

# Oracle® Identity Governance

## Configuring the Workday Application



12c (12.2.1.3.1)  
F32597-05

ORACLE®

Oracle Identity Governance Configuring the Workday Application, 12c (12.2.1.3.1)

F32597-05

Copyright © 2020, 2023, Oracle and/or its affiliates.

Primary Author: Maya Chakrapani

Contributors: Syam Kumar Battu

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

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

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

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

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

Oracle®, Java, and MySQL 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 This Guide?

---

Software Updates	x
Documentation-Specific Updates	xi

## 1 About the Workday Connectors

---

1.1	Certified Components	1-2
1.2	Usage Recommendation	1-2
1.3	Certified Languages	1-2
1.4	Supported Connector Operations	1-3
1.5	Connector Architecture	1-4
1.6	Supported Connector Features Matrix	1-6
1.7	Connector Features	1-7
1.7.1	Support for Trusted Source and Target Resource Reconciliation	1-7
1.7.2	Support for Full and Incremental Reconciliation	1-8
1.7.3	Support for Reconciliation with Transaction Days	1-8
1.7.4	Support for Limited (Filtered) Reconciliation	1-8
1.7.5	Support for the Connector Server	1-8
1.7.6	Transformation and Validation of Account Data	1-8
1.7.7	Support for Cloning Applications and Creating Instance Applications	1-9
1.7.8	Secure Communication to the Target System	1-9

## 2 Creating an Application By Using the Workday Connectors

---

2.1	Process Flow for Creating an Application By Using the Connector	2-1
2.2	Prerequisites for Creating an Application By Using Connector	2-2

2.2.1	Downloading the Connector Installation Package	2-2
2.2.2	Creating an Integrated System User in Workday to Perform Connector Operations	2-3
2.2.3	Configuring Raas Reports on workday	2-4
2.3	Creating an Application By Using the Connector	2-5

### 3 Configuring the Workday Connector for a Target Application

---

3.1	Basic Configuration Parameters for the Workday Target Connector	3-1
3.2	Advanced Setting Parameters for the Workday Target Connector	3-2
3.3	Attribute Mapping for the Workday Target Connector	3-7
3.4	Correlation Rules for the Workday Target Connector	3-14
3.5	Reconciliation Jobs for the Workday Target Connector	3-15

### 4 Configuring the Workday Connector for an Authoritative Application

---

4.1	Basic Configuration Parameters for the Workday Authoritative Connector	4-1
4.2	Advanced Setting Parameters for the Workday Authoritative Connector	4-2
4.3	Attribute Mapping for the Workday Authoritative Connector	4-3
4.4	Correlation Rules for the Workday Authoritative Connector	4-5
4.5	Reconciliation Jobs for the Workday Authoritative Connector	4-7

### 5 Performing the Postconfiguration Tasks for the Workday Connectors

---

5.1	Configuring Oracle Identity Governance	5-1
5.1.1	Creating and Activating a Sandbox	5-1
5.1.2	Creating a New UI Form	5-1
5.1.3	Publishing a Sandbox	5-2
5.1.4	Updating an Existing Application Instance with a New Form	5-2
5.2	Configuring SSL	5-3
5.3	Configuring the IT Resource for the Connector Server	5-4
5.4	Managing Logging	5-5
5.4.1	Understanding Log Levels	5-5
5.4.2	Enabling logging	5-6
5.5	Localizing Field Labels in UI Forms	5-7

### 6 Using the Workday Connectors

---

6.1	Configuring Reconciliation	6-1
6.1.1	Performing Full and Incremental Reconciliation	6-1
6.1.2	Performing Reconciliation with Transaction Days	6-2
6.1.3	Performing Limited Reconciliation	6-2

6.2	Configuring Reconciliation Jobs	6-3
6.3	Performing Provisioning Operations	6-4
6.3.1	Creating Users	6-4
6.3.2	Modifying Users	6-5
6.4	Handling Start Date and End Date	6-6
6.4.1	Handling Start Date	6-6
6.4.2	Handling End Date	6-6
6.5	Uninstalling the Connector	6-7

## 7 Extending the Functionality of the Workday Connectors

---

7.1	Configuring Transformation and Validation of Data	7-1
7.2	Configuring Action Scripts	7-1
7.3	Configuring the Connector for Multiple Tenants	7-2

## 8 Upgrading the Connector

---

8.1	Upgrading Applications	8-1
8.2	Post-upgrade Steps	8-2

## 9 Frequently Asked Questions

---

## 10 Troubleshooting the Connector

---

## A Files and Directories in the Connector Installation Package

---

## List of Figures

---

1-1	Connector Architecture of the Workday Target Connector	1-5
2-1	Overall Flow of the Process for Creating an Application By Using the Connector	2-2
2-2	Security Groups Raas report columns	2-4
2-3	Organization Raas report columns	2-5
3-1	Default Attribute Mappings for Workday Target User Account	3-9
3-2	Default Attribute Mappings for Role	3-10
3-3	Default Attributes for Secondary Phone Number Child Form	3-12
3-4	Default Attributes for Secondary Email Child Form	3-13
3-5	Default Attribute Mappings for Security Groups	3-14
3-6	Simple Correlation Rules for the Workday Target Connector	3-15
4-1	Workday Authoritative User Account Schema Attributes	4-5
4-2	Simple Correlation Rule for an Authoritative Application	4-6

## List of Tables

---

1-1	Certified Components	1-2
1-2	Supported Connector Operations	1-3
1-3	Supported Connector Features Matrix	1-6
3-1	Parameters in the Basic Configuration Section for the Workday Target Connector	3-1
3-2	Advanced Setting Parameters for the Workday Target Connector	3-2
3-3	Workday Target Account Schema Attributes	3-7
3-4	Default Attribute Mappings for Roles	3-10
3-5	Default Attribute Mappings for Secondary Phone Number Child Attribute	3-10
3-6	Default Attribute Mappings for Secondary Email Child Attribute	3-12
3-7	Default Attribute Mappings for Security Groups	3-13
3-8	Predefined Identity Correlation Rule for Workday Target Connector	3-14
3-9	Predefined Situations and Responses for a Target Application	3-15
3-10	Parameters of the Workday Target User Reconciliation Job	3-16
4-1	Parameters in the Basic Configuration Section for the Workday Authoritative Connector	4-1
4-2	Advanced Setting Parameters for the Workday Authoritative Connector	4-2
4-3	Workday Authoritative User Account Schema Attributes	4-4
4-4	Predefined Identity Correlation Rule for Workday Target Connector	4-6
4-5	Predefined Situations and Responses for an Authoritative Application	4-6
4-6	Parameters of the Workday Authoritative User Reconciliation Job	4-7
5-1	Parameters of the IT Resource for the Connector Server	5-4
5-2	Log Levels and ODL Message Type:Level Combinations	5-5
10-1	Troubleshooting the Workday Connector	10-1
A-1	Files and Directories in the Workday Connector Installation Package	A-1

# Preface

This guide describes the connector that is used to onboard the Workday application 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 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>

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	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.



<b>Convention</b>	<b>Meaning</b>
<code>monospace</code>	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 release 12.2.1.3.0.

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

- [Software Updates](#)  
This section describes updates made to the connector software.
- [Documentation-Specific Updates](#)  
This section describes major changes made to this guide. These changes are not related to software updates.

## Software Updates

These are the updates made to the connector software.

- [Software Updates in Release 12.2.1.3.1](#)
- [Software Updates in Release 12.2.1.3.0](#)

### Software Updates in Release 12.2.1.3.1

The following software updates have been made in release 12.2.1.3.1:

#### Resolved Issues in Release 12.2.1.3.1

The following table lists the issues resolved in release 12.2.1.3.1:

Bug Number	Issue	Resolution
32082689	Account provisioning not supported.	This issue has been resolved.

### Software Updates in Release 12.2.1.3.0

The following is a 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 Workday target. This helps in quicker onboarding of the applications for Workday 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 "03" of this guide:

- Image [Figure 1-1](#) updated to add **Create** operation.

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

- **Create User, Update User, and Reset Password** operations added to the **User Management** section of [Table 1-2](#) table.
- **Add Group, Update Group, and Remove Group** operations added to the **Licence Grant Management** section of [Table 1-2](#) table.
- **Provision User Account, Reset Password, Add or Remove Security Groups (Entitlement), and Reconcile Account Attributes and Security Groups** features added to the [Table 1-3](#) table.
- Sections [Creating Users](#) and [Modifying Users](#) added.
- Added **Workday ID, Password, and Account Disabled** attributes to [Table 3-3](#).
- Added [Upgrading the Connector](#) chapter.

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

- This is the first release of this connector. Therefore, there are no documentation-specific updates in this release.

# 1

## About the Workday Connectors

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 Workday connector lets you create and onboard Workday 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 term **Provisioning** in this guide refers to Updating Worker Contact Details operation only.

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.

You can use Workday connectors to create and onboard Target applications and Authoritative applications in Oracle Identity Governance. The connector bundle provides two separate versions (XML files) of the connector for this purpose.

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

- [Certified Components](#)
- [Usage Recommendation](#)
- [Certified Languages](#)
- [Supported Connector Operations](#)
- [Connector Architecture](#)
- [Supported Connector Features Matrix](#)
- [Connector Features](#)

**Note:**

In this guide, **Workday connectors** refers to connectors for both Authoritative and a Target application.

## 1.1 Certified Components

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

**Table 1-1 Certified Components**

Component	Requirement for AOB Application
Oracle Identity Governance	You can use one of the following releases: <ul style="list-style-type: none"><li>• Oracle Identity Governance 12c (12.2.1.4.0)</li><li>• Oracle Identity Governance 12c (12.2.1.3.0)</li></ul>
Target System	Workday 2020 R1 or later
Connector Server	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 or later

## 1.2 Usage Recommendation

If you are using Oracle Identity Governance 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.

## 1.3 Certified Languages

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 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 for Authoritative Connector?	Supported for Target Connector?
<b>User Management</b>		
Create Workday Account	No	Yes
Update Workday Account	No	Yes
Reset Workday Account Password	No	Yes
Reconcile Worker	Yes	Yes
Update Contact Details	No	Yes
<b>Secondary Phone Numbers Management</b>		
Add secondary phone number	No	Yes
Update secondary phone number	No	Yes

**Table 1-2 (Cont.) Supported Connector Operations**

Operation	Supported for Authoritative Connector?	Supported for Target Connector?
Remove secondary phone number	No	Yes
<b>Secondary Email Management</b>		
Add secondary email	No	Yes
Update secondary email	No	Yes
Remove secondary email	No	Yes
<b>Security Group Management</b>		
Add Group	No	Yes
Remove Group	No	Yes

 **Note:**

Update Contact Details in the guide refers to update of work email, home email, work phone, work phone device type, home phone, and home phone device type attributes.

 **Note:**

Create Workday Account, Update Workday Account, Reset Workday Account Password, and Security Group Management features are supported from version 12.2.1.3.1 (Target Connector).

## 1.5 Connector Architecture

The connector uses Workday webservices to synchronize user attributes between Oracle Identity Governance and Workday Directory, and is implemented using the Identity Connector Framework (ICF) component.

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

You can configure the connector to run in one of the following modes:

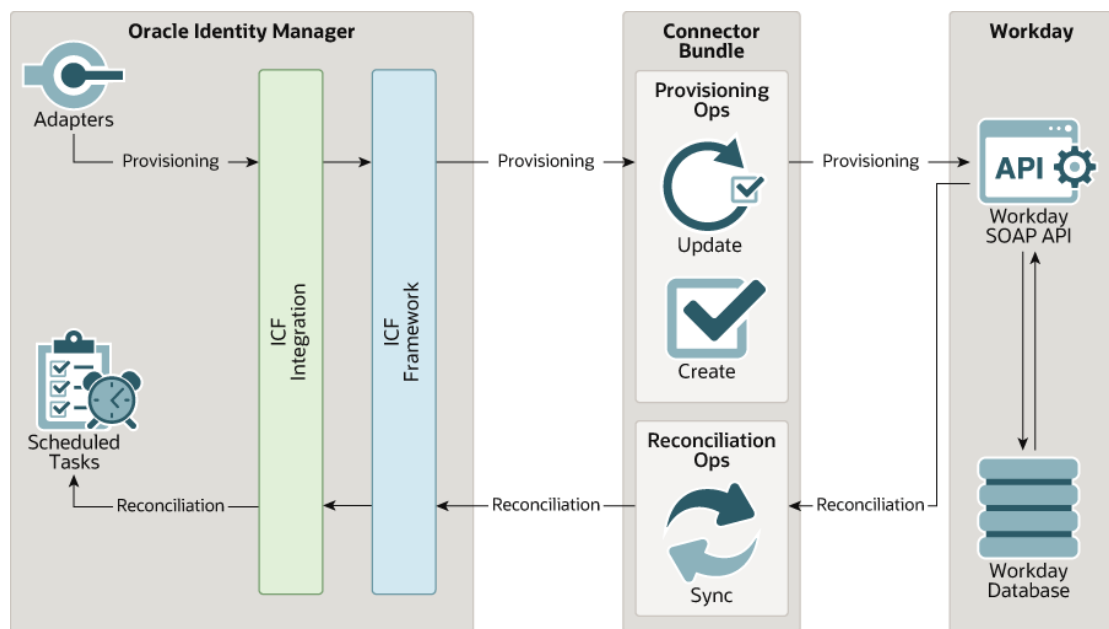
- **Identity Reconciliation:** Identity reconciliation is also known as authoritative or trusted source reconciliation. In this mode, the target system is used as the trusted source and users are directly created and modified on it. During reconciliation, each user record fetched from the target system is compared with existing OIM Users. If a match is found between the target system record and the OIM User,

then the OIM User attributes are updated with changes made to the target system record. If no match is found, then the target system record is used to create an OIM User.

- **Account Management:** Account management is also known as target resource management. In this mode, the target system is used as a target resource and the connector enables the following operations:
  - **Target Resource Reconciliation:** The basic function of this connector is to enable management of employee data on the Workday target application through Oracle Identity Governance. You can create and manage employee records for OIG users through provisioning. In addition, data related to newly created and modified employee records can be reconciled (using scheduled tasks) and linked with existing OIG users and provisioned resources.
  - **Update Contact Data:** Provisioning involves creating or updating worker contact data (Email and Phone data) on the target system through Oracle Identity Governance.

Figure 1-1 shows the architecture of the Workday connector.

**Figure 1-1 Connector Architecture of the Workday Target Connector**



As shown in this figure, the Workday connector enables you to use the target system as a managed resource (target) of identity data for Oracle Identity Governance.

Through the provisioning operations that are performed on Oracle Identity Governance, contact details are updated in the target system for Oracle Identity Governance Users. During provisioning, the Adapters invoke ICF operation, ICF inturn invokes update operation on the Workday Identity Connector Bundle and then the bundle calls the target system API for provisioning operations. The Workday SOAP API on the target system accepts provisioning data from the bundle, carries out the required operation on the target system, and returns the response from the target system back to the bundle, which passes it to the adapters.

During reconciliation, a scheduled task invokes an ICF operation. ICF inturn invokes a sync operation on the Workday Identity Connector Bundle and then the bundle calls Workday Get Workers API for reconciliation operation. The API extracts user records that match the



reconciliation criteria and hands them over through the bundle and ICF back to the scheduled task, which brings the records to Oracle Identity Governance.

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

The Workday Identity Connector Bundle communicates with the Workday Human Resources webservices using the HTTPS protocol. The Workday Human Resources webservices provides programmatic access through SOAP API endpoints. Applications can use the Workday Human Resources webservices to perform read and update operations on users.

#### See Also:

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


## 1.6 Supported Connector Features Matrix

Provides the list of features supported by the AOB application.

**Table 1-3 Supported Connector Features Matrix**

Feature	AOB Application
Perform full reconciliation	Yes
Perform reconciliation with Transaction Days	Yes
Perform incremental reconciliation	Yes
Perform limited reconciliation	Yes
Reconciliation of Contingent Workers	Yes
Reconciliation of Workers Without Account	Yes
Use connector server	Yes
Configure validation and transformation of account data	Yes
Support for pagination	Yes
Test connection	Yes
Clone applications or create new application instances	Yes
Provide secure communication to the target system through SSL	Yes

**Table 1-3 (Cont.) Supported Connector Features Matrix**

Feature	AOB Application
<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;">  <b>Note:</b>            features below are supported from version 12.2.1.3.1 (Target Connector).         </div>	
Perform Provisioning	Yes
Reset Password	Yes
Add or Remove Security Groups (Entitlement)	Yes
Reconcile the Account Attributes and Security Groups	Yes

## 1.7 Connector Features

The features of the connector include full reconciliation, batched reconciliation, limited reconciliation, connection pooling, SSL communication, and so on.

The following are the features of the connector:

- [Support for Trusted Source and Target Resource Reconciliation](#)
- [Support for Full and Incremental Reconciliation](#)
- [Support for Reconciliation with Transaction Days](#)
- [Support for Limited \(Filtered\) Reconciliation](#)
- [Support for the Connector Server](#)
- [Transformation and Validation of Account Data](#)
- [Support for Cloning Applications and Creating Instance Applications](#)
- [Secure Communication to the Target System](#)

### 1.7.1 Support for Trusted Source and Target Resource Reconciliation

There are two versions of the connectors available to provide support for trusted source (authoritative application) and target resource (Target application) reconciliation.

You can use the Workday authoritative connector to integrate Workday as a trusted source of Oracle Identity Governance. In this mode, the connector reconciles all the person types that are supported by the Workday application.

In the target resource mode, you can use the Workday target connector to create a Target application to provision and reconcile user records from the Workday application.

## 1.7.2 Support for Full and Incremental Reconciliation

In full reconciliation, all records are fetched from the target system to Oracle Identity Governance. In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

You can switch from incremental to full reconciliation at any time after you deploy the connector. See [Performing Full and Incremental Reconciliation](#) for more information on performing full and incremental reconciliation runs.

## 1.7.3 Support for Reconciliation with Transaction Days

To fetch the future hire date for contactors and future termination date for an employee during a reconciliation run, you must specify the value for Transaction Days attribute of the user reconciliation scheduled job.

The Transaction Days attribute helps you to specify the number of days for which the transactions have to be checked for the value of future hire date and future termination date. See [Performing Reconciliation with Transaction Days](#) for more information on performing reconciliation for transaction days.

## 1.7.4 Support for Limited (Filtered) Reconciliation

You can reconcile records from the target system based on a specified filter criterion.

You can set a reconciliation filter as the value of the Filter Query attribute of the user reconciliation scheduled job. This filter specifies the subset of newly added and modified target system records that must be reconciled. The Filter Query attribute helps you to assign filters to the webservices based on which you will get a filtered response from the target system.

See [Performing Limited Reconciliation](#) for more information on performing limited reconciliation.

## 1.7.5 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*.

## 1.7.6 Transformation and Validation of Account Data

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

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

## 1.7.7 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 an Instance Application* in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

## 1.7.8 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.

For information on SSL, see [Configuring SSL](#).

# 2

## Creating an Application By Using the Workday Connectors

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

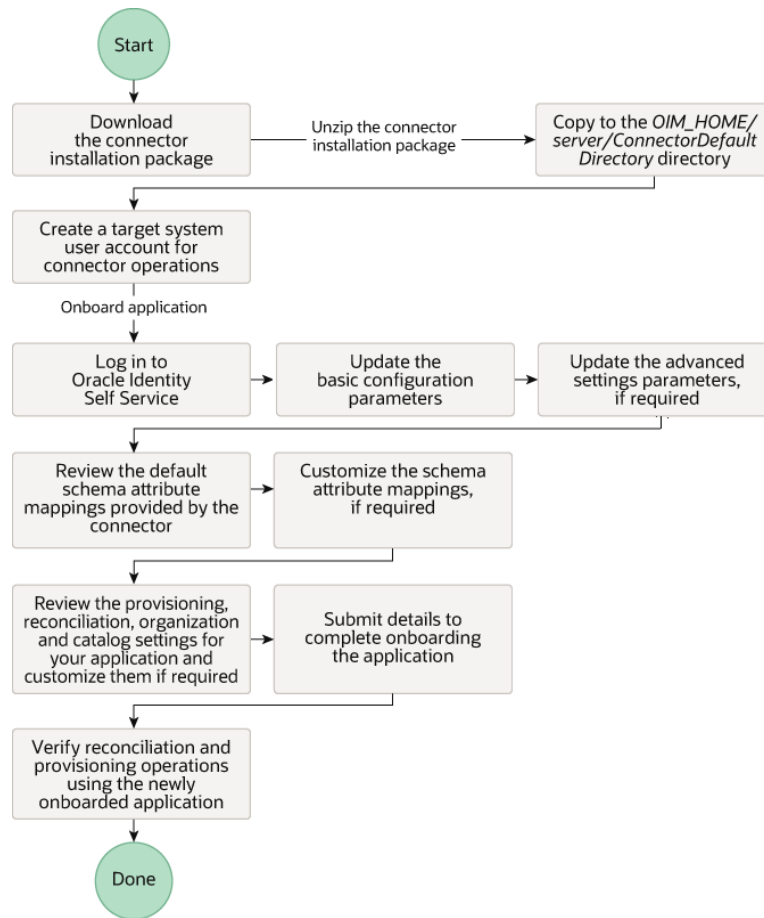
- [Process Flow for Creating an Application By Using the Connector](#)
- [Prerequisites for Creating an Application By Using Connector](#)
- [Creating an Application By Using the Connector](#)

### 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 Connector

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

- [Downloading the Connector Installation Package](#)
- [Creating an Integrated System User in Workday to Perform Connector Operations](#)
- [Configuring Raas Reports on workday](#)

### 2.2.1 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/ConnectorDefaultDirectory* directory.

## 2.2.2 Creating an Integrated System User in Workday to Perform Connector Operations

To perform connector operations, create an integrated system user in Workday.

To create an integrated system user:

1. Log in to Workday with an account that provides administrative privileges.
2. Create required users, and add them to a group as follows:
  - a. Search for and open the **Create Integration System User** task.
  - b. Configure and save the integration system user.
  - c. Search for and open the **Create Security Group** task.
  - d. In the **Type of Tenanted Security Group** field, choose **Integration System Security Group (Unconstrained)**.
  - e. Enter a group name and click **OK**.
  - f. Select all users you created from the **Integration System Users** choice list, click **OK**, and then click **Done**.
3. Add the integration security group to domains as follows:
  - a. Search for **domain: manage org** and open the **Manage: Organization Integration** domain.
  - b. Click the ellipsis (...) next to **Manage Organization Information**.
  - c. In the new window, point to **Domain** and select **Edit Security Policy Permissions**.
  - d. Under **Integration Permissions**, add the security group that you created and click **OK**.
  - e. Repeat previous steps to add the security group to the following domains:
    - domain: Worker Data: public worker reports
    - domain: Worker Data: Personal Data
    - domain: Worker Data: Current Staffing Information
    - domain: Worker Data: Contingent Worker Assignment Details
    - domain: Worker Data: Employment Data

- domain: Worker Data: Worker ID
  - domain: Manage: Location
  - domain: Manage: Organization Integration
  - domain: Organization: Cost Center
  - domain: Job Information
  - domain: Personal Data: Personal Information
  - domain: External Account Provisioning
  - domain: User-Based Security Group Administration
  - domain: Workday Accounts
4. Activate **Pending Security Policy Changes** as follows:
    - a. Search for **activate**.
    - b. Click **Activate Pending Security Policy Changes**.
    - c. Enter a comment and click **OK**.

## 2.2.3 Configuring Raas Reports on workday

- Search for Create Custom Report>>Provide Report name>>Report Type = Advanced>>
- DataSource="SecurityGroups"/" Assignable Roles"(Depending upon the use case)>>Click Ok Add columns as shown in the below provide figure.

### Note:

This is applicable from Workday 12.2.1.3.1C.

**Figure 2-2 Security Groups Raas report columns**

Columns	Sort	Filter	Subfilter	Prompts	Output	Share	Advanced
3 items							
Order	*Business Object	Field	Column Heading Override	Column Heading Override XML Alias			
+	Security Group	Reference ID		Reference_ID			
+	Security Group	Workday ID		workdayID			
+	Security Group	Security Group		Security_Group			



**Figure 2-3 Organization Raas report columns**

Columns   Sort   Filter   Subfilter   Prompts   Output   Share   Advanced						
3 items						
Order	*Business Object	Field	Column Heading Override	Column Heading Override XML Alias		
	× Assignable Role	× Role		Role		
	× Assignable Role	× Workday ID		workdayID		
	× Assignable Role	× Reference ID		referenceID		

>>Click on Share>>Provide the privileged user who can have access to these reports.

## 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.
  - 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.

 **Note:**

In the Authoritative (Trusted) application, the prompt window will not be displayed.

2. Verify reconciliation and provisioning operations on the newly created application.

 **See Also:**

- [Configuring the Workday Connector for a Target Application](#) and [Configuring the Workday Connector for an Authoritative Application](#) 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 Workday Connector for a Target Application

While creating a Target application, you must configure the 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.

- [Basic Configuration Parameters for the Workday Target Connector](#)
- [Advanced Setting Parameters for the Workday Target Connector](#)
- [Attribute Mapping for the Workday Target Connector](#)
- [Correlation Rules for the Workday Target Connector](#)
- [Reconciliation Jobs for the Workday Target Connector](#)

### 3.1 Basic Configuration Parameters for the Workday Target Connector

These are the connection-related parameters that Oracle Identity Governance requires to connect to the Workday target connector. These parameters are applicable for target applications only.

**Table 3-1 Parameters in the Basic Configuration Section for the Workday Target Connector**

Parameter	Mandatory?	Description
hostName	Yes	Enter the Workday host name. Sample value: wd2-impl-services1
Password	Yes	Enter the password for the user name of the target system account to be used for connector operations.
tenant	Yes	Enter the Workday tenant ID. Sample value: xyz_gms1
username	Yes	Enter the user name of the target system that you create for performing connector operations. Sample value: johndoe

**Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the Workday Target Connector**

Parameter	Mandatory?	Description
Connector Server Name	No	By default, this field is blank. If you are using this connector with the Java Connector Server, then provide the name of Connector Server IT Resource here.
proxyHost	No	Enter the name of the proxy host used to connect to an external target. <b>Sample value:</b> 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. <b>Sample value:</b> 80
proxyUser	No	Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system.

## 3.2 Advanced Setting Parameters for the Workday Target Connector

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

**Table 3-2 Advanced Setting Parameters for the Workday Target Connector**

Parameter	Mandatory?	Description
Bundle Version	Yes	This parameter holds the version of the connector bundle class. <b>Default Value:</b> 12.3.0
Connector Name	Yes	This parameter holds the name of the connector class. <b>Default Value:</b> org.identityconnectors.workday.WorkdayConnector

**Table 3-2 (Cont.) Advanced Setting Parameters for the Workday Target Connector**

Parameter	Mandatory?	Description
Bundle Name	Yes	This parameter holds the name of the connector bundle package. <b>Default Value:</b> <code>org.identityconnectors.workday</code>
version	Yes	This parameter holds the version of Workday API you are using. <b>Default Value:</b> <code>v34.1</code>
pageCount	Yes	This parameter holds the number of records in each batch that must be fetched from the target system during a reconciliation run. While specifying a value for <code>pageCount</code> , ensure to specify between 1 and 999. <b>Default Value:</b> <code>100</code>
workerWithAccount	Yes	Set the value to true if you want the parameter to reconcile only workers having a Workday account. <b>Default Value:</b> <code>true</code>
timezone	Yes	This parameter holds the Workday timezone value. <b>Default Value:</b> <code>PST</code>

**Table 3-2 (Cont.) Advanced Setting Parameters for the Workday Target Connector**

Parameter	Mandatory?	Description
raasreportUrl	Yes	This parameter holds the Workday RAAS Report URI's in the below format. "securitygroups:<ReportOwnerName>/<ReportName>", "organizationroles:<ReportOwnerName>/<ReportName>"



**N**

**o**

**t**

**e**

**:**

**T**

**h**

**i**

**s**

**A**

**t**

**t**

**r**

**i**

**b**

**u**

**t**

**e**

**a**

**p**

**p**

**l**

**i**

**c**

**a**

**b**

**l**

**e**

**f**

**r**

**o**

**m**

**W**

**o**

**r**

**k**

**d**

**a**

**y**

**-**

**1**

**Table 3-2 (Cont.) Advanced Setting Parameters for the Workday Target Connector**

Parameter	Mandatory?	Description
		2
		.
		2
		.
		1
		.
		3
		.
		1
		C
		.

**Table 3-2 (Cont.) Advanced Setting Parameters for the Workday Target Connector**

Parameter	Mandatory?	Description
integration_System_Id	Yes	This parameter holds the Integration System Id of the derived attributes form Workday. Format:"(Enter Integration sys ID)"



**N**

**o**

**t**

**e**

**:**

**T**

**h**

**i**

**s**

**A**

**t**

**r**

**i**

**b**

**u**

**t**

**e**

**a**

**p**

**p**

**l**

**i**

**c**

**a**

**b**

**l**

**e**

**r**

**o**

**m**

**W**

**o**

**r**

**k**

**d**

**a**

**y**

**-**

**1**

**2**

**.**



**Table 3-2 (Cont.) Advanced Setting Parameters for the Workday Target Connector**

Parameter	Mandatory?	Description
		2 . 1 . 3 . 1 C .

### 3.3 Attribute Mapping for the Workday Target Connector

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

#### Workday Target User Account Attributes

[Table 3-3](#) lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and Workday target columns. 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 in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-3 Workday Target Account Schema Attributes**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Worker ID	__UID__	String	No	No	Yes	Yes	No
Employee ID	__NAME__	String	No	No	Yes	No	Not applicable
Workday ID	workdayID	String	No	Yes	Yes	No	No
User Name	userID	String	No	No	Yes	No	Not applicable
Password	__PASSWORD__	String	No	Yes	No	No	No
First Name	firstname	String	No	No	Yes	No	Not applicable

**Table 3-3 (Cont.) Workday Target Account Schema Attributes**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Last Name	lastName	String	No	No	Yes	No	Not applicable
Full Name	fullName	String	No	No	Yes	No	Not applicable
Work Email	emailAddressWork	String	No	Yes	Yes	No	Not applicable
Home Email	emailAddressHome	String	No	Yes	Yes	No	Not applicable
Work Phone Device Type	phoneDeviceTypeWork	String	No	Yes	Yes	No	Not applicable
Work Phone	phoneNumberWork	String	No	Yes	Yes	No	Not applicable
Home Phone Device Type	phoneDeviceTypeHome	String	No	Yes	Yes	No	Not applicable
Home Phone	phoneNumberHome	String	No	Yes	Yes	No	Not applicable
Position	positionTitle	String	No	No	Yes	No	Not applicable
Employee Type	workerType	String	No	No	Yes	No	Not applicable
Manager	managerName	String	No	No	Yes	No	Not applicable
Cost Center	costCenter	String	No	No	Yes	No	Not applicable
Supervisory Org	supervisoryOrg	String	No	No	Yes	No	Not applicable
Address	streetAddress	String	No	No	Yes	No	Not applicable
City	municipality	String	No	No	Yes	No	Not applicable
State	state	String	No	No	Yes	No	Not applicable
Country	country	String	No	No	Yes	No	Not applicable
Postal Code	postalCode	String	No	No	Yes	No	Not applicable
Hire Date	continuousServiceDate	String	No	No	Yes	No	Not applicable
Termination Date	terminationDate	String	No	No	Yes	No	Not applicable

**Table 3-3 (Cont.) Workday Target Account Schema Attributes**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provisioning Field?	Recon Field?	Key Field?	Case Insensitive?
Status	__ENABLE__	String	No	No	Yes	No	Not applicable
IT Resource Name		Long	No	No	Yes	No	Not applicable

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

**Figure 3-1 Default Attribute Mappings for Workday Target User Account**

Application Attribute		Provisioning Property		Reconciliation Properties				
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive
Select a value	Worker ID	__UID__	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Select a value	Employee ID	__NAME__	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Workday ID	workdayID	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	User Name	userID	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Password	__PASSWORD__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Account Disable	accountDisabled	Boolean	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	First Name	firstName	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Last Name	lastName	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Full Name	fullName	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Work Email	emailAddressWork	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Home Email	emailAddressHome	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Work Phone De	phoneDeviceTypeWork	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Work Phone	phoneNumberWork	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Home Phone De	phoneDeviceTypeHome	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Home Phone	phoneNumberHome	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Position	positionTitle	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Employee Type	workerType	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Cost Center	costCenter	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Supervisory Org	supervisoryOrg	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Manager	managerName	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Address	streetAddress	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	City	municipality	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	State	state	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Country	country	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Postal Code	postalCode	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Hire Date	continuousServiceDate	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Termination Dat	terminationDate	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	Status	__ENABLE__	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select a value	IT Resource Nam		Long	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Roles Attribute**

Table 3-4 lists the roles-specific attribute mappings between the process form fields in Oracle Identity Governance and Workday target application attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

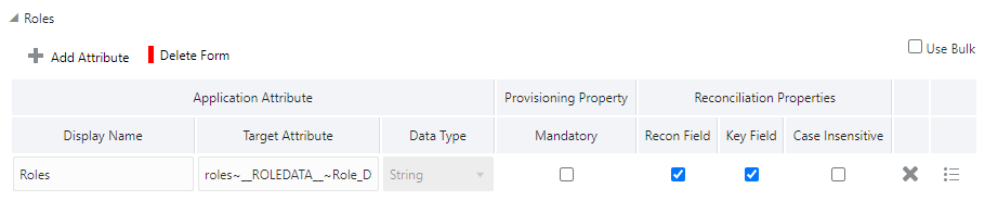
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-4 Default Attribute Mappings for Roles**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Organization Roles	roles~__ROLEDATA__~Role_Data	String	No	Yes	Yes	No

Figure 3-2 shows the default roles entitlement mapping.

**Figure 3-2 Default Attribute Mappings for Role**



### Secondary Phone Numbers Attribute

Table 3-5 lists secondary phone numbers attribute mappings between the process form fields in Oracle Identity Governance and the Workday Target application columns.

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

**Table 3-5 Default Attribute Mappings for Secondary Phone Number Child Attribute**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Advanced Settings
Country Code	__Phone__~__Phone__~countrycode	String	Yes	Yes	No	List of value: Lookup.Wor kday.Countr yCode Length : 200

**Table 3-5 (Cont.) Default Attribute Mappings for Secondary Phone Number Child Attribute**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Advanced Settings
Phone Number	__Phone__ ~__Phone_ __~phonenu mber	String	Yes	Yes	Yes	No
Extension	__Phone__ ~__Phone_ __~extension	String	No	Yes	No	No
Device Type	__Phone__ ~__Phone_ __~devicetyp e	String	Yes	Yes	Yes	List of value: Lookup.Wor kday.Device Type Length : 200
Phone Type	__Phone__ ~__Phone_ __~phonetyp e	String	Yes	Yes	Yes	List of value: Lookup.Wor kday.Phone Type Length : 200
Public	__Phone__ ~__Phone_ __~public	String	Yes	Yes	Yes	List of value: Lookup.Wor kday.Boolea nValues Length : 200

Figure 3-3 shows the default attributes for the secondary phone number child form attribute.

**Figure 3-3 Default Attributes for Secondary Phone Number Child Form**

Secondary Phone Numbers

+ Add Attribute | Delete Form  Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Country Code	__Phone__~__Phone__~count	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Phone Number	__Phone__~__Phone__~phone	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Extension	__Phone__~__Phone__~extent	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Type	__Phone__~__Phone__~device	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Phone Type	__Phone__~__Phone__~phone	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	__Phone__~__Phone__~public	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

 **Note:**

The Phone Number Type and Phone\_Device\_Type\_ID attributes in the Workday target must be identical and must match with the code and decode values of the Lookup Lookup.Workday.DeviceType. You can find these values in the Workday Phone Device Types Report.

**Secondary Email Attribute**

Table 3-6 lists secondary email attribute mappings between the process form fields in Oracle Identity Governance and the Workday Target application columns.

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

**Table 3-6 Default Attribute Mappings for Secondary Email Child Attribute**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Advanced Settings
Email Address	__Mail__~__Mail__~emailsecondary	String	Yes	Yes	Yes	No
Email Public	__Mail__~__Mail__~emailpublic	String	Yes	Yes	No	List of values :Lookup.Workday.Boolean/Values Length : 200

**Table 3-6 (Cont.) Default Attribute Mappings for Secondary Email Child Attribute**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Advanced Settings
Email Type	__Mail__~__Mail__~emailtype	String	Yes	Yes	No	List of values :Lookup.Workday.PhoneType Length : 200

Figure 3-4 shows the default attributes for the secondary email child form.

**Figure 3-4 Default Attributes for Secondary Email Child Form**

Application Attribute			Provisioning Property	Reconciliation Properties			
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive	
Email Address	__Mail__~__Mail__~emailsecor	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Email Public	__Mail__~__Mail__~emailpubli	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Email Type	__Mail__~__Mail__~emailtype	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮

### Security Groups Attribute

Table 3-7 lists the group attribute mappings between the process form fields in Oracle Identity Governance and the Workday Target application columns.

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

**Table 3-7 Default Attribute Mappings for Security Groups**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Security Groups	securitygroups~__SECURITYGROUP__~SecurityGroups	String	No	Yes	Yes	No

Default Attribute Mappings for Security Groups shows the default security groups entitlement mapping.

**Figure 3-5 Default Attribute Mappings for Security Groups**

The screenshot shows a configuration interface for 'Security Groups'. At the top, there are buttons for '+ Add Attribute' and 'Delete Form', and a checkbox for 'Use Bulk'. Below is a table with columns for 'Application Attribute', 'Provisioning Property', and 'Reconciliation Properties'. The table contains one row for 'Security Groups' with the following details:

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Security Groups	securitygroups-__SECURITYG	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## 3.4 Correlation Rules for the Workday Target Connector

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

### Predefined Identity Correlation Rules

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

[Table 3-8](#) lists the default simple correlation rule for the Workday target application. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-8 Predefined Identity Correlation Rule for Workday Target Connector**

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

- `__NAME__` is a single-valued attribute on the target system that identifies the user account.
- User Login is the field on the OIG User form.

[Figure 3-6](#) shows the simple correlation rule for a Workday Target application.



**Figure 3-6 Simple Correlation Rules for the Workday Target Connector**

Identity Correlation Rule

Choose Type of Correlation Rule

Simple Correlation Rule  Complex Correlation Rule

+ Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
_NAME_	Equals	User Login	<input type="checkbox"/>	X

Rule Operator

Select a value

### Predefined Situations and Responses

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

Table 3-9 lists the default situations and responses for a target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

**Table 3-9 Predefined Situations and Responses for a Target Application**

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

## 3.5 Reconciliation Jobs for the Workday Target Connector

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

You must specify values for the parameters of user reconciliation jobs.

### Workday Target User Reconciliation Job

The Workday Target User Reconciliation job is used to fetch all the workers from the 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*.

Table 3-10 describes the parameters of the Workday Target User Reconciliation job.

**Table 3-10 Parameters of the Workday Target 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.  Do <i>not</i> modify this value.
Filter Query	Enter the search filter for fetching records from the target system during a reconciliation run. Sample value: <code>Employee_ID=21220</code>  For <a href="#">Performing Limited Reconciliation</a> for more information about filtered reconciliation.
Sync Token	This attribute holds the date and time stamp at when the last full or incremental reconciliation run started.  <b>Default value:</b> <code>&lt;String&gt;0&lt;/String&gt;</code>  <b>Note:</b> <ul style="list-style-type: none"> <li>If you are running a schedule job with incremental reconciliation, sync token will be updated automatically.</li> <li>If you know a valid value for sync token, you can enter it in the following example format: <code>&lt;String&gt;2020-05-19T18:29:49&lt;/String&gt;</code></li> <li>This attribute stores values in an XML serialized format.</li> </ul>
Transaction Days	Enter the number of days that corresponds to the official notice period of the Organization.  <b>Default value:</b> 0  See <a href="#">Performing Reconciliation with Transaction Days</a> for more information about reconciliation with Transaction Days.
Object Type	Type of the scheduled job you want to reconcile.  <b>Default value:</b> <code>User</code>
Scheduled Task Name	Name of the scheduled job used for reconciliation.  <b>Default value:</b> <code>&lt;Application Name&gt;</code> <code>Workday Target User Reconciliation</code>  <b>Note:</b> 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

## Configuring the Workday Connector for an Authoritative 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 mappings between reconciliation fields in Oracle Identity Governance and target system columns, predefined correlation rules, situations and responses, and reconciliation jobs.

- [Basic Configuration Parameters for the Workday Authoritative Connector](#)
- [Advanced Setting Parameters for the Workday Authoritative Connector](#)
- [Attribute Mapping for the Workday Authoritative Connector](#)
- [Correlation Rules for the Workday Authoritative Connector](#)
- [Reconciliation Jobs for the Workday Authoritative Connector](#)

### 4.1 Basic Configuration Parameters for the Workday Authoritative Connector

These are the connection-related parameters that Oracle Identity Governance requires to connect to your target system. These parameters are applicable for authoritative applications only.

**Table 4-1 Parameters in the Basic Configuration Section for the Workday Authoritative Connector**

Parameter	Mandatory?	Description
hostName	Yes	Enter the Workday host name. Sample value: wd2-impl-services1
Password	Yes	Enter the password for the user name of the target system account to be used for connector operations.
tenant	Yes	Enter the Workday tenant ID. Sample value: xyz_gms1
username	Yes	Enter the user name of the target system that you create for performing connector operations. Sample value: johndoe

**Table 4-1 (Cont.) Parameters in the Basic Configuration Section for the Workday Authoritative Connector**

Parameter	Mandatory?	Description
Connector Server Name	No	By default, this field is blank. If you are using this connector with the Java Connector Server, then provide the name of Connector Server IT Resource here.
proxyHost	No	Enter the name of the proxy host used to connect to an external target. <b>Sample value:</b> 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. <b>Sample value:</b> 80
proxyUser	No	Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system.

## 4.2 Advanced Setting Parameters for the Workday Authoritative Connector

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

**Table 4-2 Advanced Setting Parameters for the Workday Authoritative Connector**

Parameter	Mandatory?	Description
Bundle Version	Yes	This parameter holds the version of the connector bundle class. <b>Default Value:</b> 12.3.0
Connector Name	Yes	This parameter holds the name of the connector class. <b>Default Value:</b> org.identityconnectors.workday.WorkdayConnector

**Table 4-2 (Cont.) Advanced Setting Parameters for the Workday Authoritative Connector**

Parameter	Mandatory?	Description
Bundle Name	Yes	This parameter holds the name of the connector bundle package. <b>Default Value:</b> <code>org.identityconnectors.workday</code>
version	Yes	This parameter holds the version of Workday API you are using. <b>Default Value:</b> <code>v34.1</code>
pageCount	Yes	This parameter holds the number of records in each batch that must be fetched from the target system during a reconciliation run. While specifying a value for <code>pageCount</code> , ensure to specify between 1 and 999. <b>Default Value:</b> <code>100</code>
workerWithAccount	Yes	Set the value to true if you want the parameter to reconcile only workers having a Workday account. <b>Default Value:</b> <code>true</code>
timezone	Yes	This parameter holds the Workday timezone value. <b>Default Value:</b> <code>PST</code>

## 4.3 Attribute Mapping for the Workday Authoritative Connector

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

**Table 4-3** lists the user-specific attribute mappings between the reconciliation fields in Oracle Identity Governance and target system columns. The table also lists the data type for a given attribute and specifies whether it is a mandatory attribute for reconciliation.

You may use the default schema that has been set for you or update and change it before continuing to the next step. You can edit the attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 4-3 Workday Authoritative User Account Schema Attributes**

Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Default Value for Identity Display Name
Worker GUID	__UID__	String	No	Yes	Not Applicable
User Login	__NAME__	String	No	Yes	Not Applicable
Status	__ENABLE__	String	No	Yes	Not applicable
First Name	firstname	String	Yes	Yes	Not applicable
Last Name	lastName	String	Yes	Yes	Not applicable
Display Name	fullName	String	No	Yes	Not applicable
Email	emailAddress Work	String	No	Yes	Not applicable
Telephone Number	phoneNumber Work	String	No	Yes	Not applicable
Home Phone	phoneNumber Home	String	No	Yes	Not applicable
Title	positionTitle	String	No	Yes	Not applicable
Postal Address	streetAddress	String	No	Yes	Not applicable
State	state	String	No	Yes	Not applicable
Country	country	String	No	Yes	Not applicable
Postal Code	postalCode	String	No	Yes	Not applicable
Start Date	continuousServiceDate	Date	No	Yes	Not applicable
End Date	terminationDate	Date	No	Yes	Not applicable
Manager Login	managerID	String	No	Yes	Not applicable
Xellerate Type		Long	No	Yes	End-User
Organization Name		String	No	Yes	Xellerate Users
Role		String	No	Yes	Full-Time

Figure 4-1 shows the default User account attribute mappings.

**Figure 4-1 Workday Authoritative User Account Schema Attributes**

Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
Workday GUID	__UID__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
User Login	__NAME__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Status	__ENABLE__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
First Name	firstName	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Last Name	lastName	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Display Name	fullName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Email	emailAddressWork	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Telephone Number	phoneNumberWork	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Home Phone	phoneNumberHome	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Title	positionTitle	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Postal Address	streetAddress	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
State	state	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Country	country	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Postal Code	postalCode	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Start Date	continuousServiceDate	Date	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
End Date	terminationDate	Date	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Manager Login	managerID	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Xellerate Type		String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Organization Name		String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Role		String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

## 4.4 Correlation Rules for the Workday Authoritative Connector

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

### Predefined Identity Correlation Rules

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

[Table 4-4](#) lists the default simple correlation rule for Workday Authoritative application. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see *Updating Identity Correlation Rule in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 4-4 Predefined Identity Correlation Rule for Workday Target Connector**

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

- \_\_NAME\_\_ is a single-valued attribute on the target system that identifies the user account.
- User Login is the field on the OIG User form.

Figure 4-2 shows the simple correlation rule for a Workday Target application.

**Figure 4-2 Simple Correlation Rule for an Authoritative Application**

The screenshot shows the 'Identity Correlation Rule' configuration page. Under 'Choose Type of Correlation Rule', 'Simple Correlation Rule' is selected. Below, there is an 'Add Rule Element' button and a table with the following data:

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
__NAME__	Equals	User Login	<input type="checkbox"/>	<input type="button" value="X"/>

Below the table is a 'Rule Operator' dropdown menu currently showing 'Select a value'.

### Predefined Situations and Responses

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

Table 4-5 lists the default situations and responses for an authoritative application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see *Updating Identity Correlation Rule in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

**Table 4-5 Predefined Situations and Responses for an Authoritative Application**

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



## 4.5 Reconciliation Jobs for the Workday Authoritative Connector

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

You must specify values for the parameters of user reconciliation jobs.

### Workday Trusted User Reconciliation Job

The Workday Trusted User Reconciliation job is used to fetch all the workers from the 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*.

[Table 4-6](#) describes the parameters of the Workday Trusted User Reconciliation job.

**Table 4-6 Parameters of the Workday Authoritative 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. Do <i>not</i> modify this value.
Filter Query	Enter the search filter for fetching records from the target system during a reconciliation run. Sample value: Employee_ID=21220 For <a href="#">Performing Limited Reconciliation</a> for more information about filtered reconciliation.
Sync Token	This attribute holds the date and time stamp at when the last full or incremental reconciliation run started. <b>Default value:</b> <String>0</String> <b>Note:</b> <ul style="list-style-type: none"> <li>If you are running a schedule job with incremental reconciliation, sync token will be updated automatically.</li> <li>If you know a valid value for sync token, you can enter it in the following example format: &lt;String&gt;2020-05-19T18:29:49&lt;/String&gt;</li> <li>This attribute stores values in an XML serialized format.</li> </ul>

**Table 4-6 (Cont.) Parameters of the Workday Authoritative User Reconciliation Job**

Parameter	Description
Transaction Days	<p>Enter the number of days that corresponds to the official notice period of the organization or number of days a contractor hiring process is initiated before the original hire date, whichever is larger.</p> <p><b>Default value:</b> 0</p> <p>See <a href="#">Performing Reconciliation with Transaction Days</a> for more information about reconciliation with Transaction Days.</p>
Object Type	<p>Type of the scheduled job you want to reconcile.</p> <p><b>Default value:</b> User</p>
Scheduled Task Name	<p>Name of the scheduled job used for reconciliation.</p> <p><b>Default value:</b> &lt;Application Name&gt; Workday Trusted User Reconciliation</p> <p><b>Note:</b> 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.</p>

# 5

## Performing the Postconfiguration Tasks for the Workday Connectors

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

- [Configuring Oracle Identity Governance](#)
- [Configuring SSL](#)
- [Configuring the IT Resource for the Connector Server](#)
- [Managing Logging](#)
- [Localizing Field Labels in UI Forms](#)

### 5.1 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](#)

#### 5.1.1 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*.

#### 5.1.2 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.

### 5.1.3 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 as Administrator and activate the sandbox 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*.

### 5.1.4 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*

## 5.2 Configuring SSL

Configure SSL to secure data communication between Oracle Identity Governance and the Workday target system.

### Note:

If you are using this connector along with a Connector Server, then there is no need to configure SSL. You can skip this section.

To configure SSL:

1. Obtain the SSL public key certificate of Workday.
2. Copy the public key certificate of Workday 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 -alias ALIAS -trustcacerts -file CERT_FILE_NAME -keystore  
KEYSTORE_NAME -storepass PASSWORD
```

In this command:

- *ALIAS* is the public key certificate alias.
- *CERT\_FILE\_NAME* is the full path and name of the certificate store (the default is `cacerts`).
- *KEYSTORE\_NAME* is the name of the keystore.
- *PASSWORD* is the password of the keystore.

The following are sample values for this command:

- ```
keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file  
<Cert_Location>/GeoTrustTLRSACAG1.crt -storepass changeit -alias  
GeoTrustTLRSACAG1t_1
```
- ```
keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file  
<Cert_Location>/DigiCertGlobalRootG2.crt -storepass changeit -alias  
DigiCertGlobalRootG2_1
```
- ```
keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file  
<Cert_Location>/GeoTrustTLRSACAG1.crt -storepass  
DemoTrustKeyStorePassPhrase -alias GeoTrustTLRSACAG1t_1
```
- ```
keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file  
<Cert_Location>/DigiCertGlobalRootG2.crt -storepass  
DemoTrustKeyStorePassPhrase -alias DigiCertGlobalRootG2_1
```

 **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
- Ensure that the system date for Oracle Identity Governance is in sync with the validity date of the SSL certificate to avoid any errors during SSL communication.

## 5.3 Configuring the IT Resource for the Connector Server

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

After you create the application for your target system, you must create an IT resource for the Connector Server as described in *Creating IT Resource of Oracle Fusion Middleware Administering Oracle Identity Governance*. While creating the IT resource, ensure to use to select **Connector Server** from the **IT Resource Type** list.

In addition, specify values for the parameters of the IT resource for the Connector Server listed in [Table 5-1](#).

**Table 5-1 Parameters of the IT Resource for the Connector Server**

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: <code>myhost.com</code>
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. By default, this value is blank. You must enter the port number that is displayed on the terminal when you start the Connector Server. Sample value: <code>8759</code>
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. Recommended value: <code>0</code> A value of <code>0</code> means that the connection never times out.
UseSSL	Enter <code>true</code> to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter <code>false</code> . Default value: <code>false</code> <b>Note:</b> It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see <i>Setting SSL for Connector Server and OIM in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance</i> .

## 5.4 Managing Logging

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](#)

### 5.4.1 Understanding Log Levels

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

- `SEVERE.intValue()+100`  
This level enables logging of information about fatal errors.
- `SEVERE`  
This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.
- `WARNING`  
This level enables logging of information about potentially harmful situations.
- `INFO`  
This level enables logging of messages that highlight the progress of the application.
- `CONFIG`  
This level enables logging of information about fine-grained events that are useful for debugging.
- `FINE, FINER, FINEST`  
These levels enable logging of information about fine-grained events, where `FINEST` logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in [Table 5-2](#).

**Table 5-2 Log Levels and ODL Message Type:Level Combinations**

Log Level	ODL Message Type:Level
<code>SEVERE.intValue()+100</code>	<code>INCIDENT_ERROR:1</code>
<code>SEVERE</code>	<code>ERROR:1</code>
<code>WARNING</code>	<code>WARNING:1</code>
<code>INFO</code>	<code>NOTIFICATION:1</code>
<code>CONFIG</code>	<code>NOTIFICATION:16</code>
<code>FINE</code>	<code>TRACE:1</code>

**Table 5-2 (Cont.) Log Levels and ODL Message Type:Level Combinations**

Log Level	ODL Message Type:Level
FINER	TRACE:16
FINEST	TRACE:32

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

*DOMAIN\_HOME*/config/fmwconfig/servers/*OIM\_SERVER*/logging.xml

Here, *DOMAIN\_HOME* and *OIM\_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

## 5.4.2 Enabling logging

Perform these steps 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='workday-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>
</log_handlers>

<logger name='ORG.IDENTITYCONNECTORS.WORKDAY' level='[LOG_LEVEL]'
useParentHandlers='false'>
  <handler name='workday-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 5-2 lists the supported message type and level combinations.

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

The following blocks show sample values for [LOG\_LEVEL] and [FILE\_NAME] :

```
<log_handler name='workday-handler' level='TRACE:32'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
  <property name='logreader:' value='off' />
  <property name='path' value='${<OIM_DOMAIN%>}/servers/oim_server1/
logs/workdaylogs.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>
</log_handlers>

<loggers>
  <logger name='ORG.IDENTITYCONNECTORS.WORKDAY' level='TRACE:32'
  useParentHandlers='false'>
    <handler name='workday-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 `TRACE:32` 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.

## 5.5 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 field label that you add in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand Application Deployments and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive (oracle.iam.console.identity.sysadmin.ear\_V2.0\_metadata.zip) to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:

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

### Note:

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

## 6. Edit the BizEditorBundle.xlf file in the following manner:

## a. Search for the following text:

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

## b. Replace with the following text:

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

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

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

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_Workday_Target_USER_NAME__c_description']">
  <source>User Name</source>
  <target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.WorkdayTargetForm1.entity
.WorkdayTargetForm1EO.UD_Workday_Target_USER_NAME__c_LABEL">
<source>User Name</source>
<target/>
```

## d. Open the resource file (for example, Workday.properties) from the connector package, and get the value of the attribute from the file, for example, global.udf.UD\_WD\_USER\_NAME=\u30E6\u30FC\u30B6\u30FC\u540D.

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_Workday_Target_USER_NAME__c_description']">
  <source>User Name</source>
  <target>\u30E6\u30FC\u30B6\u30FC\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.WorkdayTargetForm1.entity
.WorkdayTarget1EO.UD_Workday_Target_USER_NAME__c_LABEL">
  <source>User Name</source>
  <target>\u30E6\u30FC\u30B6\u30FC\u540D</target>
</trans-unit>
```

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

g. Save the file as BizEditorBundle\_LANG\_CODE.xlf. In this file name, replace *LANG\_CODE* with the code of the language to which you are localizing.

Sample file name: BizEditorBundle\_ja.xlf.

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

 **See Also:**

Deploying and Undeploying Customizations in *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 Enterprise Manager.

# 6

## Using the Workday Connectors

You can use the Workday Connectors for performing reconciliation and provisioning operations after configuring your application to meet your requirements.

This chapter contains the following sections:

- [Configuring Reconciliation](#)
- [Configuring Reconciliation Jobs](#)
- [Performing Provisioning Operations](#)
- [Handling Start Date and End Date](#)
- [Uninstalling the Connector](#)



### Note:

Perform sections [Configuring Reconciliation Jobs](#) and [Performing Provisioning Operations](#) if you are using the Workday Target application only.

## 6.1 Configuring Reconciliation

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

- [Performing Full and Incremental Reconciliation](#)
- [Performing Reconciliation with Transaction Days](#)
- [Performing Limited Reconciliation](#)

### 6.1.1 Performing Full and Incremental Reconciliation

Full reconciliation involves reconciling all existing workers from the target system into Oracle Identity Governance. During incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

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

To perform a full reconciliation, remove (delete) any value assigned to **Filter Query** and **Transaction Days**, set **Sync Token** value to `<String>0</String>` and run one of the following reconciliation jobs:

- For a Workday target application: `<Application Name> Workday Target User Reconciliation`
- For a Workday authoritative application: `<Application Name> Workday Trusted User Reconciliation`

After the full reconciliation job is completed, the connector updates the **Sync Token** value with the date and time stamp when the reconciliation run started. Perform a reconciliation operation with **Transaction Days** after you perform a full reconciliation, to reconcile **Future hire date** and **Future termination date** attributes. Ideally, reconciliation with **Transaction Days** is performed only once as part of initial setup. See [Performing Reconciliation with Transaction Days](#) for detailed information.

To perform an incremental reconciliation, make sure the **Sync Token** is updated with the time stamp of the last reconciliation run and remove (delete) any value assigned to **Filter Query** and **Transaction Days**.

 **Note:**

Sync Token is only updated when a Full reconciliation or Incremental reconciliation operation is performed. It does not get updated when a Filter reconciliation or Reconciliation with transaction days is performed.

See [Reconciliation Jobs for the Workday Target Connector](#) and [Reconciliation Jobs for the Workday Authoritative Connector](#) for information about the jobs for full and incremental reconciliation.

## 6.1.2 Performing Reconciliation with Transaction Days

Whenever a full or limited reconciliation is performed, the Hire date of a contract employee is not reconciled if he/she is hired with a future effective date. Similarly, the Termination Date of a regular employee is not reconciled if he/she is terminated with a future effective date.

To reconcile these values, you must run the reconciliation job by providing a value for the **Transaction Days** parameter. This is the value of max number of days a regular employee would be active in an organization after he is terminated, or max number of days contractors can be pre-hired in an organization, whichever is larger.

For example, if an organization has a notice period of 45 days, it means that an employee can be active for a maximum duration of 45 days after the termination process is initiated. If contractor hiring process is initiated 30 days before their original hire date, then provide the value for the **Transaction Days** parameter as 45.

 **Note:**

Whenever an incremental reconciliation is performed, the **Future hire date** and **Future termination date** attribute values are also reconciled. Hence, it is recommended to perform reconciliation with transaction days after a full reconciliation or a filter reconciliation only.

## 6.1.3 Performing Limited Reconciliation

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. You do this by creating filters for the reconciliation module.

This connector provides a **Filter Query** parameter (a reconciliation job parameter) that allows you to use various filter conditions to filter the target system records. When you specify a value for the Filter Query parameter, the connector reconciles only the target system records that match the filter criterion into Oracle Identity Governance.

The following are filters that are supported by the Workday connector:

- Filter workers using WID.  
For example, `WID=06f0036f384a016c1da65076fa5f6d0a`  
  
Here any user with WID as `06f0036f384a016c1da65076fa5f6d0a` is reconciled.
- Filter workers using **Employee\_ID** and **Contingent\_Worker\_ID** .  
To reconcile regular employees, use `Employee_ID=21220`, where 22120 is the employee ID of an employee. To reconcile contractors, use `Contingent_Worker_ID=22406`, where 22406 is contingent worker ID of a contractor.
- Filter workers using Organization Id.  
For example, `Organization_Reference_Id=Global_Modern_Services_supervisory`  
  
Here `Global_Modern_Services_supervisory` is the Organization ID and all users belonging to this organization are reconciled.
- Filter workers using Country  
For example, `Country=US`  
  
Here US is the ISO Alpha-2 country code of United States. All users in Workday that belong to US are reconciled.
- Filter workers using National Id  
For example, `National_ID_Type_Code=IND-PAN&Identifier_ID=AXXPX1234K`  
  
Here IND-PAN is the National ID Type code of the National ID and AXXPX1234K is the Identification value of National ID.

**Note:**

Workday connector does not support any other filters.

## 6.2 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.

## 6.3 Performing Provisioning Operations

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

- [Creating Users](#)
- [Modifying Users](#)

### 6.3.1 Creating Users

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**.

## 6.3.2 Modifying Users

You can update an existing user in Identity Self Service by using the **Modify User** page.

To perform provisioning operations in Oracle Identity Governance:

1. Log in to Identity Self Service.
2. From the **Users** tab, right-click the account you wish to update, and then select **Modify**.
3. From the **Modify Account** page, you can specify and update values for the following fields:
  - Work Email
  - Home Email
  - Work Phone Device Type
  - Work Phone
  - Home Phone Device Type
  - Home Phone
4. You can also update the Secondary Phone Number and Secondary Email information by specifying values for the respective fields in the child form present at the end of the tab.

 **Note:**

All fields in the secondary phone number child form, except **Extension** are mandatory.

5. Click **Update**, and **Submit**.



 **Note:**

While updating contact data for a worker, ensure the following:

- Provide value for Work Phone or Home Phone attributes in the +91-0123456789x123 format. Here, 91 is the country code with + as prefix, 0123456789 is the phone number with - as prefix, and 123 is the extension number with x as prefix.
- You cannot add secondary contact details without adding primary contact details. For example, without adding work phone in the parent form, Workday does not allow you to add secondary phone number of **Phone type: Work**.
- When a worker has primary and secondary contact data of the same type, Workday system does not all allow you to delete primary contact data. You must first delete the secondary contact details, then only you can delete the primary contact details.
- If contact data of a worker is updated in Workday with a future effective date, then you cannot update the worker contact data until the transaction is occurred or it is revoked in the Workday system.

## 6.4 Handling Start Date and End Date

You can configure the Workday Trusted connector to handle Start and End date for workers.

- [Handling Start Date](#)
- [Handling End Date](#)

### 6.4.1 Handling Start Date

When a worker is reconciled from the Workday application (in a Workday Trusted connector), and a user is being created, Oracle Identity Manager evaluates the **Start Date** attribute. If the attribute is set to the current day or an earlier date, the user is created in Oracle Identity Manager. An event handler evaluates the start date, and Oracle Identity Manager sets this account as **Active**.

While creating a user with a start date set to a future date, Oracle Identity Manager creates the user in a **Disabled until start date** state. Once the start date is reached, the **Enable User After Start Date** evaluates the Start Date attribute and enables all users whose start date has passed during the reconciliation run. This sets the user's state to **Active**.

### 6.4.2 Handling End Date

The End Date attribute controls termination and automates the process ensuring that the account closures do not get lost in the shuffle.

The Disable/Delete User After End Date scheduled job evaluates the End Date attribute, and either disables or deletes all users whose end date is before the current date at the time of the reconciliation run. All accounts provisioned to the user will then

be placed in either disabled or revoked state, depending on the configuration of the scheduled job.

 **Note:**

The schedulers for **Enable User After Start Date** and **Disable/Delete User After End Date** is often set to run once per day at a specified time. The attributes will not get evaluated until the scheduled job runs. It is recommended to set to run the Enable User After Start Date scheduled job before the normal business hours and Disable/Delete User After End Date scheduled job after the normal business hours.

## 6.5 Uninstalling the Connector

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

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

Below are examples to uninstall ResourceObjects and ScheduleJobs respectively:

- `ObjectType=ResourceObject`  
`ObjectValues=<Application Name>`
- `ObjectType= ScheduleJob`  
`ObjectValues= <Application Name>Workday Target User Reconciliation`

 **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*.

# 7

## Extending the Functionality of the Workday Connectors

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

This chapter contains the following sections:

- [Configuring Transformation and Validation of Data](#)
- [Configuring Action Scripts](#)
- [Configuring the Connector for Multiple Tenants](#)

### 7.1 Configuring Transformation and Validation of Data

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

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to update the value for Work Email 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*.

### 7.2 Configuring Action Scripts

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

These scripts can be configured to run before or after updating an account for 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*.

## 7.3 Configuring the Connector for Multiple Tenants

You must clone the application of your base application to configure it for multiple tenants.

The following example illustrates this requirement:

XYZ corporation has multiple tenants including an independent schema. 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*.

# 8

## Upgrading the Connector

If you are already using the 12.2.1.3.0 version of the Workday connector, then you can upgrade the connector to version 12.2.1.3.1.

You can upgrade the applications that are created through application onboarding by using the **Upgrade** option on the Applications page.

Before you perform the upgrade procedure:

- It is strongly recommended that you create a backup of the Oracle Identity Governance database and the connector JARs before you perform an upgrade operation.
- As a best practice, first perform the upgrade procedure in a test environment.



### Note:

The upgrade process described in the following sections is applicable only to Target applications, it is not applicable for Authoritative applications.

### 8.1 Upgrading Applications

To upgrade the application:

1. **Upgrade the connector using wizard mode:** Login into Identity Console and navigate to Applications under **Manage** tab. Click on **Connector Upgrade**.
2. **Target Basic & Advance Config:** Both target and trusted Workday applications will be upgraded in a single go. First, all the differences of the target type will be shown and then authoritative. On the **Target Basic Information** schema page, basic and advanced configurations differences are shown. A checkbox is provided for each property which user can select or deselect. For example, if the user has checked the removed basic property, this property will be removed from all the applications of this type of connector. Similarly, you can choose for advance configurations as well. Click **Next**.
3. **Target Schema:** All the changes related to parent schema such as the addition of new schema attributes or removal of schema attributes are shown here. Changes in child forms, if any, are also shown here. You have the flexibility of choosing the applicable changes. Click **Next**.
4. **Target Reconciliation & Provisioning Settings:** Changes related to addition or removal of jobs are shown here. Changes in the old job configuration such as addition or removal of job params are also visible here. Click **Next**.
5. **Summary:** On the review screen all the checked changes are shown. Also, all the impacted applications, both trusted and target, are also shown. After clicking **Upgrade**, you will be taken to the Upgrade Status screen where you can see the status of each individual application.

**Note:**

Further details can be reviewed in Managing Application OnBoarding.

**Note:**

For the updated Basic Configuration, schema attribute and Reconciliation jobs please refer to [Configuring the Workday Connector for a Target Application](#).

## 8.2 Post-upgrade Steps

Post-upgrade steps involve uploading new connector JAR files, configuring the upgraded IT resource of the source connector, deploying and reconfiguring the Connector Server, and deleting duplicate entries for lookup definitions.

1. Delete the old Connector JARs. Run the Oracle Identity Governance Delete JARs (`$ORACLE_HOME/bin/DeleteJars.sh`) utility to delete the existing ICF bundle `org.identityconnectors.workday-12.3.0.jar` from the Oracle Identity Governance database. When you run the Delete JARs utility, you are prompted to enter the login credentials of the Oracle Identity Governance administrator, URL of the Oracle Identity Governance host computer, context factory value, type of JAR file being deleted, and the name of the JAR file to be removed. Specify 4 as the value of the JAR type.
2. Upload the new connector JARs.
  - a. Run the Oracle Identity Governance Upload JARs (`$ORACLE_HOME/bin/UploadJars.sh`) utility to upload the connector JARs.
  - b. Upload the `org.identityconnectors.workday-12.3.0.jar` bundle as an ICF Bundle. Run the Oracle Identity Governance Upload JARs utility to post the new ICF bundle `org.identityconnectors.workday-12.3.0.jar` file to the Oracle Identity Governance database. When you run the Upload JARs utility, you are prompted to enter the login credentials of the Oracle Identity Governance administrator, URL of the Oracle Identity Governance host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 4 as the value of the JAR type.
3. Restart Oracle Identity Governance.
4. If the connector is deployed on a Connector Server, then:
  - a. Stop the connector server.
  - b. Replace the existing bundle JAR file **`org.identityconnectors.workday-12.3.0.jar`** with the new bundle JAR file **`org.identityconnectors.workday-12.3.0.jar`**.
  - c. Start the connector server.
5. Create a new version of the process form.
6. Create new form and add to the upgraded Target application.

7. Publish a new sandbox.
8. Make sure the following Schema attributes are updated.
  - Workday ID
  - Password
  - Account Disabled
  - Security Groups
9. Make sure the following Advance settings attributes are added.
  - generateRandomPassword
  - newPasswordAtNextSignIn
  - reconAccountAttributes
  - reconSecurityAttributes
10. Run Form Upgrade job.
11. Perform Full Reconciliation



**Note:**

If you have not retained customizations, you must reapply them after you upgrade the connector.

# 9

## Frequently Asked Questions

This chapter provides information on the frequently asked questions about the Workday connector.

1. What happens when an invalid or negative integer value is provided for the Transaction Days attribute while performing reconciliation?

**Answer:** When an invalid or negative integer is provided, the connector defaults the Transaction Days value to 0 and reconciliation is performed with an error logged in the logs.

Below is the error message logged for an invalid integer value:

```
Level: ERROR    Message: Invalid Transaction Days value provided. Number
Format Exception: For inputstring: "30.5"
Level: ERROR    Message: Performing reconciliation with Transaction days =
0
```

Below is the error message logged for a negative integer value:

```
Level: ERROR    Message: Transaction Days value cannot be -ve
Level: ERROR    Message: Performing reconciliation with Transaction days =
0
```

2. Why is the following error encountered while running the Connector Server in SSL=True mode?

```
java.security.InvalidKeyException: The security strength of SHA-1 digest
algorithm is not sufficient for this key size
```

**Answer:** connectorserver.keyStore will carry a value of identity keystore which will be generated using the Java\_home used by your connector server using the below command:

```
$CONNECTOR_SERVER_JAVA_HOME/jre/bin/keytool -genkey {-alias ALIAS} {-keyalg
KEYALG} {-keysize KEYSIZE} {-sigalg SIGALG} [-dname DNAME] [-keypass
KEYPASS] {-validity VAL_DAYS} {-storetype STORETYPE} {-keystore KEYSTORE} [-
storepass STOREPASS
```

**For example:** JAVA\_HOME/jre/bin/keytool -genkey -alias javaconnectorserver -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -dname "CN=localhost, OU=Identity, O=Oracle Corporation,C=US" -keypass weblogic1 -keystore javaconnectorserver.jks -storepass weblogic1

3. Why is the value for few attributes blank when you reconcile an inactive worker with future effective hire date?

**Answer:** A worker in the Workday system would be in an inactive state if the worker is hired with a future effective date. While we try to reconcile, attributes like Manager Login, Supervisory Organization, Cost Center, Title, Address, City, State, Country and Postal



Code attributes will be not be reconciled. The worker must be reconciled again after the worker is active to fetch these attributes.

4. Can we update or reconcile primary contact details with visibility as Private?

**Answer:** Workday Connector supports primary contact data through parent form and with default visibility type as Public. This means that you can update or reconcile primary contact details of the type Public. Workday does not support primary contact data with visibility as Private, whereas non-primary contact details with visibility of both Public and Private are supported through the child form.

For example, when you add the Work Email attribute in the parent form, in Workday it gets updated in the Work Contact information with Type as Primary and Visibility as Public.

5. Why is the following error encountered when you reconcile phone numbers having more than 20 characters including country code and extension in the Trusted application mode?

```
value too large for column "DEV00_OIM"."USR"."USR_HOME_PHONE" (actual: 21, maximum: 20)
```

**Answer:** It is recommended to increase the size of attributes when you face such errors.

6. What are supported range of values for the Page Count attribute in Advance Settings?

**Answer:** Workday supports page count between the range of 1 to 999.

7. What is the significance of Timezone attribute in Advance Settings?

**Answer:** The Timezone attribute represents the timezone of the Workday system. While performing incremental reconciliation, the sync token is updated as per the provided timezone value. Similarly, Start Date (Hire Date) and End Date (Termination Date) attributes are updated as per the provided Workday timezone.

# 10

## Troubleshooting the Connector

This is a solution to a problem you might encounter while using the Workday connector.

**Table 10-1 Troubleshooting the Workday Connector**

Problem	Solution
<p>OIG Users are not created after running the Workday User Trusted Recon scheduled job. The following message is displayed in the reconciliation event generated for the user:</p> <pre>'Data Validation Failed' as the current status and 'Invalid ManagerLogin : &lt;Manager ID&gt;' as Note.</pre>	<p>This issue is encountered due to the dependency of manager information of users. OIG User creation fails if the manager of the user is not already present in Oracle Identity Governance. To fix this issue, you must remove the manager field mapping, run the Workday User Trusted Recon scheduled job, and then add back the manager field mapping as follows:</p> <p>In Identity Self Service, remove the Manager field mapping as follows:</p> <ol style="list-style-type: none"><li>1. Log in to Identity Self Service.</li><li>2. Search for and open the Authoritative application corresponding to your target system for editing. For example, search for the <b>Workday</b> application.</li><li>3. From the Schema page, uncheck the <b>Manager Login</b> reconciliation mapping.</li><li>4. Apply changes.</li></ol> <p>Run the Workday User Trusted Recon scheduled job.</p> <p>In Identity Self Service, add the manager field mapping as follows:</p> <ol style="list-style-type: none"><li>1. Log in to Identity Self Service.</li><li>2. Search for and open the Authoritative application corresponding to your target system for editing. For example, search for the <b>Workday</b> application.</li><li>3. From the Schema page, select the <b>Manager Login</b> reconciliation mapping checkbox.</li><li>4. Apply changes.</li></ol> <p>Set the value of the Sync Token parameter to <code>&lt;String&gt;0&lt;/String&gt;</code> in the Workday Trusted User Reconciliation scheduled job and then run it.</p>

# A

## Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the Workday connector.

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

File in the Installation Package	Description
/bundle/org.identityconnectors.workday-12.3.0	This JAR is the ICF connector bundle.
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 Oracle Identity database. <b>Note:</b> A <b>resource bundle</b> is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
xml/Workday-auth-template.xml	This file contains definitions for the connector objects required for creating an Authoritative application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/Workday-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.
xml/Workday-preconfig.xml	This XML file contains definitions for the User Metadata and Lookups. Below are the User Metadata and Lookups: <ul style="list-style-type: none"><li>• Lookup.Workday.CountryCode</li><li>• Lookup.Workday.BooleanValues</li><li>• Lookup.Workday.DeviceType</li><li>• Lookup.Workday.PhoneType</li><li>• usr_udf_workdayguid</li></ul>