

Oracle® Identity Manager Connector Guide for Concur



Release 11.1.1

E75739-02

May 2020

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Identity Manager Connector Guide for Concur, Release 11.1.1

E75739-02

Copyright © 2016, 2020, Oracle and/or its affiliates.

Primary Author: Gowri.G.R

Contributors: Neha Bagalkot

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs 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" or "commercial computer software documentation" 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 and Java 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	viii
Documentation Accessibility	viii
Related Documents	viii
Conventions	viii

What's New in Oracle Identity Manager Connector for Concur?

Software Updates	x
Documentation-Specific Updates	x

1 About the Concur Connector

1.1	Introduction to the Concur Connector	1-1
1.2	Certified Components for the Concur Connector	1-2
1.3	Certified Languages for the Concur Connector	1-2
1.4	Architecture of the Concur Connector	1-3
1.5	Use Cases Supported by the Concur Connector	1-4
1.6	Features of the Concur Connector	1-4
1.6.1	Full Reconciliation	1-5
1.6.2	Support for the Connector Server	1-5
1.6.3	Limited Reconciliation	1-5
1.6.4	Transformation and Validation of Account Data	1-5
1.7	Lookup Definitions Used During Connector Operations	1-6
1.7.1	Lookup.Concur.Configuration	1-6
1.7.2	Lookup.Concur.UM.Configuration	1-10
1.7.3	Lookup.Concur.UM.ProvAttrMap	1-10
1.7.4	Lookup.Concur.UM.ReconAttrMap	1-11
1.7.5	Lookup.Concur.BooleanValues	1-11
1.7.6	Lookup.Concur.Locale	1-12
1.7.7	Lookup.Concur.CountryofResidence	1-12
1.7.8	Lookup.Concur.Currency	1-13
1.7.9	Lookup.Concur.EmployeeAdminCountry	1-13

1.7.10	Lookup.Concur.Ledger	1-14
1.8	Connector Objects Used During Target Resource Reconciliation	1-14
1.8.1	User Fields for Target Resource Reconciliation	1-15
1.8.2	Reconciliation Rules for Target Resource Reconciliation	1-15
1.8.3	Viewing Reconciliation Rules for Target Resource Reconciliation	1-15
1.8.4	Reconciliation Action Rules for Target Resource Reconciliation	1-16
1.8.5	Viewing Reconciliation Action Rules for Target Resource Reconciliation	1-16
1.9	Connector Objects Used During Provisioning	1-17
1.9.1	Provisioning Functions	1-17
1.9.2	User Fields for Provisioning	1-18
1.10	Roadmap for Deploying and Using the Concur Connector	1-18

2 Deploying the Concur Connector

2.1	Preinstallation	2-1
2.2	Installation	2-1
2.2.1	Understanding Installation of the Concur Connector	2-1
2.2.2	Running the Connector Installer	2-2
2.2.3	Configuring the IT Resource for the Target System	2-3
2.2.3.1	IT Resource Parameters	2-3
2.2.3.2	Specifying Values for IT Resource Parameters	2-5
2.3	Postinstallation	2-5
2.3.1	Configuring Oracle Identity Manager	2-6
2.3.1.1	Creating and Activating a Sandbox	2-6
2.3.1.2	Creating a New UI Form	2-6
2.3.1.3	Associating the Form with the Application Instance	2-6
2.3.1.4	Publishing a Sandbox	2-7
2.3.1.5	Harvesting Entitlements and Sync Catalog	2-7
2.3.1.6	Updating an Existing Application Instance with a New Form	2-7
2.3.2	Localizing Field Labels in UI Forms	2-8
2.3.3	Clearing Content Related to Connector Resource Bundles from the Server Cache	2-10
2.3.4	Managing Logging for the Concur Connector	2-11
2.3.4.1	Understanding Log Levels	2-11
2.3.4.2	Enabling Logging	2-12
2.3.5	Configuring SSL for the Concur Connector	2-13

3 Using the Concur Connector

3.1	Configuring Reconciliation for the Concur Connector	3-1
3.1.1	Full Reconciliation	3-1
3.1.2	Limited Reconciliation for the Concur Connector	3-2

3.1.3	Reconciling Large Number of Records	3-2
3.1.4	Reconciliation Scheduled Job for Concur Connector	3-3
3.2	Configuring Scheduled Jobs	3-3
3.3	Guidelines on Performing Provisioning Operations	3-4
3.4	Performing Provisioning Operations	3-5
3.5	Uninstalling the Connector	3-5

4 Extending the Functionality of the Concur Connector

4.1	Adding User Attributes for Reconciliation	4-1
4.1.1	Adding New Attributes on the Process Form	4-2
4.1.2	Adding Attributes to the Resource Object	4-2
4.1.3	Creating Reconciliation Field Mapping	4-3
4.1.4	Creating Entries in Lookup Definitions for Reconciliation	4-4
4.1.5	Performing Changes in a New UI Form	4-5
4.2	Adding User Attributes for Provisioning	4-6
4.2.1	Adding New Attributes for Provisioning	4-6
4.2.2	Creating Entries in Lookup Definitions for Provisioning	4-7
4.2.3	Creating a Task to Enable Update Operations	4-8
4.2.4	Replicating Form Designer Changes to a New UI Form	4-11
4.3	Configuring Validation of Data During Reconciliation and Provisioning	4-11
4.4	Configuring Transformation of Data During User Reconciliation	4-13
4.5	Configuring the Concur Connector for Multiple Installations of the Target System	4-15
4.6	Defining the Concur Connector	4-15

5 Known Issues and Workarounds for the Concur Connector

A Files and Directories on the Concur Connector Installation Media

List of Figures

1-1	Architecture of the Concur Connector	1-3
1-2	Concur User Recon Rule	1-16
1-3	Reconciliation Action Rules for Target Resource Reconciliation	1-17
4-1	New Fields Added to the Concur User Form	4-2
4-2	New Reconciliation Field added to the Resource Object	4-3
4-3	New Reconciliation Field Mapped to a Process Data Field in the Process Definition	4-4
4-4	Entry Added to the Lookup Definition for Reconciliation	4-5
4-5	New Field Added to the Concur User Form	4-7
4-6	Entry Added to the Lookup Definition for Provisioning	4-8
4-7	New Task Added to the Process Definition	4-9
4-8	List of Adapter Variables	4-10

List of Tables

1-1	Certified Components	1-2
1-2	Entries in the Lookup.Concur.Configuration Lookup Definition	1-6
1-3	Entries in the Lookup.Concur.UM.Configuration Lookup	1-10
1-4	Default Entries in the Lookup.Concur.UM.ProvAttrMap Lookup Definition	1-10
1-5	Default Entries in the Lookup.Concur.UM.ReconAttrMap Lookup Definition	1-11
1-6	Default Entries in the Lookup.Concur.BooleanValues Lookup Definition	1-12
1-7	Sample Entries in the Lookup.Concur.Locale Lookup Definition	1-12
1-8	Default Entries in the Lookup.Concur.CountryofResidence Lookup Definition	1-12
1-9	Default Entries in the Lookup.Concur.Currency Lookup Definition	1-13
1-10	Default Entries in the Lookup.Concur.EmployeeAdminCountry Lookup Definition	1-13
1-11	Default Entries of the Lookup.Concur.Ledger Lookup Definition	1-14
1-12	Entries in the Lookup.Concur.UM.ReconAttrMap Lookup Definition	1-15
1-13	Action Rules for Target Resource Reconciliation	1-16
1-14	User Provisioning Functions	1-18
1-15	Entries in the Lookup.Concur.UM.ProvAttrMap Lookup Definitions	1-18
2-1	IT Resource Parameters	2-3
2-2	Log Levels and ODL Message Type:Level Combinations	2-12
3-1	Attributes of the Concur User Reconciliation Scheduled Job	3-3
A-1	Files and Directories on the Concur Connector Installation Media	A-1

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Concur.

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

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in Oracle Identity Manager Connector for Concur?

These are the updates made to the software and documentation for the Oracle Identity Manager Connector for Concur in release 11.1.1.5.0.

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

- [Software Updates](#)

This section provides details on the updates that are made to the connector software. This section also provides information on the sections of this guide that have changed in response to each software update.

- [Documentation-Specific Updates](#)

This section provides details on the major changes that are made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager Connector for Concur. Therefore, there are no software updates in this release.

Documentation-Specific Updates

The following section provides information on documentation-specific updates.

Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific update has been made in revision "02" of this guide:

The "Oracle Identity Governance or Oracle Identity Manager" row of [Table 1-1](#) has been updated to include support for Oracle Identity Governance release 12c PS4 (12.2.1.4.0).

The following documentation-specific update has been made in revision "01" of this guide:

This is the first release of the Oracle Identity Manager Connector for Concur. Therefore, there are no documentation-specific updates in this release.

1

About the Concur Connector

The Concur connector integrates Oracle Identity Manager with the Concur target system.

This chapter contains the following sections:

- [Introduction to the Concur Connector](#)
- [Certified Components for the Concur Connector](#)
- [Certified Languages for the Concur Connector](#)
- [Architecture of the Concur Connector](#)
- [Use Cases Supported by the Concur Connector](#)
- [Features of the Concur Connector](#)
- [Lookup Definitions Used During Connector Operations](#)
- [Connector Objects Used During Target Resource Reconciliation](#)
- [Connector Objects Used During Provisioning](#)
- [Roadmap for Deploying and Using the Concur Connector](#)

1.1 Introduction to the Concur Connector

Oracle Identity Manager is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premise or on the Cloud. Oracle Identity Manager connectors are used to integrate Oracle identity Manager with the external and identity-aware applications. The Concur connector enables you to use Concur as a managed (target) resource of identity data for Oracle identity Manager.

The Concur connector uses OAuth 2.0 security protocol (Native Flow) for connecting to Concur and performing user authentication.

You can configure the Concur connector to run in the Account Management (or target resource management) mode. In this mode of the connector, information about users that are created or modified directly on Concur can be reconciled into Oracle identity Manager. This data is used to add or modify resources (that is, accounts) that are allocated to Oracle Identity Manager Users. In addition, you can use Oracle Identity Manager to provision or update Concur accounts that are assigned to Oracle Identity Manager Users.

Note:

At some places in this guide, Concur has been referred to as the **target system**.

1.2 Certified Components for the Concur Connector

These are the software components and their versions required for installing and using the connector.

Table 1-1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: <ul style="list-style-type: none">• Oracle Identity Governance 12c (12.2.1.4.0)• Oracle Identity Governance 12c (12.2.1.3.0)• Oracle Identity Manager 11g Release 2 PS2 BP09 (11.1.2.2.9)• Oracle Identity Manager 11g Release 2 PS3 BP06 (11.1.2.3.6)
Target system	Concur
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 or later

1.3 Certified Languages for the Concur Connector

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English (US)
- 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 Architecture of the Concur Connector

The Concur connector can be configured to run in the Account Management (or target resource management) mode, and is implemented using the Integrated Common Framework (ICF) component.

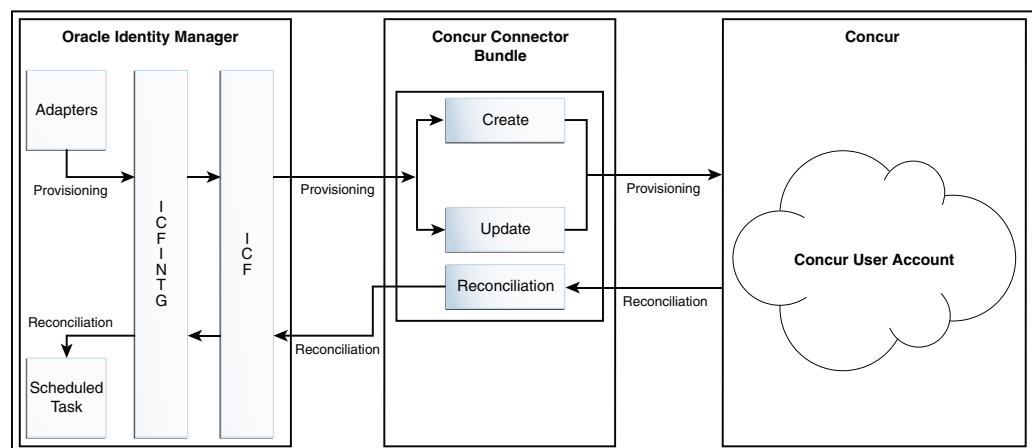
This connector enables the following operations:

- Provisioning

Provisioning involves creating and updating users on Concur through Oracle Identity Manager. When you allocate (or provision) a Concur resource to an Oracle Identity Manager User, the operation results in the creation of an account on Concur for that user. In the Oracle Identity Manager context, the term "provisioning" is also used to mean updates (for example enabling or disabling) made to the Concur account through Oracle Identity Manager.
- Target resource reconciliation

To perform target resource reconciliation, the Concur Recon scheduled job is used. The connector then fetches the user attribute values from Concur.

Figure 1-1 Architecture of the Concur Connector



As shown in [Figure 1-1](#), Concur is configured as a target resource of Oracle Identity Manager. Through the provisioning operations that are performed on Oracle Identity Manager, accounts are created and updated on Concur for Oracle Identity Manager Users.

Through reconciliation, account data that is created and updated directly on Concur is fetched into Oracle Identity Manager and stored against the corresponding Oracle Identity Manager Users.

The Concur connector is implemented using the ICF component. The ICF component provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. ICF is distributed together with Oracle Identity Manager. Therefore, you do not need to configure or modify ICF.

During provisioning, the adapters invoke ICF operation, ICF invokes the Create operation on Concur Connector Bundle, and then the bundle calls the OAuth API. The OAuth API uses OAuth method (Native Flow) to connect to Concur. Concur accepts provisioning data from the bundle, carries out the operation, and returns the response back to the bundle. The bundle then passes it to the adapters.

1.5 Use Cases Supported by the Concur Connector

The Concur connector provides user management functionality that helps in managing users and their accounts in Concur through Oracle Identity Manager.

The following is a scenario in which the Concur connector can be used:

Organizations use Concur for managing their travel and expense (T&E) information. The administrator needs to create and grant login access to the concerned employees in the Concur portal. When the employee leaves the organization, the administrator needs to ensure that the employee must no longer be able to access the sensitive information using their Concur account. Doing these tasks manually for every employee is cumbersome and error-prone. The Concur connector enables automation of provisioning and deprovisioning of the user accounts in Concur. Whenever a new employee joins the organization, based on the access policies defined in Oracle Identity Manager, a Concur account is automatically provisioned to that employee with appropriate access rights. Similarly, upon quitting the organization, the same account is automatically deactivated. This saves time and provides robust security as there is little manual intervention.

1.6 Features of the Concur Connector

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

The Concur Connector supports the following features:

- [Full Reconciliation](#)
- [Support for the Connector Server](#)
- [Limited Reconciliation](#)
- [Transformation and Validation of Account Data](#)

1.6.1 Full Reconciliation

In full reconciliation, all records are fetched from the target system to Oracle Identity Manager.

See [Full Reconciliation](#) for more information on performing full and incremental reconciliation.

1.6.2 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.

See [Installation](#) for more information about the installation options for this connector.

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

1.6.3 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 Manager 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 Filter Suffix attribute of the user reconciliation scheduled job. The Filter Suffix attribute helps you to assign filters to the API based on which you get a filtered response from the target system.

See [Limited Reconciliation for the Concur Connector](#) for more information on limited reconciliation.

1.6.4 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation.

The following sections provide more information:

- [Configuring Transformation of Data During User Reconciliation](#)
- [Configuring Validation of Data During Reconciliation and Provisioning](#)

1.7 Lookup Definitions Used During Connector Operations

Lookup definitions used during reconciliation and provisioning are preconfigured. Preconfigured lookup definitions are automatically created in Oracle Identity Manager after you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

The preconfigured lookup definitions are as follows:

- [Lookup.Concur.Configuration](#)
- [Lookup.Concur.UM.Configuration](#)
- [Lookup.Concur.UM.ProvAttrMap](#)
- [Lookup.Concur.UM.ReconAttrMap](#)
- [Lookup.Concur.BooleanValues](#)
- [Lookup.Concur.Locale](#)
- [Lookup.Concur.CountryofResidence](#)
- [Lookup.Concur.Currency](#)
- [Lookup.Concur.EmployeeAdminCountry](#)
- [Lookup.Concur.Ledger](#)

1.7.1 Lookup.Concur.Configuration

The `Lookup.Concur.Configuration` lookup definition holds connector configuration entries that are used during the target resource reconciliation and provisioning operations.

[Table 1-2](#) lists the default entries in this lookup definition.



Note:

Do not modify the entries in this lookup definition.

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

Code Key	Decode	Description
Bundle Name	org.identityconnectors.genericrest	This entry holds the name of the connector bundle.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle.
Connector Name	org.identityconnectors.genericrest.GenericRESTConnector	This entry holds the name of the connector class.
customAuthClassName	oracle.iam.connectors.concur.auth.ConcurNativeAuth	This entry holds the name of the Auth Class that is used for authorizing user access to the target system.

Table 1-2 (Cont.) Entries in the Lookup.Concur.Configuration Lookup Definition

Code Key	Decode	Description
customParserClassName	oracle.iam.connectors.concur.parser.ConcurResponseParser	This entry holds the name of the Parser Class that is used for parsing responses for the connector operations that are not in the standard JSON format.
customPayload	"__ACCOUNT__.CREATEOP=<batch xmlns="http://www.concursolutions.com/api/user/2011/02/"><UserProfile><EmpId>\$(EmployeeID)</EmpId> <FeedRecordNumber>1</FeedRecordNumber><LoginId>\$(__NAME__)</LoginId><FirstName>\$(FirstName)</FirstName><LastName>\$(LastName)</LastName><Password>##\$(__PASSWORD__)##</Password><CtryCode>\$(CountryofResidence)</CtryCode><LocaleName>\$(Locale)</LocaleName><CrnKey>\$(ReimbursementCurrency)</CrnKey><Custom21>\$(EmployeeAdministrationCountry)</Custom21><Active>\$(__ENABLE__)</Active><EmailAddress>\$(EmailAddress)</EmailAddress><LedgerKey>\$(Ledger)</LedgerKey><Mi>\$(MiddleName)</Mi><ExpenseApproverEmployeeID>\$(ExpenseApproverEmployeeID)</ExpenseApproverEmployeeID></UserProfile></batch>",<UserProfile><EmpId>\$(EmployeeID)</EmpId><FeedRecordNumber>1</FeedRecordNumber><LoginId>\$(__NAME__)</LoginId><FirstName>\$(FirstName)</FirstName><LastName>\$(LastName)</LastName><Password>##\$(__PASSWORD__)##</Password><CtryCode>\$(CountryofResidence)</CtryCode><LocaleName>\$(Locale)</LocaleName><CrnKey>\$(ReimbursementCurrency)</CrnKey><Custom21>\$(EmployeeAdministrationCountry)</Custom21><Active>\$(__ENABLE__)</Active><EmailAddress>\$(EmailAddress)</EmailAddress><LedgerKey>\$(Ledger)</LedgerKey><Mi>\$(MiddleName)</Mi><ExpenseApproverEmployeeID>\$(ExpenseApproverEmployeeID)</ExpenseApproverEmployeeID></UserProfile></batch>", "__ACCOUNT__.__PASSWORD__.UPDATEOP=<UserBatch xmlns="http://www.concursolutions.com/api/user/2011/02/"><User><LoginID>\$(__UID__)</LoginID><Password>##\$(__PASSWORD__)##</Password></User></UserBatch>"	This entry lists the request payload formats for all the connector operations that are not in the standard JSON format.

Table 1-2 (Cont.) Entries in the Lookup.Concur.Configuration Lookup Definition

Code Key	Decode	Description
httpHeader Accept	application/json	This entry holds the accept type expected from the target system in the header.
httpHeader ContentTy pe	application/xml	This entry holds the content type expected by the target system in the header.
jsonResour cesTag	"__ACCOUNT__=Items"	This entry holds the JSON tag value that is used during reconciliation for parsing multiple entries in a single payload.
nameAttrib utes	"__ACCOUNT__.LoginID"	This entry holds the name attribute for all the objects that are handled by this connector. For example, for the __ACCOUNT__ object class that it used for User accounts, the name attribute is LoginID.
opTypes	"__ACCOUNT__.CREATEOP=POST","__ACCOUN T__.UPDATEOP=POST","__ACCOUNT__.SEARCH OP=GET","__ACCOUNT__._PASSWORD__.UPD ATEOP=POST"	This entry specifies the HTTP operation type for each object class supported by the connector. Values are comma separated and are in the following format: <i>OBJ_CLASS.OP=HTTP_OP</i> In this format, <i>OBJ_CLASS</i> is the connector object class, <i>OP</i> is the connector operation (for example, CreateOp, UpdateOp, SearchOp), and <i>HTTP_OP</i> is the HTTP operation (GET, PUT, or POST).
passwordA ttribute	Password	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector in OIM.

Table 1-2 (Cont.) Entries in the Lookup.Concur.Configuration Lookup Definition

Code Key	Decode	Description
relURLs	"__ACCOUNT__.CREATEOP=/api/user/v1.0/users"; "__ACCOUNT__.UPDATEOP=/api/user/v1.0/users"; "__ACCOUNT__.PASSWORD__.UPDATEOP=/api/user/v1.0/users/password"; "__ACCOUNT__.SEARCHOP=/api/v3.0/common/users/\$(Filter Suffix)\$"	<p>This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes.</p> <p>For example, the <code>__ACCOUNT__.CREATEOP=/api/user/v1.0/users</code> value implies that <code>/api/user/v1.0/users</code> is the relative URL for all create provisioning operations that are performed on the <code>__ACCOUNT__</code> object class.</p>
statusAttributes	"__ACCOUNT__.Active"	<p>This entry lists the name of the target system attribute that holds the status of an account. For example, for the <code>__ACCOUNT__</code> object class that it used for User accounts, the status attribute is Active.</p>
uidAttributes	"__ACCOUNT__.LoginID"	<p>This entry holds the UID attribute for the User object class that is handled by this connector.</p> <p>The value <code>"__ACCOUNT__.LoginID"</code> in decode implies that the <code>__UID__</code> attribute (that is, GUID) of the connector for <code>__ACCOUNT__</code> object class is mapped to LoginID, which is the corresponding UID attribute for user accounts in the target system.</p>
User Configuration Lookup	Lookup.Concur.UM.Configuration	<p>This entry holds the name of the lookup definition that stores configuration information used during user management operations.</p>

1.7.2 Lookup.Concur.UM.Configuration

The Lookup.Concur.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations in the target resource mode.

[Table 1-3](#) lists the entries in this lookup definition.

Table 1-3 Entries in the Lookup.Concur.UM.Configuration Lookup

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.Concur.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. This lookup definition is used during user provisioning operations.
Recon Attribute Map	Lookup.Concur.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes.. This lookup definition is used during reconciliation.

1.7.3 Lookup.Concur.UM.ProvAttrMap

The Lookup.Concur.UM.ProvAttrMap lookup definitions hold mappings between process form fields and target system attributes. This lookup definition is preconfigured, and is used during provisioning.

You can add entries in this lookup definition if you want to map new target system attributes for provisioning. See [Adding User Attributes for Provisioning](#).

[Table 1-4](#) lists the default entries in this lookup definition.

Table 1-4 Default Entries in the Lookup.Concur.UM.ProvAttrMap Lookup Definition

Code	Decode
Country of Residence	CountryofResidence
Email Address	EmailAddress
Employee Administration Country	EmployeeAdministrationCountry
Employee ID	EmployeeID
First Name	FirstName
Id	__UID__
Last Name	LastName
Ledger	Ledger
Locale	Locale
Login ID	__NAME__

Table 1-4 (Cont.) Default Entries in the Lookup.Concur.UM.ProvAttrMap Lookup Definition

Code	Decode
Manager	ExpenseApproverEmployeeID
Middle Name	MiddleName
Password	__PASSWORD__
Reimbursement Currency	ReimbursementCurrency
Status	__ENABLE__

1.7.4 Lookup.Concur.UM.ReconAttrMap

The Lookup.Concur.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is preconfigured, and is used during reconciliation.

You can add entries in this lookup definition if you want to map new target system attributes for target resource reconciliation. See [Adding User Attributes for Reconciliation](#).

[Table 1-5](#) lists the default entries in this lookup definition.

Table 1-5 Default Entries in the Lookup.Concur.UM.ReconAttrMap Lookup Definition

Code	Decode
Email Address	PrimaryEmail
Employee ID	EmployeeID
First Name	FirstName
IsActive	IsActive=__ENABLE__?'Y':'N'
Last Name	LastName
ID	__UID__
Login ID	__NAME__
Middle Name	MiddleName
Status	__ENABLE__

1.7.5 Lookup.Concur.BooleanValues

The Lookup.Concur.BooleanValues lookup definition maps boolean values that are used for some of the fields in the target system with the corresponding boolean values to be displayed in the fields of the OIM User form.

[Table 1-6](#) lists the default entries in this lookup definition.

Table 1-6 Default Entries in the Lookup.Concur.BooleanValues Lookup Definition

Code	Decode
N	False
Y	True

1.7.6 Lookup.Concur.Locale

The Lookup.Concur.Locale lookup definition holds information about the supported locale codes for a target system account. This setting determines the display formats for date and time, users' names, addresses, and commas and periods in numbers.

This is a static lookup definition. You must manually populate the entries of this lookup definition.

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

- **Code Key:** Supported locale code for a target system account
- **Decode:** Name of the corresponding locale

[Table 1-7](#) lists the sample entries in this lookup definition.

Table 1-7 Sample Entries in the Lookup.Concur.Locale Lookup Definition

Code	Decode
en_US	English (United States)

1.7.7 Lookup.Concur.CountryofResidence

The Lookup.Concur.CountryofResidence lookup definition holds information about countries that you can assign as a country of residence for a target system user account that you create through Oracle Identity Manager. This is a static lookup definition. You must populate the entries of this lookup definition manually.

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

- **Code Key:** 2–letter ISO code for a country
- **Decode:** Country name

[Table 1-8](#) lists the default entries in this lookup definition.

Table 1-8 Default Entries in the Lookup.Concur.CountryofResidence Lookup Definition

Code Key	Decode
US	UNITED STATES

1.7.8 Lookup.Concur.Currency

The Lookup.Concur.Currency lookup definition holds information about the currency codes that you can assign as a reimbursement currency for a target system user account.

You can either assign a default currency code based on the country that is configured for the user in the Lookup.Concur.CountryofResidence lookup definition or update the currency code by selecting a value from this lookup definition.

This is a static lookup definition, and you must manually populate the entries of this lookup definition.

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

- **Code Key:** 3–letter ISO code for a currency
- **Decode:** 2–letter code of the corresponding country and the currency name

[Table 1-9](#) lists the default entries in this lookup definition.

Table 1-9 Default Entries in the Lookup.Concur.Currency Lookup Definition

Code Key	Decode
USD	US, Dollar

1.7.9 Lookup.Concur.EmployeeAdminCountry

The Lookup.Concur.EmployeeAdminCountry lookup definition holds information about the country from where you want to administer the employee that you select for a target system account.

All of the policies of the specific country are applicable to the employee. For example, if you specify United States for an employee in Canada, the United States policies are applicable to the employee.

This is a static lookup definition. You must manually populate the entries of this lookup definition.

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

- **Code Key:** 2–letter country code from where you want to administer the employee
- **Decode:** Name of the country

[Table 1-10](#) lists the default entries in this lookup definition.

Table 1-10 Default Entries in the Lookup.Concur.EmployeeAdminCountry Lookup Definition

Code	Decode
US	United States

1.7.10 Lookup.Concur.Ledger

The Lookup.Concur.Ledger lookup definition holds the accepted account code ledger value for a target system user account.



Note:

Do not add entries or modify values of this lookup definition.

[Table 1-11](#) lists the default entries in this lookup definition.

Table 1-11 Default Entries of the Lookup.Concur.Ledger Lookup Definition

Code	Decode
DEFAULT	DEFAULT

1.8 Connector Objects Used During Target Resource Reconciliation

Connector objects such as reconciliation rules, reconciliation action rules, and scheduled jobs are used for reconciling user records from the target system into Oracle Identity Manager.

The Concur Target Resource User Reconciliation scheduled job is used to initiate a reconciliation run. See [Reconciliation Scheduled Job for Concur Connector](#) for more information on this scheduled job.



See Also:

Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for generic information about connector reconciliation

This section contains the following topics related to connector objects:

- [User Fields for Target Resource Reconciliation](#)
- [Reconciliation Rules for Target Resource Reconciliation](#)
- [Viewing Reconciliation Rules for Target Resource Reconciliation](#)
- [Reconciliation Action Rules for Target Resource Reconciliation](#)
- [Viewing Reconciliation Action Rules for Target Resource Reconciliation](#)

1.8.1 User Fields for Target Resource Reconciliation

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

In this lookup definition, entries are in the following format:

- **Code Key:** Reconciliation field of the resource object
- **Decode:** Name of the target system attribute

Table 1-12 lists the entries in this lookup definition.

Table 1-12 Entries in the Lookup.Concur.UM.ReconAttrMap Lookup Definition

Code Key	Decode
Email Address	PrimaryEmail
Employee ID	EmployeeID
First Name	FirstName
IsActive	IsActive=__ENABLE__?'Y':'N'
Id	__UID__
Last Name	LastName
Login ID	__NAME__
Middle Name	MiddleName
Status	__ENABLE__

1.8.2 Reconciliation Rules for Target Resource Reconciliation

Reconciliation rules for target resource reconciliation are used by the reconciliation engine to determine the identity to which Oracle Identity Manager must assign a newly discovered account on the target system.

The following is the process-matching rule for users:

Rule name: Concur User Recon Rule

Rule element: Email Equals Login ID

In this rule element:

- Email is the email address attribute of a user.
- Login ID is a unique ID attribute of the Concur account.

1.8.3 Viewing Reconciliation Rules for Target Resource Reconciliation

You can view reconciliation rules by using Oracle Identity Manager Design Console.

To view reconciliation rules for target resource reconciliation:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**.

3. Double-click **Reconciliation Rules**.
4. Search for and open the Concur User Recon Rule.

Figure 1-2 Concur User Recon Rule

1.8.4 Reconciliation Action Rules for Target Resource Reconciliation

Reconciliation action rules define that actions the connector must perform based on the reconciliation rules defined for Users.

[Table 1-13](#) lists the rule condition and the corresponding action to be performed during target resource reconciliation.

Table 1-13 Action Rules for Target Resource Reconciliation

Rule Condition	Action
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.8.5 Viewing Reconciliation Action Rules for Target Resource Reconciliation

You can view reconciliation action rules on the Object Reconciliation tab of a resource object in Oracle Identity Manager Design Console.

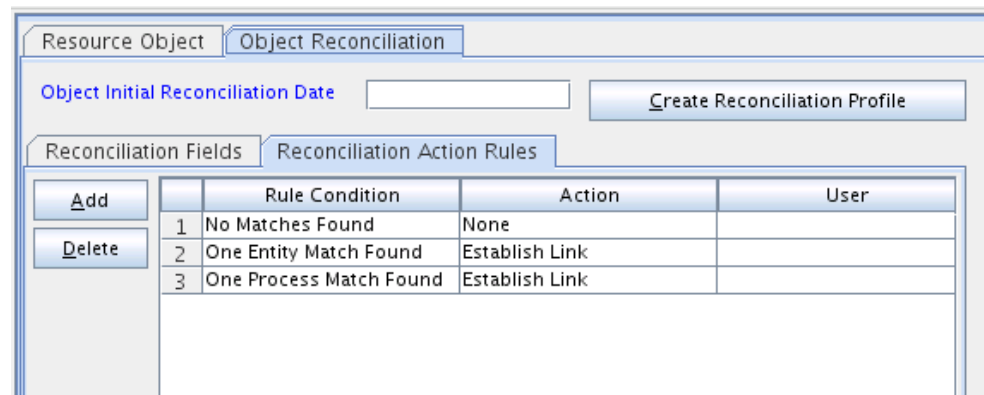
To view reconciliation action rules for target resource reconciliation:

1. Log in to Oracle Identity Manager Design Console.

2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Concur User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab.

The Reconciliation Action Rules tab displays the action rules defined for this connector.

Figure 1-3 Reconciliation Action Rules for Target Resource Reconciliation



1.9 Connector Objects Used During Provisioning

Connector objects such as adapters are used for performing provisioning operations on the target system. These adapters perform provisioning functions on the fields defined in the lookup definition for provisioning.

This section contains the following topics:

- [Provisioning Functions](#)
- [User Fields for Provisioning](#)

1.9.1 Provisioning Functions

These are the supported provisioning functions and the adapters that perform these functions for the connector.

The Adapter column in [Table 1-14](#) gives the name of the adapter that is used when the function is performed.

See Also:

Types of Adapters in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about process tasks and adapters

Table 1-14 User Provisioning Functions

Function	Adapter
Create User	adpCONCURCREATEUSER
Update User	adpCONCURUPDATEUSER
Enable user	adpCONCUREENABLETASK
Disable user	adpCONCURDISABLETASK
Change or reset password	adpCONCURPASSWORDUPDATE

1.9.2 User Fields for Provisioning

The Lookup.Concur.UM.ProvAttrMap lookup definition holds the user fields for provisioning. This lookup definition holds mapping between process form fields and target system attributes.

[Table 1-15](#) lists the entries in the lookup definition.

Table 1-15 Entries in the Lookup.Concur.UM.ProvAttrMap Lookup Definitions

Code Key	Decode
Country of Residence	CountryofResidence
Email Address	EmailAddress
Employee Administration Country	EmployeeAdministrationCountry
Employee ID	EmployeeID
First Name	FirstName
Id	__UID__
Last Name	LastName
Ledger	Ledger
Locale	Locale
Login ID	__NAME__
Manager	ExpenseApproverEmployeeID
Middle Name	MiddleName
Password	__PASSWORD__
Reimbursement Currency	ReimbursementCurrency
Status	__ENABLE__

1.10 Roadmap for Deploying and Using the Concur Connector

This is the organization of information available in this guide for deploying and using the connector.

The rest of this guide is divided into the following chapters:

- [Deploying the Concur Connector](#) describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- [Using the Concur Connector](#) describes guidelines on using the connector, and explains procedures to configure reconciliation runs and perform provisioning operations.
- [Extending the Functionality of the Concur Connector](#) describes procedures that you can perform if you want to extend the functionality of the connector.
- [Files and Directories on the Concur Connector Installation Media](#) lists the files and directories that comprise the connector installation media.

2

Deploying the Concur Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, and postinstallation.

The following topics provide details on these stages:

- [Preinstallation](#)
- [Installation](#)
- [Postinstallation](#)

2.1 Preinstallation

Preinstallation involves setting up a developer sandbox and obtaining the consumer key value. It also involves registering your partner application with Concur for accessing user management APIs.

To obtain these values, perform the following tasks on the target system:

1. Set up the Concur developer sandbox, and obtain the consumer key for your Concur Developer Sandbox account.

You provide the consumer key value for the `customAuthHeaders` parameter while configuring the IT resource.

2. Register your partner application (that is the Concur connector) with Concur.

The detailed instructions for performing these preinstallation tasks are available in the Concur product documentation. For more information, visit the Concur website at <https://developer.concur.com/>.

2.2 Installation

You must install the connector in Oracle Identity Manager. If necessary, you can also deploy the connector in a Connector Server.

The following topics provide details on installing the Concur connector:

- [Understanding Installation of the Concur Connector](#)
- [Running the Connector Installer](#)
- [Configuring the IT Resource for the Target System](#)

2.2.1 Understanding Installation of the Concur Connector

You can run the connector code either locally in Oracle Identity Manager or remotely in a Connector Server.

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

- Run the connector code locally in Oracle Identity Manager.
In this scenario, you deploy the connector in Oracle Identity Manager. Deploying the connector in Oracle Identity Manager involves performing the procedures described in [Running the Connector Installer](#) and [Configuring the IT Resource for the Target System](#).
- Run the connector code remotely in a Connector Server.
In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. For information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server, see *Using an Identity Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.2.2 Running the Connector Installer

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

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:
`OIM_HOME/server/ConnectorDefaultDirectory`

 **Note:**

If this is the first time you are running the Connector Installer for deploying the connector bundle in a Connector Server, then place the bundle in the connector server bundle directory.

2. Log in to Oracle Identity System Administration.
3. In the left pane, under System Management, click **Manage Connector**.
4. In the Manage Connector page, click **Install**.
5. From the Connector List list, select **Concur Connector RELEASE_NUMBER**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory: `OIM_HOME/server/ConnectorDefaultDirectory`
If you have copied the installation files into a different directory, then:
 - a. In the **Alternative Directory** field, enter the full path and name of that directory.
 - b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
 - c. From the Connector List list, select **Concur Connector RELEASE_NUMBER**.
6. Click **Load**.
7. To start the installation process, click **Continue**. The following tasks are performed in sequence:
 - a. Configuration of connector libraries
 - b. Import of the connector XML files (by using the Deployment Manager)

c. Compilation of adapters

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

- a. To retry the installation, click **Retry**.
 - b. To cancel the installation and restart the installation process, click **Cancel**, and then repeat Step 3 through Step 8.
8. If all three tasks of the connector installation process are successful, then a message indicating successful installation appears.

In addition, a list of the steps that you must perform after the installation appears. These steps are as follows:

- a. Configuring the IT resource for the connector. The procedure to configure the IT resource is described later in this guide.
- b. Configuring the scheduled tasks that are created when you installed the connector. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in [Files and Directories on the Concur Connector Installation Media](#).

2.2.3 Configuring the IT Resource for the Target System

An IT resource for your target system is created after you install the connector. You configure this IT resource to enable the connector to connect Oracle Identity Manager with your target system.

This section contains the following topics:

- [IT Resource Parameters](#)
- [Specifying Values for IT Resource Parameters](#)

2.2.3.1 IT Resource Parameters

An IT resource is composed of parameters that store connection and other generic information about a target system. Oracle Identity Manager uses this information to connect to a specific installation or instance of your target system.

[Table 2-1](#) displays each parameter of the Concur IT resource in an alphabetical order.

Table 2-1 IT Resource Parameters

Parameter	Description
authenticationServerUrl	Enter the URL of the authentication server that validates the consumer key for your target system. Sample value: <code>https://www.concursolutions.com/net2/oauth2/accesstoken.ashx</code>

Table 2-1 (Cont.) IT Resource Parameters

Parameter	Description
authenticationType	Type of authentication that is used by your target system. This connector supports the OAuth 2.0 custom authentication type. Default value: <code>custom</code> Do <i>not</i> modify the value of the parameter.
customAuthHeaders	Enter the consumer key in the following format: "X-ConsumerKey=CONSUMER_KEY" In this format, replace <code>CONSUMER_KEY</code> with the consumer key that is assigned to you after you register for the Concur developer sandbox. Sample value: "X-ConsumerKey=abc12345Abc12345AbcXYZ" See Preinstallation for more information on obtaining the consumer key.
Configuration Lookup	Name of the lookup definition that stores configuration information used during the reconciliation and provisioning operations. Default value: <code>Lookup.Concur.Configuration</code>
Connector Server Name	If you have deployed the Concur connector in the Connector Server, then enter the name of the IT resource for the Connector Server.
host	Enter the host name of the computer hosting your target system. Sample value: <code>www.concursolutions.com</code>
password	Enter the password for connecting to the Connector platform. This is the password that you specified while registering for the Concur developer sandbox.
port	Enter the port number at which the target system is listening.
proxyHost	Enter the name of the proxy host that is used to connect to an external target. Sample value: <code>www.example.com</code>
proxyPort	Enter the proxy port number.
proxyUser	Enter the proxy user name of the target system user account that Oracle Identity Manager uses to connect to the target system.
proxyPassword	Enter the password of the proxy user ID of the target system user account that Oracle Identity Manager uses to connect to the target system.
sslEnabled	If the target system requires SSL connectivity, then set the value of this parameter to <code>true</code> . Otherwise set the value to <code>false</code> . Default value: <code>true</code>

Table 2-1 (Cont.) IT Resource Parameters

Parameter	Description
username	Enter the user name for connecting to the Concur platform. This is the email address that you specified while registering for the Concur developer sandbox.

2.2.3.2 Specifying Values for IT Resource Parameters

The IT resource for the target system contains connection information about the target system. Oracle Identity Governance uses this information during provisioning and reconciliation. The Concur IT resource is automatically created when you run the Connector Installer, and you must specify values for the parameters of the IT resource.

To specify values for the parameters of the IT resource:

1. Log in to Identity System Administration.
2. Create and activate a sandbox. See *Creating a Sandbox and Activating and Deactivating a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
3. In the left pane, under Configuration, click **IT Resource**.
4. In the **IT Resource Name** field on the Manage IT Resource page, enter `Concur` and then click **Search**.
5. Click the Edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. [IT Resource Parameters](#) describes each parameter.
8. To save the values, click **Update**.

2.3 Postinstallation

Postinstallation for the connector involves configuring Oracle Identity Manager, enabling logging to track information about all connector events, and configuring SSL. It also involves performing some optional configurations such as localizing the user interface.

The postinstallation steps are divided across the following sections:

- [Configuring Oracle Identity Manager](#)
- [Localizing Field Labels in UI Forms](#)
- [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)
- [Managing Logging for the Concur Connector](#)
- [Configuring SSL for the Concur Connector](#)

2.3.1 Configuring Oracle Identity Manager

You must create a UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations. In addition, you must run the entitlement and catalog synchronization jobs.

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

- [Creating and Activating a Sandbox](#)
- [Creating a New UI Form](#)
- [Associating the Form with the Application Instance](#)
- [Publishing a Sandbox](#)
- [Harvesting Entitlements and Sync Catalog](#)
- [Updating an Existing Application Instance with a New Form](#)

2.3.1.1 Creating and Activating a Sandbox

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 and Deactivating a Sandbox](#) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.1.2 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 Manager*.

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

2.3.1.3 Associating the Form with the Application Instance

By default, an application instance named **Concur Application Instance** is automatically created after you install the connector. You must associate this application instance with the form created in [Creating a New UI Form](#). See [Modifying Application Instances](#) in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

After updating the application instance, you must publish it to an organization to make the application instance available for requesting and subsequent provisioning to users.

As a best practice, perform the following procedure before publishing the application instance:

1. In Identity System Administration, deactivate the sandbox.
2. Log out of Identity System Administration.
3. Log in to Oracle Identity Self Service and activate the sandbox that you deactivated in Step 1.

4. In the Catalog, check for the Application Instance UI (form fields) and ensure that it appears correctly.
5. Publish the application instance only if everything appears correctly. Otherwise, fix the issues and then publish the application instance.

For instructions on publishing an application instance to an organization, see *Managing Organizations Associated With Application Instances* in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

2.3.1.4 Publishing a Sandbox

Before publishing a sandbox, perform the following 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 Concur application instance form appears with correct fields.
5. Publish the sandbox. See *Publishing a Sandbox* in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.1.5 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 Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
2. 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.

2.3.1.6 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

1. Create and activate a sandbox. See *Creating a Sandbox and Activating and Deactivating a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
2. Create a new UI form for the resource. See *Creating Forms By Using the Form Designer in Oracle Fusion Middleware Administering Oracle Identity Manager*.
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 *Publishing a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.2 Localizing Field Labels in UI Forms

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

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

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

```
SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime  
\BizEditorBundle_en.xlf"
```

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

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

- b. Replace with the following text:

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

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

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

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

```
<trans-unit
id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResource
Bundle']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.us
erEO.UD_LOGINID__c_description']]">
<source>Login ID</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ConcurForm.entity.Co
ncurFormEO.UD_LOGINID __c_LABEL">
<source>Login ID</source>
<target/>
</trans-unit>
```

In this text, ConcurForm is the current form instance name associated with the Concur application instance.

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

```
global.UD_CONCUR_LOGINID =\u30A2\u30AB\u30A6\u30F3\u30C8\u540D.
```

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

```
<trans-unit
id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResource
Bundle']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.us
erEO.UD_CONCUR_LOGINID__c_description']]">
<source>LoginID</source>
<target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.Concur.entity
sEO.UD_CONCUR__c_LABEL">
<source>First Name</source>
<target>\u30A2\u30F3\u30C8\u540D</target>
</trans-unit>
```

- f. Repeat Step 6 a through Step 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.

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. Whenever you add a new resource bundle to the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, switch to the `OIM_HOME/server/bin` directory.
2. Enter one of the following commands:
 - **On Microsoft Windows:** `PurgeCache.bat All`
 - **On UNIX:** `PurgeCache.sh All`

 **Note:**

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

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

- `PurgeCache.bat MetaData`
- `PurgeCache.sh MetaData`

Before running the `PurgeCache` utility, ensure the `WL_HOME` and `JAVA_HOME` environment variables are set.

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

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

In this format:

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

2.3.4 Managing Logging for the Concur Connector

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

The following topics provide detailed information about logging:

- [Understanding Log Levels](#)
- [Enabling Logging](#)

2.3.4.1 Understanding Log Levels

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. ODL is the principle logging service used by Oracle Identity Manager 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 Manager to continue running.
- `WARNING`
This level enables logging of information about potentially harmful situations.
- `INFO`
This level enables logging of messages that highlight the progress of the application.
- `CONFIG`
This level enables logging of information about fine-grained events that are useful for debugging.
- `FINE`, `FINER`, `FINEST`
These levels enable logging of information about fine-grained events, where `FINEST` logs information about all events.

These message types are mapped to ODL message type and level combinations as shown in [Table 2-2](#).

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

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	TRACE16
FINEST	TRACE32

The configuration file for OJDL is logging.xml, which is located at the following path:
DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

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

2.3.4.2 Enabling Logging

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:
 - a. Add the following blocks in the file:

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

<logger name="ORG.IDENTITYCONNECTORS.CONCUR" level="[LOG_LEVEL]"
useParentHandlers="false">
  <handler name="Concur-handler" />
  <handler name="console-handler" />
</logger>
```

- b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. [Understanding Log Levels](#) 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='Concur-handler' level='NOTIFICATION:
1'class='oracle.core.ojdl.logging.ODLHandlerFactory'>
  <property name='logreader:' value='off' />
  <property name='path' value='F:\MyMachine\middleware
\user_projects\domains\base_domain1\servers\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.CONCUR" level="NOTIFICATION:1"
useParentHandlers="false">
  <handler name="Concur-handler" />
  <handler name="console-handler" />
</logger>
```

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

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:
 - For Microsoft Windows: set WLS_REDIRECT_LOG=**FILENAME**
 - For UNIX: export WLS_REDIRECT_LOG=**FILENAME**

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

4. Restart the application server.

2.3.5 Configuring SSL for the Concur Connector

You configure SSL to secure data communication between Oracle Identity Manager and the target system.

To configure SSL:

1. Obtain the SSL certificate by obtaining the public key certificate of the target system.
2. Copy the public key certificate of the target system to the computer hosting Oracle Identity Manager.
3. Run the following keytool command to import the public key certificate into the identity key store in Oracle Identity Manager:

```
keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -file
CERT_FILE_NAME -storepass PASSWORD
```

In this command:

- *CERT_FILE_NAME* is the full path and name of the certificate file
- *PASSWORD* is the password of the keystore.

The following is a sample value for this command:

```
keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -  
file /home/target.cert -storepass DemoTrustKeyStorePassPhrase
```

 **Note:**

Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool arguments.

3

Using the Concur Connector

You can use the Concur connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.

This chapter contains the following topics:

Note:

These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before performing the procedures.

- [Configuring Reconciliation for the Concur Connector](#)
- [Configuring Scheduled Jobs](#)
- [Guidelines on Performing Provisioning Operations](#)
- [Performing Provisioning Operations](#)
- [Uninstalling the Connector](#)

3.1 Configuring Reconciliation for the Concur Connector

You can configure the connector to specify the type of reconciliation and its schedule.

This section provides details on the following topics related to configuring reconciliation:

- [Full Reconciliation](#)
- [Limited Reconciliation for the Concur Connector](#)
- [Reconciling Large Number of Records](#)
- [Reconciliation Scheduled Job for Concur Connector](#)

3.1.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager.

After you deploy the connector, you must first perform full reconciliation. To perform a full reconciliation run, ensure that no value is specified for the Filter attribute of the scheduled job for reconciling users. If the target system contains more number of records than what it can return in a single response, then use the Flat File connector to perform full reconciliation. For more information on reconciling large number of records, see [Reconciling Large Number of Records](#).

3.1.2 Limited Reconciliation for the Concur Connector

You can perform limited reconciliation by creating filters for the reconciliation module, and reconcile records from the target system based on a specified filter criterion.

Limited or filtered reconciliation is the process of limiting the number of records being reconciled based on a set filter criteria. 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.

This connector provides a Filter Suffix attribute (a scheduled task attribute) that allows you to use any of the attributes of the target system to filter target system records. You specify a value for the Filter Suffix attribute (for example, EmployeeID) while configuring the user reconciliation scheduled job.

 **Note:**

If the target system contains more number of records than what it can return in a single response, then use the Flat File connector to perform limited reconciliation. See [Reconciling Large Number of Records](#) for more information.

For more information on Concur filters, see information on user resources related to API Explorer on the Concur Developer Center page at <https://developer.concur.com/>.

3.1.3 Reconciling Large Number of Records

During a reconciliation run, if the target system contains more number of records than what it can return in a single response, you can fetch all the records into Oracle Identity Manager using the Flat File connector. The Flat File connector consumes information in a flat file, and generates connector metadata using the metadata generation utility.

To reconcile a large number of records from the target system into Oracle Identity Manager:

1. Export all users in the target system to a flat file.
2. Copy the flat file to a location that is accessible from Oracle Identity Manager.
3. Create a schema file representing the structure of the flat file. See *Creating a Schema File* in *Oracle Identity Manager Connector Guide for Flat File* for instructions on creating a schema file.
4. Install the Flat File connector. See *Running the Connector Installer* in *Oracle Identity Manager Connector Guide for Flat File* for instructions on installing the Flat File connector.
5. Configure the Flat File IT resource. See *Configuring the IT Resource* in *Oracle Identity Manager Connector Guide for Flat File* for instructions on configuring Flat File IT resource.
6. Configure and run the Flat File Accounts Loader scheduled job. See *Flat File Accounts Loader and IT_RES_NAME Flat File Accounts Loader* in *Oracle Identity*

Manager Connector Guide for Flat File for instructions on configuring and running the Flat File Accounts Loader scheduled job.

While configuring this scheduled job, ensure that you set the value of the **Target IT Resource Name** attribute to `Concur` and **Target Resource Object Name** to `Concur User`.

3.1.4 Reconciliation Scheduled Job for Concur Connector

When you run the Connector Installer, reconciliation scheduled jobs are automatically created in Oracle Identity Manager. You must configure these scheduled jobs to suit your requirements by specifying values for its attributes.

The Concur User Reconciliation scheduled job is used to reconcile user account data from the target system in the target resource (account management) mode of the connector.

[Table 3-1](#) describes the attributes of the scheduled job.

Table 3-1 Attributes of the Concur User Reconciliation Scheduled Job

Attribute	Description
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. See Limited Reconciliation for the Concur Connector for more information.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: <code>Concur</code>
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: <code>User</code> Do <i>not</i> change the default value.
Resource Object Name	Name of the resource object against which reconciliation runs are performed. Default value: <code>Concur User</code> Do <i>not</i> change the default value.

3.2 Configuring Scheduled Jobs

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

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

To configure a scheduled job:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:

- a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
 - b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the 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 Manager*.

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.
- See [Reconciliation Scheduled Job for Concur Connector](#) for the list of scheduled tasks and their attributes.

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.

3.3 Guidelines on Performing Provisioning Operations

These are the guidelines that you must apply while performing provisioning operations.

- Ensure that you provision only one Concur account for an Oracle Identity Manager User.
- During the Create User provisioning operation, if you want to assign a manager for the user, you must specify the Employee ID of the user that you want to assign as a manager in the Manager field.
- While performing the Enable User, Disable User, or Reset Password provisioning operations for the first time for a Concur resource that is created in Oracle Identity Manager through a reconciliation run, ensure that values are populated for all the mandatory user fields in Oracle Identity Manager. If there are any user fields

without values, then you must specify the values by performing the Update User provisioning operations.

3.4 Performing Provisioning Operations

You create a new user in 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 Manager:

1. Log in to Identity Self Service.
2. Create a user as follows:
 - a. 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 configured for the connector that you configured earlier, and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.

See Also:

Creating a User in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for details about the fields on the Create User page

3.5 Uninstalling the Connector

Uninstalling the concur connector deletes all the account related data associated with 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: `Concur User`

 **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*.

4

Extending the Functionality of the Concur Connector

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

This chapter contains the following topics:

Note:

From Oracle Identity Manager Release 11.1.2 onwards, lookup queries are not supported. For information on managing lookups by using the Form Designer in Identity System Administration, see *Managing Lookups in Oracle Fusion Middleware Administering Oracle Identity Manager*.

- [Adding User Attributes for Reconciliation](#)
- [Adding User Attributes for Provisioning](#)
- [Configuring Validation of Data During Reconciliation and Provisioning](#)
- [Configuring Transformation of Data During User Reconciliation](#)
- [Configuring the Concur Connector for Multiple Installations of the Target System](#)
- [Defining the Concur Connector](#)

4.1 Adding User Attributes for Reconciliation

The connector provides a default set of attribute mappings for reconciliation between Oracle Identity Manager and the target system. If required, you can add new user attributes for reconciliation.

The default attribute mappings for reconciliation are listed in [Table 1-12](#).

The following topics provide details on adding new user attributes for reconciliation:

- [Adding New Attributes on the Process Form](#)
- [Adding Attributes to the Resource Object](#)
- [Creating Reconciliation Field Mapping](#)
- [Creating Entries in Lookup Definitions for Reconciliation](#)
- [Performing Changes in a New UI Form](#)

4.1.1 Adding New Attributes on the Process Form

You can add a new attribute on the process form in the Form Designer section of Oracle Identity Manager Design Console.

To add a new attribute on the process form:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_Concur** process form.
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the field.

For example, if you are adding the MiddleName field, enter UD_Concur_MIDDLENAME in the Name field and then enter other details such as Variable Type, Length, Field Label, and Field Type.

6. Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form.

Figure 4-1 New Fields Added to the Concur User Form

The screenshot shows the 'Form Designer' interface for the 'UD_CONCUR' process form. The 'Table Information' section shows the table name 'UD_CONCUR' and description 'Concur User Form'. The 'Form Type' is set to 'Process'. The 'Version Information' section shows the latest and active versions as 'Concur'. The 'Operations' section includes a dropdown for 'Current Vers...' set to 'Concur' and buttons for 'Create NewVersion' and 'Make Version Active'. Below these sections is a table of 'User Defined Fields' with columns for Name, Variant Ty..., Len..., Field Label, Field Type, and Default Value.

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value
1	UD_CONCUR_ADMINCOUNTRY	String	255	Employee Adminis	LookupField	
2	UD_CONCUR_EMAILADDRESS	String	255	Email Address	TextField	
3	UD_CONCUR_LEDGER	String	255	Ledger	LookupField	
4	UD_CONCUR_STATUS	String	5	Status	DOField	Y
5	UD_CONCUR_ID	String	255	Id	DOField	
6	UD_CONCUR_MANAGEREMPID	String	255	Manager	TextField	
7	UD_CONCUR_MIDDLENAME	String	255	Middle Name	TextField	
8	UD_CONCUR_IT_RESOURCE	long		IT Resource	ITResourceLookup	
9	UD_CONCUR_PASSWORD	String	255	Password	PasswordField	
10	UD_CONCUR_LOGINID	String	255	Login ID	DOField	
11	UD_CONCUR_EMPLOYEEID	String	255	Employee ID	TextField	
12	UD_CONCUR_FIRSTNAME	String	255	First Name	TextField	
13	UD_CONCUR_LASTNAME	String	255	Last Name	TextField	
14	UD_CONCUR_COUNTRYOFRESIDENCE	String	255	Country of Reside	LookupField	
15	UD_CONCUR_LOCALE	String	255	Locale	LookupField	

4.1.2 Adding Attributes to the Resource Object

You can add the new attribute to the resource object in the Resource Objects section of Oracle Identity Manager Design Console.

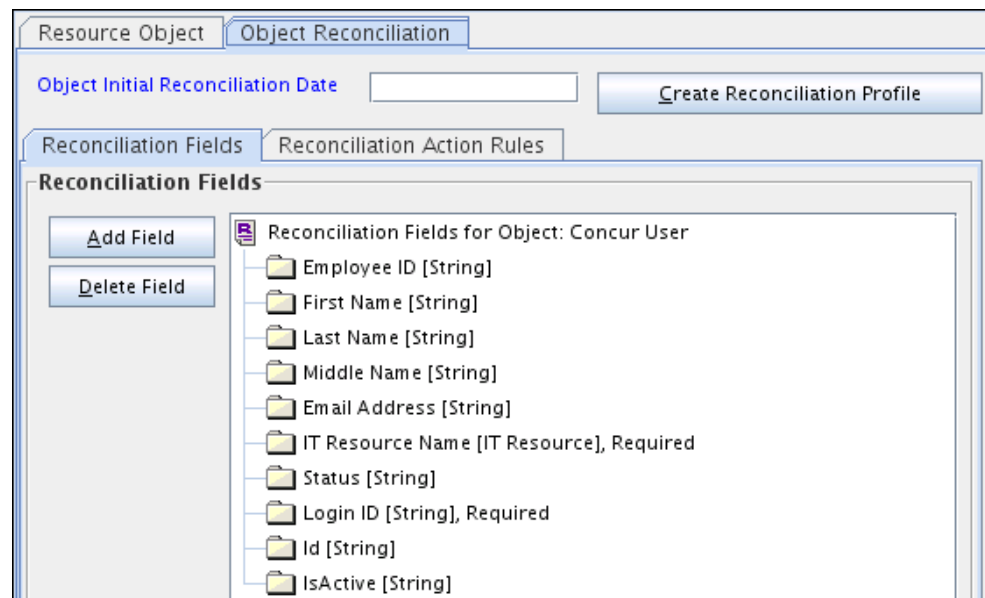
To add the new attribute to the list of reconciliation fields in the resource object:

1. Expand **Resource Management**, and double-click **Resource Objects**.
2. Search for and open the **Concur User** resource object.
3. On the Object Reconciliation tab, click **Add Field**.
4. Enter the details of the field.

For example, enter `Middle Name` in the **Field Name** field and select **String** from the **Field Type** list. Later in this procedure, you enter the field name as the Code value of the entry that you create in the lookup definition for reconciliation.

5. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:

Figure 4-2 New Reconciliation Field added to the Resource Object



6. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

4.1.3 Creating Reconciliation Field Mapping

You can create reconciliation field mapping for the new attribute in the Process Definition section of Oracle Identity Manager Design Console.

To create reconciliation field mapping for the new attribute in the process definition:

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the **Concur User** process definition for Users.
3. On the Reconciliation Field Mappings tab of the process definition, click **Add Field Map**.
4. From the Field Name list, select the field that you want to map.
5. Double-click the **Process Data Field** field, and then select the column for the attribute. For example, select `UD_CONCUR_MIDDLENAME`.
6. Click the **Save** icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:

Figure 4-3 New Reconciliation Field Mapped to a Process Data Field in the Process Definition

The screenshot displays the 'Process Definition' window for 'Concur User'. The 'Name' field is 'Concur User', 'Type' is 'Provisioning', and 'Object Name' is 'Concur User'. The 'Form Assignment' section shows 'Table Name' as 'UD_CONCUR'. The 'Reconciliation Field Mappings' tab is active, showing a list of mappings for the process. The mappings are:

- Employee ID [String] = UD_CONCUR_EMPLOYEEID
- First Name [String] = UD_CONCUR_FIRSTNAME
- Last Name [String] = UD_CONCUR_LASTNAME
- Middle Name [String] = UD_CONCUR_MIDDLENAME
- Email Address [String] = UD_CONCUR_EMAILADDRESS
- IT Resource Name [IT Resource] = UD_CONCUR_IT_RESOURCE
- Status [String] = OIM_OBJECT_STATUS
- Login ID [String] = UD_CONCUR_LOGINID, <KEY>
- Id [String] = UD_CONCUR_ID
- IsActive [String] = UD_CONCUR_STATUS

4.1.4 Creating Entries in Lookup Definitions for Reconciliation

You can create an entry for the newly added attribute in the lookup definition that holds attribute mappings for reconciliation.

To create an entry for the newly added attribute in the lookup definition for reconciliation:

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open the following lookup definition for Users:

Lookup.Concur.UM.ReconAttrMap

4. Click **Add**, and enter the Code Key and Decode values for the field.

The Code Key value must be the name of the field in the resource object. The Decode value must be the name of the target system field in Concur.

5. Click the Save icon.

Figure 4-4 Entry Added to the Lookup Definition for Reconciliation

The screenshot shows a 'Lookup Definition' form with the following fields:

- Code: `Lookup.Concur.UM.ReconAttrMap`
- Field: (empty text box)
- Lookup Type: (selected), Field Type
- Required:
- Group: `Concur`

Below the form is a section titled 'Lookup Code Information' containing a table with the following data:

	Code Key	
1	Status	__ENABLE__
2	Login ID	__NAME__
3	Id	__UID__
4	Employee ID	EmployeeID
5	First Name	FirstName
6	IsActive	IsActive=__ENABLE__?'Y':'N'
7	Last Name	LastName
8	Middle Name	MiddleName
9	Email Address	PrimaryEmail

4.1.5 Performing Changes in a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

To perform changes in a new UI form:

1. Log in to Identity System Administration.
2. Create and activate a sandbox. See *Creating a Sandbox and Activating and Deactivating a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
3. Create a new UI form to view the newly added field along with the rest of the fields. See *Creating Forms By Using the Form Designer in Oracle Fusion Middleware Administering Oracle Identity Manager*.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See *Publishing a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

4.2 Adding User Attributes for Provisioning

The connector provides a default set of attribute mappings for provisioning between Oracle Identity Manager and the target system. If required, you can add new user attributes for provisioning.

The default attribute mappings for provisioning are listed in [Table 1-15](#).

The following topics provide details on adding new user attributes for provisioning:

- [Adding New Attributes for Provisioning](#)
- [Creating Entries in Lookup Definitions for Provisioning](#)
- [Creating a Task to Enable Update Operations](#)
- [Replicating Form Designer Changes to a New UI Form](#)

4.2.1 Adding New Attributes for Provisioning

You add a new attribute on the process form in the Form Designer section of Oracle Identity Manager Design Console.

 **Note:**

If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

To add a new attribute on the process form:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the following process form for Users.
UD_CONCUR
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the attribute.

For example, if you are adding the Middle Name field, enter UD_CONCUR_MIDDLENAME in the Name field, and then enter the rest of the details of this field.

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

The following screenshot shows the new field added to the process form:

Figure 4-5 New Field Added to the Concur User Form

The screenshot shows the 'Form Designer' window for the 'UD_CONCUR' table. The 'Table Information' section shows the table name 'UD_CONCUR' and description 'Concur User Form'. The 'Form Type' is set to 'Process'. The 'Version Information' section shows the latest and active version as 'Concur'. The 'Operations' section shows the current version as 'Concur' and buttons for 'Create New Version' and 'Make Version Active'.

Below the configuration sections is a table with the following columns: Name, Variant Ty..., Len..., Field Label, Field Type, and Default Value. The table contains 15 rows of fields:

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value
1	UD_CONCUR_ADMINCOUNTRY	String	255	Employee Adminis	LookupField	
2	UD_CONCUR_EMAILADDRESS	String	255	Email Address	TextField	
3	UD_CONCUR_LEDGER	String	255	Ledger	LookupField	
4	UD_CONCUR_STATUS	String	5	Status	DOField	Y
5	UD_CONCUR_ID	String	255	Id	DOField	
6	UD_CONCUR_MANAGEREMPID	String	255	Manager	TextField	
7	UD_CONCUR_MIDDLENAME	String	255	Middle Name	TextField	
8	UD_CONCUR_IT_RESOURCE	long		IT Resource	ITResourceLookup	
9	UD_CONCUR_PASSWORD	String	255	Password	PasswordField	
10	UD_CONCUR_LOGINID	String	255	Login ID	DOField	
11	UD_CONCUR_EMPLOYEEID	String	255	Employee ID	TextField	
12	UD_CONCUR_FIRSTNAME	String	255	First Name	TextField	
13	UD_CONCUR_LASTNAME	String	255	Last Name	TextField	
14	UD_CONCUR_COUNTRYOFRESIDENCE	String	255	Country of Reside	LookupField	
15	UD_CONCUR_LOCALE	String	255	Locale	LookupField	

4.2.2 Creating Entries in Lookup Definitions for Provisioning

You can create an entry for the newly added attribute in the lookup definition that holds attribute mappings for provisioning.

To create an entry for the newly added attribute in the lookup definition for provisioning:

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open the following lookup definition for Users:
Lookup.Concur.UM.ProvAttrMap
4. Click **Add**, and then enter the Code Key and Decode values for the attribute.

Note that the Decode value must be the name of the target system field.

Figure 4-6 Entry Added to the Lookup Definition for Provisioning

Lookup Definition

Code:

Field:

Lookup Type Field Type

Required:

Group:

Lookup Code Information

		Code Key	Decode
<input type="button" value="Add"/>	1	Employee ID	EmployeeID
<input type="button" value="Delete"/>	2	First Name	FirstName
	3	Last Name	LastName
	4	Middle Name	MiddleName
	5	Country of Residence	CountryofResidence
	6	Locale	Locale
	7	Reimbursement Currency	ReimbursementCurrency
	8	Employee Administration Country	EmployeeAdministrationCountry
	9	Email Address	EmailAddress
	10	Ledger	Ledger
	11	Manager	ExpenseApproverEmployeeID
	12	Password	__PASSWORD__
	13	Id	__UID__
	14	Status	__ENABLE__
	15	Login ID	__NAME__

4.2.3 Creating a Task to Enable Update Operations

You create a task to enable updates on the new user or group attribute during provisioning operations. If you do not perform this procedure, you cannot modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the new user attribute as follows:

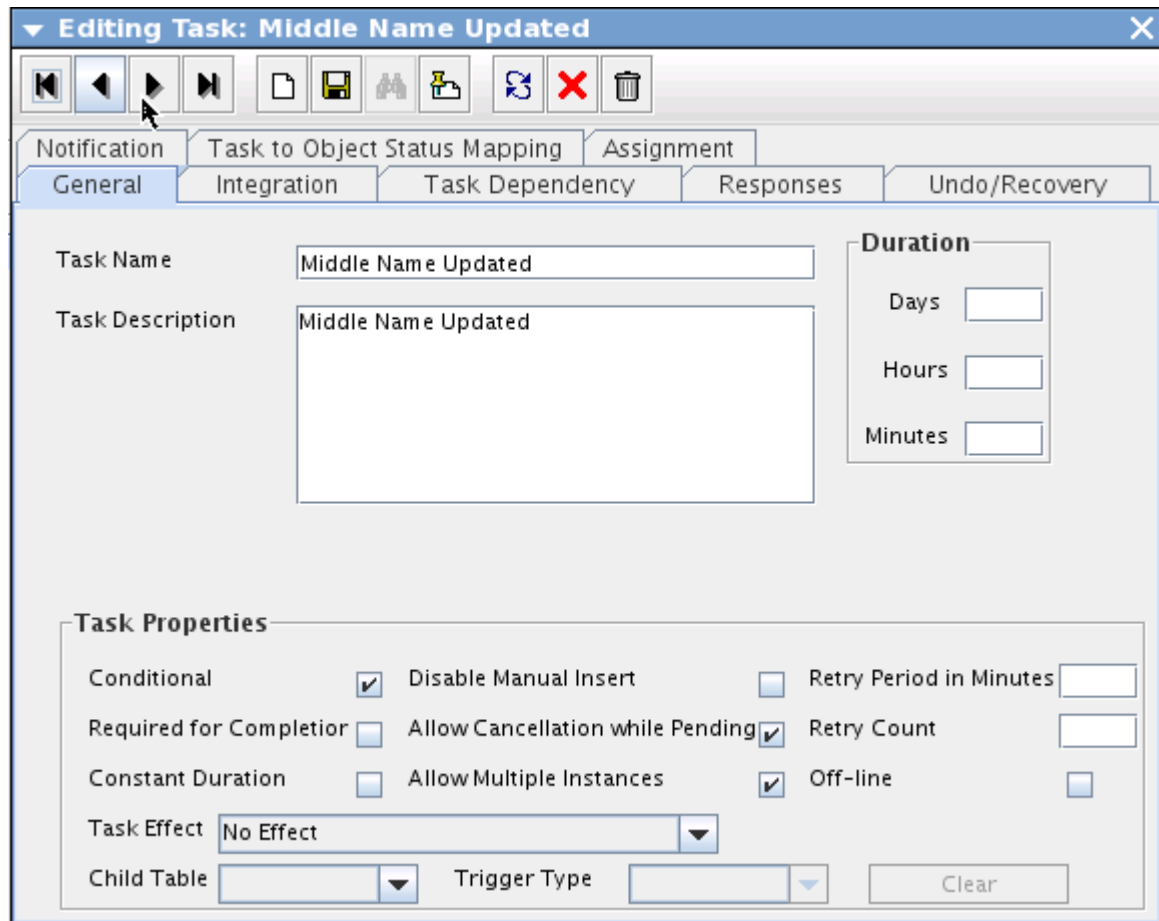
1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the following process definition for Users:

Concur User

3. Click **Add**.
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
 - Conditional
 - Required for Completion
 - Allow Cancellation while Pending
 - Allow Multiple Instances
5. Click the Save icon.

The following screenshot shows the new task added to the process definition:

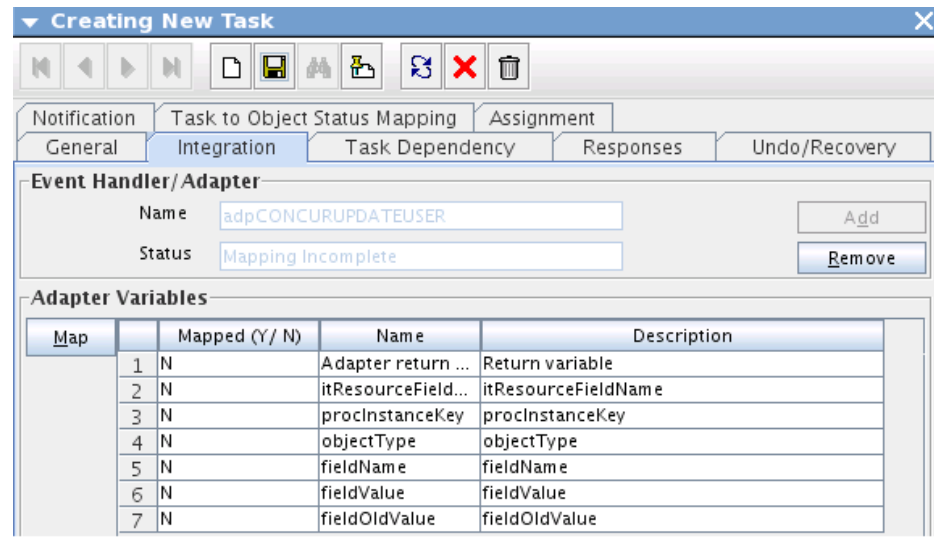
Figure 4-7 New Task Added to the Process Definition



6. In the provisioning process, select the adapter name in the Handler Type section as follows:
 - a. Go to the Integration tab, click **Add**.
 - b. In the Handler Selection dialog box, select **Adapter**.
 - c. From the Handler Name column, select **adpCONCURUPDATEUSER**.
 - d. Click Save and close the dialog box.

The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:

Figure 4-8 List of Adapter Variables



7. In the Adapter Variables region, click the **proInstanceKey** variable.
8. In the dialog box that is displayed, map the adapter variable as follows:
 - a. Click **Map**. The Data Mapping for Variable window is displayed.
 - b. Complete the following fields:
 - **Variable Name:** proInstanceKey
 - **Map To:** Process Data
 - **Qualifier:** Process Instance
9. Click **Save** and close the dialog box.

The mapping status for the adapter variable changes from N to Y. This indicates that the adapter variable has been mapped.

10. If you are enabling update provisioning operations for a User attribute, repeat Step 7 through Step 9 for the remaining variables listed in the Adapter Variables region.

The following table lists the values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
Adapter Return Value	Response Code	NA	NA
Object Type	Literal	String	User
itResourceFieldName	Literal	String	UD_CONCUR_IT_RESOURCE
fieldName	Literal	String	UD_CONCUR_MIDDLENAME
fieldOldValue	Process Data	Middle Name	NA

Note: Ensure that the **Old Value** check box is selected.

Variable	Map To	Qualifier	Literal Value
fieldValue	Process Data	Middle Name	NA

Note: Ensure that the **Old Value** check box is not selected.

11. On the Responses tab, click Add to add at least the SUCCESS response code, with Status C. This ensures that if the task is successfully run, then the status of the task is displayed as Completed.
12. Click the Save icon and close the dialog box, and then save the process definition.

4.2.4 Replicating Form Designer Changes to a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

To replicate Form Designer changes to a new UI form:

1. Log in to Identity System Administration.
2. Create and activate a sandbox. See *Creating a Sandbox and Activating and Deactivating a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
3. Create a new UI form to view the newly added field along with the rest of the fields. See *Creating Forms By Using the Form Designer in Oracle Fusion Middleware Administering Oracle Identity Manager*.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See *Publishing a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

4.3 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements.

For example, you can validate data fetched from the User Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the User Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations. For data that fails the validation check, the following message is displayed or recorded in the log file: Validation failed for attribute *ATTRIBUTE_NAME*.

To configure validation of data:

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

The validation class must implement validate method with the following method signature:

```
boolean validate(HashMap hmUserDetails, HashMap hmEntitlementDetails,
String field)
```

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

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

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to Oracle Identity Manager database.

Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

 **Note:**

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

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

For UNIX: *OIM_HOME/server/bin/UploadJars.sh*

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host

computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. If you created the Java class for validating a process form field for reconciliation, then:
 - a. Log in to the Design Console.
 - b. Create a lookup definition named **Lookup.Concur.UM.ReconValidation**.
 - c. Save the changes to the lookup definition.
 - d. Search for and open the **Lookup.Concur.UM.Configuration** lookup definition.
 - e. In the Code Key column, enter `Recon Validation Lookup`. In the Decode column, enter `Lookup.Concur.UM.ReconValidation`.
 - f. Save the changes to the lookup definition.
5. Add an entry in the `Lookup.Concur.UM.Configuration` lookup definition to enable transformation as follows:
 - a. Expand Administration, and then double-click **Lookup Definition**.
 - b. Search for and open the **Lookup.Concur.UM.Configuration** lookup definition.
 - c. In the Code Key column, enter `Recon Transformation Lookup`. In the Decode column, enter `Lookup.Concur.UM.ReconTransformation`.
 - d. Save the changes to the lookup definition.

4.4 Configuring Transformation of Data During User Reconciliation

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

To configure transformation of single-valued account data fetched during reconciliation:

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

The transformation class must implement the transform method with the following method signature:

```
Object transform(HashMap hmUserDetails, HashMap hmEntitlementDetails,  
String sField)
```

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

```
package oracle.iam.connectors.common.transform;  
import java.util.HashMap;  
public class TransformAttribute {  
    /*  
        Description:Abstract method for transforming the attributes
```

```

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

```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to Oracle Identity Manager database.

Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

 **Note:**

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

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

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

4. If you created the Java class for transforming a process form field for reconciliation, then:
 - a. Log in to the Design Console.
 - b. Create a lookup definition named **Lookup.Concur.UM.ReconTransformation**.
 - c. In the Code Key column, enter the resource object field name on which you want to apply transformation. For example, User Name. In the Decode

column, enter the name of the class that implements the transformation logic. For example, `oracle.iam.connectors.common.transform.TransformAttribute`.

- d. Save the changes to the lookup definition.
5. Add an entry in the **Lookup.Concur.UM.Configuration** lookup definition to enable transformation as follows:
 - a. Expand Administration, and then double-click **Lookup Definition**.
 - b. Search for and open the **Lookup.Concur.UM.Configuration** lookup definition.
 - c. In the Code Key column, enter Recon Transformation Lookup. In the Decode column, enter `Lookup.Concur.UM.ReconTransformation`.
 - d. Save the changes to the lookup definition.

4.5 Configuring the Concur Connector for Multiple Installations of the Target System

You must create copies of the connector 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. The company has recently installed Oracle Identity Governance, and they want to configure Oracle Identity Governance to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must create copies of the connector. See Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4.6 Defining the Concur Connector

Defining a connector is equivalent to registering the connector with Oracle Identity Governance. You can define a customized or reconfigured connector using Oracle Identity System Administration. After you define a connector, a record representing the connector is created in the Oracle Identity Governance database.

See Defining Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

5

Known Issues and Workarounds for the Concur Connector

This chapter provides solutions to the commonly encountered issues associated with the Concur connector.

- The delete operation is not supported by Concur APIs. So, revoking a Concur account through OIM may result in the corresponding tasks going to an undefined state.
- Re-provisioning a Concur account for an OIM User may result in multiple Concur accounts at OIM referring to the same account at Concur.

A

Files and Directories on the Concur Connector Installation Media

These are the components of the connector installation media that comprise the Concur connector.

[Table A-1](#) lists the files and directories on the connector installation media that comprise the Concur connector.

Table A-1 Files and Directories on the Concur Connector Installation Media

File in the Installation Media Directory	Description
bundle/ org.identityconnectors.genericrest-1.0.1115.jar	This JAR is the ICF connector bundle.
configuration/Concur-CI.xml	This XML file contains configuration information that is used during connector installation.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the Oracle Identity Manager database. Note: A resource bundle is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/Concur-ConnectorConfig.xml	This XML file contains definitions for the following connector objects: <ul style="list-style-type: none">• IT resource definition• Process forms• Process tasks and adapters• Lookup definitions• Resource objects• Process definition• Scheduled tasks• Reconciliation rules

Index

A

account management, [1-1](#)

C

configure scheduled jobs, [3-3](#)
connector architecture, [1-3](#)
connector features, [1-4](#)
connector files and directories, [A-1](#)
connector installation media, [A-1](#)

F

features of the concur connector, [1-4](#)
filtered reconciliation, [3-2](#)
full reconciliation, [1-5](#)

I

identity management, [1-1](#)
identity reconciliation, [1-1](#)
IT resource
 configuring, [2-3](#)
 parameters, [2-3](#)

L

limited reconciliation, [3-2](#)

P

provisioning operations, [1-1](#)

R

reconciliation
 limited, [3-2](#)

S

support for the connector server, [1-5](#)

T

target resource reconciliation, [1-1](#), [1-3](#)
transformation, [4-13](#)

V

validation, [4-11](#)