user does not exist	R
ERROR	Siebel User Modification Failed	R
UNKNOWN	An unknown response was received	R
CONNECTION_FAILED	Cannot make connection to the resource	R
CONNECTOR_EXCEPTION	Siebel User Modification Failed	R
CONFIGURATION_ERROR	Connector configuration is wrong	R
SUCCESS	Siebel User Modification Successful	C

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

8. Define the connector. If you are planning to perform any of the other procedures described in this chapter, perform those procedures and then define the connector. See Defining the Connector for more information.

9. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for the procedures.

4.4 Adding New Multivalued Attributes for Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to add new multivalued attributes for target resource reconciliation.
>
> The new attributes you add for reconciliation must contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, only the Siebel Responsibility and Siebel Position 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.

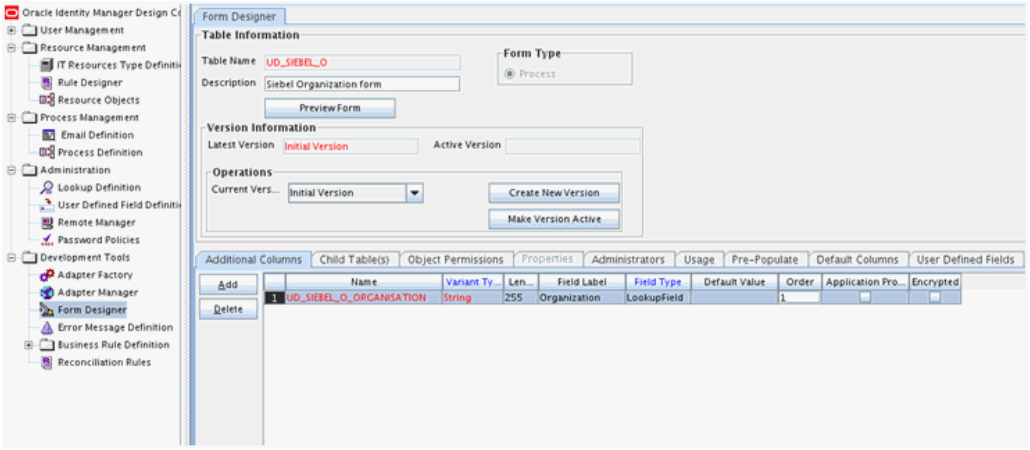
To add a new multivalued attribute for target resource reconciliation:

1. Perform the procedure described in Creating and Populating a New Lookup Definition.

   > **Note:**
   >
   > You can skip this step if you are not adding a lookup-based attribute or if you have created and populated a new lookup definition earlier.

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

Field	Value
Name	Organization
Variant Type	String
Length	255
Field Label	Organization
Order	1
Field Type	LookupField

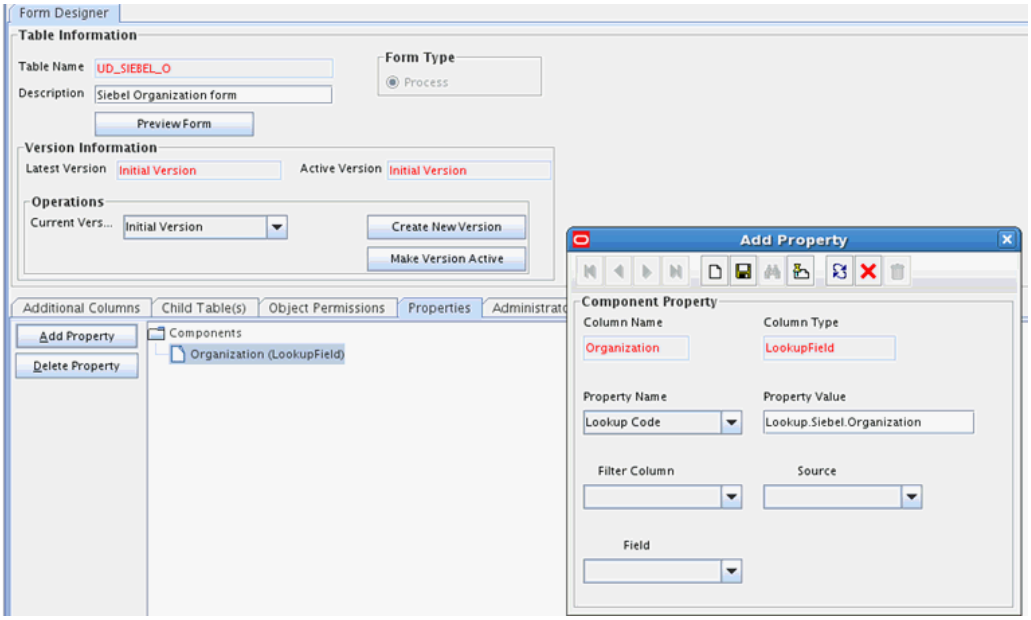


e. Click **Save.**

f. Go to **Properties** tab and add a property to the newly added attribute Primary Organization with the following values:

Property Name: `Lookup Code`

Property Value: `Lookup.Siebel.Organization`



Click the **Save** icon.

g. Click **Make Version Active.**

3. Add the form created for the multivalued attribute as a child form of the process form as follows:

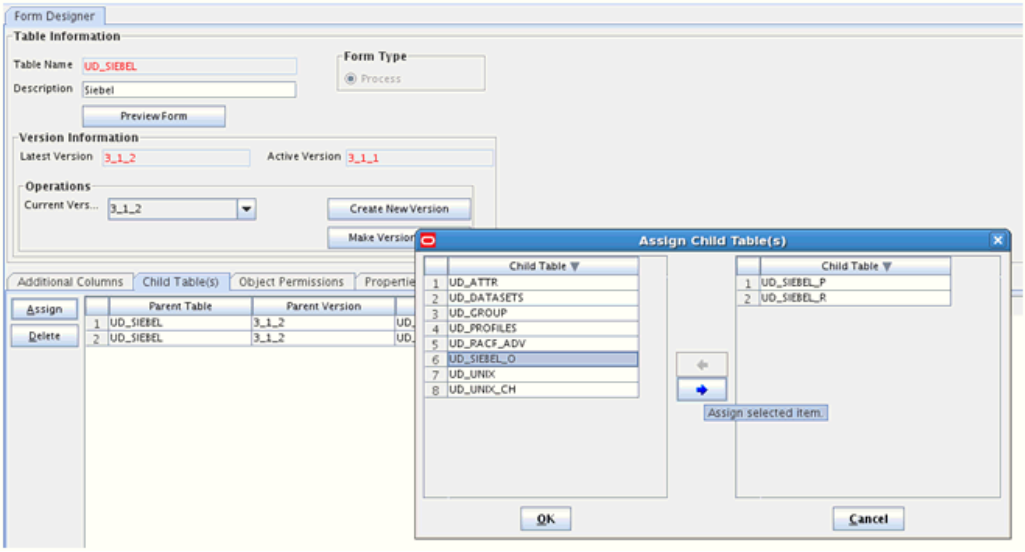
a. Search for and open the **UD_SIEBEL** process form.

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**.



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, go to **Reconciliation Fields,** and then 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.

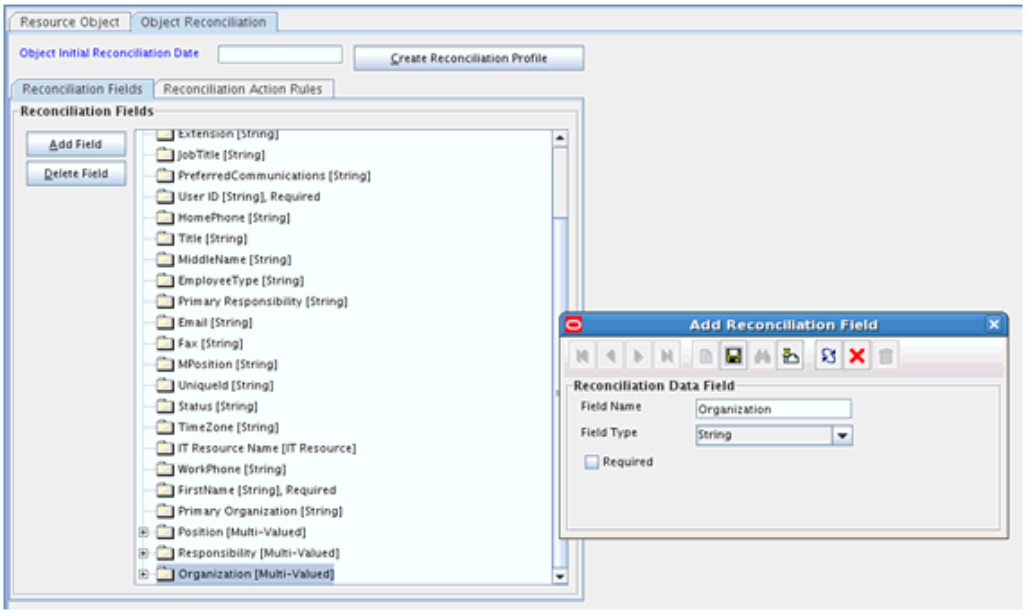
   f. Click **Save** and then close the dialog box.

   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.



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

k. 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:

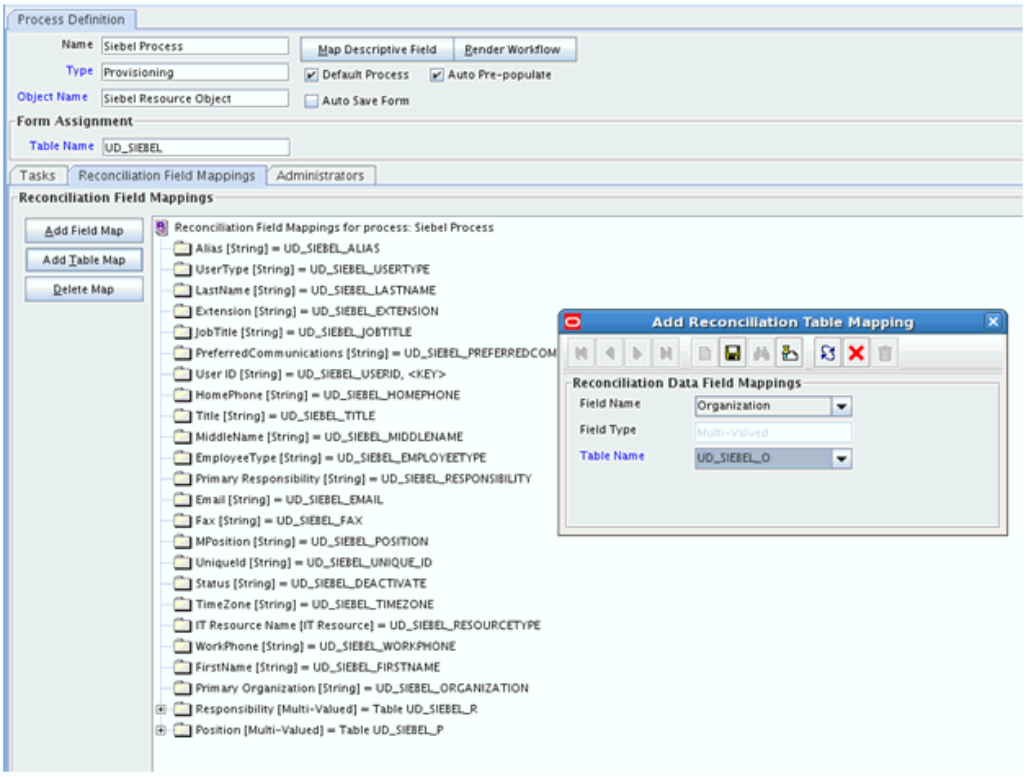
   a. Expand **Process Management**.

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

   c. Search for and open the **Siebel Process** 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.

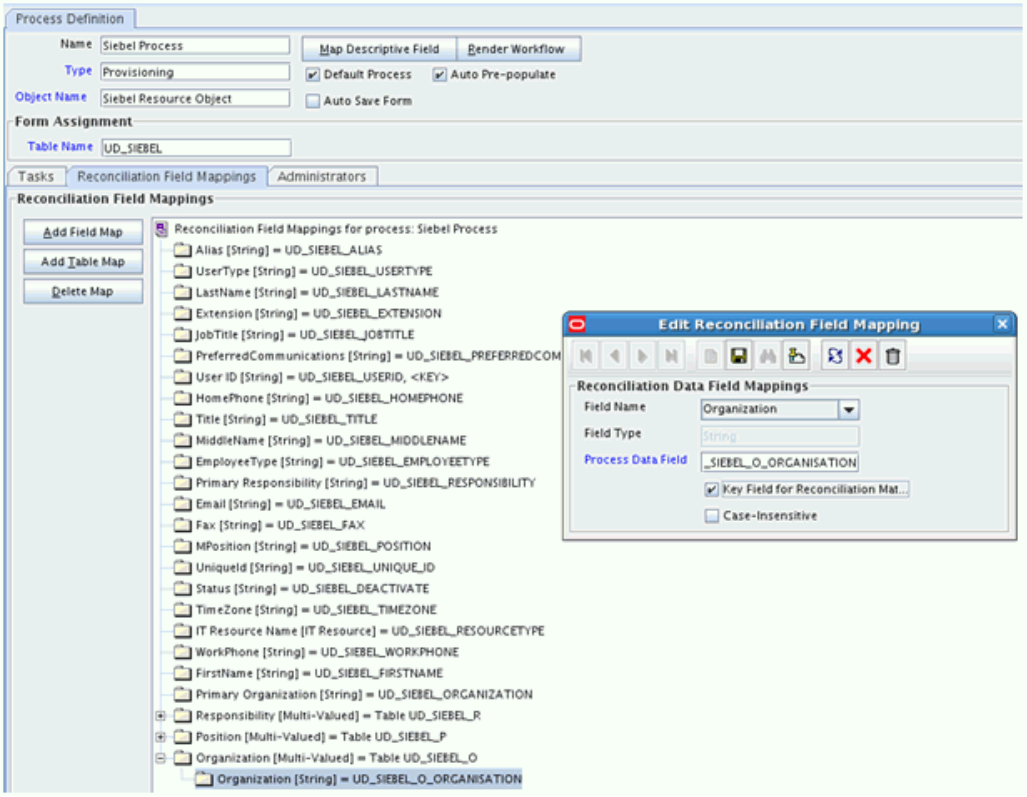


f. Right-click the newly created field, and select **Define Property Field Map**.

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**.

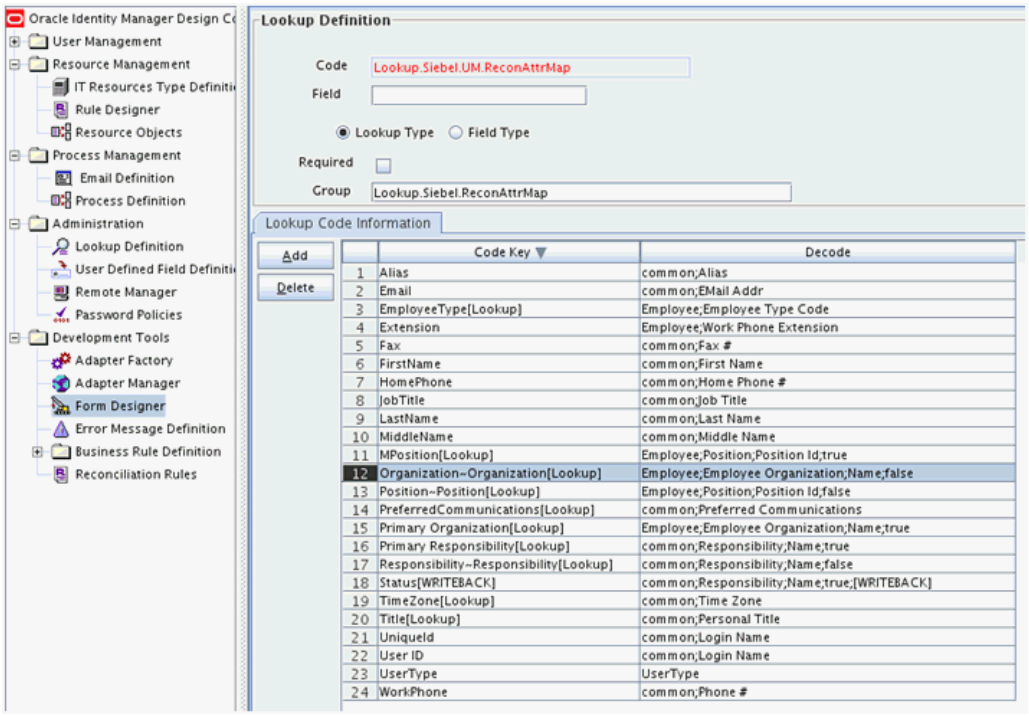


6. Create an entry for the attribute in the lookup definition for reconciliation as follows:
   a. Expand **Administration**.
   b. Double-click **Lookup Definition.**
   c. Search for and open the **Lookup.Siebel.UM.ReconAttrMap** lookup definition.
   d. Add the Code Key and Decode of the multivalued attribute in the lookup definition. The Code Key value must be the name of the attribute in the Resource Object along with the containing multivalued attribute name in tilde notation. The Decode value must be the name of the attribute in the target system. See User Attributes for Reconciliation for more information about the format of the Code Key and Decode values.

      For example:

      Code Key: `Organization~Organization[Lookup]`

      Decode: `Employee;Employee Organization;Name;false`



7. Define the connector. If you are planning to perform any of the other procedures described in this chapter, perform those procedures and then define the connector. See Defining the Connector for more information.
8. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for the procedures.

4.5 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.

To add a new multivalued attribute for provisioning:

1. Perform the procedure described in Creating and Populating a New Lookup Definition.

   > **Note:**
   >
   > You can skip this step if you are not adding a lookup-based attribute or if you have created and populated a new lookup definition earlier.

2. In the Oracle Identity Manager Design Console, create a process form and add attributes for the multivalued attribute by performing Step 2 of Adding New Multivalued Attributes for Reconciliation.

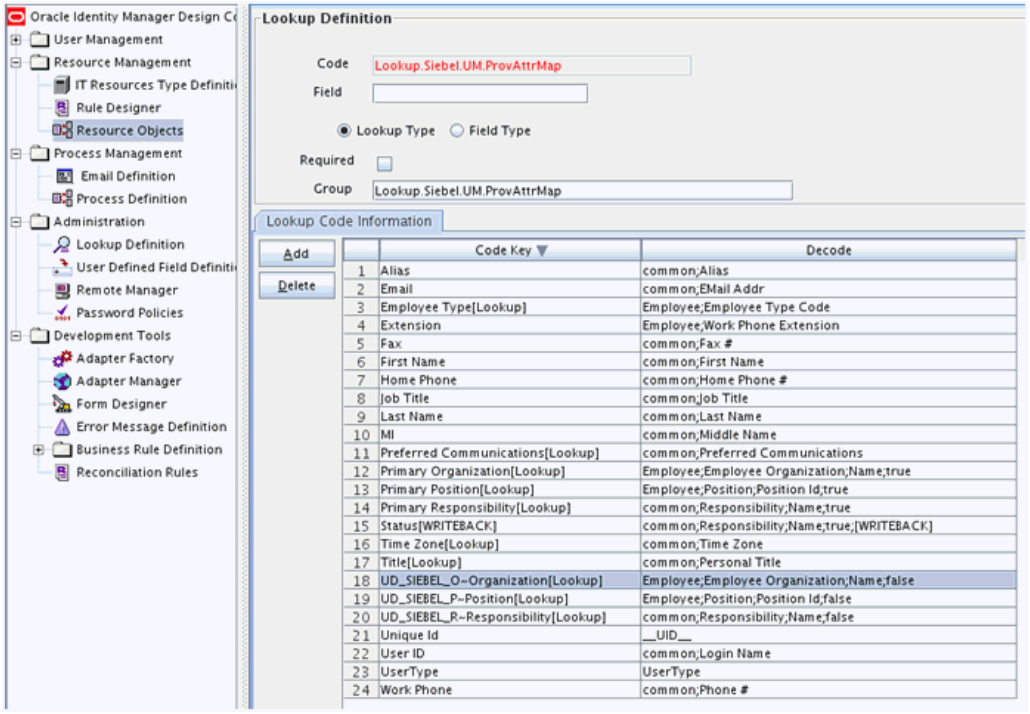
   If you have already performed this procedure, then ignore this step.

3. Create an entry for the attribute in the lookup definition for provisioning as follows:
   a. Expand **Administration,** and then double-click **Lookup Definition.**
   b. Search for and open the **Lookup.Siebel.UM.ProvAttrMap** lookup definition.
   c. Add the Code Key and Decode of the multivalued attribute in the lookup definition. See User Attributes for Provisioning for more information about the format of the Code Key and Decode values.

      For example:

      Code Key: `UD_SIEBEL_O~Organization[lookup]`

      Decode: `Employee;Employee Organization;Name;false`



4. To enable the update of a new multivalued attribute for provisioning:
   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. To do so, click **Add**, enter the name of the task for adding multivalued attributes, and enter the task description.
   e. 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 **Organization** from the list.

      Select **Insert** as the trigger type for adding multivalued data. Alternatively, select **Delete** as the trigger type for removing multivalued data and select **Update** as the trigger type for updating multivalued data.
   f. On the **Integration** tab, click **Add**, and then click **Adapter**.
   g. Select the **adpSIEBELUPDATECHILDTABLE** adapter, click **Save**, and then click **OK** in the message.
   h. 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	Literal Value
Adapter return value	Object	Response code	NA	NA	NA
objectType	String	Literal	String	NA	User
childTableName	String	Literal	String	NA	UD_SIEBEL_O
itResourceFieldName	String	Literal	String	NA	UD_SIEBEL_RESOURCETYPE
iProcessInstanceKey	Long	Process data	processinstance	NA	NA

i. Click the **Save** icon and then close the dialog box.

j. Create similar tasks for insert, delete and update of child form, changing only the trigger type.

> **Note:**
>
> Perform steps 5 through 7 only if you want to perform request-based provisioning.

5. 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.

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

```
<AttributeReference
name = "Siebel Organization form"
attr-ref = "UD_SIEBEL_O"
type = "String"
widget = "text"
length = "255"
available-in-bulk = "false"/>
    <AttributeReference
    name = "organisation"
    attr-ref = "Organization"
    type = "String"
    widget = "lookup"
    length = "255"
    available-in-bulk = "false"/>
</AttributeReference>
```

      In the parent AttributeReference element:

- For the name attribute, enter the value in the description field of the newly created process form.

  For example, if "Siebel Organization form" is the description of the UD_SIEBEL_O table, then you must specify `Siebel Organization form` as the value of the name attribute in the AttributeReference element.

  - For the attr-ref attribute, enter the full table name, such as UD_SIEBEL_O.

  - For the type attribute, enter `String`, the value that you entered in the Variant Type column of the process form while performing Step 3.

  - For the widget attribute, enter `text`, the widget name corresponding to the value entered in the Field Type column of the process form while performing Step 3.

  - 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`.

c. Add child AttributeReference elements for each attribute in the new process form by performing the procedure in Step 4 of Adding New Attributes for Provisioning.

d. Save and close the XML file.

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

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

   See Importing Request Datasets for detailed information about the procedure.

8. Define the connector. If you are planning to perform any of the other procedures described in this chapter, perform those procedures and then define the connector. See Defining the Connector for more information.

9. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Creating a New UI Form and Updating an Existing Application Instance with a New Form for the procedures.

4.6 Adding New Siebel Business Objects and Business Components for Reconciliation

Note:

- This section describes an optional procedure. Perform this procedure only if you want to add new Siebel Business Objects and Business Components for reconciliation.
- **Account Object:** We do support all account related objects in Siebel connector and we ship OIM artifacts for "Employee" and "User" objects. For supporting other account related objects, you need to write the OIM artifacts for the same as per the instructions given in Adding New Siebel Business Objects and Business Components for Reconciliation, and Adding New Siebel Business Objects and Business Components for Provisioning.
- **Non-account objects:** We do support Siebel's non-account object for create operation only, but not for other operations (that is, update and reconciliation). By default, we do not ship any artifacts for non-account objects. You need to write the whole set of OIM artifact for non-account objects. Oracle Identity Manager supports User, Org and Group entities only and resource object can either be attached to User or Org. Therefore, in case of supporting non-account objects of target system, you can use the following solution:
  - You can create an Org in Oracle Identity Manager with name (SiebelPositionManagement) and open this Org.
  - Click the **Resource** tab and provision the new Siebel positions to the target.

To add a new business object or business component for reconciliation, perform the following procedure:

1. Log in to the Administrative and User Console.
2. Ensure that you have specified appropriate values for the following:
   - The userBusObj and userBusComp IT resource parameters. See Configuring the IT Resource for the Target System for more information.
   - The userType attribute of the Siebel Target User Reconciliation scheduled job. See Scheduled Jobs for Reconciliation of User Records for more information.
3. Log in to the Design Console.
4. Add attributes for the new business object or business component to the existing **Siebel** process form. See Step 2 of Adding New Attributes for Reconciliation for more information.

   Alternatively, you can create a new process form and then add attributes for the new business object or business component to it. See Creating A Process Definition in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about creating a process form.
5. Add the new attribute for the business object or business component to the list of reconciliation fields in the **Siebel** resource object. See 3 of Adding New Attributes for Reconciliation for more information.

6. Create an entry in the Lookup.Siebel.UM.ReconAttrMap lookup definition for the newly added business object or business component. See Step 5 of Adding New Attributes for Reconciliation for more information.
7. If you are planning to perform procedures related to connector lifecycle management features (for example, upgrading, cloning, or uninstalling the connector), then define the connector. See Defining the Connector for more information.

> **See Also:**
>
> Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about connector lifecycle management features

4.7 Adding New Siebel Business Objects and Business Components for Provisioning

> **Note:**
>
> - This section describes an optional procedure. Perform this procedure only if you want to add new Siebel Business Objects and Business Components for provisioning.
> - **Account Object:** We do support all account related objects in Siebel connector and we ship OIM artifacts for "Employee" and "User" objects. For supporting other account related objects, you need to write the OIM artifacts for the same as per the instructions given in Adding New Siebel Business Objects and Business Components for Reconciliation, and Adding New Siebel Business Objects and Business Components for Provisioning.
> - **Non-account objects:** We do support Siebel's non-account object for create operation only, but not for other operations (that is, update and reconciliation). By default, we do not ship any artifacts for non-account objects. You need to write the whole set of OIM artifact for non-account objects. Oracle Identity Manager supports User, Org and Group entities only and resource object can either be attached to User or Org. Therefore, in case of supporting non-account objects of target system, you can use the following solution:
>   - You can create an Org in Oracle Identity Manager with name (SiebelPositionManagement) and open this Org.
>   - Click the **Resource** tab and provision the new Siebel positions to the target.

To add a new business object or business component, perform the following procedure:

1. Log in to the Administrative and User Console.
2. Ensure that you have specified values appropriate values for the userBusObj and userBusComp IT resource parameters. See Configuring the IT Resource for the Target System for more information.
3. Log in to the Design Console.

4. Add attributes for the new business object or business component to the process form.

> **Note:**
>
> Directly proceed to Step 5 if you have already added attributes for the business object or business component to the process form while performing the procedure described in Adding New Siebel Business Objects and Business Components for Reconciliation.

You can add attributes for the business object or business component to the existing **Siebel** process form as described in Step 2 of Adding New Attributes for Provisioning for more information.

Alternatively, you can create a new process form and then add the business object or business component as an attribute. See Creating A Process Definition in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about creating a process form.

5. Create an entry in the Lookup.Siebel.UM.ProvAttrMap lookup definition for the newly added business object or business component. See Step 5 of Adding New Attributes for Reconciliation for more information.
6. If you are planning to perform procedures related to connector lifecycle management features (for example, upgrading, cloning, or uninstalling the connector), then define the connector. See Defining the Connector for more information.

> **See Also:**
>
> Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about connector lifecycle management features

4.8 Configuring Transformation of Data During User 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. Write code that implements the required transformation logic in a Java class.

This transformation class must implement the oracle.iam.connectors.common.transform.Transformation interface and the transform method.

> **See Also:**
>
> The Javadocs shipped with the connector for more information about this interface

The following sample transformation class creates a value for the Full Name attribute by using values fetched from the First Name and Last Name attributes of the target system:

```
package oracle.iam.connectors.common.transform;

import java.util.HashMap;

public class TransformAttribute implements Transformation {

      /*
      Description:Abstract method for transforming the attributes

      param hmUserDetails<String,Object>

      HashMap containing parent data details

      param hmEntitlementDetails <String,Object>

      HashMap containing child data details

      */
      public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails,String sField) {
      /*
       * You must write code to transform the attributes.
       Parent data attribute values can be fetched by
       using hmUserDetails.get("Field Name").
       *To fetch child data values, loop through the
       * ArrayList/Vector fetched by hmEntitlementDetails.get("Child          Table")
       * Return the transformed attribute.
       */
      String sFirstName= (String)hmUserDetails.get("First Name");
      String sLastName= (String)hmUserDetails.get("Last Name");
      String sFullName=sFirstName+"."+sLastName;
      return sFullName;
      }
}
```

2. Create a JAR file to hold the Java class.
3. Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

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

- For Microsoft Windows: *OIM_HOME*/server/bin/UploadJars.bat
- For UNIX: *OIM_HOME*/server/bin/UploadJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. Add an entry in the Lookup.Transform.Siebel lookup definition as following:

   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`

   a. Log in to the Design Console.
   b. Search for and open the **Lookup.Siebel.UM.ReconTransformation** lookup definition.
   c. In the **Code Key** column, enter the name of the attribute on which you want to apply the transformation. For example: `FirstName`.
   d. In the **Decode** column, enter the name of the class file. For example: `com.thortech.xl.schedule.tasks.AppendTransformer`.
   e. Save the changes to the lookup definition.
   f. Save the changes to the lookup definition.

4.9 Configuring Validation of Data During Reconciliation and Provisioning

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

For data that fails the validation check, the following message is displayed or recorded in the log file:

`Value returned for field` *`FIELD_NAME`* `is false.`

> **Note:**
>
> This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

   This validation class must implement the oracle.iam.connectors.common.validate.Validator interface and the validate method.

   > **See Also:**
   >
   > The Javadocs shipped with the connector for more information about this interface

   The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
public boolean validate(HashMap hmUserDetails,
              HashMap hmEntitlementDetails, String field) {
            /*
          * You must write code to validate attributes. Parent
          * data values can be fetched by using hmUserDetails.get(field)
          * For child data values, loop through the
          * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
          * Depending on the outcome of the validation operation,
          * the code must return true or false.
          */
          /*
          * In this sample code, the value "false" is returned if the field
          * contains the number sign (#). Otherwise, the value "true" is
          * returned.
          */
             boolean valid=true;
             String sFirstName=(String) hmUserDetails.get(field);
             for(int i=0;i<sFirstName.length();i++){
               if (sFirstName.charAt(i) == '#'){
                     valid=false;
                     break;
               }
             }
             return valid;
      }
```

2. Create a JAR file to hold the Java class.
3. Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

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

   - For Microsoft Windows: *OIM_HOME*/server/bin/UploadJars.bat
   - For UNIX: *OIM_HOME*/server/bin/UploadJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Search for and open the **Lookup.Siebel.UM.ReconValidation** lookup definition.
   c. In the Code Key, enter the resource object field name. In the Decode, enter the class name.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.Siebel.UM.Configuration** lookup definition.
   f. Ensure that the value of the **Recon Validation Lookup** entry is set to `Lookup.Siebel.UM.ReconValidation`.
   g. Save the changes to the lookup definition.
5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Search for and open the **Lookup.Siebel.UM.ProvValidation** lookup definition.
   c. In the **Code Key** column, enter the process form field name. In the **Decode** column, enter the class name.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.Siebel.UM.Configuration** lookup definition.
   f. Ensure that the value of the **Recon Transformation Lookup** entry is set to `Lookup.Siebel.UM.ReconTransformation`.
   g. Save the changes to the lookup definition.

4.10 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

You can use access policies to manage multiple installations of the target system.

> **Note:**
>
> If you want to create copies of all the objects that constitute the connector, then see Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*

4.11 Defining the Connector

By using the Administrative and User Console, you can define a customized or reconfigured connector. Defining a connector is equivalent to registering the connector with Oracle Identity Manager.

A connector is automatically defined when you install it using the Install Connectors feature or when you upgrade it using the Upgrade Connectors feature. You must manually define a connector if:

- You import the connector by using the Deployment Manager.
- You customize or reconfigure the connector.
- You upgrade Oracle Identity Manager.

The following events take place when you define a connector:

- A record representing the connector is created in the Oracle Identity Manager database. If this record already exists, then it is updated:
- The status of the newly defined connector is set to Active. In addition, the status of a previously installed release of the same connector automatically is set to Inactive.

See Defining Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the procedure to define connectors.

4.12 Configuring the Connector for Multiple Versions of the Target System

For multiple versions of the target system:

1. Configure values for the parameters of the connector server IT resource.
2. After configuring follow below steps :
    a. Copy the bundle/org.identityconnectors.siebel-12.3.0.jar file into the *CONNECTOR_SERVER_HOME*/bundles directory.
    b. Depending on the target system that you are using, copy the following third-party JAR files from the *SIEBEL_INSTALLATION_DIRECTORY*/siebsrvr/CLASSES directory into the *CONNECTOR_SERVER_HOME*/lib directory:
    - - For Siebel 7.5 through 7.7:
    - SiebelJI.jar
    - SiebelJI_Common.jar
    - SiebelJI_enu.jar
    - - For Siebel 7.8 through 8.2.2 and Siebel Innovation Pack 2015, 2016, 2017, 2018, Siebel 19.*x*and Siebel 20.*x*:
        – Siebel.jar
        – SiebelJI_enu.jar
3. Start the connector server.

See Also:

- For more information on installing and running connector server, see Using an Identity Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance.

4.13 Configuring the Connector to Remove Old Primary Position or Responsibility

Note:

Perform the procedure described in this section if you want to remove the old primary position or responsibility when it is changed.

To configure the connector to remove the old primary position or responsibility:

1. Log in to the Design Console.
2. Search for and open the **Siebel Process** process definition.
3. From the list of process tasks displayed, search for and open the **Primary Position Update** process task.
4. On the Responses tab, click the **Success** response.
5. Select the **Tasks To Generate** tab and click **Assign.**
6. Select the **Child Position Update** task and click the right arrow on the table. This will move the selected task to the right hand side of Task Name table. Click **OK.**
7. Click **Save** to save the task.
8. Click **Save** once again to save the process definition.
9. To remove the old primary responsibility, repeat Steps 3 through 8 with the following difference:

   While performing Steps 3 and 6, select the **Child Responsibility Update** task instead of the Child Position Update task.

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:

- Testing Provisioning Operations
- Troubleshooting

5.1 Testing Provisioning Operations

You can use the testing utility to test basic provisioning operations such as create, update, or delete on the target system. The testing utility is implemented using ICF to invoke connector operations on this connector.

To use the testing utility:

1. Add the following JAR files to the CLASSPATH environment variable and the *JAVA_HOME*/jre/lib/ext directory:

   > **Note:**
   >
   > These JAR files are delivered as part of the OIM EAR application, and they are located in the oim.ear/APP-INF/lib directory.

   - connector-framework.jar
   - connector-framework-internal.jar
   - groovy-all.jar

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

   - For Siebel 7.5 through 7.7, the following JAR files located in the *OIM_HOME*/ConnectorDefaultDirectory/targetsystems-lib/siebel-***RELEASE_NUMBER*** directory:

     SiebelJI.jar

     SiebelJI_Common.jar

     SiebelJI_enu.jar

   - For Siebel 7.8 through 8.2.2 and Siebel Innovation Pack 2015, 2016, 2017, 2018, and Siebel 19.*x*, the following JAR files located in the *OIM_HOME*/ConnectorDefaultDirectory/targetsystems-lib/siebel-***RELEASE_NUMBER*** directory:

     Siebel.jar

     SiebelJI_enu.jar

2. Update the test-utility/example-config.groovy file on the installation media to reflect the configuration information of your environment. The following table describes the sections in the example-config.groovy file and whether you are required to configure those sections:

Section	Information	Preconfigured?
ICF Configuration	Parameters specific to the ICF configuration	Yes
Connector Configuration	Parameters required to connect to the target system These parameters are the same as the parameters of the IT resource. See Configuring the IT Resource for the Target System for more information about these parameters.	No, you must specify values for the properties in this section.
Create Account Attribute	Values required to create a user	Yes
Update Account Attribute	Values required to modify a user	Yes
Delete Account Attribute	User ID of the user to be deleted	No Comment this section if you do not want the user to be deleted.

3. Depending on the target system that you are using, run one of the following commands to test connector provisioning:

   - For Siebel 7.5 through 7.7:

     ```
     java -classpath ./test-utility.jar:./connector-framework-internal.jar:./groovy-
     all.jar:./connector-framework.jar:./SiebelJI.jar:./SiebelJI_Common.jar:./
     SiebelJI_enu.jar oracle.iam.connectors.testutility.Main example-config.groovy
     ```

   - For Siebel 7.8 through 8.2.2 and Siebel Innovation Pack 2015, 2016, 2017, 2018, and Siebel 19.*x*:

     ```
     java -classpath ./test-utility.jar:./connector-framework-internal.jar:./groovy-
     all.jar:./connector-framework.jar:./SiebelJI_enu.jar:/Siebel.jar
     oracle.iam.connectors.testutility.Main example-config.groovy
     ```

   You should see an output similar to the following:

```
Thread Id: 1    Time: 2011-06-05 20:05:28.413   Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest  Level: OK
Message: Using local bundle with url: [file:/scratch/jdoe/view_storage/
jdoe_oimcp_ade/idc/integration/oim/siebel/dist/siebel-11.1.1.6.0/bundle/
org.identityconnectors.siebel-1.0.1.jar]
Thread Id: 1    Time: 2011-06-05 20:05:28.545   Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest  Level: OK
Message: Using ConnectorKey [ConnectorKey( bundleName=org.identityconnectors.siebel
bundleVersion=1.0.1 connectorName=org.identityconnectors.siebel.SiebelConnector )]
Thread Id: 1    Time: 2011-06-05 20:05:28.546   Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest  Level: OK
Message: Using ConnectorInfo
[org.identityconnectors.framework.impl.api.local.LocalConnectorInfoImpl@142c778]
Thread Id: 1    Time: 2011-06-05 20:05:28.627   Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest  Level: INFO
Message: Connector configured
Thread Id: 1    Time: 2011-06-05 20:05:28.658   Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest  Level: INFO
Message: Got Connector Instance, ready to do the tests
Thread Id: 1    Time: 2011-06-05 20:05:28.660   Class:
org.identityconnectors.framework.impl.api.local.ConnectorPoolManager     Method:
getPool2        Level: INFO     Message: Creating new pool:
ConnectorKey( bundleName=org.identityconnectors.siebel bundleVersion=1.0.1
connectorName=org.identityconnectors.siebel.SiebelConnector )
Thread Id: 1    Time: 2011-06-05 20:05:28.668   Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest  Level: INFO
```

```
Message: Running 'test' operation on connector
Thread Id: 1    Time: 2011-06-05 20:05:31.762   Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest  Level: INFO
Message: 'test' operation succeeded
Thread Id: 1    Time: 2011-06-05 20:05:31.762   Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest  Level: INFO
Message: Running 'create' operation on connector
```

5.2 Troubleshooting

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

- Connection Errors
- Create User Errors
- Delete User Errors
- 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	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	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	Review the log for more details.

6
Known Issues and Workarounds

These are the known issues, workarounds, and FAQs associated with this release of the connector.

6.1 Connector Issues

The following are issues and workarounds associated with the connector:

6.1.1 Enabling SSO on Siebel

If single sign-on (SSO) is enabled on Siebel, then the connector operations may fail.

Workaround:

1. Open SIEBEL IT Resource Definition.
2. Update the **Trusted Token** field name to `trustedToken` and save it.
3. Ensure that all Siebel IT resources now contain trustedToken parameter rather than "Trusted Token" parameter.
4. Enter a dummy password in the **password** parameter of Siebel IT resource as it is a mandatory field in the OOTB connector.
5. Run the `PurgeCache.bat All` or `PurgeCache.sh All` command.
6. Restart Oracle Identity Manager.

6.1.2 Clearing a Non-Mandatory Field

If you clear a non-mandatory field for a provisioned user, the connector does not clear the value on the target system, but only in the process form in Oracle Identity Manager. In addition, the corresponding task is completed.

Workaround: This issue has been fixed and customers can request for a one-off patch for Bug 16700762 on top of this connector release.

6.2 Oracle Identity Manager Issues

The following are issues and workarounds associated with Oracle Identity Manager:

- Delete Reconciliation Revokes Accounts from All Siebel Target Systems

6.2.1 Updating Responsibility or Position on the Process Form

In Oracle Identity Manager release 11.1.2 BP04 (11.1.2.0.4), child table (both Responsibility and Position child forms) update does not function correctly. However, add and remove operations function correctly.

This issue has been fixed in Oracle Identity Manager release 11*g* R2 PS1.

6.2.2 Delete Reconciliation Revokes Accounts from All Siebel Target Systems

If a single OIM User has accounts provisioned in multiple Siebel target systems and if you delete an account from only one target system and run the delete reconciliation scheduled job, it is observed that the user accounts from all the target system are revoked.

For example, suppose you have configured two Siebel IT resources, called Siebel US and Siebel Global, and have provisioned a user "jdoe" to both. If jdoe's Siebel US account is deleted and perform delete reconciliation, it is expected that the status of jdoe's Siebel US account in Oracle Identity Manager is Revoked.However, it is observed that jdoe's account is set to Revoked status for both Siebel US and Siebel Global accounts.

This issue has been fixed in Oracle Identity Manager release 11*g* R2.

6.3 Target System Issues

The following are issues and workarounds associated with the target system:

- Setting Secondary and Primary Responsibility
- Deleting Position or Responsibility Assigned to a User
- Incremental Reconciliation Might Fail With Siebel Target System Version 20.*x*

6.3.1 Setting Secondary and Primary Responsibility

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.

There is no workaround available for this issue.

6.3.2 Deleting Position or Responsibility Assigned to a User

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. There is no workaround available for this issue.

6.3.3 Incremental Reconciliation Might Fail With Siebel Target System Version 20.*x*

If you are using Siebel target system version 20.*x*, incremental reconciliation may fail with the following error message:

```
SEVERE: <com.siebel.om.sisnapi.RequestException>
<Error><ErrorCode>7667856</ErrorCode>
<ErrMsg>Could not find `Business Object named `Get Users Data¿.
This object is inactive or nonexistent.(SBL-DAT-00144)</ErrMsg></Error>
</com.siebel.om.sisnapi.RequestException>
org.identityconnectors.framework.common.exceptions.ConnectorException:
<com.siebel.om.sisnapi.RequestException>
```

As a workaround, perform the following steps on Web Tools or Siebel Tools in the Siebel target system:

1. Create a Dev Workspace and activate a Business Object.
2. Get User Data and Business Component.
3. Get User Data and submit Dev Workspace for delivery.
4. Deliver Dev Workspace to the Integration branch (Main).

6.4 FAQs

The following is a frequently asked question (FAQ) associated with this connector:

Question: Does this connector support the Lock/Unlock functions?

Answer: No, because the target system does not support the Lock/Unlock.

Question: Does this connector support the Disable/Enable functions?

Answer: Yes, since the target system support the Disable/Enable.

A

Files and Directories on the Installation Media

These are the files and directories in the connector installation media that comprise the connector.
Table A-1 describes the files and directories on the installation media.

Table A-1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
bundle/org.identityconnectors.siebel-1.0.1.jar	This JAR file is the ICF bundle that the connector is using for the current release.
configuration/SiebelConnector-CI.xml	This XML file contains configuration information that is used during connector installation.
Files in the Datasets directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
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 Oracle Identity Manager database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.
test-utility/example-config.groovy	This file contains a sample configuration that you can modify to test basic provisioning operations.
test-utility/test-utility.jar	This JAR file contains the testing utility to conduct basic provisioning tests (create, update, and delete) on the connector.
xml/Siebel-ConnectorConfig.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/SiebelConnectorRequestDatasets.xml	This XML file contains the dataset related definitions for the create and modify user provisioning operations. This file is used if you want to enable request-based provisioning by using the deployment manager. **Note:** Use this file only if you are using Oracle Identity Manager release prior to 11.1.2.

B

Scheduled Jobs for Lookup Field Synchronization and Reconciliation

These are all the scheduled jobs that you can configure for lookup field synchronization and reconciliation.
Table B-1 lists the scheduled jobs that you can configure.

Table B-1 Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Scheduled Job	Description
Siebel Lookup Recon for Employee Type Code	This scheduled job is used for employee type code lookup field synchronization. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
Siebel Lookup Recon for Personal Title	This scheduled job is used for personal title lookup field synchronization. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
Siebel Lookup Recon for Position	This scheduled job is used for position lookup field synchronization. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
Siebel Lookup Recon for Preferred Communications	This scheduled job is used for preferred communication lookup field synchronization. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
Siebel Lookup Recon for Responsibility	This scheduled job is used for responsibility lookup field synchronization. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
Siebel Lookup Recon for TimeZone	This scheduled job is used for time zone lookup field synchronization. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
Siebel Target Resource User Recon	This scheduled job is used for user reconciliation in the target resource (account management) mode of the connector. See Scheduled Jobs for Reconciliation of User Records for information about this scheduled job.
Siebel Target Resource User Delete Reconciliation	This scheduled job is used for reconciliation of deleted user records in the target resource (account management) mode of the connector. See Scheduled Job for Reconciliation of Deleted Users Records for information about this scheduled job.
Siebel Trusted User Reconciliation	This scheduled job is used for user reconciliation in the trusted source (identity management) mode of the connector. See Scheduled Jobs for Reconciliation of User Records for information about this scheduled job.
Siebel Trusted User Delete Reconciliation	This scheduled job is used for reconciliation of deleted user records in the trusted source (identity management) mode of the connector. See Scheduled Job for Reconciliation of Deleted Users Records for information about this scheduled job.

Index