Oracle® Identity Governance

Configuring the Siebel User Management Connector

12.2.1.3.0
F84737-04
June 2025

Oracle Identity Governance Configuring the Siebel User Management Connector, 12.2.1.3.0

F84737-04

Copyright © 2017, 2025, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

Preface

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

1 Introduction to the Connector

1.1 Certified Components 1-1
1.2 Usage Recommendation 1-2
1.3 Certified Languages 1-2
1.4 Supported Connector Operations 1-3
1.5 Connector Architecture 1-3
1.6 Use Cases Supported by the Connector 1-5
1.7 Connector Features 1-6
1.7.1 User Provisioning 1-6
1.7.2 Full Reconciliation 1-7
1.7.3 Limited Reconciliation 1-7
1.7.4 Reconciliation Based on User Type 1-7
1.7.5 Reconciliation of Deleted User Records 1-7
1.7.6 Support for the Connector Server 1-7
1.7.7 Transformation and Validation of Account Data 1-8
1.7.8 Support for Enabling and Disabling Accounts 1-8

2 Creating an Application by Using the Connector

2.1 Prerequisites to be done in Siebel Target to Use the Enable/Disable Feature in the Connector 2-1
2.1.1 Manually Making Configuration Changes 2-1
2.1.2 Importing SIF File 2-3
2.2 Prerequisites for Creating an Application By Using the Connector 2-4
2.2.1 Configuring the Target System 2-4
2.2.1.1 Enabling RSA Encryption on Siebel 2-4

2.2.1.2 Configuring the Siebel Web Server Extension for RSA Encryption 2-5
2.2.1.3 Enabling RSA Encryption for the Siebel Call Center Application 2-5
2.2.1.4 Starting the Siebel Software Configuration Wizard 2-5
2.2.2 Using External Code Files 2-6
2.2.3 Creating the Target System User Account for Connector Operations 2-6
2.2.4 Downloading the Connector Installation Package 2-7
2.3 Process Flow for Creating an Application By Using the Connector 2-8
2.4 Creating an Application By Using the Siebel Connector 2-9

3 Configuring the Connector

3.1 Basic Configuration Parameters 3-1
3.2 Advanced Settings Parameters 3-7
3.3 Attribute Mappings 3-7
3.3.1 Attribute Mappings for the Target Application 3-7
3.3.2 Attribute Mappings for an Authoritative Application 3-11
3.4 Additional Configuration to Support the Enable/Disable Functionality 3-12
3.5 Correlation Rules 3-13
3.5.1 Correlation Rules for the Target Application 3-13
3.5.2 Correlation Rules for the Authoritative Application 3-15
3.6 Reconciliation Jobs 3-17

4 Performing Postconfiguration Tasks for the Connector

4.1 Configuring Oracle Identity Governance 4-1
4.1.1 Creating and Activating a Sandbox 4-1
4.1.2 Creating a New UI Form 4-1
4.1.3 Publishing a Sandbox 4-2
4.1.4 Updating an Existing Application Instance with a New Form 4-2
4.2 Harvesting Entitlements and Sync Catalog 4-3
4.3 Managing Logging for the Connector Server 4-3
4.3.1 Understanding Logging on the Connector Server 4-3
4.3.2 Enabling Logging for the Connector Server 4-4
4.3.3 Understanding Log Levels 4-4
4.3.4 Enabling Logging 4-5
4.4 Configuring the IT Resource for the Connector Server 4-6
4.5 Localizing Field Labels in UI Forms 4-7

5 Using the Connector

5.1 Guidelines to Apply While Using the Connector 5-1
5.2 Performing First-Time Reconciliation 5-1

5.3 Scheduled Job for Lookup Field Synchronization 5-2
5.4 Configuring Reconciliation 5-4
5.4.1 Performing Full Reconciliation 5-4
5.4.2 Performing Limited Reconciliation 5-4
5.4.3 Reconciliation Based on User Type 5-6
5.4.4 Reconciliation Scheduled Jobs 5-7
5.4.4.1 Scheduled Jobs for Reconciliation of User Records 5-7
5.4.4.2 Scheduled Job for Reconciliation of Deleted Users Records 5-8
5.5 Configuring Reconciliation Jobs 5-9
5.6 Configuring Provisioning 5-10
5.6.1 Performing Provisioning Operations 5-10
5.7 Connector Objects Used During Target Resource Reconciliation 5-10
5.7.1 User Attributes for Reconciliation 5-11
5.7.2 Reconciliation Rule for Target Resource Reconciliation 5-11
5.7.2.1 Target Resource Reconciliation Rule 5-12
5.7.2.2 Viewing Target Resource Reconciliation Rules in the Design Console 5-12
5.7.3 Reconciliation Action Rules for Target Resource Reconciliation 5-12
5.7.3.1 Target Resource Reconciliation Action Rules 5-12
5.7.3.2 Viewing Target Resource Reconciliation Action Rules in the Design Console 5-13
5.8 Connector Objects Used During Trusted Source Reconciliation 5-13
5.8.1 Reconciliation Rule for Trusted Source Reconciliation 5-13
5.8.1.1 Trusted Source Reconciliation Rule 5-14
5.8.1.2 Viewing Trusted Source Reconciliation Rule 5-14
5.8.2 Reconciliation Action Rules for Trusted Source Reconciliation 5-15
5.8.2.1 Trusted Source Reconciliation Action Rules 5-15
5.8.2.2 Viewing Trusted Source Reconciliation Action Rules 5-15
5.9 Uninstalling the Connector 5-16

6 Extending the Functionality of the Connector

6.1 Configuring Transformation and Validation of Data 6-1
6.2 Configuring Action Scripts 6-1
6.3 Configuring the Connector for Multiple Installations of the Target System 6-2
6.4 Configuring the Connector for Multiple Versions of the Target System 6-2

7 Known Issues and Workarounds

7.1 Connector Issues 7-1
7.1.1 Enabling SSO on Siebel 7-1
7.1.2 Clearing a Non-Mandatory Field 7-1
7.2 Oracle Identity Manager Issues 7-1

7.2.1 Updating Responsibility or Position on the Process Form 7-2
7.2.2 Delete Reconciliation Revokes Accounts from All Siebel Target Systems 7-2
7.3 Target System Issues 7-2
7.3.1 Setting Secondary and Primary Responsibility 7-2
7.3.2 Deleting Position or Responsibility Assigned to a User 7-2
7.3.3 Incremental Reconciliation Might Fail With Siebel Target System Version 20.x 7-3
7.4 FAQs 7-3

8 Files and Directories on the Installation Media

Index

List of Figures

1-1	Siebel Connector Architecture	1-4
2-1	Overall Flow of the Prcoess for Creating an Application By Using the Connector	2-8
3-1	Default Attribute Mappings for Siebel User Account	3-9
3-2	Default Attribute Mappings for Siebel Positions	3-10
3-3	Default Attribute Mappings for Responsibilities	3-11
3-4	Default Attribute Mappings for Siebel Authoritative Application	3-12
3-5	Default Attribute Mappings for Siebel Target Application to Support the Enable/Disable Functionality	3-13
3-6	Default Attribute Mappings for Siebel Authoritative Application to support Enable/Disable functionality	3-13
3-7	Simple Correlation Rule for an Siebel Target Application	3-14
3-8	Predefined Situations and Responses for an Siebel Target Application	3-15
3-9	Simple Correlation Rule for an Siebel Authoritative Application	3-16
3-10	Predefined Situations and Responses for a Siebel Authoritative Application	3-17
5-1	Target Resource Reconciliation Action Rules	5-13
5-2	Reconciliation Rule for Trusted Source Reconciliation	5-14
5-3	Reconciliation Action Rules for Trusted Source Reconciliation	5-15

List of Tables

1-1	Certified Components	1-2
1-2	Supported Connector Operations	1-3
1-3	Supported Connector Features Matrix	1-6
3-1	Parameters in the Basic Configuration	3-1
3-2	Advanced Settings Parameters	3-7
3-3	Default Attributes for Siebel Target Application	3-8
3-4	Default Attribute Mappings for Positions	3-10
3-5	Default Attribute Mappings for Responsibilities	3-10
3-6	Default Attribute Mappings for Siebel Authoritative Application	3-11
3-7	Default Attributes for Siebel Target Application to Support the Enable/Disable Functionality	3-13
3-8	Default Attributes for Siebel Authoritative Application to Support the Enable/Disable Functionality	3-13
3-9	Predefined Identity Correlation Rule for a Siebel Target Application	3-14
3-10	Predefined Situations and Responses for an Siebel Target Application	3-15
3-11	Predefined Identity Correlation Rule for an Siebel Authoritative Application	3-15
3-12	Predefined Situations and Responses for an Siebel Authoritative Application	3-16
3-13	Parameters of the Siebel Full User Reconciliation Job	3-17
3-14	Parameters of the Siebel User Trusted Reconciliation Job	3-19
3-15	Parameters of the Siebel Target User Delete Reconciliation Job	3-20
3-16	Parameters of the Siebel Trusted User Delete Reconciliation Job	3-21
3-17	Parameters of the Reconciliation Jobs for Entitlements	3-21
4-1	Log Levels and ODL Message Type:Level Combinations	4-5
4-2	Parameters of the IT Resource for the Siebel Connector Server	4-6
5-1	Attributes of the Scheduled Jobs for Lookup Field Synchronization	5-2
5-2	Attributes of the Scheduled Jobs for Reconciliation of User Records	5-7
5-3	Attributes of the Scheduled Job for Reconciliation of Deleted Users Records	5-8
5-4	Target Resource Reconciliation Action Rules	5-12
5-5	Action Rules for Trusted Source Reconciliation	5-15
8-1	Files and Directories on the Installation Media	8-1

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.

1
Introduction to the Connector

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

The Siebel Connector lets you create and onboard Siebel applications in Oracle Identity Governance.

> **Note:**
>
> In this guide, the connector that is deployed using the **Applications** option on the **Manage** tab of Identity Self Service is referred to as an **AOB application**.

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

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

The following topics provide a high-level overview of the connector:

- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations
- Connector Architecture
- Use Cases Supported by the Connector
- Connector Features

1.1 Certified Components

These are the software components and their versions required for installing and using the Siebel 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) or later version • Oracle Identity Governance 12c (12.2.1.3.0) or later version
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later version
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*, 23.*x*, 24.*x*, 25.*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*, 25.*x* target systems.
Connector Server	12.2.1.3.0 or 11.1.2.1.0
Connector Server JDK	JDK 1.8 and later version
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*,23.*x*,24.*x*, 25.*x*: Siebel.jar and SiebelJI_enu.jar

1.2 Usage Recommendation

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

1.3 Certified Languages

This release of the connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Czech
- Danish
- Dutch
- English
- Finnish
- French

- French (Canadian)
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.4 Supported Connector Operations

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

Table 1-2 Supported Connector Operations

Operation	Supported
User Management	
Create user	Yes
Update user	Yes
Enable user	Yes
Disable user	Yes
Delete user	Yes
Reset Password	No
Position Grant Management	
Assign and Revoke Position	Yes
Responsibility Grant Management	
Assign and Revoke Responsibility	Yes

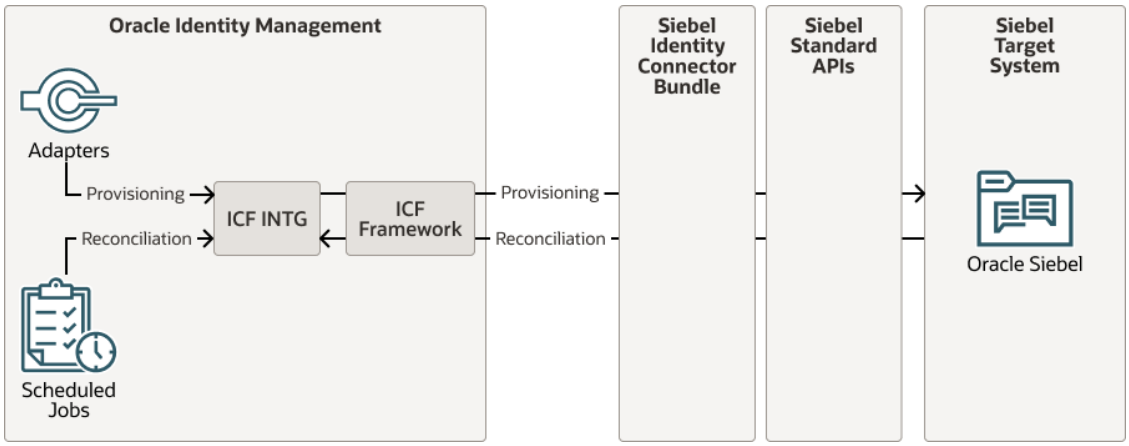
1.5 Connector Architecture

The Siebel is implemented by using the Identity Connector Framework (ICF).

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

Figure 1-1 shows the architecture of the Siebel.

Figure 1-1 Siebel Connector Architecture



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

- Account management
  Account management is also known as target resource management. In this mode, the target system is used as a target resource and the connector enables the following operations:
  - Provisioning
    Provisioning involves creating, updating, or deleting users on the target system through Oracle Identity Governance. During provisioning, the Adapters invoke ICF operation, ICF in turn invokes create operation on the Siebel Identity Connector Bundle and then the bundle calls the target system API (Siebel API) for provisioning operations. The API on the target system accepts provisioning data from the bundle, carries out the required operation on the target system, and returns the response from the target system back to the bundle, which passes it to the adapters.
  - Target resource reconciliation
    During reconciliation, a scheduled task invokes an ICF operation. ICF in turn invokes a search operation on the Siebel Identity Connector Bundle and then the bundle calls Siebel API for Reconciliation operation. The API extracts user records that match the reconciliation criteria and hands them over through the bundle and ICF back to the scheduled task, which brings the records to Oracle Identity Governance.

    Each record fetched from the target system is compared with Siebel resources that are already provisioned to OIM Users. If a match is found, then the update made to the Siebel record from the target system is copied to the Siebel resource in Oracle Identity Governance. If no match is found, then the Name of the record is compared with the User Login of each OIM User. If a match is found, then data in the target system record is used to provision an Siebel resource to the OIM User.

The Siebel Identity Connector Bundle communicates with the Siebel API using the HTTPS protocol. The Siebel API provides programmatic access to Siebel through Siebel API endpoints. Apps can use the Siebel API to perform create, read, update, and delete (CRUD) operations on directory data and directory objects, such as users, positions, and responsibilities.

See Also:

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

1.6 Use Cases Supported by the Connector

The Siebel is used to integrate Oracle Identity Governance with Siebel to ensure that all Siebel accounts are created, updated, and deactivated on an integrated cycle with the rest of the identity-aware applications in your enterprise. The Siebel supports management of identities for Cloud Identity, Synchronized Identity, and Federated Identity models of Siebel. In a typical IT scenario, an organization using Oracle Identity Governance wants to manage accounts, positions, and responsibilities across Siebel Service. The following are some of the most common scenarios in which this connector can be used:

- **Siebel User Management**:
  An organization using Siebel wants to integrate with Oracle Identity Governance to manage identities. The organization wants to manage its user identities by creating them in the target system using Oracle Identity Governance. The organization also wants to synchronize user identity changes performed directly in the target system with Oracle Identity Governance. In such a scenario, a quick and an easy way is to install the Siebel and configure it with your target system by providing connection information.

  To create a new user in the target system, fill in and submit the OIM process form to trigger the provisioning operation. The connector executes the CreateOp operation against your target system and the user is created on successful execution of the operation. Similarly, operations like delete and update can be performed.

  To search or retrieve the user identities, you must run a scheduled task from Oracle Identity Governance. The connector will run the corresponding SearchOp against the user identities in the target system and fetch all the changes to Oracle Identity Governance
- **Siebel Position Management**:
  An organization has several Siebel positions allowing its users to set up new positions, manage, and delete positions. The organization now wants to know the list of positions that have not been recently accessed or who has no position. In such a scenario, you can use the Siebel to highlight the usage trend for positions. By using the Siebel, you can leverage the reporting capabilities of Oracle Identity Governance to track any operations (such as create, update, delete) performed on positions.
- **Siebel Responsibility Management**:
  In large organizations, it may be necessary for an administrator to designate other employees to act as administrators to serve different functions. For example, you can set responsibilities for your IT staff that can act as support agents to other employees, partners, customers, and vendors. With the Siebel, you can assign or revoke a Siebel responsibility to users as an entitlement, thus facilitating you to leverage the delegated administration capability of Siebel.

1.7 Connector Features

The features of the connector include support for connector server, full reconciliation, limited reconciliation, and reconciliation of deleted account data.

Table 1-3 provides the list of features supported by the AOB application.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application
Full reconciliation	Yes
Limited reconciliation	Yes
Delete reconciliation	Yes
Use connector server	Yes
Transformation and validation of account data	Yes
Perform connector operations in multiple domains	Yes
Support for paging	No
Test connection	Yes
Reset password	No
Siebel Position assignment	Yes
Siebel Responsibility assignment	Yes
User Provisioning	Yes

The following topics provide more information on the features of the AOB application:

- User Provisioning
- Full Reconciliation
- Limited Reconciliation
- Reconciliation Based on User Type
- Reconciliation of Deleted User Records
- Support for the Connector Server
- Transformation and Validation of Account Data
- Support for Enabling and Disabling Accounts

1.7.1 User Provisioning

User provisioning involves creating or modifying the account data on the target system through Oracle Identity Governance.

> **Note:**
>
> For more information, see Performing Provisioning Operations.

1.7.2 Full Reconciliation

You can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance.

After the first full reconciliation run, you can configure your connector if the target system contains an attribute that holds the timestamp at which an object is created or modified.

1.7.3 Limited Reconciliation

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

You can set a reconciliation filter as the value of the Custom Recon Query attribute of the user reconciliation scheduled job. The Custom Recon Query attribute helps you to assign filters to the API based on which you get a filtered response from the target system.

For more information, see Performing Limited Reconciliation.

1.7.4 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.

1.7.5 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.

1.7.6 Support for the Connector Server

Connector Server is one of the features provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles.

A Java connector server is useful when you do not want 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 if the bundle works faster when deployed on the same host as the native managed resource.

> **See Also:**
>
> Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installing and configuring connector server and running the connector server

1.7.7 Transformation and Validation of Account Data

You can configure transformation and validation of account data that is brought into or sent from Oracle Identity Governance during reconciliation and provisioning operations by writing Groovy scripts while creating your application.

For more information, see Validation and Transformation of Provisioning and Reconciliation Attributes in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.7.8 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.

2

Creating an Application by Using the Connector

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

- Prerequisites to be done in Siebel Target to Use the Enable/Disable Feature in the Connector
- Prerequisites for Creating an Application By Using the Connector
- Process Flow for Creating an Application By Using the Connector
- Creating an Application By Using the Siebel Connector

2.1 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 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

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

2.1.2 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.**
    b. Enter the name of your Workspace and provide comments to create the workspace. The workspace is now visible under Main.
    c. 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.
    b.
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.

2.2 Prerequisites for Creating an Application By Using the Connector

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

- Configuring the Target System
- Using External Code Files
- Creating the Target System User Account for Connector Operations
- Downloading the Connector Installation Package

2.2.1 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

2.2.1.1 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.

2.2.1.2 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.

2.2.1.3 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**.

2.2.1.4 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.

2.2.2 Using External Code Files

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

- 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, Siebel 19.x, Siebel 20.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

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

2.2.3 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.

2.2.4 Downloading the Connector Installation Package

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

To download the connector installation package:

1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html.
2. Click **OTN License Agreement** and read the license agreement.
3. Select the **Accept License Agreement** option.

   You must accept the license agreement before you can download the installation package.
4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*

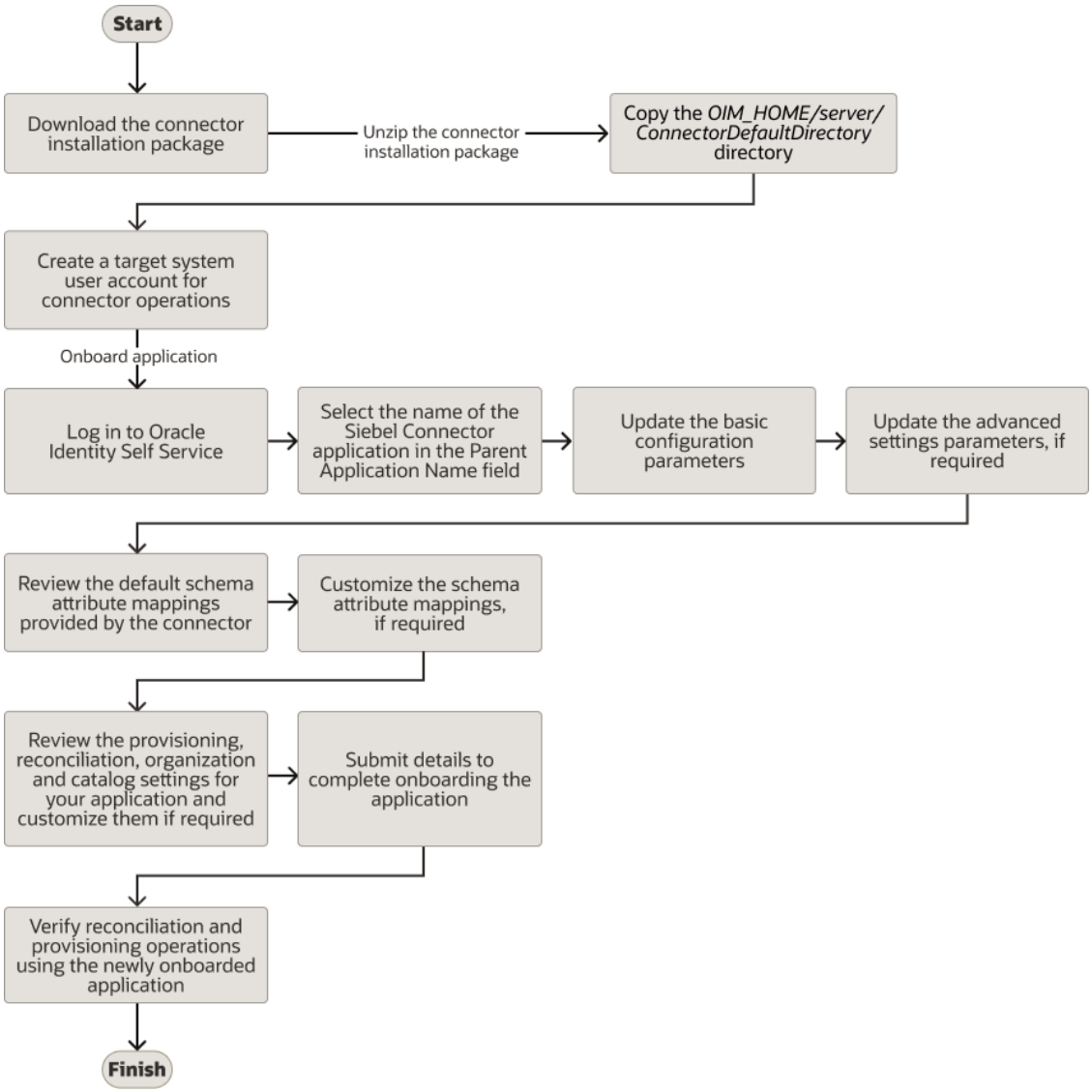
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

2.3 Process Flow for Creating an Application By Using the Connector

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

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

Figure 2-1 Overall Flow of the Prcoess for Creating an Application By Using the Connector



2.4 Creating an Application By Using the Siebel Connector

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

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

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

1. Create an application in Identity Self Service. The high-level steps are as follows:
   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
   b. Ensure that the **Connector Package** option is selected when creating an application.
   c. Update the basic configuration parameters to include connectivity-related information.
   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.
   e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.
   f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.
   g. Review the details of the application and click **Finish** to submit the application details. The application is created in Oracle Identity Governance.
   h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.
   If you click **Yes**, then the default form is automatically created and is attached with the newly created application. The default form is created with the same name as the application. The default form cannot be modified later. Therefore, if you want to customize it, click **No** to manually create a new form and attach it with your application.
2. Verify reconciliation and provisioning operations on the newly created application.

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

3
Configuring the Connector

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

- Basic Configuration Parameters
- Advanced Settings Parameters
- Attribute Mappings
- Additional Configuration to Support the Enable/Disable Functionality
- Correlation Rules
- Reconciliation Jobs

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to a Siebel application.

> **Note:**
>
> Unless specified, do not modify entries in the below table.

Table 3-1 Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
keyFieldName	Yes	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
userBusComp	Yes	Business Component of 'User' userTypeDefault value: User
password	Yes	Password of the target system user account that you want to use for connector operations Sample value: password

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
objectManager	Yes	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`
encryption	No	The 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.
employeeBusObj	Yes	The business object of Employee userType. Default value: Employee

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
Connector Server Name	No	The name of the IT resource of the type "Connector Server." **Note:** Enter a value for this parameter only if you have deployed the Siebel User Management connector in the Connector Server.
userName	Yes	The User ID of the target system user account that you want to use for connector operations Sample value: johnsmith

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
Configuration Lookup	No	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`.
gatewayServerPort	No	Listening port number for Siebel Connection Broker (SCBroker). Sample value : 2321
userBusObj	Yes	Business Object of the 'User' userType Default value: Users.
siebelServer	Yes	Name of the target system server Sample value: `SBA_SIEBEL`
gatewayServer	Yes	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: `phoenix200458.appsdev1.fusionappsdphx1.oraclevcn.com`

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
Version	Yes	The 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

Table 3-1 (Cont.) Parameters in the Basic Configuration

Parameter	Mandatory ?	Description
		target system, then enter 7.5.
ssoFlag	Yes	Enter True to specify that the target system is configured to use a SSO solution for authentication. Otherwise, enter False. Default value: false
trustedToken	No	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. Sample value: no
enterpriseServer	Yes	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
Language	Yes	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
employeeBusComp	Yes	Business Component of Employee userType Default value: Employee

3.2 Advanced Settings Parameters

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

> **Note:**
>
> - Unless specified, do not modify entries in the below table.
> - All parameters in the below table are mandatory.

Table 3-2 Advanced Settings Parameters

Parameter	Description
Bundle Name	This entry holds the name of the connector bundle. **Default value**: `org.identityconnectors.siebel`
Bundle Version	This entry holds the version of the connector bundle. **Default value**: 12.3.0
Connector Name	This entry holds the name of the connector class. **Default value**: `org.identityconnectors.siebel.SiebelConnector`

3.3 Attribute Mappings

The following topic provides the attribute mappings details.

- Attribute Mappings for the Target Application
- Attribute Mappings for an Authoritative Application

3.3.1 Attribute Mappings for the Target Application

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

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

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

Table 3-3 Default Attributes for Siebel Target Application

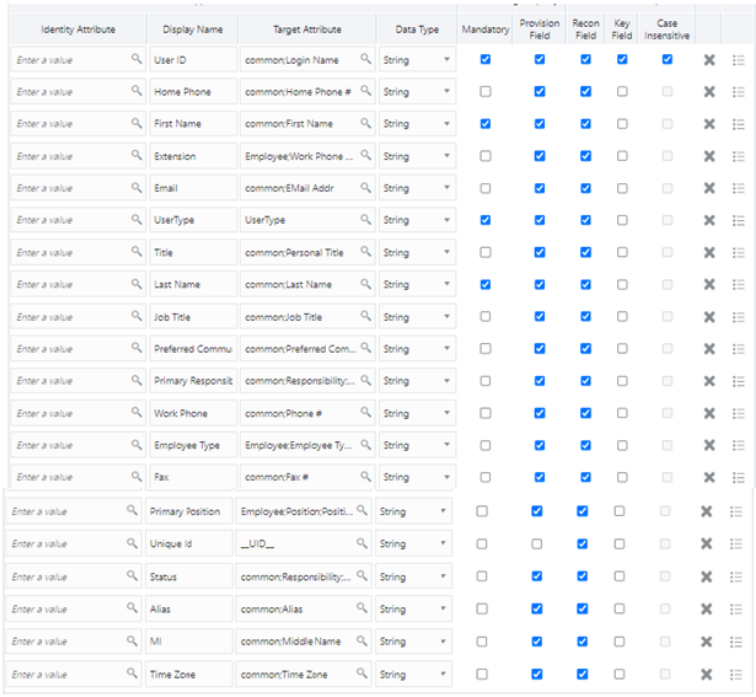
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User Id	common;Login Name	String	Yes	Yes	Yes	Yes	Yes
Home Phone	common;Home Phone #	String	No	Yes	Yes	No	Not applicable
First Name	common;First Name	String	Yes	Yes	Yes	No	Not applicable
Extension	Employee; Work Phone Extension	String	No	Yes	Yes	No	Not applicable
Email	common;E Mail Addr	String	No	Yes	Yes	No	Not applicable
UserType	UserType	String	Yes	Yes	Yes	No	Not applicable
Title	common;Personal Title	String	No	Yes	Yes	No	Not applicable
Last Name	common;Last Name	String	Yes	Yes	Yes	No	Not applicable
Job Title	common;Job Title	String	No	Yes	Yes	No	Not applicable
Preferred Communications	common;Preferred Communications	String	No	Yes	Yes	No	Not applicable
Primary Responsibility	common;Responsibility;Name;true	String	No	Yes	Yes	No	Not applicable
Work Phone	common;Phone #	String	No	Yes	Yes	No	Not applicable
Employee Type	Employee; Employee Type Code	String	No	Yes	Yes	No	Not applicable
Fax	common;Fax #	String	No	Yes	Yes	No	Not applicable
Primary Position	Employee; Position;Position Id;true	String	No	Yes	Yes	No	Not applicable
Unique Id	__UID__	String	No	No	Yes	No	Not applicable

Table 3-3 (Cont.) Default Attributes for Siebel Target Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Status	common;Responsibility;Name;true; [WRITEBACK]	String	No	Yes	Yes	No	Not applicable
Alias	common;Alias	String	No	Yes	Yes	No	Not applicable
MI	common;Middle Name	String	No	Yes	Yes	No	Not applicable
Time Zone	common;Time Zone	String	No	Yes	Yes	No	Not applicable

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

Figure 3-1 Default Attribute Mappings for Siebel User Account



Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive
Enter a value	User ID	common;Login Name	String	☑	☑	☑	☑	☑
Enter a value	Home Phone	common;Home Phone #	String	☐	☑	☑	☐	☐
Enter a value	First Name	common;First Name	String	☑	☑	☑	☐	☐
Enter a value	Extension	Employee;Work Phone ...	String	☐	☑	☑	☐	☐
Enter a value	Email	common;EMail Addr	String	☐	☑	☑	☐	☐
Enter a value	UserType	UserType	String	☑	☑	☑	☐	☐
Enter a value	Title	common;Personal Title	String	☐	☑	☑	☐	☐
Enter a value	Last Name	common;Last Name	String	☑	☑	☑	☐	☐
Enter a value	Job Title	common;Job Title	String	☐	☑	☑	☐	☐
Enter a value	Preferred Commu	common;Preferred Com...	String	☐	☑	☑	☐	☐
Enter a value	Primary Responsit	common;Responsibility;...	String	☐	☑	☑	☐	☐
Enter a value	Work Phone	common;Phone #	String	☐	☑	☑	☐	☐
Enter a value	Employee Type	Employee;Employee Ty...	String	☐	☑	☑	☐	☐
Enter a value	Fax	common;Fax #	String	☐	☑	☑	☐	☐
Enter a value	Primary Position	Employee;Position;Positi...	String	☐	☑	☑	☐	☐
Enter a value	Unique Id	__UID__	String	☐	☐	☑	☐	☐
Enter a value	Status	common;Responsibility;...	String	☐	☑	☑	☐	☐
Enter a value	Alias	common;Alias	String	☐	☑	☑	☐	☐
Enter a value	MI	common;Middle Name	String	☐	☑	☑	☐	☐
Enter a value	Time Zone	common;Time Zone	String	☐	☑	☑	☐	☐

Siebel Position Entitlement

Table 3-4 lists the positions forms attribute mappings between the process form fields in Oracle Identity Governance and Siebel target application attributes. The table lists whether a given

attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

Default Attribute Mappings for Positions

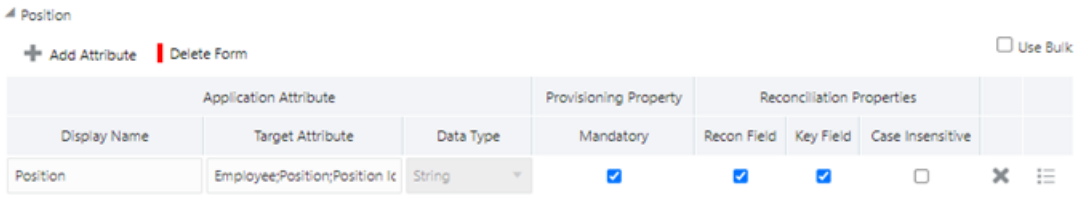
Table 3-4 shows the default attribute mappings for positions.

Table 3-4 Default Attribute Mappings for Positions

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Position	Employee;Position;PositionId;false	String	Yes	Yes	Yes	No

Figure 3-2 shows the default Positions Entitlement mapping.

Figure 3-2 Default Attribute Mappings for Siebel Positions



Siebel Responsibilities Entitlement

Table 3-5 lists the responsibility forms attribute mappings between the process form fields in Oracle Identity Governance and Siebel target application attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliationand whether it is a matching key field for fetching records during reconciliation.

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

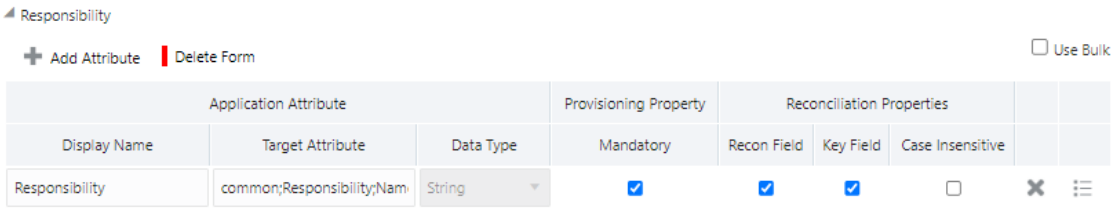
Table 3-5 shows the default attribute mappings for responsibilities.

Table 3-5 Default Attribute Mappings for Responsibilities

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Responsibility	common;Responsibility;Name;false	String	Yes	Yes	Yes	No

Figure 3-3 shows the default attribute mappings for responsibilities.

Figure 3-3 Default Attribute Mappings for Responsibilities



3.3.2 Attribute Mappings for an Authoritative Application

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

Table 3-6 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Siebel Authoritative Application Attributes.

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

You may use the default schema that has been set for you or update and change it before continuing to the next step.

The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form. They cannot be left blank during reconciliation. The target attribute mappings for these identity attributes are empty by default because there are no corresponding columns in the target system. Therefore, the connector provides default values (as listed in the "Default Value for Identity Display Name" column of Table 3-6) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

Table 3-6 Default Attribute Mappings for Siebel Authoritative Application

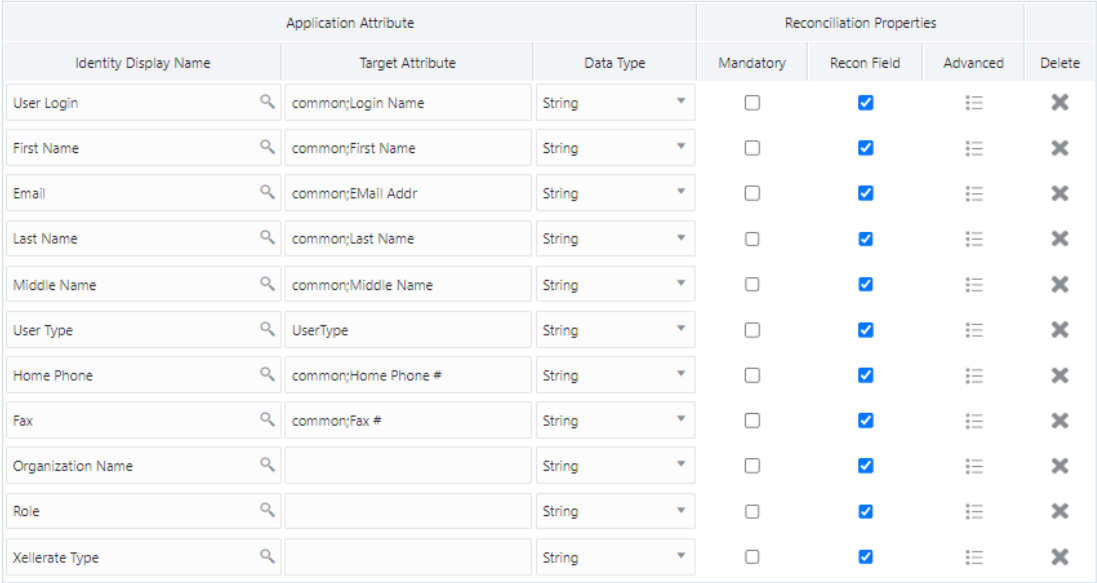
Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Advanced Flag Settings	Default Value for Identity Display Name
User Login	common;Login Name	String	No	Yes	Yes	NA
First Name	common;First Name	String	No	Yes	Yes	NA
Email	common;EMail Addr	String	No	Yes	Yes	NA
Last Name	common;Last Name	String	No	Yes	Yes	NA
Middle Name	common;Middle Name	String	No	Yes	Yes	NA
User Type	UserType	String	No	Yes	Yes	Employee

Table 3-6 (Cont.) Default Attribute Mappings for Siebel Authoritative Application

Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Advanced Flag Settings	Default Value for Identity Display Name
Home Phone	common;Home Phone #	String	No	Yes	Yes	NA
Fax	common:Fax #	String	No	Yes	Yes	NA
Organization Name	NA	String	No	Yes	Yes	Xellerate Users
Role	NA	String	No	Yes	Yes	Full-Time
Xellerate Type	NA	String	No	Yes	Yes	End-User

Figure 3-4 shows the default User account attribute mappings.

Figure 3-4 Default Attribute Mappings for Siebel Authoritative Application



Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
User Login	common;Login Name	String	☐	☑		
First Name	common;First Name	String	☐	☑		
Email	common;EMail Addr	String	☐	☑		
Last Name	common;Last Name	String	☐	☑		
Middle Name	common;Middle Name	String	☐	☑		
User Type	UserType	String	☐	☑		
Home Phone	common;Home Phone #	String	☐	☑		
Fax	common;Fax #	String	☐	☑		
Organization Name		String	☐	☑		
Role		String	☐	☑		
Xellerate Type		String	☐	☑		

3.4 Additional Configuration to Support the Enable/Disable Functionality

While onboarding an application in the schema page, add the following schema attribute or add it post configuring the application.

Table 3-7 Default Attributes for Siebel Target Application to Support the Enable/Disable Functionality

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User Status	__ENABLE__	String	No	Yes	Yes	No	NA

Figure 3-5 Default Attribute Mappings for Siebel Target Application to Support the Enable/Disable Functionality

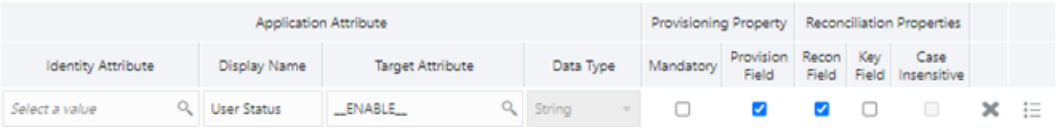
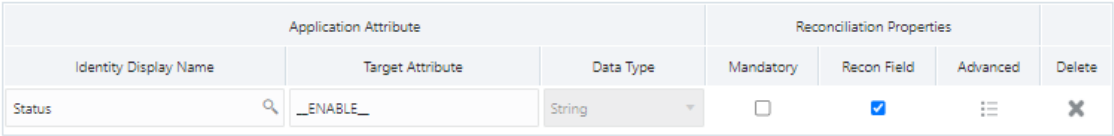


Table 3-8 Default Attributes for Siebel Authoritative Application to Support the Enable/Disable Functionality

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Advanced Flag Settings	Default Value for Identity Display Name
Status	__ENABLE__	String	No	Yes	Yes	NA

Figure 3-6 Default Attribute Mappings for Siebel Authoritative Application to support Enable/Disable functionality



3.5 Correlation Rules

Learn about the predefined rules, responses and situations for Target and Authoritative applications. The connector uses these rules and responses for performing reconciliation.

- Correlation Rules for the Target Application
- Correlation Rules for the Authoritative Application

3.5.1 Correlation Rules for the Target Application

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

Predefined Identity Correlation Rule for a Siebel Target Application

By default, the Siebel connector provides a simple correlation rule when you create a target application. The connector uses this correlation rule to compare the entries in Oracle Identity

Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

Table 3-9 lists the default simple correlation rule for an Siebel connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-9 Predefined Identity Correlation Rule for a Siebel Target Application

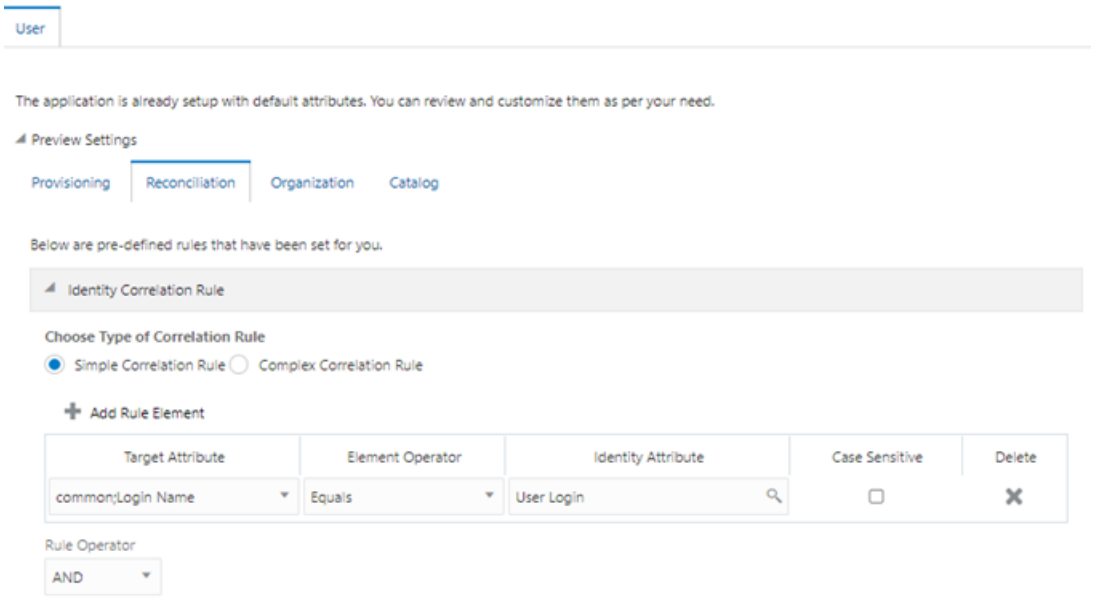
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
common;Login Name	Equals	User Login	No

In this identity rule:

- common;Login Name is a single-valued attribute on the target system that identifies the user account.
- User Login is the field on the OIG User form.
- Rule operator : AND

Figure 3-7 shows the simple correlation rule for an Siebel target application.

Figure 3-7 Simple Correlation Rule for an Siebel Target Application



Predefined Situations and Responses

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

Table 3-10 lists the default situations and responses for an Siebel Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and

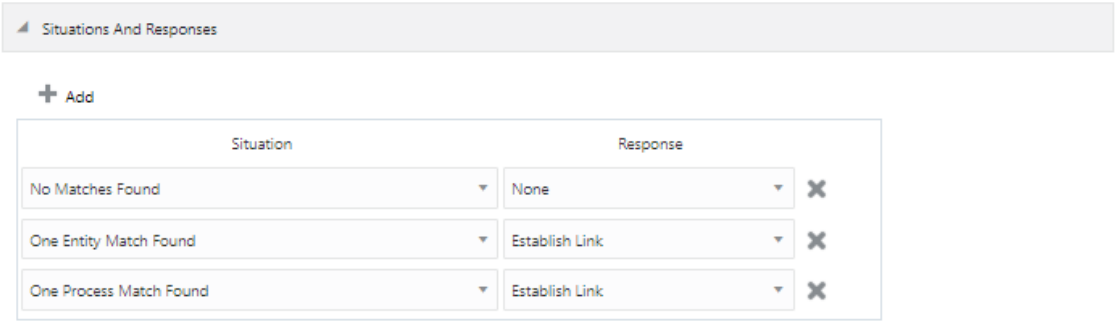
Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-10 Predefined Situations and Responses for an Siebel Target Application

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

Figure 3-8 shows the situations and responses for an Siebel that the connector provides by default.

Figure 3-8 Predefined Situations and Responses for an Siebel Target Application



3.5.2 Correlation Rules for the Authoritative Application

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

Predefined Identity Correlation Rules

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

Table 3-11 lists the default simple correlation rule for an Siebel connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-11 Predefined Identity Correlation Rule for an Siebel Authoritative Application

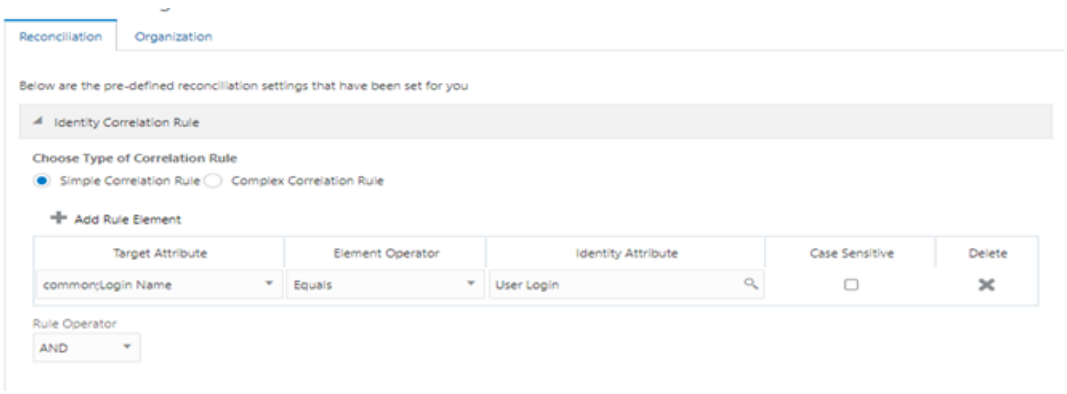
Authoritative Attribute	Element Operator	Identity Attribute	Case Sensitive?
common;Login Name	Equals	User Login	No

In this identity rule:

- common;Login Name is a single-valued attribute on the target system that identifies the user account.
- User Login is the User ID field of the OIG User form.
- Rule operator: AND

Figure 3-9 shows the simple correlation rule for an Siebel Authoritative application.

Figure 3-9 Simple Correlation Rule for an Siebel Authoritative Application



Predefined Situations and Responses

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

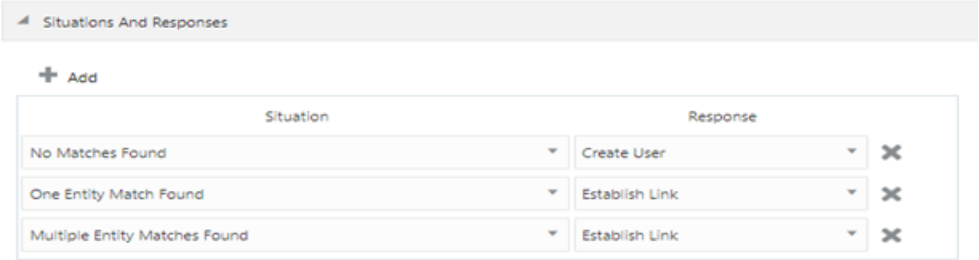
Table 3-12 lists the default situations and responses for an Siebel Authoritative Application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.*

Table 3-12 Predefined Situations and Responses for an Siebel Authoritative Application

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

Figure 3-10 shows the situations and responses for an Siebel Authoritative application that the connector provides by default.

Figure 3-10 Predefined Situations and Responses for a Siebel Authoritative Application



3.6 Reconciliation Jobs

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

User Reconciliation Jobs

You can either use these predefined jobs or edit them to meet your requirements. Alternatively,you can create custom reconciliation jobs.

For information about editing these predefined jobs or creating new ones, see Updating Reconciliation Jobs in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance.

The following reconciliation jobs are available for reconciling user data:

- Siebel Full User Reconciliation: Use this reconciliation job to reconcile user data from a target applications.
- Siebel User Trusted Reconciliation: Use this reconciliation job to reconcile user data from an authoritative application.

Table 3-13 describes the parameters of the Siebel Full User Reconciliation job.

Table 3-13 Parameters of the Siebel Full User Reconciliation Job

Parameter	Description
Application name	Name of the AOB application with which the reconciliation job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application. Do*not*change the default value.

Table 3-13 (Cont.) Parameters of the Siebel Full User Reconciliation Job

Parameter	Description
Custom Recon Query	Provide a value for this attribute if you want to reconcile the subset of added or modified target system records. Simple query with user attributes, for example: • First Name=John&Last Name=Doe • First Name=John • Login Name=JOHN • First Name=John|First Name=Jane Query based on positions and responsibilities, for example: • Position=Proxy Employee|Position=ERM AnonUser • Responsibility=CEO&Responsibility=Consultant • Responsibility=CEO& Position=ERM AnonUser Complex queries, for example: • First Name=John&Position=Proxy Employee|Position=ERM AnonUser • LastName=Doe|Position=Proxy Employee&Responsibility=CEO
Object Type	This parameter holds the name of the object type for the reconciliation run. **Default value**:User Do*not*change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do*not*modify the value of this parameter.
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
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
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
Time Zone	Enter the time zone of the target system database. Default value: GMT-08:00

Table 3-13 (Cont.) Parameters of the Siebel Full User Reconciliation Job

Parameter	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. • 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.

Table 3-14 describes the parameters of Siebel User Trusted Reconciliation job.

Table 3-14 Parameters of the Siebel User Trusted Reconciliation Job

Parameter	Description
Application name	Name of the AOB application with which the reconciliation job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not change the default value
Custom Recon Query	Provide a value for this attribute if you want to reconcile the subset of added or modified target system records. Simple query with user attributes, for example: • First Name=John&Last Name=Doe • Login Name=JOHN • First Name=John • First Name=John|First Name=Jane
Object Type	This parameter holds the name of the object type for the reconciliation run. **Default value**:User Do not change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do*not*modify the value of this parameter.
Day Light Saving	Enter the time, in minutes, that must be added to the time-stamp value stored in the LastExecution Timestamp attribute. Day Light Saving Default value: 0
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

Table 3-14 (Cont.) Parameters of the Siebel User Trusted Reconciliation Job

Parameter	Description
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
Time Zone	Enter the time zone of the target system database. Default value: GMT-08:00
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. • 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.

Target User Delete Reconciliation Job

The Siebel User Target Delete Recon job is used to reconcile data about deleted users from Siebel target application. During a reconciliation run, for each deleted user account on the target system, the Siebel resource is revoked for the corresponding OIM User.

Table 3-15 Parameters of the Siebel Target User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do*not*modify this value.
Object Type	This parameter holds the type of object you want to reconcile. **Default value**:User **Note:** If you configure the connector to provision users to a custom class (for example, InetOrgPerson)then enter the value of the object class here.

Trusted User Delete Reconciliation Job

The Siebel User Trusted Delete Recon job is used to reconcile data about deleted users from an Authoritative application. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted.

Table 3-16 Parameters of the Siebel Trusted User Delete Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do*not*modify this value.
Object Type	This parameter holds the type of object you want to reconcile. **Default value**:User **Note:** If you configure the connector to provision users to a custom class (for example, InetOrgPerson)then enter the value of the object class here.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- Siebel Employee Type Code Lookup Reconciliation
- Siebel Personal Title Lookup Reconciliation
- Siebel Position Lookup Reconciliation
- Siebel Preferred Communications Lookup Reconciliation
- Siebel Responsibility Lookup Reconciliation
- Siebel Time Zone Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-17 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Current AOB application name with which the reconciliation job is associated. Do*not*modify this value.

Table 3-17 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Code Key Attribute	Name of the connector attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). • For Siebel Employee Type Code Lookup Reconciliation – Code Key attribute value: Value • For Siebel Personal Title Lookup Reconciliation – Code Key attribute value: Value • For Siebel Position Lookup Reconciliation – Code Key attribute value: Position Id • For Siebel Preferred Communications Lookup Reconciliation – Code Key attribute value: Value • For Siebel Responsibility Lookup Reconciliation – Code Key attribute value: Name • For Siebel Time Zone Lookup Reconciliation – Code Key attribute value: Name
Decode Attribute	Name of the connector attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). • For Siebel Employee Type Code Lookup Reconciliation – DCode Key attribute value: Description • For Siebel Personal Title Lookup Reconciliation – DCode Key attribute value: Description – • For Siebel Position Lookup Reconciliation – DCode Key attribute value: Name • For Siebel Preferred Communications Lookup Reconciliation – DCode Key attribute value: Description • For Siebel Responsibility Lookup Reconciliation – DCode Key attribute value: Description • For Siebel Time Zone Lookup Reconciliation DCode Key attribute value: Standard Abbreviation"

Table 3-17 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system. Depending on the Reconciliation job that you are using, the default values are as follows: • Lookup.Siebel.EmployeeTypeCode • Lookup.Siebel.PersonalTitle • Lookup.Siebel.Position • Lookup.Siebel.PreferredCommunications • Lookup.Siebel.Responsibility • Lookup.Siebel.TimeZone – If you create a copy of any of these lookup definitions,then enter the name of that new lookup definition as the value of the Lookup Name attribute.

Object Type	Enter the type of object you want to reconcile.
	Dependingon the reconciliation job that you are using, the default values are as follows:
	• For Siebel Employee Type Code Lookup Reconciliation
	  – Employee;Employee;Employee Type Code;Value;Description
	• For Siebel Personal Title Lookup Reconciliation
	  – Employee;Employee;Personal Title;Value;Description
	• For Siebel Position Lookup Reconciliation
	  – Position;Position;Position Id;Name
	• For Siebel Preferred Communications Lookup Reconciliation
	  – Employee;Employee;Preferred Communications;Value;Description
	• For Siebel Responsibility Lookup Reconciliation
	  – Responsibility;Responsibility;Name;Description
	• For Siebel Time Zone Lookup Reconciliation
	  – Employee;Employee;Time Zone Name - Translation;Name;Standard Abbreviation
	Note:Do not change the value of this parameter

4

Performing Postconfiguration Tasks for the Connector

You can perform the following tasks after creating an application in Oracle Identity Governance.

- Configuring Oracle Identity Governance
- Harvesting Entitlements and Sync Catalog
- Managing Logging for the Connector Server
- Configuring the IT Resource for the Connector Server
- Localizing Field Labels in UI Forms

4.1 Configuring Oracle Identity Governance

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

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

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

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

4.1.1 Creating and Activating a Sandbox

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

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

4.1.2 Creating a New UI Form

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

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

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

4.1.3 Publishing a Sandbox

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

1. In Identity System Administration, deactivate the sandbox.
2. Log out of Identity System Administration.
3. Log in to Identity Self Service using the xelsysadm user credentials and then activate the sandbox that you deactivated in Step 1.
4. In the Catalog, ensure that the application instance form for your resource appears with correct fields.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.1.4 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

1. Create and activate a sandbox.
2. Create a new UI form for the resource.
3. Open the existing application instance.
4. In the Form field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox.

See Also:

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

4.2 Harvesting Entitlements and Sync Catalog

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

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Reconciliation Jobs.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

> **See Also:**
>
> Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for a description of the Entitlement List and Catalog Synchronization Job scheduled jobs

4.3 Managing Logging for the Connector Server

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

The following topics provide detailed information about logging:

- Understanding Logging on the Connector Server
- Enabling Logging for the Connector Server
- Understanding Log Levels
- Enabling Logging

4.3.1 Understanding Logging on the Connector Server

When you enable logging, the connector server stores in a log file information about events that occur during the course of provisioning and reconciliation operations for different statuses. By default, the connector server logs are set at INFO level and you can change this level to any one of these.

- Error

  This level enables logging of information about errors that might allow connector server 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 operation.

- FINE, FINER, FINEST

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

4.3.2 Enabling Logging for the Connector Server

Edit the logging.properties file located in the *CONNECTOR_SERVER_HOME*/Conf directory to enable logging.

To do so:

1. Navigate to the *CONNECTOR_SERVER_HOME*/Conf directory.
2. Open the logging.properties file in a text editor.
3. Edit the following entry by replacing INFO with the required level of logging:

   ```
   .level=INFO
   ```

4. Save and close the file.
5. Restart the connector server.

4.3.3 Understanding Log Levels

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

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

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

These message types are mapped to ODL message type and level combinations as shown in Table 4-1.

Table 4-1 Log Levels and ODL Message Type:Level Combinations

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

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

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

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

4.3.4 Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

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 4-1 lists the supported message type and level combinations. Similarly, replace [FILE_NAME] with the full path and name of the log file in which you want log messages to be recorded. The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]:**

```
<log_handler name='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\server
s\oim_server1\logs\oim_server1-diagnostic-1.log'/>     <property
name='format'
          value='ODL-Text'/>     <property name='useThreadName'
          value='true'/>     <property name='locale'
          value='en'/>     <property name='maxFileSize'
          value='5242880'/>     <property name='maxLogSize'
          value='52428800'/>     <property name='encoding'
          value='UTF-8'/>   </log_handler> <logger
name="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 Governance, 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.

4.4 Configuring the IT Resource for the Connector Server

If you have used the Connector Server, then you must configure values for the parameters of the Connector Server IT resource.

After you create the application for your target system, you must create an IT resource for the Connector Server as described in Creating IT Resources of *Oracle Fusion Middleware Administering Oracle Identity Governance.*While creating the IT resource, ensure to select Connector Server from the IT Resource Type list. In addition, specify values for the parameters of IT resource for the Connector Server listed in Table 4-2. For more information about searching for IT resources and updating its parameters, see Managing IT Resources in Oracle Fusion Middleware Administering Oracle Identity Governance

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

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: `HostName`
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. Sample value: `8763`

Table 4-2 (Cont.) Parameters of the IT Resource for the Siebel Connector Server

Parameter	Description
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. If the value is zero or if no value is specified, the timeout is unlimited. Sample value: `0` (recommended value)
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Governance 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, see Configuring the Java Connector Server with SSL for OIG in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.5 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. Resource bundles are available in the connector installation media.

To localize field labels 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 (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer**.**
5. Extract the contents of the archive, and open the following file in a text editor:

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

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

6. Edit the `BizEditorBundle.xlf` file in the following manner:
   a. Search for the following text:

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

b. Replace with the following text:

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

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

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

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

```
<trans-unit
      id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBund
le']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO
.UD_SIEBEL_ALIAS__c_description']}"><source>Alias</source></target></
trans-unit><trans-unit

id="sessiondef.oracle.iam.ui.runtime.form.model.SIEBEL.entity.SIEBELEO.U
D_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.BaseRuntimeResourceBund
le']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO
.UD_SIEBEL_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.U
D_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 Governance* for more information about exporting and importing metadata files

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

5
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:

- Guidelines to Apply While Using the Connector
- Performing First-Time Reconciliation
- Scheduled Job for Lookup Field Synchronization
- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Configuring Provisioning
- Connector Objects Used During Target Resource Reconciliation
- Connector Objects Used During Trusted Source Reconciliation
- Uninstalling the Connector

5.1 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.

5.2 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.

> **See Also:**
>
> Reconciliation Jobs for more information about the attributes of the scheduled job.
>
> Configuring Reconciliation Jobs for information about running scheduled jobs.

5.3 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 5-1 describes the attributes of these scheduled jobs. Configuring Reconciliation Jobs describes the procedure to configure scheduled jobs.

Table 5-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Application Name	Current AOB application name with which the reconciliation job is associated. Do *not* modify this value.

Table 5-1 (Cont.) Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Name of the connector attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). • For Siebel Employee Type Code Lookup Reconciliation – Code Key attribute value: Value • For Siebel Personal Title Lookup Reconciliation – Code Key attribute value: Value • For Siebel Position Lookup Reconciliation – Code Key attribute value: Position Id • For Siebel Preferred Communications Lookup Reconciliation – Code Key attribute value: Value • For Siebel Responsibility Lookup Reconciliation – Code Key attribute value: Name • For Siebel Time Zone Lookup Reconciliation – Code Key attribute value: Name
Decode Attribute	Name of the connector attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). • For Siebel Employee Type Code Lookup Reconciliation – DCode Key attribute value: Description • For Siebel Personal Title Lookup Reconciliation – DCode Key attribute value: Description • For Siebel Position Lookup Reconciliation – DCode Key attribute value: Name • For Siebel Preferred Communications Lookup Reconciliation – DCode Key attribute value: Description • For Siebel Responsibility Lookup Reconciliation – DCode Key attribute value: Description • For Siebel Time Zone Lookup Reconciliation – DCode Key attribute value: Standard Abbreviation
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`

Table 5-1 (Cont.) Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system. Depending on the Reconciliation job that you are using, the default values are as follows: • `Lookup.Siebel.EmployeeTypeCode` • `Lookup.Siebel.PersonalTitle` • `Lookup.Siebel.Position` • `Lookup.Siebel.PreferredCommunications` • `Lookup.Siebel.Responsibility` • `Lookup.Siebel.TimeZone` If you create a copy of any of these lookup definitions, then enter the name of that new lookup definition as the value of the Lookup Name attribute.

5.4 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:

- Performing Full Reconciliation
- Performing Limited Reconciliation
- Reconciliation Based on User Type
- Reconciliation Scheduled Jobs

5.4.1 Performing Full Reconciliation

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

5.4.2 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.

5.4.3 Reconciliation Based on User Type

This section discusses the UserType attribute of the scheduled job.

Siebel supports the definition of the following user types:

- Employee
- 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.

5.4.4 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

5.4.4.1 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 5-2 describes the attributes of both scheduled jobs.

Table 5-2 Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description
Application Name	Name of the AOB application with which the reconciliation job is associated. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* change the default value.
Custom Recon Query	Provide a value for this attribute if you want to reconcile the subset of added or modified target system records.
Object Type	This parameter holds the name of the object type for the reconciliation run. Do not change the default value.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Do not modify the value of this parameter.
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`
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`

Table 5-2 (Cont.) Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description
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`
Time Zone	Enter the time zone of the target system database. Default value: `GMT-08:00`
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. • `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.

5.4.4.2 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 5-3 describes the attributes of both scheduled jobs.

Table 5-3 Attributes of the Scheduled Job for Reconciliation of Deleted Users Records

Attribute	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Object Type	This parameter holds the type of object you want to reconcile. **Default value**: `User` **Note**: If you configure the connector to provision users to a custom class (for example, InetOrgPerson) then enter the value of the object class here.

5.5 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

> **Note:**
>
> If you are using OIG 12cPS4 with 2022OCTBP or later version, log in to Identity Console, click **Manage**, and then under System Configuration, click **Scheduler**.

1. Log in to Identity System Administration.
2. In the left pane, under System Configuration, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled task:
   - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

   In addition to modifying the job details, you can enable or disable a job.
5. On the **Job Details** tab, in the Parameters region, specify values for the attributes of the scheduled task.

   > **Note:**
   >
   > Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
6. Click **Apply** to save the changes.

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

5.6 Configuring Provisioning

You can configure the provisioning operation for the Siebel connector.

This section provides information on the following topics:

- Performing Provisioning Operations

5.6.1 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

1. Log in to Oracle Identity Self Service.
2. Create a user.
   a. To create a user, in Identity Self Service, **click Manage**. The Home tab displays the different Manage option. Click Users. The Manage Users page is displayed.
   b. From the Actions menu, select **Create**. Alternatively, you can click Create on the toolbar. The Create User page is displayed with input fields for user profile attributes.
   c. Enter details of the user in the Create User page
3. On the Account tab, click **Request Accounts**.
4. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit.**

5.7 Connector Objects Used During Target Resource Reconciliation

This section discusses the following topics:

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

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

5.7.1 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.

5.7.2 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

5.7.2.1 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.

5.7.2.2 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**.

5.7.3 Reconciliation Action Rules for Target Resource Reconciliation

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

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

5.7.3.1 Target Resource Reconciliation Action Rules

Table 5-4 lists the action rules for Target Resource reconciliation.

Table 5-4 Target Resource Reconciliation Action Rules

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

Table 5-4 (Cont.) Target Resource Reconciliation Action Rules

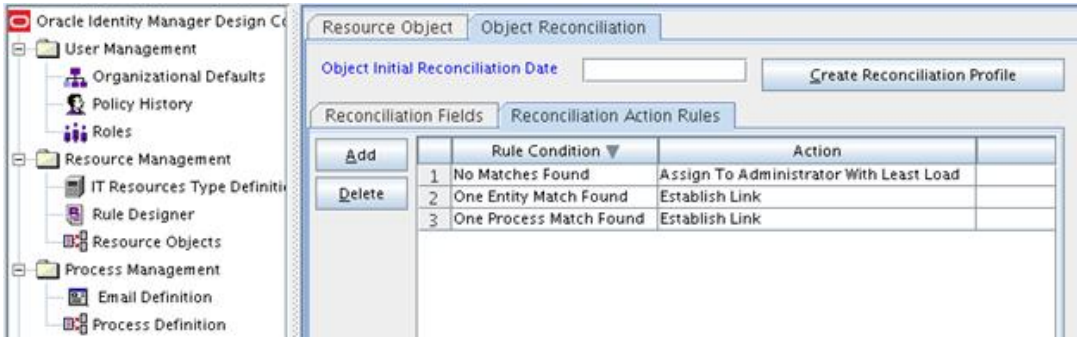
Rule Condition	Action
One Process Match Found	Establish Link

5.7.3.2 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 5-1 shows the reconciliation action rules for target resource reconciliation.

Figure 5-1 Target Resource Reconciliation Action Rules



5.8 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

5.8.1 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

5.8.1.1 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.

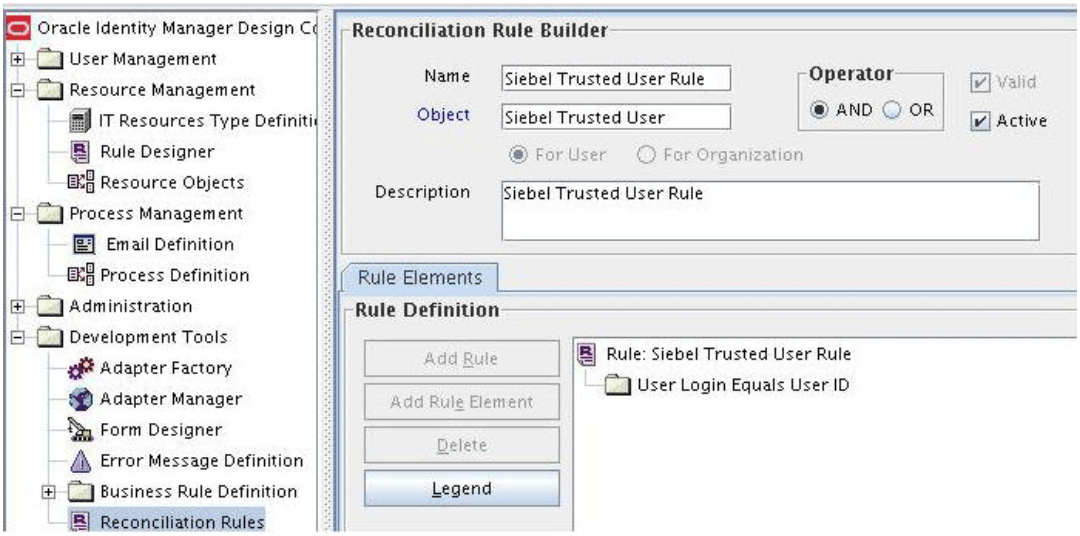
5.8.1.2 Viewing Trusted Source Reconciliation Rule

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 5-2 shows the reconciliation rule for trusted source reconciliation.

Figure 5-2 Reconciliation Rule for Trusted Source Reconciliation



5.8.2 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

5.8.2.1 Trusted Source Reconciliation Action Rules

Table 5-5 lists the action rules for trusted source reconciliation.

Table 5-5 Action Rules for Trusted Source Reconciliation

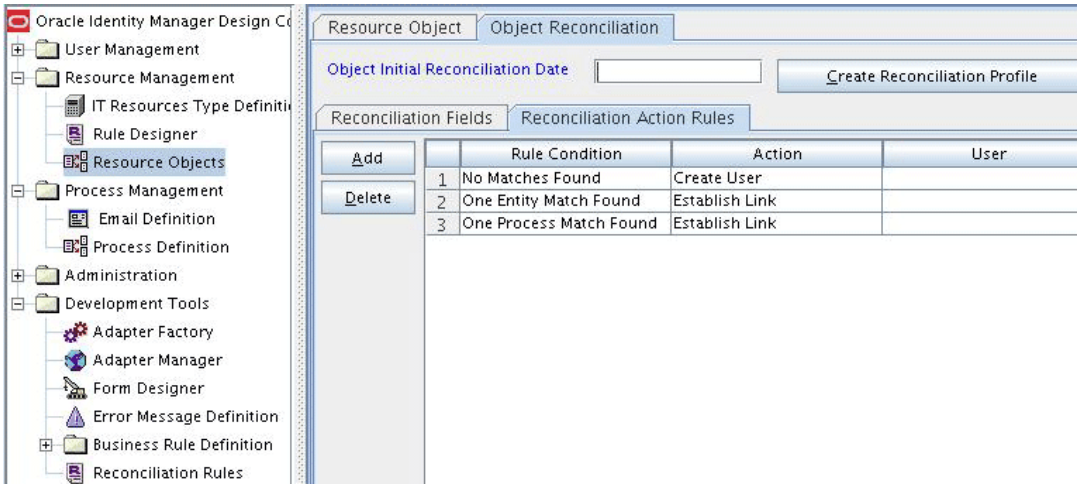
Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

5.8.2.2 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 5-3 shows the reconciliation action rule for trusted source reconciliation.

Figure 5-3 Reconciliation Action Rules for Trusted Source Reconciliation



5.9 Uninstalling the Connector

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

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

For example: `Siebel User; Siebel Position`

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

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

6
Extending the Functionality of the Connector

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

This section discusses the following topics:

- Configuring Transformation and Validation of Data
- Configuring Action Scripts
- Configuring the Connector for Multiple Installations of the Target System
- Configuring the Connector for Multiple Versions of the Target System

6.1 Configuring Transformation and Validation of Data

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

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

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

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

6.2 Configuring Action Scripts

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

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

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

6.3 Configuring the Connector for Multiple Installations of the Target System

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

The following example illustrates this requirement:

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

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

6.4 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.
- For more information, see Configuring the IT Resource for the Connector Server.

7
Known Issues and Workarounds

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

- Connector Issues
- Oracle Identity Manager Issues
- Target System Issues
- FAQs

7.1 Connector Issues

The following are issues and workarounds associated with the connector:

- Enabling SSO on Siebel
- Clearing a Non-Mandatory Field

7.1.1 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.

7.1.2 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.

7.2 Oracle Identity Manager Issues

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

- Updating Responsibility or Position on the Process Form

- Delete Reconciliation Revokes Accounts from All Siebel Target Systems

7.2.1 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.

7.2.2 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.

7.3 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*

7.3.1 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.

7.3.2 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.

7.3.3 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).

7.4 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.

8

Files and Directories on the Installation Media

These are the files and directories on the connector installation package that comprise the Siebel connector.
Table 8-1 describes the files and directories on the installation media.

Table 8-1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
bundle/org.identityconnectors.siebel-12.3.0.jar	This JAR file is the ICF bundle that the connector is using for the current release.
configuration/SiebelConnector-CI.xml	This file is used for installing a CI-based connector. 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 are displayed on the Administrative and User Console. These text strings 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 definition • Process forms • Process task and adapters • Lookup definition • Resource objects • Process definition • Scheduled tasks • Reconciliation 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.

Table 8-1 (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
xml/Siebel-auth-template.xml	This file contains definitions for the connector objects required for creating an Authoritative application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/Siebel-pre-config.xml	This XML file contains definitions for static lookup.
xml/Siebel-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
upgrade/ PostUpgradeScriptSiebel.sql	This file contains the scripts that are run after performing an upgrade of the connector.

Index

C

connector features, *1-6*

E

enable logging, *4-5*

F

features of connector, *1-6*

full reconciliation, *1-7*

L

localizing, *4-7*
logging, *4-5*

S

support for the connector server, *1-7*