Oracle® Identity Governance

Configuring the Concur Application

12c (12.2.1.3.0)
F14101-04
October 2020

Oracle Identity Governance Configuring the Concur Application, 12c (12.2.1.3.0)

F14101-04

Primary Author: Alankrita Prakash

Contributors: Gowri.G.R

Contents

List of Figures

List of Tables

Preface

This guide describes the connector that is used to onboard Concur applications to Oracle Identity Governance.

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 Governance 12.2.1.3.0, visit the following Oracle Help Center page:

`http://docs.oracle.com/middleware/12213/oig/index.html`

For information about installing and using Oracle Identity Manager 11.1.2.3, visit the following Oracle Help Center page:

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

For information about Oracle Identity Governance Connectors 12.2.1.3.0 documentation, visit the following Oracle Help Center page:

`http://docs.oracle.com/middleware/oig-connectors-12213/index.html`

For information about Oracle Identity Manager Connectors 11.1.1 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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide

These are the updates made to the software and documentation for the release 12.2.1.3.0 of Configuring the Concur Application.

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on the Concur target system. This helps in quicker onboarding of the applications for this target system into Oracle Identity Governance by using an intuitive UI.

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific update has been made in revision "04" of this guide:

Logger names present in Enabling Logging have been updated.

The following documentation-specific update has been made in revision "03" of this guide:

A Note regarding the installation of any other generic rest connector has been added to Files and Directories in the Concur Connector Package.

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 12*c* 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 Governance Connector for Concur. Therefore, there are no documentation-specific updates in this release.

1

About the Concur Connector

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

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

> **Note:**
>
> In this guide, the connector that is deployed using the **Applications** option on the **Manage** tab of Identity Self Service is referred to as an **AOB application**. The connector that is deployed using the **Manage Connector** option in Oracle Identity System Administration is referred to as a **CI-based connector** (Connector Installer-based connector).

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

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

> **Note:**
>
> In this guide, Concur is sometimes referred to as the **target system**.

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

- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations
- Connector Architecture

- Supported Use Cases
- Supported Connector Features Matrix
- Connector Features

> **Note:**
>
> In this guide, the term Oracle Identity Governance server refers to the computer on which Oracle Identity Governance is installed.

1.1 Certified Components

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

> **Note:**
>
> If you are using Oracle Identity Manager release 11.1.x, then you can install and use the connector only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0.

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Manager or Oracle Identity Governance	You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) **Note:** If you are using Oracle Identity Governance 12*c* (12.2.1.3.0), then ensure to download and apply patches 26616250 and 25323654 from My Oracle Support.	You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 BP06 (11.1.2.3.6)
Target system	Concur	Concur
Connector Server	11.1.2.1.0 or later	11.1.2.1.0 or later
Connector Server JDK	JDK 1.8 or later	JDK 1.8 or later

1.2 Usage Recommendation

These are the recommendations for the Concur connector versions that you can deploy and use depending on the Oracle Identity Governance or Oracle Identity Manager version that you are using.

- If you are using Oracle Identity Governance release 12c (12.2.1.3.0) or later, then use the latest 12.2.1.*x* version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.
- If you are using any of the Oracle Identity Manager releases listed in the "Requirement for CI-Based Connector" column of Table 1-1, then use the 11.1.1.*x* version of the Concur connector. If you want to use the 12.2.1.*x* version of this connector, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12c (12.2.1.3.0) or later.

> **Note:**
>
> If you are using the latest 12.2.1.*x* version of the Concur connector in the CI-based mode, then see *Oracle Identity Manager Connector Guide for Concur*, Release 11.1.1 for complete details on connector deployment, usage, and customization.

1.3 Certified Languages

The connector supports the following languages:

- 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 Supported Connector Operations

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

Table 1-2 Supported Connector Operations

Operation	Supported?
User Management	
Create User	Yes
Update User	Yes
Enable User	Yes
Disable User	Yes
Change or Reset Password	Yes

1.5 Connector Architecture

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.

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 Governance. This data is used to add or modify resources (that is, accounts) that are allocated to Oracle Identity Governance Users. In addition, you can use Oracle Identity Governance to provision or update Concur accounts that are assigned to Oracle Identity Governance Users.

This connector enables the following operations:

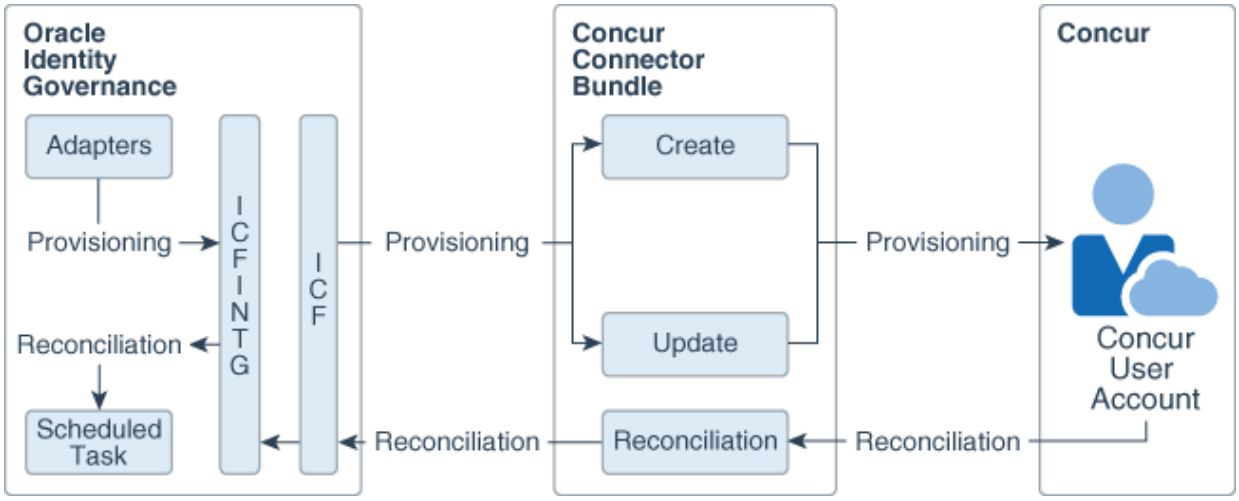
- Provisioning

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

- 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 Governance. Through the provisioning operations that are performed on Oracle Identity Governance, accounts are created and updated on Concur for Oracle Identity Governance Users.

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

1.6 Supported Use Cases

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

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 Governance, 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 due to less manual intervention.

1.7 Supported Connector Features Matrix

Provides the list of features supported by the AOB application and CI-based connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Perform full reconciliation	Yes	Yes
Support for connector server	Yes	Yes
Support for limited reconciliation of account based on filters	Yes	Yes
Transformation and validation of account data	Yes	Yes
Clone applications or create new application instances	Yes	Yes
Use connector server	Yes	Yes
Provide secure communication to the target system through SSL	Yes	Yes
Support for paging	Yes	Yes
Test connection	Yes	No

1.8 Connector Features

The features of the connector include support for provisioning user accounts, target resource reconciliation, reconciliation of all existing or modified account data, limited reconciliation, transformation and validation of account data during reconciliation and

provisioning, support for the connector server, multiple installations of the target system, secure communication to the target system through SSL, and so on.

The Concur Connector supports the following features:

- Support for Full Reconciliation
- Support for Limited Reconciliation
- Transformation and Validation of Account Data
- Support for the Connector Server
- Support for Cloning Applications and Creating Instance Applications
- Secure Communication to the Target System

1.8.1 Support for Full Reconciliation

After you create the application, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance.

You can perform a full reconciliation run at any time. See Performing Full Reconciliation.

1.8.2 Support for Limited Reconciliation

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

You can set a reconciliation filter as the value of the 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 Performing Limited Reconciliation.

1.8.3 Transformation and Validation of Account Data

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

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

1.8.4 Support for the Connector Server

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

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

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 Governance*.

1.8.5 Support for Cloning Applications and Creating Instance Applications

You can configure this connector for multiple installations of the target system by cloning applications or by creating instance applications.

When you clone an application, all the configurations of the base application are copied into the cloned application. When you create an instance application, it shares all configurations as the base application.

For more information about these configurations, see Cloning Applications and Creating Instance Applications in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.6 Secure Communication to the Target System

To provide secure communication to the target system, SSL is required. You can configure SSL between Oracle Identity Governance and the Connector Server and between the Connector Server and the target system.

If you do not configure SSL, passwords can be transmitted over the network in clear text. For example, this problem can occur when you are creating a user or modifying a user's password.

See Configuring SSL.

2

Creating an Application By Using the Concur Connector

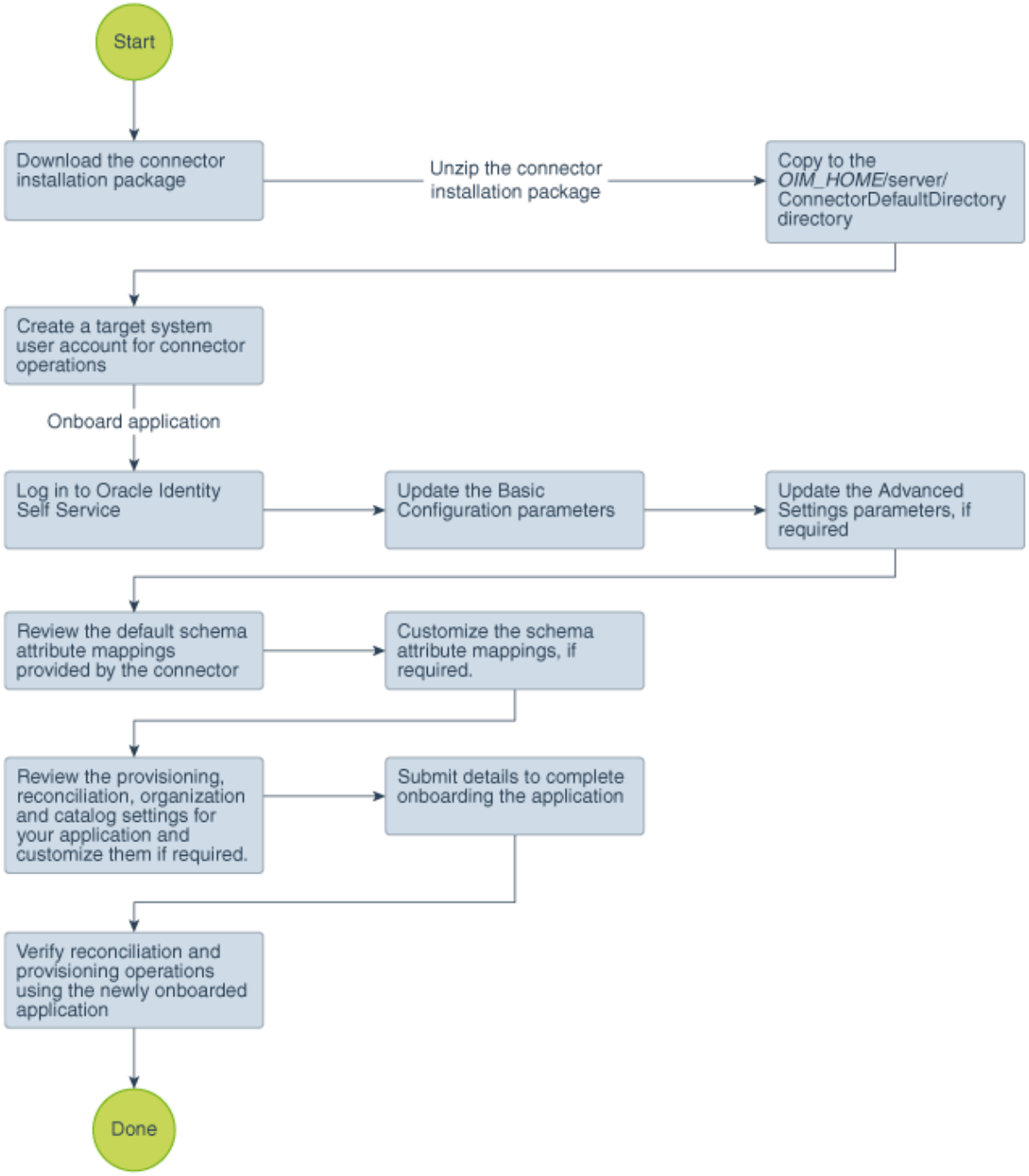
Learn about onboarding applications using the connector and the prerequisites for doing so.

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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



2.2 Prerequisites for Creating an Application By Using the Connector

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

- Configuring the Target System
- Downloading the Connector Installation Package

2.2.1 Configuring the Target System

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/Getting-Started/.

2.2.2 Downloading the Connector Installation Package

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

To download the connector installation package:

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

   You must accept the license agreement before you can download the installation package.

4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

2.3 Creating an Application By Using the Connector

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

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

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

1. Create an application in Identity Self Service. The high-level steps are as follows:
   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
   b. Ensure that the **Connector Package** option is selected when creating an application.
   c. Update the basic configuration parameters to include connectivity-related information.
   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.
   e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.
   f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.
   g. Review the details of the application and click **Finish** to submit the application details.

      The application is created in Oracle Identity Governance.
   h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.

      If you click **Yes**, then the default form is automatically created and is attached with the newly created application. The default form is created with the same name as the application. The default form cannot be modified later. Therefore, if you want to customize it, click **No** to manually create a new form and attach it with your application.
2. Verify reconciliation and provisioning operations on the newly created application.

See Also:

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

3
Configuring the Concur Connector

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

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to Concur.

Table 3-1 Basic Configuration Parameters for Concur

Parameter	Mandatory?	Description
authenticationServerUrl	No	Enter the URL of the authentication server that validates the consumer key for your target system. **Sample value**: `https://www.concursolutions.com/net2/oauth2/accesstoken.ashx`
authenticationType	Yes	Type of authentication that is used by your target system. This connector supports the OAuth 2.0 custom authentication type. **Default value**: `custom` **Note**: Do *not* modify the value of the parameter.
customAuthHeaders	No	Enter the consumer key in the following format: `"X-ConsumerKey=CONSUMER_KEY"` In this format, replace CONSUMER_KEY with the consumer key that is assigned to you after you register for the Concur developer sandbox in Configuring the Concur Connector. **Sample value**:`"X-ConsumerKey=abc12345ABc12345AbcXYZ"`
host	Yes	Enter the host name of the computer hosting your target system. **Sample value**: `www.concursolutions.com`

Table 3-1 (Cont.) Basic Configuration Parameters for Concur

Parameter	Mandatory?	Description
password	No	Enter the password for connecting to the Connector platform. This is the password that you specified while registering for the Concur developer sandbox in Configuring the Concur Connector.
port	No	Enter the port number at which the target system is listening. **Sample value**: `80`
proxyHost	No	Enter the name of the proxy host that is used to connect to an external target. **Sample value**: `www.example.com`
proxyPassword	No	Enter the password of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.
proxyPort	No	Enter the proxy port number. **Sample value**: `1105`
proxyUser	No	Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system. **Sample value**: `johnsmith`
sslEnabled	No	If the target system requires SSL connectivity, then set the value of this parameter to `true`. Otherwise set the value to `false`. **Default value**: `true`
username	No	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 in Configuring the Target System.
Connector Server Name	No	If you have deployed the Concur connector in the Connector Server, then enter the name of the IT resource for the Connector Server. **Sample value**: `concurConnectorServer`

3.2 Advanced Settings Parameters

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

Table 3-2 Advanced Settings Parameters for Concur

Parameter	Mandatory ?	Description

relURIs	Yes	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.
		Default value:
		`"__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?$(FilterSuffix)$&limit=$(PAGE_SIZE)$&offset=$(PAGE_TOKEN)$`

nameAttributes	Yes	This entry indicates the attributes that need to be treated as the __NAME__ attribute for an Object class. **Default value**: `"__ACCOUNT__.LoginID"`
uidAttributes	Yes	This entry holds the UID attribute for objects that are handled by the connector. For example, the UID attribute is LoginID for the Account class. **Default value**: `"__ACCOUNT__.LoginID"`
pageTokenRegex	No	This entry provides the number of resources that appear on a page for a search operation. **Default value**: `(?<=offset=).*`
pageSize	No	This entry provides the number of resources that appear on a page for a search operation. **Default value**: `100`
pageTokenAttribute	No	This entry provides the name of the target attribute for the Pagination token. This token is an opaque string that identifies a page and provides permissions to APIs that read, write, or modify the data on that page. **Default value**: `NextPage`
Bundle Version	No	This entry holds the version of the connector bundle. **Default value**: `12.3.0`
Connector Name	No	This entry holds the name of the connector class. **Default value**: `org.identityconnectors.genericrest-12.3.0`

opTypes	No	This entry determines the target supported HTTP operation for each attribute in each object class.
		Default value:
		`"__ACCOUNT__.CREATEOP=POST","__ACCOUNT__.UPDATEOP=POST",`
		`"__ACCOUNT__.SEARCHOP=GET","__ACCOUNT__.__PASSWORD__.UPDATEOP=POST"`

jsonResourcesTag	No	This JSON tag value is used during reconciliation for parsing multiple entries in a single response payload. **Default value**: `"__ACCOUNT__=Items"`
httpHeaderContentType	No	This entry indicates the type of the body of the request. **Default value**: `application/xml`

Table 3-2 (Cont.) Advanced Settings Parameters for Concur

Parameter	Mandatory ?	Description
httpHeaderAccept	No	The Accept request-header field can be used to specify certain media types that are acceptable for the response. **Default value**: `application/json`
enableEmptyString	No	This entry converts empty or null value to an empty string. **Default value**: `true`
customPayload	No	This entry provides the custom format of request payload.
customAuthClassName	No	This entry provides the class name of Custom Auth implementation. **Default value**: `oracle.iam.connectors.concur.auth.ConcurNativeAuth`
customParserClassName	No	This entry provides the class name of custom parser implementation. **Default value**: `oracle.iam.connectors.concur.parser.ConcurResponseParser`
statusAttributes	No	This entry lists the name of the target system attribute that holds the status of an account, that is __ENABLE__ field on the target system for each object class. **Default value**: `"__ACCOUNT__.Active"`
passwordAttribute	No	This entry provides the target attribute for user password. **Default value**: `Password`
Bundle Name	No	This entry holds the name of the connector bundle package. **Default value**: `org.identityconnectors.genericrest`
statusDisableValue	No	Enter the boolean value that indicates the value that must be sent to the target system during a Disable operation. **Note**: You must enter a value for this parameter only if the target system expects a different value for a Disable operation, from what Oracle Identity Governance sends by default. **Default value**: `false`
statusEnableValue	No	Enter the boolean value that indicates the value that must be sent to the target system during an Enable operation. **Note**: You must enter a value for this parameter only if the target system expects a different value for an Enable operation from the one that Oracle Identity Governance sends by default. **Default value**: `true`

3.3 Attribute Mappings

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

Concur User Account Attributes

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

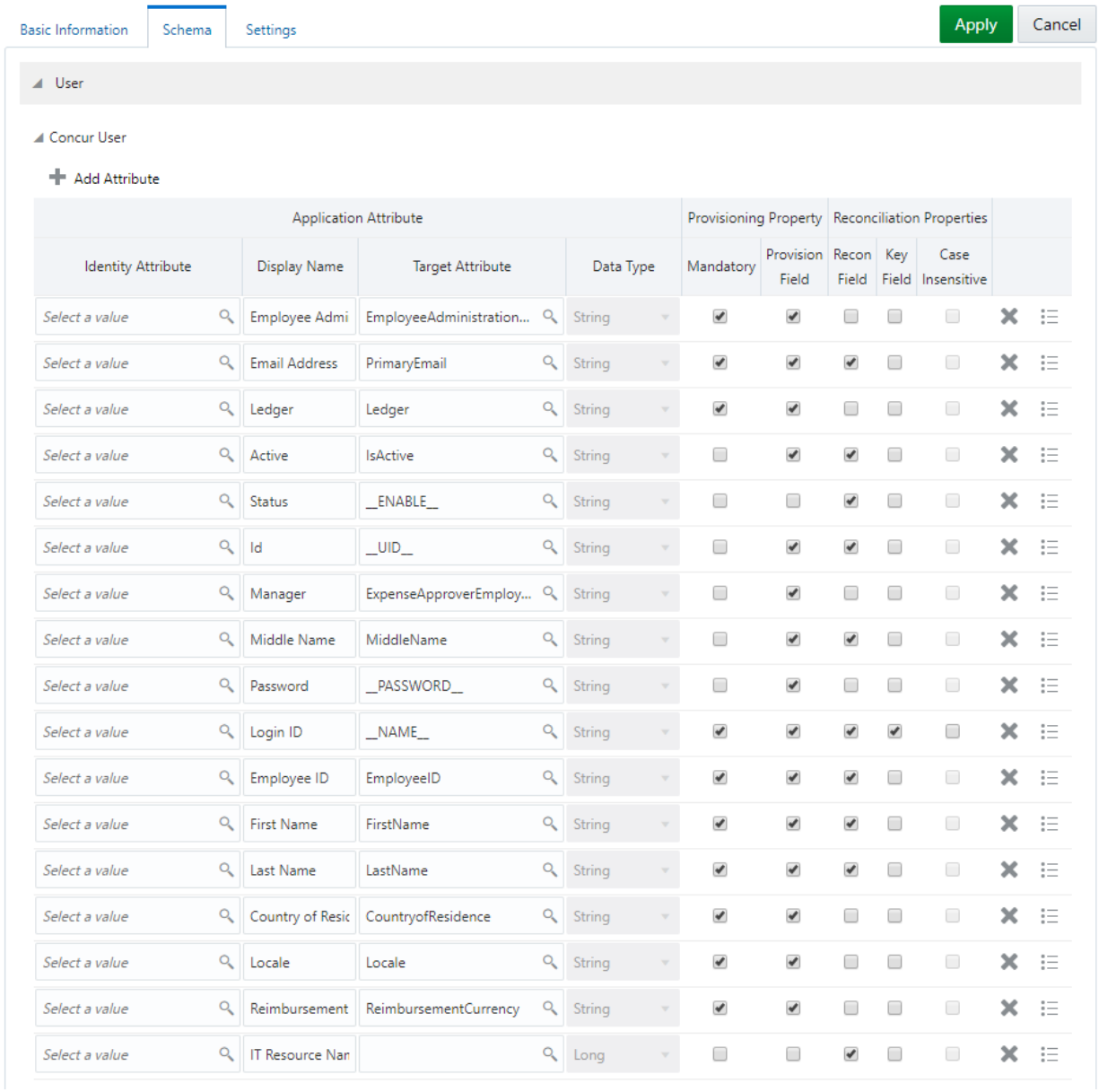
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attribute Mappings for Concur User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive ?
Email Address	PrimaryEmail	String	Yes	Yes	Yes	No	Not Applicable
Active	IsActive	String	No	Yes	Yes	No	Not Applicable
Id	__UID__	String	No	Yes	Yes	No	Not Applicable
Middle Name	MiddleName	String	No	Yes	Yes	No	Not Applicable
Login ID	__NAME__	String	Yes	Yes	Yes	Yes	Not Applicable
Employee ID	EmployeeID	String	Yes	Yes	Yes	No	Not Applicable
First Name	FirstName	String	Yes	Yes	Yes	No	Not Applicable
Last Name	LastName	String	Yes	Yes	Yes	No	Not Applicable
Status	__ENABLE__	String	No	No	Yes	No	Not Applicable
Country of Residence	CountryofResidence	String	Yes	Yes	No	No	Not Applicable
Locale	Locale	String	Yes	Yes	No	No	Not Applicable
Reimbursement Currency	ReimbursementCurrency	String	Yes	Yes	No	No	Not Applicable
Employee Administration Country	EmployeeAdministrationCountry	String	Yes	Yes	No	No	Not Applicable
Ledger	Ledger	String	Yes	Yes	No	No	Not Applicable
Manager	ExpenseApproverEmployeeID	String	No	Yes	No	No	Not Applicable
Password	__PASSWORD__	String	No	Yes	No	No	Not Applicable

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

Figure 3-1 Default Attribute Mappings for Concur User Account



3.4 Correlation Rules, Situations, and Responses

Learn about the predefined rules, responses and situations for the Concur application. The connector use these rules and responses for performing reconciliation.

Predefined Identity Correlation Rules

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

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

Table 3-4 Predefined Identity Correlation Rule for a Concur Target Application

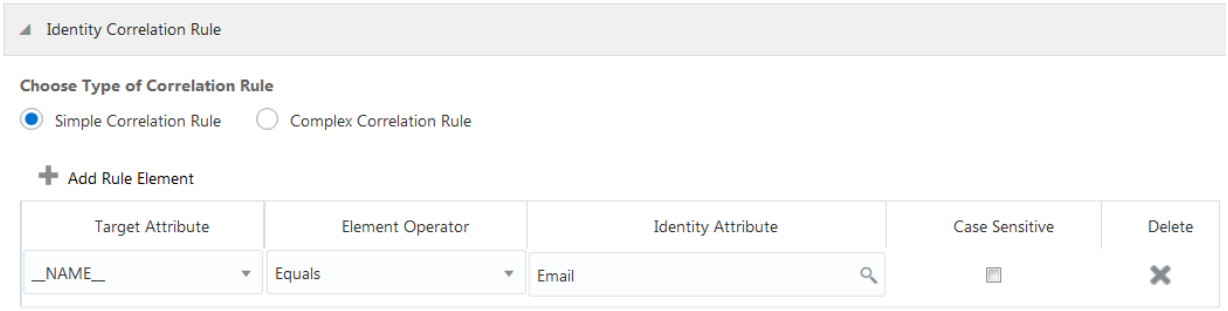
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	Email	No

In this identity rule:

- __NAME__ is a single-valued attribute on the target system that identifies the user account.
- Email is the field on the OIG User form.
- Rule operator is AND.

Figure 3-2 shows the simple correlation rule for the Concur connector.

Figure 3-2 Predefined Identity Correlation Rules



Predefined Situations and Responses

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

The following table lists the default situations and responses for the Concur connector. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Predefined Situations and Responses for a Concur Target Application

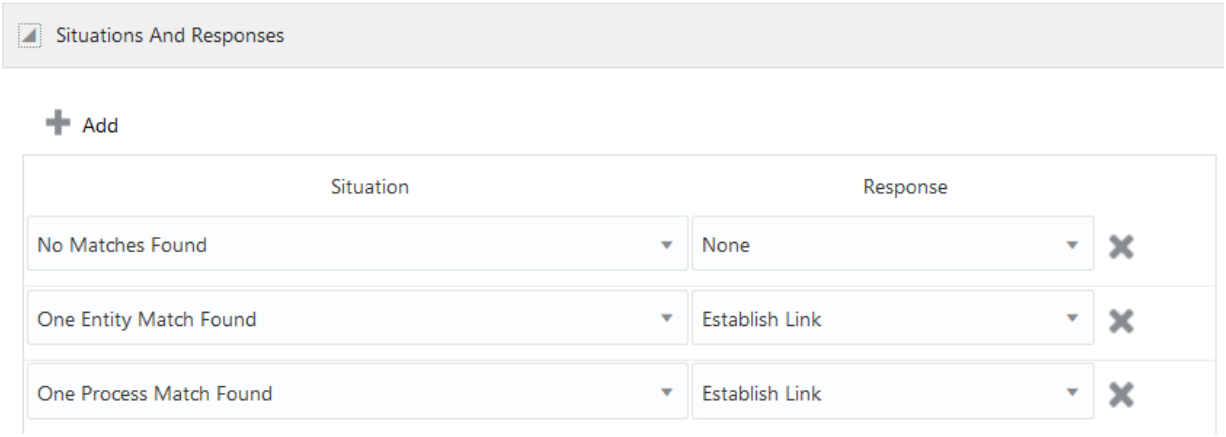
Situation	Response
No Matches Found	None
One Entity Match Found	Establish Link

Table 3-5 (Cont.) Predefined Situations and Responses for a Concur Target Application

Situation	Response
One Process Match Found	Establish Link

Figure 3-3 shows the default situations and responses for the Concur connector.

Figure 3-3 Default Situations and Responses



3.5 Reconciliation Jobs

Learn about the reconciliation jobs that are automatically created in Oracle Identity Governance after you create the application for your target system.

You can either use these predefined jobs or edit them to meet your requirements. Alternatively, you can create custom reconciliation jobs. For information about editing these predefined jobs or creating new ones, see Updating Reconciliation Jobs in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Concur Target Resource User Reconciliation Job

You use the Concur Target Resource User Reconciliation job to perform full reconciliation, which involves reconciling all user records from a target application into Oracle Identity Governance.

Table 3-6 Parameters of the Concur Target Resource User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. **Note**: Do *not* modify this value.
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. See Performing Limited Reconciliation.
Object Type	This attribute holds the name of the object type for the reconciliation run. **Default value**: `User` **Note**: Do *not* change the value of this attribute.
Scheduled Task Name	Name of the scheduled job. **Note**: For the scheduled job included with this connector, you must *not* change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.

4

Performing the Postconfiguration Tasks for the Concur Connector

These are the tasks that you must perform after creating an application in Oracle Identity Governance.

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

4.1 Configuring Oracle Identity Governance

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

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

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

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

4.1.1 Creating and Activating a Sandbox

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

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

4.1.2 Creating a New UI Form

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

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

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

4.1.3 Publishing a Sandbox

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

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

4.1.4 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

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

See Also:

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

4.2 Harvesting Entitlements and Sync Catalog

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

To harvest entitlements and sync catalog:

1. Run the 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.

4.3 Managing Logging for the Connector Server

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

4.3.1 Understanding Log Levels

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

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

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

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

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

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

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

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

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

4.3.2 Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

a. Add the following blocks in the file:

```
<log_handler name='Concur-handler'
level='[LOG_LEVEL]'class='oracle.core.ojdl.logging.ODLHandlerFact
ory'>
    <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.GENERICREST"
level="[LOG_LEVEL]" useParentHandlers="false">
    <handler name="Concur-handler"/>
    <handler name="console-handler"/>
</logger>


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

```
<log_handler name='Concur-handler'
level='NOTIFICATION:1'class='oracle.core.ojdl.logging.ODLHandlerF
actory'>
    <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.GENERICREST"
level="NOTIFICATION:1" useParentHandlers="false">
    <handler name="Concur-handler"/>
    <handler name="console-handler"/>
</logger>
```

```
<logger name="ORG.IDENTITYCONNECTORS.RESTCOMMON"
level="NOTIFICATION:1" useParentHandlers="false">
    <handler name="Concur-handler"/>
    <handler name="console-handler"/>
</logger>
```

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

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

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

4.4 Configuring the IT Resource for the 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 Governance with your target system.

This section contains the following topics:

- IT Resource Parameters
- Specifying Values for IT Resource Parameters

4.4.1 IT Resource Parameters

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

Table 4-2 displays each parameter of the Concur IT resource in an alphabetical order.

Table 4-2 IT Resource Parameters

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

Table 4-2 (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. **Sample value**: `custom` Do *not* modify the value of the parameter.
customAuthHeaders	Enter the consumer key in the following format: `"X-ConsumerKey=CONSUMER_KEY"` In this format, replace *CONSUMER_KEY* with the consumer key that is assigned to you after you register for the Concur developer sandbox. **Sample value**: `"X-ConsumerKey=abc12345ABc12345AbcXYZ"` See Configuring the Target System 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. **Sample value**: `Lookup.Concur.Configuration`
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**: `www.concursolutions.com`
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**: `www.example.com`
proxyPort	Enter the proxy port number.
proxyUser	Enter the proxy user name of the target system user account that Oracle Identity Governance 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 Governance uses to connect to the target system.
sslEnabled	If the target system requires SSL connectivity, then set the value of this parameter to `true`. Otherwise set the value to `false`. **Sample value**: `true`

Table 4-2 (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.

4.4.2 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**.

4.5 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. 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.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_ LOGINID__c_description']}">
<source>Login ID</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ConcurForm.entity
.ConcurFormEO.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.BaseRuntimeResou
rceBu ndle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.use rEO.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\u3FIRSTNAME0AB\u30A6\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.

4.6 Configuring SSL

You configure SSL to secure data communication between Oracle Identity Governance 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 Governance.
3. Run the following keytool command to import the public key certificate into the identity key store in Oracle Identity Governance:

```
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.

5
Using the Concur Connector

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

5.1 Configuring Reconciliation

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:

5.1.1 Performing Full Reconciliation

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

After you deploy the connector, you must first perform full reconciliation. To perform a full reconciliation run, ensure that a value is not specified for the Filter attribute of the Concur Target Resource User Reconciliation job for reconciling users. See Reconciliation Jobs for information about this reconciliation job.

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. See Reconciling Large Number of Records.

5.1.2 Performing Limited Reconciliation

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, primaryEmail=xyx@demo.com) while configuring the Concur Target Resource User Reconciliation job. See Reconciliation Jobs for information about this reconciliation 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 on Concur filters, see information on user resources related to API Explorer on the Concur Developer Center page at https://developer.concur.com/.

5.1.3 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 Governance:

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 Governance.
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*.
4. Install the Flat File connector. See Running the Connector Installer in *Oracle Identity Manager Connector Guide for Flat File*.
5. Configure the Flat File IT resource. See Configuring the IT Resource in *Oracle Identity Manager Connector Guide for Flat File*.
6. Configure and run 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`.

   See Flat File Accounts Loader and IT_RES_NAME Flat File Accounts Loader in *Oracle Identity Manager Connector Guide for Flat File* for information about the attributes of the Flat File Accounts Loader scheduled job.

5.2 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

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 Governance*.

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

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

6. Click **Apply** to save the changes.

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

5.3 Configuring Provisioning

Learn about performing provisioning operations in Oracle Identity Governance and the guidelines that you must apply while performing these operations.

- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations

5.3.1 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 Governance 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 Governance through a reconciliation run, ensure that values are populated for all the mandatory user fields in Oracle Identity Governance. If there are any user fields without values, then you must specify the values by performing the Update User provisioning operations.

5.3.2 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 Governance:

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 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 Governance* for details about the fields on the Create User page

5.4 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*.

6

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:

6.1 Adding User Attributes for Reconciliation

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

The default attribute mappings for reconciliation are listed in Attribute Mappings.

> **See Also:**
>
> To add new attributes in the CI based concur connector, see Oracle Identity Manager, 11.1.2.3 in the Oracle Help Center page: `https://docs.oracle.com/cd/E22999_01/doc.111/e75739/toc.htm`

6.2 Adding User Attributes for Provisioning

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

The default attribute mappings for provisioning are listed in Attribute Mappings.

> **See Also:**
>
> To add new attributes in the CI based concur connector, see Oracle Identity Manager, 11.1.2.3 in the Oracle Help Center page: `https://docs.oracle.com/cd/E22999_01/doc.111/e75739/toc.htm`

6.3 Configuring Transformation and Validation of Data

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

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

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

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

6.4 Configuring the Connector for Multiple Installations of the Target System

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

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

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

6.5 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*.

6.6 Configuring Action Scripts

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

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

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

7

Upgrading the Concur Connector

If you have already deployed the 11.1.1.5.0 version of the Concur connector, then you can upgrade the connector to version 12.2.1.3.0 by uploading the new connector JAR files to the Oracle Identity Manager database.

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

The following sections discuss the procedure to upgrade the connector:

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

> **See Also:**
>
> Upgrading Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information on these steps

7.1 Preupgrade Steps

Preupgrade steps for the connector involves performing a reconciliation run to fetch records from the target system, defining the source connector in Oracle Identity Manager, creating copies of the connector if you want to configure it for multiple installations of the target system, and disabling all the scheduled jobs.

Perform the following preupgrade steps:

1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
2. Perform the preupgrade procedure documented in Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
3. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made

to the connector. See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information.

4. If required, create the connector XML file for a clone of the source connector.
5. Disable all the scheduled jobs.

7.2 Upgrade Steps

This is a summary of the procedure to upgrade the connector for both staging and production environments.

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

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.

  > **Note:**
  >
  > Do not upgrade IT resource type definition. In order to retain the default setting, you must map the IT resource definition to "None".

- Production Environment

  Perform the upgrade procedure by using the silent mode.

See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the wizard and silent modes.

7.3 Postupgrade Steps

Postupgrade steps involve uploading new connector JARs, configuring the upgraded IT resource of the source connector, updating the Connector Server JARs, and deleting duplicate entries for lookup definitions.

Perform the following procedure:

1. Delete the old Connector JARs. Run the Oracle Identity Manager Delete JAR ($*ORACLE_HOME*/bin /DeleteJars.sh) utility to delete the existing ICF bundle org.identityconnectors.genericrest-1.0.11150.jar from the Oracle Identity Manager database. When you run the Delete JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being deleted, and the name of the JAR file to be removed. Specify 4 as the value of the JAR type.
2. Upload new connector JARs as follows:
   a. Run the Upload JARs utility ($*ORACLE_HOME*/bin/UploadJars.sh) for uploading connector JARs.
   b. Upload bundle/org.identityconnectors.genericrest-12.3.0.jar as ICFBundle.
   c. Delete the following Code Key and Decode entries in the Lookup.Concur.Configuration lookup definition:

      Code Key: Bundle Version; Decode: 1.0.1115

Code Key: relURIs; Decode: `"__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/$(FilterSuffix)$"`

3. If any attribute mappings are missing for custom attributes, log in to Oracle Identity Governance Design Console and update the mappings.
4. Restart Oracle Identity Governance.
5. If the connector is deployed on a Connector Server, then:
   a. Stop the Connector Server.
   b. Replace the existing bundle JAR file org.identityconnectors.genericrest-1.0.1115.jar with the new bundle JAR file org.identityconnectors.genericrest-12.3.0.jar.
   c. Start the Connector Server. After upgrading the connector, you can perform either full reconciliation or limited reconciliation. This ensures that records created or modified since the last reconciliation run are fetched into Oracle Identity Governance.

See Also:

- Configuring Oracle Identity Governance for information about creating, activating, or publishing a sandbox and creating a new UI form
- Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about deploying the Connector Server
- Configuring Reconciliation for more information about performing full or limited reconciliation

8

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 in the Concur Connector Package

These are the files and directories in the connector installation package that comprise the Concur connector.

Table A-1 Files and Directories in the Concur Connector Installation Package

File in the Installation Package	Description
bundle/ org.identityconnectors.genericrest-12.3.0.jar	This JAR file contains the connector bundle. **Note:** If you try to install any other generic rest connector like Office 365 on top of the Concur connector, then the generic rest bundle jar `org.identityconnectors.genericrest-12.3.0.jar` must be replaced with the with the Concur bundle jar. If you are using a latest generic connector released in 2020, ensure to use a connector server for Concur.
configuration/Concur-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the Connector Installer 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 Governance 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: • IT resource definition • Process forms • Process tasks and adapters • Lookup definitions • Resource objects • Process definition • Scheduled tasks • Reconciliation rules
Concur-pre-config.xml	This XML contains definitions for the connector objects associated with any non-User objects such as static fields like locale, country of residence, currency, and so on.

Table A-1 (Cont.) Files and Directories in the Concur Connector Installation Package

File in the Installation Package	Description
Concur-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.