

Oracle® Identity Governance

Configuring the Salesforce Application



12c (12.2.1.3.0)

F12377-05

October 2021

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

ORACLE®

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

F12377-05

Copyright © 2018, 2021, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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

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

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

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

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

Oracle, 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	ix

What's New In This Guide?

Software Updates	x
Documentation-Specific Updates	xi

1 About the Salesforce Connector

1.1	Certified Components	1-2
1.2	Usage Recommendation	1-3
1.3	Certified Languages	1-3
1.4	Supported Connector Operations	1-4
1.5	Connector Architecture	1-4
1.6	Supported Use Cases	1-6
1.7	Supported Connector Features Matrix	1-7
1.8	Connector Features	1-8
1.8.1	Support for Full Reconciliation	1-8
1.8.2	Support for Limited Reconciliation	1-8
1.8.3	Transformation and Validation of Account Data	1-9
1.8.4	Support for Cloning Applications and Creating Instance Applications	1-9
1.8.5	Secure Communication to the Target System	1-9
1.8.6	Support for the Connector Server	1-9

2 Creating an Application by Using the Salesforce Connector

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

2.2.2	Registering a Client Application	2-3
2.3	Creating an Application By Using the Connector	2-4

3 Configuring the Salesforce Connector

3.1	Basic Configuration Parameters	3-1
3.2	Advanced Settings Parameters	3-3
3.3	Attribute Mappings	3-9
3.3.1	Attribute Mappings for a Target Application	3-9
3.3.2	Attribute Mappings for an Authoritative Application	3-13
3.4	Rules, Situations, and Responses	3-15
3.4.1	Rules, Situations, and Responses for a Target Application	3-15
3.4.2	Rules, Situations, and Responses for an Authoritative Application	3-17
3.5	Reconciliation Jobs	3-19

4 Performing Postconfiguration Tasks for the Salesforce Connector

4.1	Configuring Oracle Identity Governance	4-1
4.1.1	Creating and Activating a Sandbox	4-1
4.1.2	Creating a New UI Form	4-2
4.1.3	Publishing a Sandbox	4-2
4.1.4	Creating an Application Instance	4-2
4.1.5	Updating an Existing Application Instance with a New Form	4-3
4.2	Harvesting Entitlements and Sync Catalog	4-3
4.3	Managing Logging	4-4
4.3.1	Understanding Log Levels	4-4
4.3.2	Enabling Logging	4-5
4.4	Configuring the IT Resource for the Connector Server	4-6
4.5	Localizing Field Labels in UI Forms	4-8
4.6	Configuring SSL for the Connector	4-10
4.7	Obtaining GUID of Roles	4-11

5 Using the Salesforce Connector

5.1	Configuring Reconciliation	5-1
5.1.1	Performing Full Reconciliation	5-1
5.1.2	Performing Limited Reconciliation	5-1
5.1.3	Reconciling Large Number of Records	5-2
5.2	Configuring Provisioning	5-3
5.2.1	Guidelines on Performing Provisioning Operations	5-3
5.2.2	Performing Provisioning Operations	5-3
5.3	Scheduled Job for Reconciliation of Groups	5-4

5.4	Configuring Reconciliation Jobs	5-5
5.5	Uninstalling the Connector	5-5

6 Extending the Functionality of the Salesforce Connector

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

7 Upgrading the Salesforce Connector

7.1	Preupgrade Steps	7-1
7.2	Upgrade Steps for CI Installation	7-2
7.3	Upgrade Steps for AOB	7-2
7.4	Postupgrade Steps for CI Installation	7-4
7.5	Post upgrade steps for AOB	7-5
7.6	Salesforce Upgrade Script for AOB	7-6

8 Known Issues and Limitations

Part I Appendices

A Appendix

A.1	Files and Directories in the Salesforce Connector Package	A-1
-----	---	-----

List of Figures

1-1	Salesforce Connector Architecture	1-5
1-2	Manage Roles, Groups, and Profiles to Control Access by the User	1-7
2-1	Overall Flow of the Process for Creating an Application By Using the Connector	2-2
3-1	Default Attribute Mappings for a Salesforce Target User Account	3-11
3-2	Simple Correlation Rule for a Salesforce Authoritative Application	3-18
4-1	Manage IT Resource Page for Connector Server IT Resource	4-7
4-2	Edit IT Resource Details and Parameters Page for the Connector Server IT Resource	4-7

List of Tables

1-1	Certified Components	1-2
1-2	Supported Connector Operations	1-4
1-3	Supported Connector Features Matrix	1-7
3-1	Parameters in the Basic Configuration	3-1
3-2	Advanced Settings Parameters for a Salesforce Target and Authoritative Application	3-3
3-3	Default Attributes Mappings for Salesforce User Account	3-10
3-4	Default Attribute Mappings for Groups	3-12
3-5	Default Attributes for Territory Entitlement	3-12
3-6	Default Attributes for Permission Sets Entitlement	3-13
3-7	Default Attributes for a Salesforce Authoritative Application	3-14
3-8	Predefined Identity Correlation Rule for a Salesforce Target Application	3-16
3-9	Predefined Situations and Responses for a Salesforce Target Application	3-16
3-10	Predefined Identity Correlation Rule for a Salesforce Authoritative Application	3-17
3-11	Predefined Situations and Responses for a Salesforce Authoritative Application	3-18
3-12	Parameters of the Target User Reconciliation Job	3-19
3-13	Parameters of the Authoritative User Reconciliation Job	3-20
3-14	Parameters of the Reconciliation Jobs for Entitlements	3-20
4-1	Log Levels and ODL Message Type:Level Combinations	4-4
4-2	Parameters of the IT Resource for the Salesforce Connector Server	4-7
5-1	Attributes of the Salesforce Group Recon Scheduled Job	5-4
A-1	Files and Directories in the Connector Installation Package	A-1

Preface

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

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

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

Related Documents

For information about installing and using Oracle Identity Governance 12.2.1.4.0, visit the following Oracle Help Center page:

<https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/index.html>

For information about installing and using Oracle Identity Governance 12.2.1.3.0, visit the following Oracle Help Center page:

<https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.3/index.html>

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

<https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html>

For information about Oracle Identity Manager Connectors 11.1.1 documentation, visit the following Oracle Help Center page:

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

Conventions

The following text conventions are used in this document:

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

What's New In This Guide?

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

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

- [Software Updates](#)

This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.
- [Documentation-Specific Updates](#)

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

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

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

Software Updates in Release 12.2.1.3.1

The following is the software update in release 12.2.1.3.1:

Support for Salesforce REST API

From this release onwards, the Connector is redesigned to use the Salesforce REST API's. In the previous releases, the Connector used is the SCIM based API's to connect to the target system and perform connector operations. The SCIM based Salesforce connector 12.2.1.3.0 has limitation with custom attributes and lookup. From this release onward, REST API's will overcome the SCIM API's limitations.

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 updates have been made in revision "3" of this guide:

- A Note on using the Salesforce-12.2.1.3.0A patch has been added to [Configuring Salesforce](#) .

The following documentation-specific updates have been made in revision "2" of this guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row of [Certified Components](#) has been updated to include support for Oracle Identity Governance release 12c PS4 (12.2.1.4.0).
- Some editorial corrections have been made.

1

About the Salesforce Connector

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

The Salesforce connector lets you create and on board Salesforce applications in Oracle Identity Governance.

Note:

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

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Oracle Identity Self Service. This capability lets business users to on board 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 on board your applications quickly and easily using only a single and simplified UI. Application on boarding is the process of registering or associating an application with Oracle Identity Governance and making that application available for provisioning and reconciliation of user information.


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

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

1.1 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	<p>You can use any one of the following releases:</p> <ul style="list-style-type: none"> • Oracle Identity Governance release 12c PS4 (12.2.1.4.0) or later • Oracle Identity Governance 12c (12.2.1.3.0) or later 	<p>You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance:</p> <ul style="list-style-type: none"> • Oracle Identity Governance release 12c PS4 (12.2.1.4.0) or later • Oracle Identity Governance 12c (12.2.1.3.0) or later • Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>Ensure that you download and apply the patch 25323654 from My Oracle Support. Failing to apply this patch prevent you from successfully testing connection between Oracle Identity Governance and your target system.</p> </div>	
Target Systems	Salesforce Winter 2012 and later releases	Salesforce Winter 2012 and later releases
Connector Server JDK	JDK 1.8.0_131 and later, or JRockit JDK 1.8.0_131 and later	JDK 1.8.0_131 and later
Connector Server	11.1.2.1.0 or 12.2.1.3.0	11.1.2.1.0 or 12.2.1.3.0

1.2 Usage Recommendation

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

- 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.
- If you are using any of the Oracle Identity Manager releases listed in the “Requirement for CI-Based Connector” column in [Table 1-1](#), then use the 11.1.2.3.0 version of the connector. If you want to use the 12.2.1.x version of this connector, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance 12c (12.2.1.3.0) or later.

 **Note:**

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

1.3 Certified Languages

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- French (Canadian)
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean

- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.4 Supported Connector Operations

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

Table 1-2 Supported Connector Operations

Operation	Supported
User Management	
Create user	Yes
Update user	Yes
Delete user	Yes
Note: The target does not support the Delete operation, and so the Delete operation from Oracle Identity Governance disables the user on the target.	
Group Management	
Create group	Yes
Remove group	Yes
Group Grant Management	
Add, Remove	Yes
Territory Grant Management	
Add, Remove	Yes
Permission set Grant Management	
Add, Remove	Yes

1.5 Connector Architecture

You can configure the Salesforce connector to run in the Target (or account management) and Authoritative (or trusted) mode, and is implemented using the Identity Connector Framework (ICF) component.

The ICF is a component that is required in order 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.

The connector is configured 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:

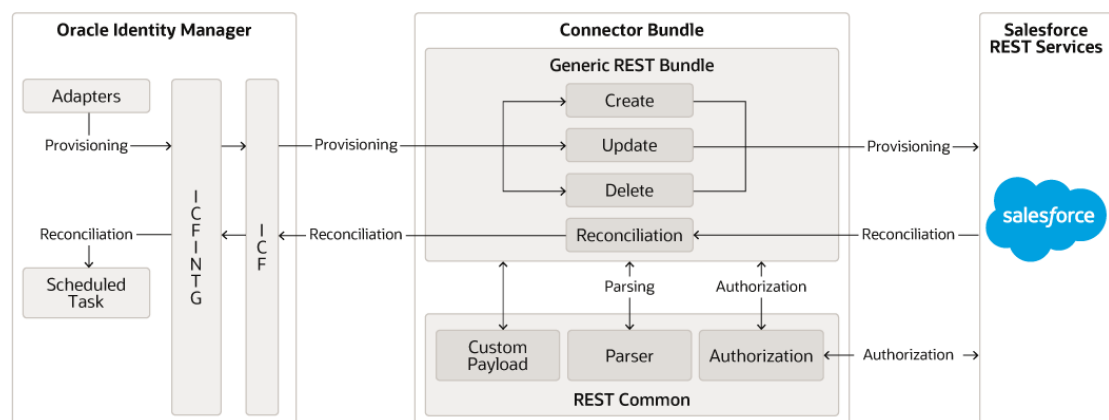
- **Provisioning**

Provisioning involves creating or updating users on the target system through Oracle Identity Governance. When you allocate (or provision) a Salesforce resource to the OIM User, the operation results in the creation of an account on Salesforce for that user. In the Oracle Identity Governance context, the term provisioning also covers updates made to the target system account through Oracle Identity Governance.

- **Target resource reconciliation**

In target resource reconciliation, data related to the newly created and modified target system accounts can be reconciled and linked with existing OIM Users and provisioned resources. A scheduled task is used for reconciliation. Salesforce.com provides the details of only the active user accounts.

Figure 1-1 Salesforce Connector Architecture



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

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

Identity Connector Framework (ICF) is a component that is required in order to use Identity Connectors. ICF is distributed together with Oracle Identity Governance. You do not need to configure or modify ICF.

During provisioning, the Adapters invoke ICF operation, ICF in turn invokes create operation on Salesforce Identity Connector Bundle and then the bundle calls Salesforce Provisioning API. The Salesforce provisioning 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 ICF operation, ICF in turn invokes create operation on Salesforce Identity Connector Bundle and then the bundle calls Salesforce Reconciliation API. 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.

1.6 Supported Use Cases

These are common scenarios in which the connector can be used.

- **Salesforce License Management**

On Salesforce.com, Profiles are used to manage licenses which are in turn associated with user types. So for a particular user type, there is a fixed set of profiles. Using the Salesforce connector, you can reconcile all the profiles from Salesforce and assign them to users without worrying about the user types. Thus, switching the user from one license type to another is accomplished easily with the use of the Salesforce connector. This will arise if one Chatter Free user is promoted to Standard user in Salesforce and can enjoy the privileges that come along with those predefined licenses.

Salesforce Connector is also used to enable specific Salesforce.com profiles for your users, you must choose one profile for each user. A profile is a template that contains a collection of predefined settings and can determine what a user can see and do within the platform. The basic rule of Profiles is whether a given user can see and use each application as well as each tab within the application.

- **One Stop Identity Solution for Multiple Cloud Applications**

Salesforce.com can act as a trusted source of identities which can be used to map users against various target cloud applications. In this case, a user from Salesforce can be created in any and every cloud and non-cloud applications that Oracle Identity Governance supports.

Salesforce.com can be used as a trusted source and an organization can use this feature to provide the list of users and further provision the account of these users to a third-party application that has been configured as target source.

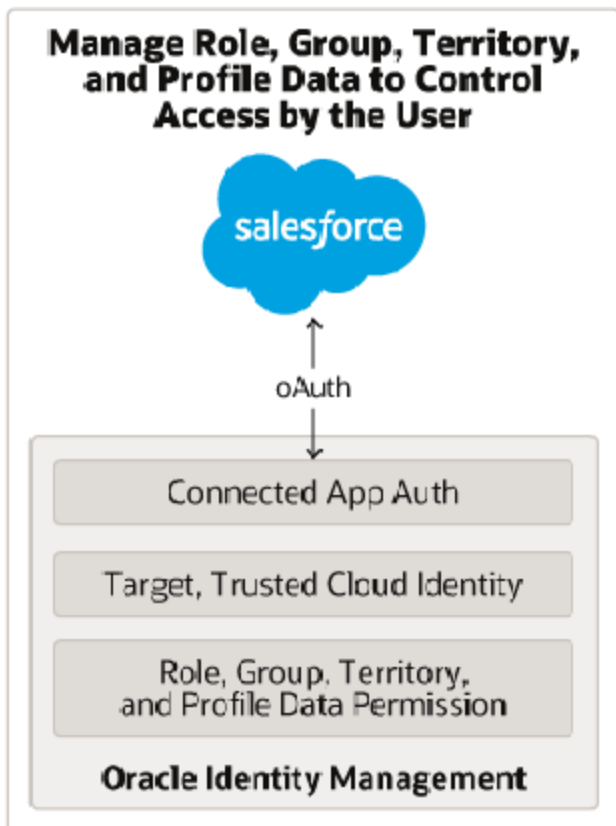
- **Evolve Identity and Data Security of Salesforce Beyond the Parameter**

Identity management solutions must support more than the traditional parameter-based authentication, and offer a single, simple, and trusted way to manage authentication and authorization of salesforce-based authentications. Enterprises making use of various IT systems (servers, devices, applications etc.) face

numerous challenges due to the proliferation of passwords. Any vulnerability for password creates an opportunity for an attacker to acquire password values and consequently impersonate users. Oracle Salesforce Connector helps reduce administrative and help desk costs by enabling self-service password reset and password change.

This following image illustrates about controlling the access that the user has by managing Roles, Groups and Profiles.

Figure 1-2 Manage Roles, Groups, and Profiles to Control Access by the User



1.7 Supported Connector Features Matrix

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

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Perform Full Reconciliation	Yes	Yes
Perform Limited Reconciliation	Yes	Yes
Configure validation and transformation of account data	Yes	Yes

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

Feature	AOB Application	CI-Based Connector
Support multiple instances and multiple versions of the target system	Yes	Yes
Use connector server	Yes	Yes
Provide secure communication to the target system through SSL	Yes	Yes

1.8 Connector Features

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

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

1.8.1 Support for Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance. After you deploy the connector, you must first perform full reconciliation. A default filter is present in the Full Reconciliation Scheduled Job. This is the default filter which needs to be present while performing full user reconciliation.

If you want to get the frozen users in the Full Reconciliation Scheduled Job use the below Filter ValueFor frozen users:

```
WHERE+Id+IN+(SELECT+UserId+FROM+UserLogin+WHERE+IsFrozen=false)
```

For more information, see [Performing Full Reconciliation](#).

1.8.2 Support for Limited Reconciliation

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

To limit or filter the records that are fetched into Oracle Identity Governance during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled. See [Performing Limited Reconciliation](#).

1.8.3 Transformation and Validation of Account Data

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

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

1.8.4 Support for Cloning Applications and Creating Instance Applications

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

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

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

1.8.5 Secure Communication to the Target System

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

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

See [Configuring SSL for the Connector](#).

1.8.6 Support for the Connector Server

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

A Java connector server is useful when you do not 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*.

2

Creating an Application by Using the Salesforce Connector

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

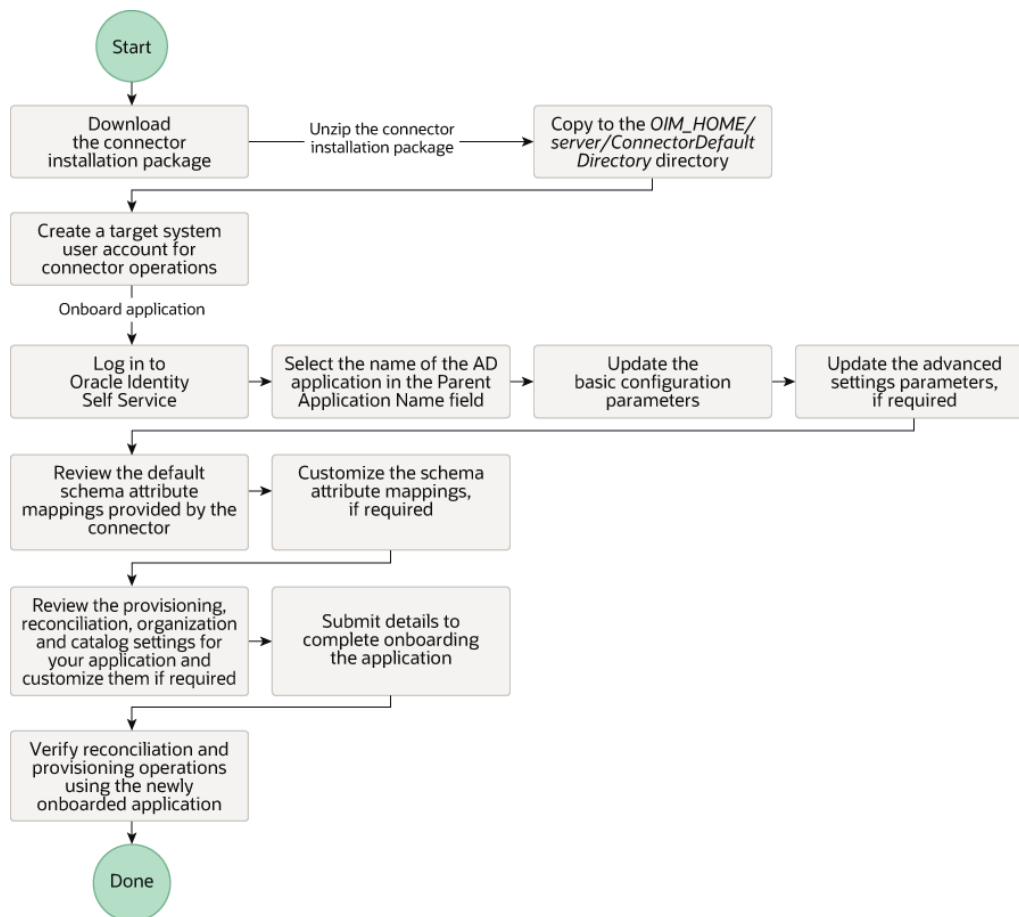
- [Process Flow for Creating an Application By Using the Connector](#)
- [Prerequisites for Creating an Application By Using the Connector](#)
- [Creating an Application By Using the Connector](#)

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 the Connector

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

- [Downloading the Connector Installation Package](#)
- [Registering a Client Application](#)

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 Registering a Client Application

Registering a client application (that is, the Salesforce connector) with the target system is a step that is performed to obtain the client ID and client secret for authenticating to the target system. It also involves creating a custom profile and an account in the target system that the connector (or client) can use for performing connector operations.

Registering a client application involves performing the following tasks on the target system:



Note:

The detailed instructions for performing these preinstallation tasks are available in the Salesforce documentation.

1. Register your client application with the target system by creating a Connected App in Salesforce. While creating the Connected App, ensure to select the OAuth scopes in the following table which represent the operations that can be performed through the Connected App you can configure. After the Connected App is created, note down the client ID and client secret values.

OAuth Scope	Description
Access your basic information (id, profile, email, address, phone).	This scope allows access to the Identity URL service.
Access and manage your data (api)	This scope allows access to the logged-in user's account using APIs, such as SCIM API and REST API. This value also includes chatter_api, which allows access to Chatter REST API resources.
Full access (full)	Allows access to all data accessible by the logged-in user, and encompasses all other scopes. full does not return a refresh token. You must explicitly request the refresh_token scope to get a refresh token.

The consumer key and consumer secret values for the Connected App are generated.

2. Note down the consumer key and consumer secret values as they are required while configuring the IT resource parameters. The consumer key corresponds to the `clientId` parameter while the consumer secret corresponds to the `clientSecret` parameter.
3. Create a custom profile by cloning a standard user profile with the following minimum set of administrative permissions:
 - API Enabled

- API Only User
 - Assign Permission Sets
 - Chatter Internal User
 - Manage Internal Users
 - Manage IP Addresses
 - Manage Login Access Policies
 - Manage Package Licenses
 - Manage Password Policies
 - Manage Profiles and Permission Sets
 - Manage Roles
 - Manage Sharing
 - Manage Unlisted Groups
 - Manage Users
 - Moderate Chatter
 - Reset User Passwords and Unlock Users
 - View All Users
 - View Help Link
 - View Setup and Configuration
4. Create a target system user account to connect to the target system during each connector operation.

2.3 Creating an Application By Using the Connector

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

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

 **Note:**

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

1. Create an application in Identity Self Service. The high-level steps are as follows:
 - a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
 - b. Ensure that the **Connector Package** option is selected when creating an application.

- c. Update the basic configuration parameters to include connectivity-related information.
- d. If required, update the advanced setting parameters to update configuration entries related to connector operations.
- e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.
- f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.
- g. Review the details of the application and click **Finish** to submit the application details.

The application is created in Oracle Identity Governance.

- h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.

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

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



See Also:

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

3

Configuring the Salesforce Connector

While creating an application, you must configure connection-related parameters that the connector uses to connect Oracle Identity Governance with your target system and perform connector operations.

In addition, you can view and edit attribute mappings between the process form fields in Oracle Identity Governance and target system columns, predefined correlation rules, situations and responses, and reconciliation jobs.

- [Basic Configuration Parameters](#)
- [Advanced Settings Parameters](#)
- [Attribute Mappings](#)
- [Rules, Situations, and Responses](#)
- [Reconciliation Jobs](#)

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to a Target or an Authoritative application.



Note:

- The parameters in the table are applicable to both target and authoritative applications.

Table 3-1 Parameters in the Basic Configuration

Parameter	Mandatory	Description
authenticationServerUrl	No	URL of the authentication server that validates the client ID and client secret. Sample Value: https://login.windows.net/mydomain /oauth2/token?api-version=1.0

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

Parameter	Mandatory	Description
clientId	No	<p>The client identifier (a unique string) issued by the authorization server to your domain during the registration process described in Registering a Client Application .</p> <p>Sample Value: 3MVG9d8..z.hDcPLzDHRsHcTMn1ZROdU0bpIYsbiqBgAkSQZWC.rUwzrpMxhrJKFTLUj6efbySMXz29U04ASw</p>
clientSecret	No	<p>Value used to authenticate the identity of your domain. This value is obtained while performing the procedure described in Registering a Client Application .</p> <p>Sample Value: D8871C69585BA0DE79889125DAE4AB01A3038289D7E9C9FD069F13FA7EFEC92A</p>
ConnectorServer Name	No	<p>If you are using Salesforce Connector together with the Java Connector Server, then provide the name of Connector Server IT Resource here.</p>
authenticationType	Yes	<p>This entry holds the authentication type expected by the target system in the header.</p> <p>Default Value: password</p>
Host	Yes	<p>Enter the host name or IP address of the computer hosting the target system.</p> <p>Sample Value: www.example.com</p>
Password	No	<p>Enter the password of the target system user account that you create for connector operations.</p>
sslEnabled	No	<p>If the target system requires SSL connectivity, set the value of this parameter to true. Otherwise set the value to false.</p>
proxyHost	No	<p>Enter the name of the proxy host used to connect to an external target.</p> <p>Sample Value: www.example.com.</p>
proxyPassword	No	<p>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.</p>

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

Parameter	Mandatory	Description
proxyPort	No	Enter the proxy port number. Sample Value: 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.
Username	No	Enter the user name of the target system that you create for performing connector operations.

3.2 Advanced Settings Parameters

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



Note:

Unless specified, the parameters in the table are applicable to both target and authoritative applications.

Table 3-2 Advanced Settings Parameters for a Salesforce Target and Authoritative Application

Parameter	Mandatory	Description
Any Incremental Recon Attribute Type	No	Default value: True
Bundle Name	No	This entry holds the name of the connector bundle package. Default Value: <code>org.identityconnectors.genericrest</code> Do not modify this entry.
Bundle Version	No	This entry holds the version of the connector bundle package. Default Value: 12.3.0 Do not modify this entry.
Connector Name	No	This entry holds the name of the connector class. Default Value: <code>org.identityconnectors.genericrest.GenericRESTConnector</code>

Table 3-2 (Cont.) Advanced Settings Parameters for a Salesforce Target and Authoritative Application

Parameter	Mandatory	Description
customPayload	No	<p>This entry holds the payloads for all operations that are not in the standard format.</p> <p>Default Value: "__ACCOUNT__.__GROUP__.UPDAT EOP={"UserOrGroupId": \"\$ (__UID__\$\", \"GroupId\": \"\$ (GroupId)\$ \"}", "__ACCOUNT__.__TERRITOR Y__.UPDATEOP={"UserId": \"\$ (__UID__\$ \", \"Territory2Id\": \"\$ (Territory2Id)\$ \"}", "__ACCOUNT__.__PERMISSI ONSSET__.UPDATEOP={"Assignee Id": \"\$ (__UID__\$ \", \"PermissionSetId\": \"\$ (PermissionSetId)\$\"}"</p>
jsonResourcesTag	No	<p>This entry holds the name of the JSON tag that holds user details in the response payload.</p> <p>Default Value: "__ACCOUNT__=records", "__PRO FILE__=records", "__GROUPLKP_ __=records", "__ROLE__=records ", "__TERRITORYLKP__=records" , "__PERMISSIONSETLKP__=reco rds", "__ACCOUNT__.__MEMBERSHI P__.__GROUP__=records", "__AC COUNT__.__MEMBERSHIP__.__TER RITORY__=records", "__ACCOUNT __.__MEMBERSHIP__.__PERMISSI ONSSET__=records"</p>
pageSize	No	<p>This entry holds the value of the number of records that can be retrieved from the target system in one go.</p> <p>Default Value: 200</p>
httpHeaderContentType	No	<p>This entry holds The content type of request body</p> <p>Default value: application/json</p>
httpHeaderAccept	No	<p>This entry holds the accept request-header field can be used to specify certain media types which are acceptable for the response</p> <p>Default Value: application/json</p>

Table 3-2 (Cont.) Advanced Settings Parameters for a Salesforce Target and Authoritative Application

Parameter	Mandatory	Description
nameAttributes	Yes	<p>This is the <code>__NAME__</code> attribute mapping of Oracle Identity Governance to the relevant attribute on target system.</p> <p>Default Value: <code>"__ACCOUNT__.Username", "__GROUP__.Name", "__TERRITORY__.Name", "__PERMISSIONSET__.Label", "__PROFILE__.Name", "__ROLE__.Name", "__GROUPLKP__.Name", "__TERRITORYLKP__.Name", "__PERMISSIONSETLKP__.Label"</code></p>
opTypes	No	<p>This entry holds Target supported HTTP operations for each attribute in each object class, it will take default value if this detail is not given.</p> <p>Default value: <code>"__ACCOUNT__.CREATEOP=POST", "__ACCOUNT__.UPDATEOP=PATCH", "__ACCOUNT__.__PASSWORD__.UPDATEOP=POST", "__ACCOUNT__.SEARCHOP=GET", "__ACCOUNT__.TESTOP=GET", "__ACCOUNT__.__GROUP__.UPDATEOP=POST", "__ACCOUNT__.__TERRITORY__.ADDATTRIBUTE=POST", "__ACCOUNT__.__PERMISSIONSET__.ADDATTRIBUTE=POST"</code></p>
passwordAttributes	No	<p>This entry holds the name of the target system attribute that is mapped to the <code>__PASSWORD__</code> attribute of the connector in OIG.</p> <p>Default Value: <code>NewPassword</code></p>

Table 3-2 (Cont.) Advanced Settings Parameters for a Salesforce Target and Authoritative Application

Parameter	Mandatory	Description
relURIs	Yes	<p>This entry holds the list of relative URI's</p> <p>Default value: "__ACCOUNT__.CREATEOP=/services/data/v50.0/subjects/User", "__ACCOUNT__.UPDATEOP=/services/data/v50.0/subjects/User/\$(__UID__\$", "__ACCOUNT__.__PASSWORD__.UPDATEOP=/services/data/v50.0/subjects/User/\$(__UID__\$/password", "__ACCOUNT__.SEARCHOP=/services/data/v50.0/query/?q=SELECT+UserName,id,LastName,FirstName,Email,ProfileId,Alias,TimeZoneSidKey,LocaleSidKey,EmailEncodingKey,LanguageLocaleKey,UserRoleId,ManagerId,IsActive,Fax,Phone,MobilePhone+from+User+\$(FilterSuffix)\$+LIMIT+\$(PAGE_SIZE)\$+OFFSET+\$(PAGE_OFFSET)\$", "__GROUPLKP__.__SEARCHOP=/services/data/v50.0/query/?q=SELECT+Name,id+from+Group+Where+Type+=+'Regular'+OR+Type+=+'Queue'+LIMIT+\$(PAGE_SIZE)\$+OFFSET+\$(PAGE_OFFSET)\$", "__TERRITORYLKP__.__SEARCHOP=/services/data/v50.0/query/?q=SELECT+Id,Name+from+Territory2+LIMIT+\$(PAGE_SIZE)\$+OFFSET+\$(PAGE_OFFSET)\$", "__PERMISSIONSETLKP__.__SEARCHOP=/services/data/v50.0/query/?q=SELECT+Id,label+from+PermissionSet+Where+PermissionSet.Profile.Name+=+null+LIMIT+\$(PAGE_SIZE)\$+OFFSET+\$(PAGE_OFFSET)\$", "__ACCOUNT__.__GROUP__.__SEARCHOP=/services/data/v50.0/query/?q=SELECT+GroupId+From+GroupMember+Where+UserOrGroupId+=+'\$(__UID__\$'", "__ACCOUNT__.__</p>

Table 3-2 (Cont.) Advanced Settings Parameters for a Salesforce Target and Authoritative Application

Parameter	Mandatory	Description
		<pre> PERMISSIONSET___.SEARCHOP=/ services/data/v50.0/query/? q=SELECT+PermissionSetId+FRO M+PermissionSetAssignment+Wh ere+Assignee.Id+=+'\$ (__UID__\$'+AND+PermissionSe t.Profile.Name+=+null", "__AC COUNT___.__TERRITORY___.SEARC HOP=/services/data/v50.0/ query/? q=SELECT+Territory2Id+from+U serTerritory2Association+Whe re+UserId+=+'\$ (__UID__\$' ", "__PROFILE___.SE ARCHOP=/services/data/v50.0/ query/? q=SELECT+Id,Name+from+Profil e+LIMIT+\$(PAGE_SIZE)\$ +OFFSET+\$ (PAGE_OFFSET)\$", "__ACCOUNT__ __.__GROUP__=/services/data/ v36.0/subjects/ GroupMember", "__ACCOUNT___.__ MEMBERSHIP___.__GROUP___.SEARC HOP=/services/data/v50.0/ query/? q=SELECT+Id+from+GroupMember +WHERE+GroupId+=+'\$ (__GROUP__.Id)\$'+AND+UserOrG roupId+=+'\$ (__UID__\$' ", "__ACCOUNT___.__ GROUP___.DELETEOP=/services/ data/v50.0/subjects/ GroupMember/\$ (__MEMBERSHIP__.Id)\$", "__ACC OUNT___.__TERRITORY__=/ services/data/v50.0/ subjects/ UserTerritory2Association", " __ACCOUNT___.__MEMBERSHIP___.__ __TERRITORY___.SEARCHOP=/ services/data/v50.0/query/? q=SELECT+Id+from+UserTerrito ry2Association+WHERE+Territo ry2Id+=+'\$ (__TERRITORY__.Id)\$'+AND+Use rId+=+'\$ (__UID__\$' ", "__ACCOUNT___.__ TERRITORY___.DELETEOP=/ services/data/v50.0/ subjects/ </pre>

Table 3-2 (Cont.) Advanced Settings Parameters for a Salesforce Target and Authoritative Application

Parameter	Mandatory	Description
		<p>UserTerritory2Association/\$ (__MEMBERSHIP__.Id)\$", "__ACCOUNT___.__PERMISSIONSET__=/services/data/v36.0/subjects/PermissionSetAssignment", "__ACCOUNT___.__MEMBERSHIP___.__PERMISSIONSET___.SEARCHOP=/services/data/v50.0/query/?q=SELECT+Id+from+PermissionSetAssignment+WHERE+PermissionSetId+=+'\$ (__PERMISSIONSET__.Id)\$'+AND+Assignee.Id+=+'\$ (__UID__)\$'", "__ACCOUNT___.__PERMISSIONSET___.DELETEOP=/services/data/v50.0/subjects/PermissionSetAssignment/\$ (__MEMBERSHIP__.Id)\$", "__ROLE___.SEARCHOP=/services/data/v50.0/query/?q=SELECT+Id,+Name+from+UserRole"</p>
specialAttributeHandling	No	<p>This entry holds Value that will represent how to send values of the corresponding special attribute to the target, Ex: SINGLE, if no value is given it means it will consider default, i.e it will send all values to the target</p> <p>Default value: "__ACCOUNT___.__GROUP___.CREATEOP=SINGLE", "__ACCOUNT___.__GROUP___.UPDATEOP=SINGLE", "__ACCOUNT___.__PERMISSIONSET___.ADDATTRIBUTE=SINGLE", "__ACCOUNT___.__PERMISSIONSET___.REMOVEATTRIBUTE=SINGLE", "__ACCOUNT___.__TERRITORY___.ADDATTRIBUTE=SINGLE", "__ACCOUNT___.__TERRITORY___.REMOVEATTRIBUTE=SINGLE"</p>
specialAttributeTargetFormat	No	<p>This entry holds format of special attribute in target</p> <p>Default Value: "__ACCOUNT___.__GROUP__=records", "__ACCOUNT___.__TERRITORY__=records", "__ACCOUNT___.__PERMISSIONSET__=records"</p>

Table 3-2 (Cont.) Advanced Settings Parameters for a Salesforce Target and Authoritative Application

Parameter	Mandatory	Description
statusAttributes	No	This is the <code>__ENABLE__</code> attribute mapping of Oracle Identity Governance to the Status attribute on target system. Default Value: <code>"__ACCOUNT__.IsActive"</code>
uidAttributes	Yes	This is the <code>__UID__</code> attribute mapping of Oracle Identity Governance to the GUID attribute on target system. Default Value: <code>"__ACCOUNT__.Id", "__GROUP__.GroupId", "__TERRITORY__.Territory2Id", "__PERMISSIONSET__.PermissionSetId", "__PROFILE__.Id", "__ROLE__.Id", "__GROUPLKP__.Id", "__TERRITORYLKP__.Id", "__PERMISSIONSETLKP__.Id", "__PROFILE__.Id"</code>

3.3 Attribute Mappings

The attribute mappings on the Schema page vary depending on whether you are creating a target application or a trusted application.

The following sections provides details for creating a target application or a trusted application:

- [Attribute Mappings for the Salesforce Target Application](#)
- [Attribute Mappings for an Authoritative Application](#)

3.3.1 Attribute Mappings for a Target Application

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

Default Attributes for Salesforce User Account

[Default Attributes for Salesforce User Account](#) lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and the Salesforce 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 3-3 Default Attributes Mappings for Salesforce User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field	Key Field?	Case Insensitive?
Profile Name	ProfileId	String	No	Yes	Yes	No	Not applicable
User Name	__NAME_	String	Yes	Yes	Yes	No	Not applicable
Last Name	LastName	String	Yes	Yes	Yes	No	Not applicable
Email	Email	String	Yes	Yes	Yes	No	Not applicable
First Name	FirstName	String	No	Yes	Yes	No	Not applicable
Id	__UID__	String	No	Yes	Yes	Yes	Yes
Password	__PASSW ORD__	String	No	Yes	No	No	Not applicable
TimeZone	TimeZone SidKey	String	Yes	Yes	Yes	No	Not applicable
Role Name	UserRoleI d	String	No	Yes	Yes	No	Not applicable
Manager	ManagerI d	String	No	Yes	Yes	No	Not applicable
Alias	Alias	String	Yes	Yes	Yes	No	Not applicable
LocaleSid Key	LocaleSid Key	String	Yes	Yes	Yes	No	Not applicable
EmailEnc odingKey	EmailEnc odingKey	String	Yes	Yes	Yes	No	Not applicable
Language LocaleKey	Language LocaleKey	String	Yes	Yes	Yes	No	Not applicable
Phone	Phone	String	No	Yes	Yes	No	Not applicable
Fax	Fax	String	No	Yes	Yes	No	Not applicable
Mobile	MobilePho ne	String	No	Yes	Yes	No	Not applicable
IsActive	IsActive	String	No	Yes	Yes	No	Not applicable
Status	__ENABL E__	String	No	No	Yes	No	Not applicable
IT Resource Name		Long	No	No	Yes	No	Not applicable

[Default Attributes for Salesforce User Account](#) shows the default User account attribute mappings.

Figure 3-1 Default Attribute Mappings for a Salesforce 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	Id	__UID__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	UserName	__NAME__	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Last Name	LastName	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	First Name	FirstName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Email	Email	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Profile Name	ProfileId	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Alias	Alias	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	TimeZone	TimeZoneSidKey	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	LocaleSidKey	LocaleSidKey	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	EmailEncodingK	EmailEncodingKey	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	LanguageLocale	LanguageLocaleKey	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Role Name	UserRoleId	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Manager	ManagerId	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Phone	Phone	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Fax	Fax	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Mobils	MobilePhone	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	IsActive	IsActive	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Status	__ENABLE__	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	Password	__PASSWORD__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select a value	IT Resource Nar		Long	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Default Attribute Mappings for Groups

[Default Attribute Mappings for Groups](#) lists the group attribute mappings between the process form fields in Oracle Identity Governance and the Salesforce Target application columns.

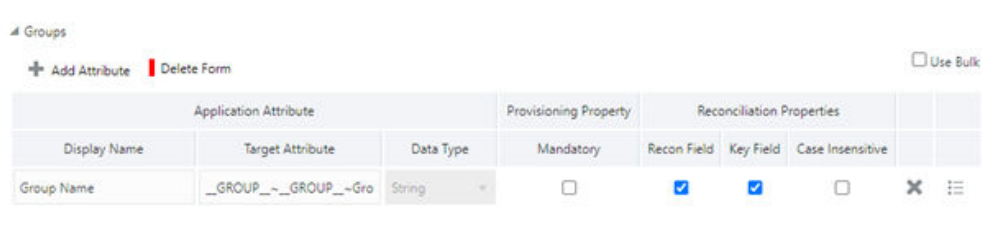
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for Groups

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive ?
Group Name	__GROUP_ ~__GROU P__~GroupI d	String	No	Yes	Yes	Not applicable

[Default Attribute Mappings for Groups](#) shows the group attributes mapping.

Default Attribute Mappings for Groups



Default Attributes for Territory Entitlement

[Default Attributes for Territory Entitlement](#) lists Territory attribute mappings the process form fields in Oracle Identity Governance and the Salesforce Target application columns.

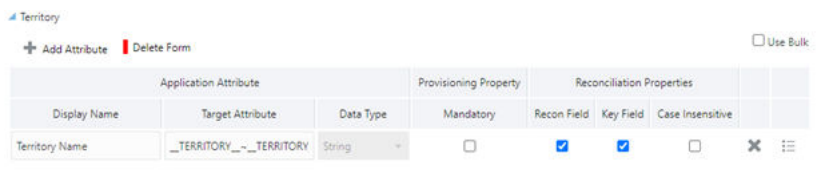
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-5 Default Attributes for Territory Entitlement

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive ?
Territory	__TERRITOR Y__~__TERR ITORY__~Te rritory2Id	String	No	Yes	Yes	Yes	Not applicable

[Default Attributes for Territory Entitlement](#) shows the default attributes for Territory entitlement.

Default Attributes for Territory Entitlement



Default Attributes for Permission Sets Entitlement

[Default Attributes for Permission Sets Entitlement](#) lists the Permission Sets attribute mappings between the process form fields in Oracle Identity Governance and the Salesforce 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 Attributes for Permission Sets Entitlement

Default Attributes for Permission Sets Entitlement	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Permission Sets	__PERMISSIONSET__~__PERMISSIONSET__~PermissionSetId	String	No	Yes	Yes	Not Applicable

Default Attributes for Permission Sets Entitlement

Application Attribute		Provisioning Property	Reconciliation Properties		
Display Name	Target Attribute	Mandatory	Recon Field	Key Field	Case Insensitive
Permission Sets	__PERMISSIONSET__~__PERM	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

3.3.2 Attribute Mappings for an Authoritative Application

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

Default Attributes for a Salesforce Authoritative Application

[Default Attributes for a Salesforce Authoritative Application](#) lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and the Salesforce Authoritative 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*.

The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form. They cannot be left blank during reconciliation. The target attribute mappings for these identity attributes are empty by default because there are no corresponding columns in the target system. Therefore, the connector provides default values

(as listed in [Default Attributes for a Salesforce Authoritative Application](#)) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

Table 3-7 Default Attributes for a Salesforce Authoritative Application

Display Name	Authoritative Attribute	Data Type	Mandatory Recon Property?	Recon Field	Case Insensitive?
Salesforce GUID	__UID__	String	No	Yes	Not applicable
User Login	__NAME__	String	No	Yes	Not applicable
First Name	FirstName	String	No	Yes	Not applicable
Last Name	LastName	String	No	Yes	Not applicable
Xellerate Type		String	No	Yes	Not applicable
Locality Name	LocaleSidKey	String	No	Yes	Not applicable
Email	Email	String	No	Yes	Not applicable
Home Phone	Phone	String	No	Yes	Not applicable
Fax	Fax	String	No	Yes	Not applicable
Mobile	MobilePhone	String	No	Yes	Not applicable
usr_locale	LanguageLocaleKey	String	No	Yes	Not applicable
Status	__ENABLE__	String	No	Yes	Not applicable
Organization Name		String	No	Yes	Not applicable
Role		String	No	Yes	Not applicable

[Default Attributes for a Salesforce Authoritative Application](#) shows the default User account attribute mappings.

Default Attributes for a Salesforce Authoritative Application

Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
User Login	__NAME__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Salesforce GUID	__UID__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
First Name	FirstName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Last Name	LastName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Email	Email	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Locality Name	LocaleSidKey	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Home Phone	Phone	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Fax	Fax	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Mobile	MobilePhone	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
usr_locale	LanguageLocaleKey	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Status	__ENABLE__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Xellerate Type		String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Role		String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕
Organization Name		String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⋮	✕

3.4 Rules, Situations, and Responses

Learn about the predefined rules, responses and situations for Target and Authoritative applications.

The connector uses these rules and responses for performing reconciliation.

- [Rules, Situations, and Responses for a Target Application](#)
- [Rules, Situations, and Responses for an Authoritative Application](#)

3.4.1 Rules, Situations, and Responses for a Target Application

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

Predefined Identity Correlation Rules

By default, the Salesforce 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.

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

Table 3-8 Predefined Identity Correlation Rule for a Salesforce Target Application

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

In the first correlation rule element:

- __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.

[Simple Correlation Rule for a Salesforce Target Application](#) shows the simple correlation rule for a Salesforce Target application.

Simple Correlation Rule for a Salesforce Target Application

The screenshot shows the configuration interface for an Identity Correlation Rule. It includes a title bar 'Identity Correlation Rule', a section to 'Choose Type of Correlation Rule' with 'Simple Correlation Rule' selected, and an 'Add Rule Element' button. Below is a table for the rule element with columns: Target Attribute, Element Operator, Identity Attribute, Case Sensitive, and Delete. The element contains: Target Attribute: __NAME__, Element Operator: Equals, Identity Attribute: User Login, Case Sensitive: No. Below the table is a 'Rule Operator' dropdown set to 'OR'.

Predefined Situations and Responses

The Salesforce 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.

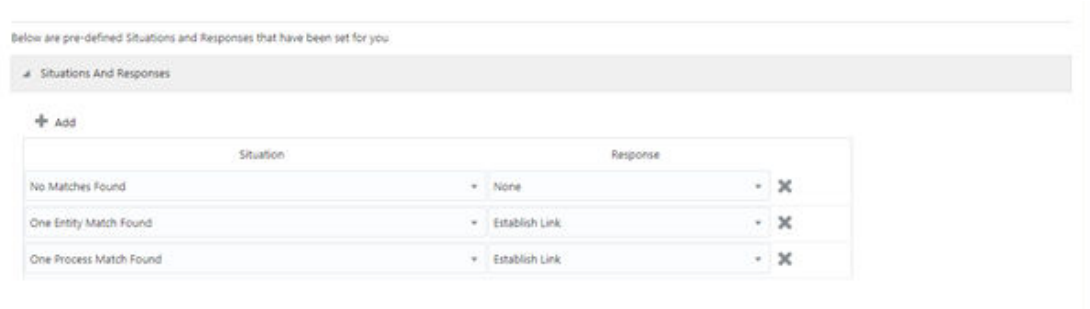
[Table 3-9](#) lists the default situations and responses for a Salesforce Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see *Creating a Target Application in Oracle Fusion Middleware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

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

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

[Predefined Situations and Responses for a Salesforce Target Application](#) shows the situations and responses for Salesforce that the connector provides by default.

Predefined Situations and Responses for a Salesforce Target Application



3.4.2 Rules, Situations, and Responses for an Authoritative Application

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

Predefined Identity Correlation Rules

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

[Predefined Identity Correlation Rule for a Salesforce Authoritative Application](#) lists the default simple correlation rule for Salesforce connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-10 Predefined Identity Correlation Rule for a Salesforce Authoritative Application

Authoritative Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No
__UID__	Equals	Salesforce GUID	No

Correlation Rule element: (__NAME__ Equals Salesforce GUID) OR (__UID__ Equals User Login)

In the first correlation rule element:

- __NAME__ is a single-valued attribute on the target system that identifies the user account.
- User Login is the unique login name of a user.

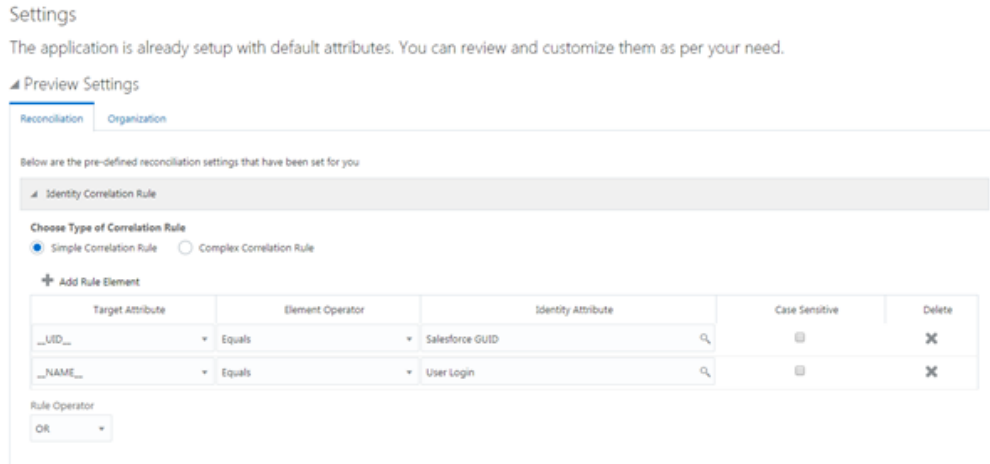
In the second correlation rule element:

- __UID__ is an attribute on the target system that uniquely identifies the user account.

- Salesforce GUID is the field on the OIG User form.
- Rule operator: OR

[Simple Correlation Rule for a Salesforce Authoritative Application](#) shows the simple correlation rule for a Salesforce Authoritative application.

Figure 3-2 Simple Correlation Rule for a Salesforce Authoritative Application



Predefined Situations and Responses

The Salesforce 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.

[Predefined Situations and Responses for a Salesforce Authoritative Application](#) lists the default situations and responses for a Salesforce 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 *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-11 Predefined Situations and Responses for a Salesforce Authoritative Application

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

[Predefined Situations and Responses for a Salesforce Authoritative Application](#) shows the situations and responses for Salesforce that the connector provides by default.

Predefined Situations and Responses for a Salesforce Authoritative Application

Below are pre-defined Situations and Responses that have been set for you

▲ Situations And Responses

+ Add

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

3.5 Reconciliation Jobs

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

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

User Reconciliation Jobs

The following reconciliation jobs are available for reconciling user data:

- Target User Reconciliation: Use this reconciliation job to reconcile user data from a Target application.
- Authoritative User Reconciliation: Use this reconciliation job to reconcile user data from an Authoritative application.

Table 3-12 Parameters of the 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 not modify this value.
Filter	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: WHERE+id+= '0057F0000082jki ' To bring frozen users: sample value: WHERE+Id+IN+ (SELECT+UserId+FROM+UserLogin+WHERE+IsFrozen=false)
Object Type	Type of object you want to reconcile. Default value: User
Scheduled Task Name	Name of the scheduled job. Note: For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.

The following table lists the parameters of the Authoritative User Reconciliation job.

Table 3-13 Parameters of the 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 not modify this value.
Filter Suffix	Enter the expression for filtering records that the scheduled job must reconcile. Sample value: WHERE+id+= '0057F0000082jki' To bring frozen users: sample value: WHERE+Id+IN+ (SELECT+UserId+FROM+UserLogin+WHERE+IsFrozen=false)
Object Type	Type of object you want to reconcile. Default Value: User
Scheduled Task Name	Name of the scheduled job. Note: For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- Salesforce Group Lookup Reconciliation
- Salesforce Profile Lookup Reconciliation
- Salesforce Territory Lookup Reconciliation
- Salesforce PermissionSet Lookup Reconciliation
- Salesforce Role Lookup Reconciliation

These reconciliation jobs are available only for a Target application. The parameters for all the reconciliation jobs are the same.

Table 3-14 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.

Table 3-14 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Lookup Name	<p>This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched.</p> <p>Depending on the reconciliation job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • For Salesforce Group Lookup Reconciliation - <code>Lookup.Salesforce.Groups</code> • For Salesforce Profile Lookup Reconciliation - <code>Lookup.Salesforce.Profiles</code> • For Salesforce Roles Lookup Reconciliation - <code>Lookup.Salesforce.Roles</code> • For Salesforce Permission Sets Lookup Reconciliation - <code>Lookup.Salesforce.PermissionSets</code> • For Salesforce Territory Lookup Reconciliation - <code>Lookup.Salesforce.Territory</code>
Object Type	<p>Enter the type of object whose values must be synchronized.</p> <p>Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> • For Salesforce Profile Lookup Reconciliation - <code>__PROFILE__</code> • For Salesforce Group Lookup Reconciliation - <code>__GROUPLKP__</code> • For Salesforce Territory Lookup Reconciliation - <code>__TERRITORYLKP__</code> • For Salesforce PermissionSets Lookup Reconciliation - <code>__PERMISSIONSETLKP__</code> • For Salesforce Role Lookup Reconciliation - <code>__ROLE__</code>
Code Key Attribute	<p>Note: Do not change the value of this attribute.</p> <p>Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute).</p> <p>Default value: <code>__UID__</code></p>
Decode Attribute	<p>Note: Do not change the value of this attribute.</p> <p>Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute).</p>

4

Performing Postconfiguration Tasks for the Salesforce Connector

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

- [Configuring Oracle Identity Governance](#)
- [Harvesting Entitlements and Sync Catalog](#)
- [Managing Logging](#)
- [Configuring the IT Resource for the Connector Server](#)
- [Localizing Field Labels in UI Forms](#)
- [Configuring SSL for the Connector](#)
- [Obtaining GUID of Roles](#)

4.1 Configuring Oracle Identity Governance

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



Note:

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

- [Creating and Activating a Sandbox](#)
- [Creating a New UI Form](#)
- [Publishing a Sandbox](#)
- [Creating an Application Instance](#)
- [Updating an Existing Application Instance with a New Form](#)

4.1.1 Creating and Activating a Sandbox

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

See [Creating a Sandbox and Activating a Sandbox](#) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

4.1.2 Creating a New UI Form

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

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

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

4.1.3 Publishing a Sandbox

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

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

4.1.4 Creating an Application Instance

Create an application instance as follows:

See *Managing Application Instances* in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

1. In the left pane of the Identity System Administration, under Configuration, click **Application Instances**. The Application Instances page appears.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Application Instance page appears.
3. Specify values for the following fields:
 - **Name:** The name of the application instance
 - **Display Name:** The display name of the application instance.
 - **Description:** A description of the application instance.
 - **Resource Object:** The resource object name. Click the search icon next to this field to search for and select **Salesforce User**.
 - **IT Resource Instance:** The IT resource instance name. Click the search icon next to this field to search for and select **Salesforce**.
 - **Form:** Select the form name (created in [Creating a New UI Form](#)).

4. Click **Save**.
The application instance is created.
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See *Managing Organizations Associated With Application Instances* in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

4.1.5 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

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

See Also:

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

4.2 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

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

See Also:

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

4.3 Managing Logging

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

The following topics provide detailed information about logging:

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

4.3.1 Understanding Log Levels

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

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

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

These message types are mapped to ODL message type and level combinations as shown in [Table 4-1](#).

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

Java Level	ODL Message Type:Level
<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>

Table 4-1 (Cont.) Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

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

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

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

4.3.2 Enabling Logging

To enable logging in the Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

- a. Add the following blocks in the file:

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

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

- b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. [Table 4-1](#) lists the supported message type and level combinations.

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

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

```
<log_handler name='Salesforce-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off' />
  <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\oim_se
rver1\logs\
  oim_server1-diagnostic-1.log' />
  <property name='format' value='ODL-Text' />
```

```

<property name='useThreadName' value='true' />
<property name='locale' value='en' />
<property name='maxFileSize' value='5242880' />
<property name='maxLogSize' value='52428800' />
<property name='encoding' value='UTF-8' />
</log_handler>

<logger name="ORG.IDENTITYCONNECTORS.GENERICREST" level="NOTIFICATION:1"
useParentHandlers="false">
  <handler name="Salesforce-handler" />
  <handler name="console-handler" />
</logger>

```

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

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

For Microsoft Windows: set WLS_REDIRECT_LOG=**FILENAME**

For UNIX: export WLS_REDIRECT_LOG=**FILENAME**

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

4. Restart the application server.

4.4 Configuring the IT Resource for the Connector Server

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



Note:

This procedure is optional and is required only when the Connector Server is being used.

To configure or modify the IT resource for the Connector Server:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see *Managing Sandboxes in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.
3. In the left pane, under Configuration, click **IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `SalesForce` and then click **Search**. [Figure 4-1](#) shows the Manage IT Resource page.

Figure 4-1 Manage IT Resource Page for Connector Server IT Resource

5. Click the edit icon corresponding to the Connector Server IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the Connector Server IT resource. [Figure 4-2](#) shows the Edit IT Resource Details and Parameters page.

Figure 4-2 Edit IT Resource Details and Parameters Page for the Connector Server IT Resource

[Table 4-2](#) provides information about the parameters of the IT resource.

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

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

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

Parameter	Description
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. If the value is zero or if no value is specified, the timeout is unlimited. Sample value: 0 (recommended value)
UseSSL	Enter <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>

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

4.5 Localizing Field Labels in UI Forms

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

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

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:
SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:
 - a. Search for the following text:

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

- b. Replace with the following text:

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

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

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

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

```
<trans-unit
id="{ADFBundle['oracle.adf.businesseditor.model.util
.BaseRuntimeResourceBundle'] ['persdef.sessiondef.orac
le.iam.ui.runtime.form.model.user.entity.use
rEO.UD_SF_USERNAME__c_description']}">

<source>Username</source>

</target> </trans-unit> <trans-unit

id="sessiondef.oracle.iam.ui.runtime.form.model.Sales
force.entity.sEO.UD_SF_USR_USERNAME__c">

<source>Username</source>

</target> </trans-unit>
```

- d. Open the resource file from the connector package, for example `Salesforce_ja.properties`, and get the value of the attribute from the file, for example, `global.udf.UD_SF_USR_USERNAME=\u30A2\u30AB\u30A6\u30F3 \u30C8\u540D`.
- e. Replace the original code shown in Step 6.c with the following:

```
<trans-unit id="{ADFBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle'] ['persdef.sessiondef.oracle.iam.ui.
runtime.form.model.user.entity.userEO.UD_SF_USR_USERNAME__c_descriptio
n']}">

<source>User Name</source>
<target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.Salesforce.entity
sEO.UD_SF_USR_USERNAME__c_LABEL
">
<source>Account Name</source>
<target>\u30A2\u30AB\u30A6\u30F3\u30C8\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.xml`. In this file name, replace `LANG_CODE` with the code of the language to which you are localizing.
Sample file name: `BizEditorBundle_ja.xml`
7. Repackage the ZIP file and import it into MDS.

 **See Also:**

Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for information about exporting and importing metadata files.

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

4.6 Configuring SSL for the Connector

Configure SSL to secure data communication between Oracle Identity Governance and Salesforce.

 **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.

Salesforce validates the client system dates to be in sync with the SSL certificate (the certificate issued by Salesforce application) date. If there is any deviation, then the target system might throw an error. The client machine date must be in sync with the certificate timestamp range. Obtain SSL certificate from the target system.

Importing the Certificate

Use the `keytool` command to import the SSL certificate from the target system into the identity keystore in Oracle Identity Governance.

```
keytool -import -alias alias -trustcacerts -file file-to-import -keystore keystore-name -storepass keystore-password
```

In the following example, the certificate file `supportcert.pem` is imported to the identity keystore `client_store.jks` with password `example_password`:

```
keytool -import -alias serverwl -trustcacerts -file supportcert.pem -keystore client_store.jks -storepass example_password
```

 **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.

4.7 Obtaining GUID of Roles

You must obtain the GUID of roles from the target system to populate the Code Key values of the Lookup.Salesforce.Roles lookup definition.

The REST services exposed by Salesforce.com do not provide any endpoint to fetch the Role GUIDs programmatically. Therefore, to manage provision roles for users, you have to populate the Lookup.Salesforce.Roles lookup manually.

To obtain GUID of roles, from your organization's role hierarchy, click on any role for which you want to determine the GUID. The GUID is available as part of the URL. For example, in the following URL, 00E800000016mY is the GUID of the selected role:

```
https://cs40.salesforce.com.00E800000016mY.setupid=Roles
```

5

Using the Salesforce Connector

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

- [Configuring Reconciliation](#)
- [Configuring Provisioning](#)
- [Scheduled Job for Reconciliation of Groups](#)
- [Configuring Reconciliation Jobs](#)
- [Uninstalling the Connector](#)

5.1 Configuring Reconciliation

Reconciliation involves duplicating in Oracle Identity Governance the creation of and modifications to user accounts on the target system.

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

- [Performing Full Reconciliation](#)
- [Performing Limited Reconciliation](#)
- [Reconciling Large Number of Records](#)

5.1.1 Performing Full Reconciliation

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

If you want to get the frozen users in the Full Reconciliation Scheduled Job use the below

Filter Value For frozen users: `WHERE+Id+IN+(SELECT+UserId+FROM+UserLogin+WHERE+IsFrozen=false)`

The connector cannot support incremental reconciliation because the target system does not provide a way for tracking the time at which account data is created or modified.

If the target system contains more than 2200 records, then use the Flat File connector to perform full reconciliation as Salesforce.com does not allow you to reconcile more than 2200 users even after pagination. See [Reconciling Large Number of Records](#).

5.1.2 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.

You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a filter attribute that allows you to use any of the attributes of the target system to filter target system records.

You specify a value for the filter attribute while configuring the user reconciliation scheduled job.

Filter value: `WHERE+id+=+'0055g00000B5GYL'`

 **Note:**

If the target system contains more than 2200 records, then use the Flat File connector to perform limited reconciliation as Salesforce does not allow you to reconcile more than 2200 users even after pagination. Otherwise, use appropriate filters to reduce the records count. See [Reconciling Large Number of Records](#).

5.1.3 Reconciling Large Number of Records

During a reconciliation run, if the target system contains more than 2200 records, then you must use the Flat File connector to fetch all the records into Oracle Identity Governance.

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

1. Export all users in the target system to a flat file.
2. Copy the flat file to a location that is accessible from Oracle Identity Governance.
3. Create a schema file representing the structure of the flat file.
4. Install the Flat File connector.
5. Configure the Flat File IT resource.
6. If you want to perform trusted source reconciliation, then configure and run the Flat File Users Loader scheduled job.

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

7. If you want to perform target resource reconciliation, then configure and run the Flat File Accounts Loader scheduled job.

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

5.2 Configuring Provisioning

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

- [Guidelines on Performing Provisioning Operations](#)
- [Performing Provisioning Operations](#)

5.2.1 Guidelines on Performing Provisioning Operations

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

- For a Create User provisioning operation, you must specify a value for the User Name field along with the domain name. For example, `jdoe@example.com`.
- During a group provisioning operation you must give a value for DisplayName.
- While assigning multiple groups with the same name, the target system appends a number to the group name. Therefore, you must execute Group target reconciliation job every time multiple groups with the same name are provisioned on the target system to bring the target system and Oracle Identity Governance in synchronization.

5.2.2 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

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



See Also:

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

5.3 Scheduled Job for Reconciliation of Groups

After you create an application, the Salesforce Group Recon scheduled job is automatically created for Group Management in Oracle Identity Governance. You must configure the scheduled job to suit your requirements by specifying values for its attributes.

Table 5-1 Attributes of the Salesforce Group Recon Scheduled Job

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records Default Value: Salesforce
Object Type	Enter the type of object whose values must be synchronized. Default Value: __GROUP__ Note: Do not change the value of this attribute.
OIM Organization Name	Enter the name of the Oracle Identity Governance organization in which reconciled groups must be created or updated.
Resource Object Name	This attribute holds the name of the resource object used for reconciliation. Default value: Salesforce Group
	<div data-bbox="1084 1098 1378 1270" style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;">  Note: Do not change the default value. </div>
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default Value: Salesforce Group Reconciliation
	<div data-bbox="1084 1476 1378 1677" style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;">  Note: Do not modify the value of this attribute </div>

5.4 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

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

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

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

 **Note:**

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

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

 **Note:**

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

5.5 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 (for example, Salesforce User; Salesforce Group) as the value of the `ObjectValues` property.

 **Note:**

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

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

6

Extending the Functionality of the Salesforce Connector

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

This section provides more information about the following topics:

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

6.1 Configuring the Connector for Multiple Installations of the Target System

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

The following example illustrates this requirement:

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

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

6.2 Configuring Transformation and Validation of Data

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

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

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

To configure transformation or validation of user account data, you must write Groovy scripts while creating your application. For more information about writing Groovy script-based validation and transformation logic, see *Validation and Transformation of Provisioning and*

Reconciliation Attributes of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

6.3 Configuring Action Scripts

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

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

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

7

Upgrading the Salesforce Connector

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



Note:

Before you perform the upgrade procedure:

- It is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
- As a best practice, perform the upgrade procedure in a test environment initially.
- Salesforce 12.2.1.3.1 is a REST base connector.

The following sections discuss the procedure to upgrade the connector:

- [Preupgrade Steps](#)
- [Upgrade Steps for CI Installation](#)
- [Upgrade Steps for AOB](#)
- [Postupgrade Steps for CI Installation](#)
- [Postupgrade steps for AOB Installation](#)
- [Salesforce Upgrade Script for AOB](#)

7.1 Preupgrade Steps

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

Perform the following preupgrade steps:

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

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

7.2 Upgrade Steps for CI Installation

This topic provides detailed steps for upgrading the Salesforce 12.2.1.3.0 to Salesforce 12.2.1.3.1 CI Upgrade for both Target and Trusted. The steps are applicable for upgrading steps from Salesforce 11.1.1.5.0 to Salesforce 12.2.1.3.1 CI Upgrade for Target and Trusted.

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

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

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

- Staging Environment
Perform the upgrade procedure by using the wizard mode.

 **Note:**

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

- Production Environment
Perform the upgrade procedure by using the silent mode.

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

7.3 Upgrade Steps for AOB

The steps to upgrade for Salesforce 12.2.1.3.0 to Salesforce 12.2.1.3.1 AOB Upgrade for Target and Auth are as follows:

See Managing Connector Lifecycle Managing Application OnBoarding in *Oracle Fusion Middleware Administering Oracle Identity Manager*

1. Update APP_TEMPLATE table. Under the DATA column, modify the XML as given below:
 - Update Bundle Name: genericscim to genericrest
 - Update Connector Name: GenericSCIMConnector to GenericRESTConnectorPerform these steps for both Target and Trusted XML.
2. Upgrade AOB through the wizard mode as follows:
 - a. Log in to **Identity Console** and navigate to **Applications** under **Manage** tab.

- b. Click Connector Upgrade.**
- 3. Target Basic and Advance Configuration:** Both target and trusted Salesforce applications are upgraded in a single go. First, all the differences of the target type are shown and then authoritative. On this **Target Basic Information** schema page, basic and advanced configurations differences are shown. A check box is provided for each property to 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**.
- 4. Target Schema:** All the changes related to the parent schema such as the addition of new schema attributes or removal of schema attributes is shown here. Changes in child forms, if any are also shown here. You have the flexibility of choosing the applicable changes. Click **Next**.
- 5. Target Reconciliation and Provisioning Settings:** The changes related to addition or removal of jobs is shown here. Changes in the old job configuration such as addition or removal of job parameters is also visible here. In the current example, a new job parameter called `Permission Sets Lookup Name` is added to the existing Salesforce Target Recon job. Also, a new Salesforce Target New Job is added.
- 6. Authoritative Basic and Advance Configuration:** In this Authoritative Basic Information schema page, the basic and advanced configurations differences are shown. A check box is provided for each property in which you can select or deselect.

For example, if you check the removed basic property, then 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**.
- 7. Authoritative Schema:** All the changes related to parent schema such as the addition of new schema attributes or removal of schema attributes is shown here. Changes in child forms if any are also shown here. You have the flexibility of choosing the applicable changes. Click **Next**.
- 8. Summary:** On this review screen all the checked changes are shown. Also, all the impacted apps of 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 and individual apps.

 **Note:**

For details on the updated Basic Configuration, schema attribute and Reconciliation jobs, see the topic [Configuring the Salesforce Connector](#).

7.4 Postupgrade Steps for CI Installation

The 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.

Note:

If you have not retained the customizations, you must reapply them after you upgrade the connector .The Postupgrade steps involve uploading new connector JAR to the Oracle Identity Manager database.

1. Delete the old Connector JARs. Run the Oracle Identity Manager Delete JARs (`$ORACLE_HOME/bin /DeleteJars.sh`) utility to delete the existing ICF bundle `org.identityconnectors.genericscim-1.0.11150.jar` from the Oracle Identity Manager database.

When you run the Delete JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being deleted, and the name of the JAR file to be removed. Specify 4 as the value of the JAR type.

2. Upload the new connector JARs:
 - a. Run the Oracle Identity Manager Upload JARs (`$ORACLE_HOME/bin/UploadJars.sh`) utility to upload the connector JARs.
 - b. Upload the `org.identityconnectors.genericcrest-12.3.0.jar` bundle as an ICF Bundle. Run the Oracle Identity Manager Upload JARs utility to post the new ICF bundle `org.identityconnectors.genericcrest-12.3.0.jar` file to the Oracle Identity Manager database.

When you run the Upload JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being 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 Manager.
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.genericscim-1.0.1115.jar` with the new bundle JAR file `org.identityconnectors.genericcrest-12.3.0.jar`.
 - c. Start the connector server.

 **Note:**

The detailed steps for Salesforce 12.2.1.3.0 to Salesforce 12.2.1.3.1 CI Upgrade for Target and Trusted, or steps for Salesforce 11.1.1.5.0 to Salesforce 12.2.1.3.1 CI Upgrade for Target and Trusted.

- For details regarding re-configuring the IT resource of the connector, refer to the [Configuring the Salesforce Connector](#).

5. Upgrading the connector will generate the duplicate entries in the Lookups, you must manually delete these duplicate entries and extra entries.

The below given lookups will update as shown:

- `Lookup.Salesforce.Configuration`
- `Lookup.Salesforce.UM.ProvAttrMap`
- `Lookup.Salesforce.UM.ReconAttrMap`
- `Lookup.Salesforce.Configuration.Trusted`

6. Run the following lookup Recon:
 - a. Salesforce Group Lookup Reconciliation
 - b. Salesforce Profile Lookup Reconciliation
 - c. Salesforce PermissionSet Lookup Reconciliation
 - d. Salesforce Role Lookup Reconciliation
 - e. Salesforce Territory Lookup Reconciliation
7. Create a new version of the process form.
8. Run Form Upgrade Job.
9. Perform full reconciliation.

7.5 Post upgrade steps for AOB

 **Note:**

You must follow the steps from 1 to 4 provided in the section [Postupgrade Steps for CI Installation](#) and then continue to follow the below steps.:

The post upgrade steps for AOB are as follows:

1. Execute `UpgradeScimToRest.sh`. For details, see [Salesforce Upgrade Script for AOB](#)
2. Verify your Target Application Basic Configuration , Advanced Settings Parameters should be manual updated as per the details in [Table 3-1](#) [Table 3-2](#).
For Target Application follow below steps
3. Verify your Target Application schema Target Attribute (Salesforce User and Child-Groups)should update as per the details in [Table 3-8](#).
4. Create a new form and add to the upgraded Target application.

5. Publish a new sandbox.

Before Running Lookup jobs make sure to update the below mentioned changes:

- Change the Application Name to the one you are using for Salesforce Territory Lookup Reconciliation.
- Change the Application Name to the one you are using for Salesforce Permission Set Lookup Reconciliation.
- Change the Application Name to the one you are using for Salesforce Role Lookup Reconciliation.
- Change the Salesforce Group Lookup Reconciliation Object Type to `__GROUPLKP__`
- Change the Salesforce Profile Lookup Reconciliation Object Type to `__PROFILE__`
- Change the Application Name to the one you are using for Salesforce Full User Reconciliation.

6. Run the **Form Upgrade Job**.

7. Perform full reconciliation.

8. Delete the older Salesforce User Reconciliation job.

For Authoritative Application follow below steps

9. Verify if your Authoritative Application schema Target Attributes is updates as per the details in Table 3-4 for Perform full reconciliation.

7.6 Salesforce Upgrade Script for AOB

The upgrade of Salesforce SCIM to REST AOB requires that you execute the upgrade script for both **Connector Name** and **Bundle Name**. Update for `cURL` script is available for Salesforce-12.2.1.3.1 Connector Upgrade\UpgradeScimToRest.shPrerequisites are provided below:

Before running this script update the `config.properties` file as per README.



Note:

Curl must be present in system.

1. Filling in the `config.properties` File.

Using a text editor, edit the file `config.properties` located in the directory:

`ORACLE_HOME/idm/server/ConnectorDefaultDirectory/`

`Salesforce-12.2.1.3.1/Upgrade` and update the following parameters and save it.

```
#OIG ADMIN username (ex: xelsysadm)
```

```
OIG.admin.username=xelsysadm
```

```
#OIG ADMIN password
```

```
OIG.admin.password=Welcome1
```

```
OIG.host=Localhost
```

```
#OIG Host address (ex: IP address or domain)
```

```
#OIG Port number (ex: 14000)
```

```
OIG.port=14000
```

```
#OIG SSL option,(ex: true or false)in lowercase
```

```
OIG.ssl.enabled=false
```

2. Run the UpgradeScimToRest.sh file

Execute `UpgradeScimToRest.sh` (on UNIX) and you must run the script in a shell environment using the following command:

```
sh UpgradeScimToRest.sh
```


8

Known Issues and Limitations

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

Preconfig XML file does not get imported as expected when another generic connector is already installed

If you are creating the Salesforce connector application in a scenario when another generic connector is already installed or created, then the xml/Salesforce-pre-config.xml file will not get imported as expected.

Workaround: As a workaround, perform the Deployment Manager import.



Note:

Verify pre-population status of the static lookup definition. If the lookup data is not getting populated, you must import the xml/Salesforce-pre-config.xml pre config XML file manually. For example, `Lookup.Salesforce.PreferredLanguage`.

With Password Attribute Account provision not possible, as pre Salesforce RESTAPI limitation

Error message:

SEVERE: Exception occurred while executing request. HTTP 400 Error: Not able to parse input, or input does not match the required entities or validation failures.

```
["message":"No such column 'NewPassword' on subject of type User", "errorCode":"INVALID_FIELD"]
```

```
org.identityconnectors.framework.common.exceptions.ConnectorException: Exception occurred while executing request. HTTP 400 Error : Not able to parse input, or input does not match required entities or validation failures.["message":"No such column 'NewPassword' on subject of type User", "errorCode":"INVALID_FIELD"]
```

Workaround: After creating the Account, you need to reset the account password.

Appendices

Information that is outside the scope of day-to-day tasks with Oracle Identity Governance Connectors for Salesforce application is discussed here.

This section contains the following topics:

- [Appendix](#)

A

Appendix

- [Files and Directories on the Installation Media](#)

A.1 Files and Directories in the Salesforce Connector Package

These are the files and directories on the connector installation package that comprise the Salesforce connector.

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

File in the Installation Media Directory	Description
org.identityconnectors.genericrest-12.3.0.jar	This JAR is the ICF connector bundle.
configuration/Salesforce-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the Connector Installer during connector installation.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the Oracle Identity Governance database. Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
xml/Salesforce-ConnectorConfig.xml	This XML file contains definitions for the following connector objects: <ul style="list-style-type: none">• IT resource definition• Process forms• Process tasks and adapters• Lookup definitions• Resource objects• Process definition• Scheduled tasks• Reconciliation rules
xml/Salesforce-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/Salesforce-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User object like Groups.

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

File in the Installation Media Directory	Description
xml/Salesforce-target-template.xml	This file contains definitions for the connector objects required for creating a Target application. It includes certain details required to connect Oracle Identity Governance with the target system. It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
upgrade/UpgradeScimToRest.sh	This file contains the script that are run after performing an AOB UI upgrade of the connector
upgrade/config.properties	This file contains the properties parameter of the UpgradeScimToRest script.
upgrade/REAMDE	This file contains the README of UpgradeScimToRest script.