Oracle® Identity Manager
Connector Guide for Salesforce

Release 11.1.1
E73604-05
September 2020

Oracle Identity Manager Connector Guide for Salesforce, Release 11.1.1

E73604-05

Primary Author: Gowri GR

Contributing Authors: Alankrita Prakash

Contents

List of Figures

List of Tables

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action or terms defined in text or the glossary.

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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

This chapter provides an overview of the updates made to the software and documentation for the Salesforce connector in release 11.1.1.5.0.

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

The following section discusses software updates:

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager connector for Salesforce. Therefore, there are no software-specific updates in this release.

Documentation-Specific Updates

The following section discusses documentation-specific updates:

Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific update has been made in revision "05" of this guide:

The description column for several IT resource parameters belonging to Table 2-1 have been updated.

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

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

The following documentation-specific updates have been made in revision "03" of this guide:

The "Oracle Identity Manager" row of Table 1-1 has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12c (12.2.1.3.0) certification.

The following documentation-specific updates have been made in revision "02" of this guide:

- Creating a New UI Form has been modified to remove the additional step of selecting the **Generate Entitlement Forms** check box.
- A "Note" about eliminating the Automated Process User of the Salesforce sandbox has been added to Full Reconciliation.

1

About the Salesforce Connector

The Salesforce connector integrates Oracle Identity Manager with the Salesforce.com target system.

This chapter contains the following sections:

1.1 Introduction to the Salesforce Connector

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

> **Note:**
>
> At some places in this guide, the term target system has been used to refer to Salesforce.com.

The Salesforce connector enables you to perform identity management-related tasks (such as creating, updating, and deleting) on user and group identities while managing their profiles at the same time.

In the account management (target resource) mode of the connector, information about all active users created or modified directly on the target system can be reconciled into Oracle Identity Manager. This data is used to add or modify resources (that is, accounts) allocated to OIM Users. In addition, you can use Oracle Identity Manager to provision or update Salesforce resources (accounts) assigned to OIM

Users. These provisioning operations performed on Oracle Identity Manager translate into the creation or updates to target system accounts.

In the identity reconciliation (trusted source) mode of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

1.2 Certified Components for the Salesforce Connector

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

Table 1-1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) • Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and any later BP in this release track
Target systems	Salesforce Winter 2012 and later releases
Connector Server	1.4.0
Connector Server JDK	JDK 1.6 or later

1.3 Certified Languages for the Salesforce Connector

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English (US)
- Finnish
- French
- French (Canadian)
- German
- Greek

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

1.4 Architecture of the Salesforce Connector

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

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 Manager 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 Manager. 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:

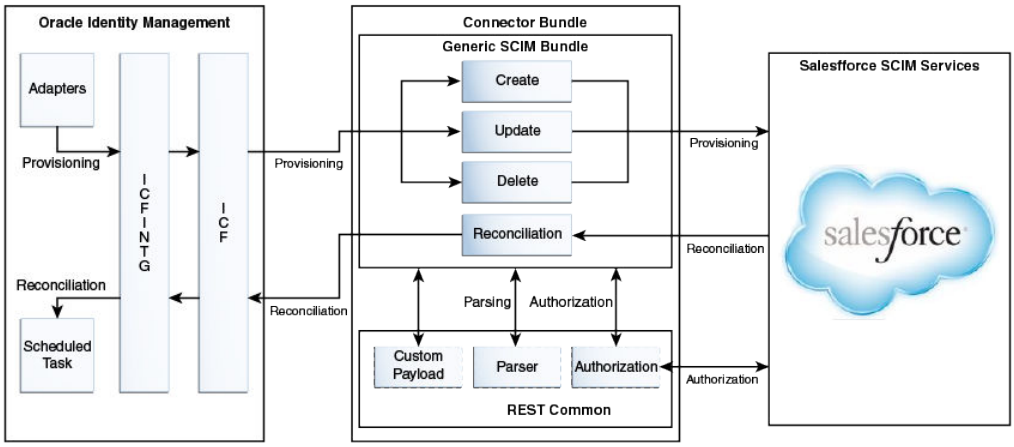
  – **Provisioning**

Provisioning involves creating or updating users on the target system through Oracle Identity Manager. 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 Manager context, the term provisioning also covers updates made to the target system account through Oracle Identity Manager.

- **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 Manager. Through provisioning operations performed on Oracle Identity Manager, accounts are created and updated on the target system for OIM Users.

Through reconciliation, account data that is created and updated directly on the target system is fetched into Oracle Identity Manager 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 Manager. You do not need to configure or modify ICF.

During provisioning, the Adapters invoke ICF operation, ICF inturn 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 inturn 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 Manager.

1.5 Use Cases Supported by the Salesforce Connector

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

- **Salesforce License Management**

  On Salesforce.com, Profiles are used to manage licences 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 Manager supports.

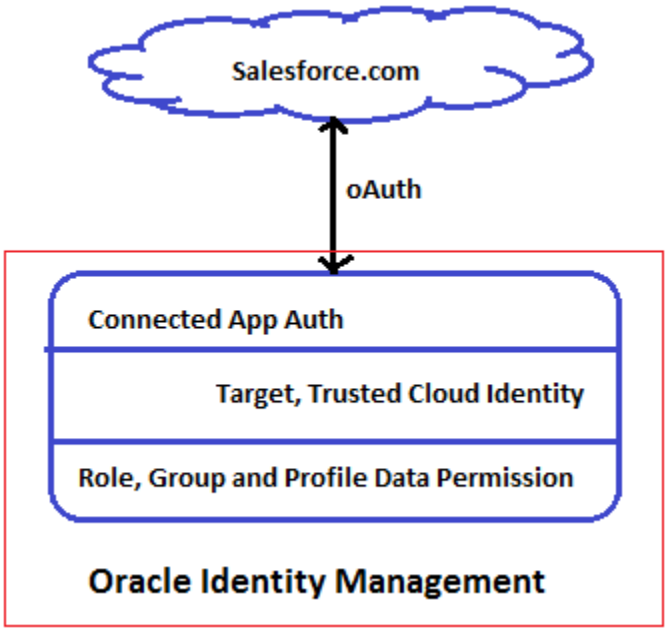
  Salesforce.com can be used as a trusted source and an organization can use this feature to provide the list of users and further provision the account of these users to a third-party application that has been configured as target source.

- **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



1.6 Features of the Salesforce Connector

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

- Full Reconciliation
- Support for the Connector Server
- Limited Reconciliation
- Transformation and Validation of Account Data

1.6.1 Full Reconciliation

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

> **Note:**
>
> To eliminate the Automated Process User that the Salesforce sandbox has and to get all the users successfully during full reconciliation, you must add the following filter, `greaterThan('userType','AutomatedProcest')|lessThan('userType','AutomatedProcess')`

To perform a full reconciliation run, remove or delete any value assigned to the Filter and run the scheduled job for user reconciliation.

Note:

- 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.

1.6.2 Support for the Connector Server

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

A Java connector server is useful when you do not want to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements if the bundle works faster when deployed on the same host as the native managed resource.

1.6.3 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 Manager during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled. See Limited Reconciliation.

1.6.4 Transformation and Validation of Account Data

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

In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

- Configuring Transformation of Data During User Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning

1.7 Lookup Definitions Used During Connector Operations

Lookup definitions used during reconciliation and provisioning are either preconfigured or can be synchronized with the target system.

Lookup definitions used during connector operations can be categorized as follows:

- Lookup Definitions Synchronized with the Target System
- Preconfigured Lookup Definitions

1.7.1 Lookup Definitions Synchronized with the Target System

Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Group Name lookup field to specify a group for the user for whom the provisioning operation is being performed. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization populates these lookup fields with values from the corresponding lookup definitions.

The following lookup definitions are populated with values fetched from the target system by the scheduled jobs for lookup field synchronization:

- Lookup.Salesforce.Groups
- Lookup.Salesforce.Profiles

1.7.1.1 Lookup.Salesforce.Groups

The Lookup.Salesforce.Groups lookup definition holds details of groups defined in Salesforce.com. You populate this lookup definition through lookup field synchronization performed using the Salesforce Group Lookup Reconciliation scheduled job.

The following is the format in which data is stored after lookup definition synchronization:

- **Code Key:** *IT_RESOURCE_KEY~GROUP_ID*

  In this format:

  - *IT_RESOURCE_KEY* is the numeric code assigned to each IT resource in Oracle Identity Manager.
  - *GROUP_ID* is GUID of the group on the target system.

- **Decode:** *IT_RESOURCE_NAME~GROUP_NAME*

  In this format:

  - *IT_RESOURCE_NAME* is the name assigned to the IT resource in Oracle Identity Manager.
  - *GROUP_NAME* is the name of the group on the target system.

Table 1-2 lists sample entries in this lookup definition.

Table 1-2 Sample Entries in the Lookup.Salesforce.Groups Lookup Definition

Code Key	Decode
461~00G80000001gXdyEAE	Salesforce~Company Labs
461~00G54000000FcXxEAK	Salesforce~IT
461~00G54000000Fcc9EAC	Salesforce~BusinessIntelligence

1.7.1.2 Lookup.Salesforce.Profiles

The Lookup.Salesforce.Profiles lookup definition holds details of profiles defined in Salesforce. You populate this lookup definition through lookup field synchronization performed using the Salesforce Profile Lookup Reconciliation scheduled job.

The following is the format in which data is stored after lookup definition synchronization:

- **Code Key:** *IT_RESOURCE_KEY~PROFILE_ID*

  In this format:

  - *IT_RESOURCE_KEY* is the numeric code assigned to each IT resource in Oracle Identity Manager.
  - *PROFILE_ID* is GUID of the Profile on the target system.

- **Decode:** *IT_RESOURCE_NAME~PROFILE_NAME*

  In this format:

  - *IT_RESOURCE_NAME* is the name assigned to the IT resource in Oracle Identity Manager.
  - *PROFILE_NAME* is the name of the profile on the target system.

Table 1-3 lists sample entries in this lookup definition.

Table 1-3 Entries in the Lookup.Salesforce.Profile Lookup definition

Code Key	Decode
161~00e80000001aotvAAA	Salesforce~Chatter Free User
161~00e30000000iEpoAAE	Salesforce~Standard Platform User
161~ooe800000018uFGAAY	Salesforce~Salesforce~S&OP 2

1.7.2 Preconfigured Lookup Definitions

Preconfigured lookup definitions are automatically created in Oracle Identity Manager after you deploy the connector.

These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed. The preconfigured lookup definitions are as follows:

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

- Lookup.Salesforce.GM.Configuration
- Lookup.Salesforce.GM.ProvAttrMap
- Lookup.Salesforce.GM.ReconAttrMap
- Lookup.Salesforce.PreferredLanguages
- Lookup.Salesforce.PhoneType
- Lookup.Salesforce.Roles
- Lookup.Salesforce.Locale

1.7.2.1 Lookup.Salesforce.Configuration

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

The Lookup.Configuration.Salesforce lookup definition contains the entries shown in Table 1-4

> **Note:**
>
> Do not modify any of the entries in Table 1-4.

Table 1-4 Entries in the Lookup.Configuration.Salesforce Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.genericscim	This entry holds the name of the connector bundle.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle.
Connector Name	org.identityconnectors.genericscim.GenericSCIMConnector	This entry holds the name of the connector class.
Group Configuration Lookup	Lookup.Salesforce.GM.Configuration	This entry holds the name of the lookup definition that contains group-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform group management operations.
User Configuration Lookup	Lookup.Salesforce.UM.Configuration	This entry holds the name of the lookup definition that stores configuration information used during user management operations.
defaultBatchSize	200	This is the number of records that can be retrieved from the target system in one go.
nameAttributes	"Users=userName","Groups=displayName","Entitlement=displayName"	This is the __NAME__ attribute mapping of Oracle Identity Manager to the relevant attribute on target system.

Table 1-4 (Cont.) Entries in the Lookup.Configuration.Salesforce Lookup Definition

Code Key	Decode	Description
attrToOClassMapping	"__ACCOUNT__.groups=Groups"	This is used to map an attribute present under one object class to another object class. For example "groups" under "__ACCOUNT__" Object Class should be mapped to "__GROUP__" object class. Sample value is "urn:ietf:params:scim:schemas:core:2.0:User;groups=Groups"
jsonResourcesTag	Resources	This entry holds the name of the JSON tag that holds user details in the response payload.
customPayload	"__ACCOUNT__.groups.AddOp={\"displayName\":\"$(__GROUP__.displayName)$\",\"members\":[{\"operation\":\"add\",\"value\":\"$(__ACCOUNT__.__UID__)$\"}]}","__ACCOUNT__.groups.RemoveOp={\"displayName\":\"$(__GROUP__.displayName)$\",\"members\":[{\"operation\":\"delete\",\"value\":\"$(__ACCOUNT__.__UID__)$\"}]}","__ACCOUNT__.phoneNumbers.RemoveOp={\"phoneNumbers\":[{\"type\":\"$(__ACCOUNT__.phoneNumbers.type)$\",\"value\":\"\"}]}"	This takes the custom payloads necessary to carry out specific operation for specific attributes on the target system.
scimVersion	1	This entry specifies the supported SCIM version of the target system.
statusAttributes	"Users=active"	This is the __ENABLE__ attribute mapping of Oracle Identity Manager to the Status attribute on target system.
uidAttributes	“Users=id","Groups=id", "Entitlement=id"	This is the __UID__ attribute mapping of Oracle Identity Manager to the GUID attribute on target system.
passwordAttributes	“Users=password"	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector in OIM.

1.7.2.2 Lookup.Salesforce.Configuration.Trusted

The Lookup.Salesforce.Configuration.Trusted lookup definition holds connector configuration entries that are used during trusted source reconciliation.

> **Note:**
>
> Do not modify any of the entries listed in Table 1-5.

Table 1-5 Entries in the Lookup.Salesforce.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.genericscim	This entry holds the name of the connector bundle.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle.
Connector Name	org.identityconnectors.genericscim.GenericSCIMConnector	This entry holds the name of the connector class.
User Configuration Lookup	Lookup.Salesforce.UM.Configuration.Trusted	This entry holds the name of the lookup definition that contains user-specific configuration properties.
defaultBatchSize	200	This is the number of records that can be retrieved from the target system in one go.
nameAttributes	"Users=userName"	This is the __NAME__ attribute mapping of Oracle Identity Manager to the relevant attribute on target system.
attrToOClassMapping	"__ACCOUNT__.groups=Groups"	This is used to map an attribute present under one object class to another object class. For example "groups" under "__ACCOUNT__" Object Class should be mapped to "__GROUP__" object class. Sample value is "`urn:ietf:params:scim:schemas:core:2.0:User;groups=Groups`"
jsonResourcesTag	Resources	This entry holds the name of the JSON tag that holds user details in the response payload.

Table 1-5 (Cont.) Entries in the Lookup.Salesforce.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
customPayload	"__ACCOUNT__.groups.AddOp={\"displayName\":\"$(__GROUP__.displayName)$\",\"members\":[{\"operation\":\"add\",\"value\":\"$(__ACCOUNT__.__UID__)$\"}]}","__ACCOUNT__.groups.RemoveOp={\"displayName\":\"$(__GROUP__.displayName)$\",\"members\":[{\"operation\":\"delete\",\"value\":\"$(__ACCOUNT__.__UID__)$\"}]}","__ACCOUNT__.phoneNumbers.RemoveOp={\"phoneNumbers\":[{\"type\":\"$(__ACCOUNT__.phoneNumbers.type)$\",\"value\":\"\"}]}"	This takes the custom payloads necessary to carry out specific operation for specific attributes on the target system.
scimVersion	1	This entry specifies the supported SCIM version of the target system.
statusAttributes	"Users=active"	This is the __ENABLE__ attribute mapping of Oracle Identity Manager to the Status attribute on target system.
uidAttributes	"Users=id"	This is the __UID__ attribute mapping of Oracle Identity Manager to the GUID attribute on target system.
passwordAttributes	"Users=password"	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute of the connector in OIM.

1.7.2.3 Lookup.Salesforce.UM.Configuration

The Lookup.Salesforce.UM.Configuration lookup definition holds configuration entries that are specific to the user object type.

This lookup definition is used during user management operations when your connector is configured in the target resource mode.

Table 1-6 lists the default entries in this lookup definition.

Table 1-6 Entries in the Lookup.Salesforce.UM.Configuration Lookup

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.Salesforce.UM.ProvAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during provisioning operations.
Recon Attribute Map	Lookup.Salesforce.UM.ReconAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during reconciliation.

1.7.2.4 Lookup.Salesforce.UM.Configuration.Trusted

The Lookup.Salesforce.UM.Configuration.Trusted lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during trusted source user reconciliation runs.

Table 1-7 Entries in the Lookup.Salesforce.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute Defaults	Lookup.Salesforce.UM.ReconAttrMap.TrustedDefaults	This entry holds the name of the lookup definition that maps reconciliation fields to their default values. See Lookup.Salesforce.UM.ReconAttrMap.TrustedDefaults.
Recon Attribute Map	Lookup.Salesforce.UM.ReconAttrMap.Trusted	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.Salesforce.UM.ReconAttrMap.Trusted.

1.7.2.5 Lookup.Salesforce.UM.ProvAttrMap

The Lookup.Salesforce.UM.ProvAttrMap lookup definitions hold mappings between process form fields and target system attributes.

This lookup definition is used during provisioning. This lookup definition is preconfigured. Table 1-17 lists the default entries.

You can add entries in this lookup definition if you want to map new target system attributes for provisioning. See Adding New User or Group Attributes for Provisioning.

1.7.2.6 Lookup.Salesforce.UM.ReconAttrMap

The Lookup.Salesforce.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes.

This lookup definition is used during reconciliation. This lookup definition is preconfigured. Table 1-13 lists the default entries.

You can add entries in this lookup definition if you want to map new target system attributes for target resource reconciliation. See Adding New User or Group Attributes for Reconciliation.

1.7.2.7 Lookup.Salesforce.UM.ReconAttrMap.Trusted

The Lookup.Salesforce.UM.ReconAttrMap.Trusted lookup definitions is used during trusted source user reconciliation runs.

The Lookup.Salesforce.UM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is preconfigured. Table 1-19 lists the default entries of this lookup definition.

> **Note:**
>
> You must not modify Code Key and Decode values of the default entries. You cannot remove the mandatory fields. You can add additional fields to manage new attributes. See Adding New User or Group Attributes for Reconciliation.

1.7.2.8 Lookup.Salesforce.UM.ReconAttrMap.TrustedDefaults

The Lookup.Salesforce.UM.ReconAttrMap.TrustedDefaults lookup definition holds mappings between reconciliation fields and their default values.

The Lookup.Salesforce.UM.ReconAttrMap.TrustedDefaults lookup definition is used when there is a mandatory field on the OIM User form, but no corresponding field in the target system from which values can be fetched during trusted source reconciliation.

Table 1-8 lists the default entries in this lookup definition.

Table 1-8 Entries in the Lookup.Salesforce.UM.ReconAttrMap.TrustedDefaults Lookup Definition

Code	Decode
Organization	Xellerate Users
User Type	End-User
Employee Type	Full-Time

You can add entries to this lookup definition in the following format, if required:

- **Code Key:** Name of the reconciliation field of the Salesforce User resource object

- **Decode:** Corresponding default value to be displayed

For example, assume a field named Preferred Communication Mode is a mandatory field on the OIM User form. Suppose the target system contains no field that stores information about the preferred mode of communication for a user account. During reconciliation, no value for the Preferred Communication Mode field is fetched from the target system. However, as the Preferred Communication Mode field cannot be left empty, you must specify a value for this field. Therefore, create an entry in this lookup definition with the Code Key value set to `Preferred Communication Mode` and Decode value set to `Email.` This implies that the value of the Preferred Communication Mode field on the OIM User form displays Email for all user accounts reconciled from the target system.

1.7.2.9 Lookup.Salesforce.GM.Configuration

The Lookup.Salesforce.GM.Configuration lookup definition holds configuration entries that are specific to the group object type.

This lookup definition is used during group management operations when the connector is configured in the target resource mode.

Table 1-9 lists the default entries in this lookup definition.

Table 1-9 Entries in the Lookup.Salesforce.GM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.Salesforce.GM.ProvAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during group provisioning operations.
Recon Attribute Map	Lookup.Salesforce.GM.ReconAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during reconciliation.

1.7.2.10 Lookup.Salesforce.GM.ProvAttrMap

The Lookup.Salesforce.GM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes.

This lookup definition is used during group provisioning operations. This lookup definition is preconfigured. Table 1-18 lists the default entries.

1.7.2.11 Lookup.Salesforce.GM.ReconAttrMap

The Lookup.Salesforce.GM.ReconAttrMap lookup definitions are used during reconciliation runs for the Group object.

The Lookup.Salesforce.GM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is preconfigured. Table 1-14 lists the default entries.

> **Note:**
>
> You must not modify the Code Key and Decode values of the default entries. You must not remove the mandatory fields. You can add additional fields to manage new attributes. See Adding New User or Group Attributes for Reconciliation.

1.7.2.12 Lookup.Salesforce.PreferredLanguages

The Lookup.Salesforce.PreferredLanguages lookup definition holds the list of languages that you can select and set a preferred language for a user account that you create through Oracle Identity Manager.

This lookup definition is a static lookup definition. You must populated its entries manually.

Table 1-10 Entries in the Lookup.Salesforce.PreferredLanguages Lookup Definition

Code Key	Decode
en_US	ENGLISH

1.7.2.13 Lookup.Salesforce.PhoneType

This is a static lookup defintion where each value denotes the Phone type specific to the target system and the values should not be changed.

Table 1-11 lists the default entries in this lookup definition.

Table 1-11 Entires in the Lookup.Salesforce.PhoneType Lookup Definition

Code	Decode
fax	FAX
mobile	MOBILE
work	WORK

1.7.2.14 Lookup.Salesforce.Roles

The Lookup.Salesforce.Roles lookup definition holds the list of roles that you can select for a user account that you create through Oracle Identity Manager.

The Lookup.Salesforce.Roles lookup definition is a static lookup definition and has to be manually populated with all the roles present on the target.

The following is the format in which data needs to be added to the lookup:

- Code Key: *ROLE_ID*

In this format, *ROLE_ID* is GUID of the Roles on the target system. See Obtaining GUID of Roles.

- Decode: *ROLE_NAME*

  In this format, *ROLE_NAME* is the name of the Role on the target system.

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

Table 1-12 Entries in the Lookup.Salesforce.Roles Lookup Definition

Code Key	Decode
00E800000024rvLEA	practices
00E800000016occ2EA	CEO

1.7.2.15 Lookup.Salesforce.Locale

The Salesforce locale settings determine the display formats for date and time, users' names, addresses, and commas and periods in numbers.

This is a static lookup where the code value is the Locale and the Decode value is the Locale name. Example code is en_US and Decode value is ENGLISH.

1.8 Connector Objects Used During Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to OIM Users.

The Salesforce.com Target Resource User Reconciliation scheduled job is used to initiate a reconciliation run. This schedule job is discussed in Reconciliation Scheduled Jobs.

This section discusses the following topics related to connector objects:

- User Fields for Target Resource Reconciliation
- Group Fields for Reconciliation
- Reconciliation Rules for Target Resource Reconciliation
- Viewing Reconciliation Rules for Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation
- Viewing Reconciliation Action Rules for Target Resource Reconciliation

1.8.1 User Fields for Target Resource Reconciliation

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

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

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

Table 1-13 lists the entries in the lookup definition.

Table 1-13 Entries in the Lookup.Salesforce.UM.ReconAttrMap Lookup Definition

Code Key (Resource Object Field)	Decode (Salesforce Field)
Role	__ACCOUNT__.roles.value
Profile[LOOKUP]	__ACCOUNT__.entitlements.value,primary:true
Status	__ENABLE__
Groups~Group Name[LOOKUP]	__ACCOUNT__.groups~__ACCOUNT__.groups~value
Phone Numbers~Value	__ACCOUNT__.phoneNumbers~__ACCOUNT__.phoneNumbers~value
Phone Numbers~Type	__ACCOUNT__.phoneNumbers~__ACCOUNT__.phoneNumbers~type
ID	__UID__
User Name	__NAME__
First Name	name.givenName
Last Name	name.familyName
Preferred Language	preferredLanguage
Title	Title
Locale	Locale
Nick Name	Nickname
Email	__ACCOUNT__.emails.value,type:work

1.8.2 Group Fields for Reconciliation

The Lookup.Salesforce.GM.ReconAttrMap lookup definition maps user resource object fields and target system attributes.

This lookup definition is used for performing target resource group reconciliation runs.

Table 1-14 lists the group fields of the target system from which values are fetched during reconciliation. The Salesforce Group Recon scheduled job is used to reconcile group data.

Table 1-14 Entries in the Lookup.Salesforce.GM.ReconAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Salesforce Field
Display Name	__NAME__
ID	__UID__
OIM Organization Name	OIM Organization Name

1.8.3 Reconciliation Rules for Target Resource Reconciliation

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

The Salesforce connector can perform reconciliation of both users and groups. Therefore, the connector has reconciliation rules defined for both users and groups.

Reconciliation Rule for Users

The following is the process-matching rule for users:

Rule name: Salesforce User Recon Rule

Rule element: User Login Equals User Name

In this first rule element:

- User Login is the User ID field of the OIM User form.
- User Name is the name attribute which is unique field of the Salesforce account.

Reconciliation Rule for Groups

The following is the process-matching rule for groups:

Rule name: Salesforce Groups Recon Rule

Rule element: Organization Name Equals OIM Org Name

In this rule element:

- Organization Name is the Organization Name field of the OIM User form.
- OIM Org Name is the organization name of the groups in Oracle Identity Manager. OIM Org Name is the value specified in the Organization Name attribute of the Salesforce Group Recon scheduled job.

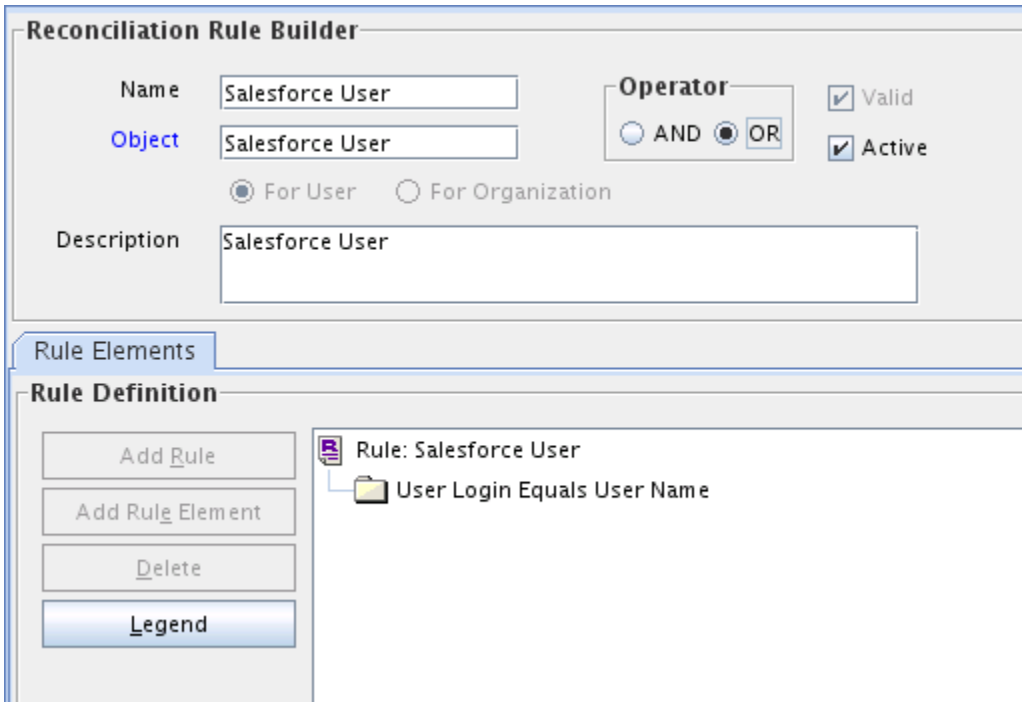
1.8.4 Viewing Reconciliation Rules for Target Resource Reconciliation

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

To view reconciliation rules for target resource reconciliation:

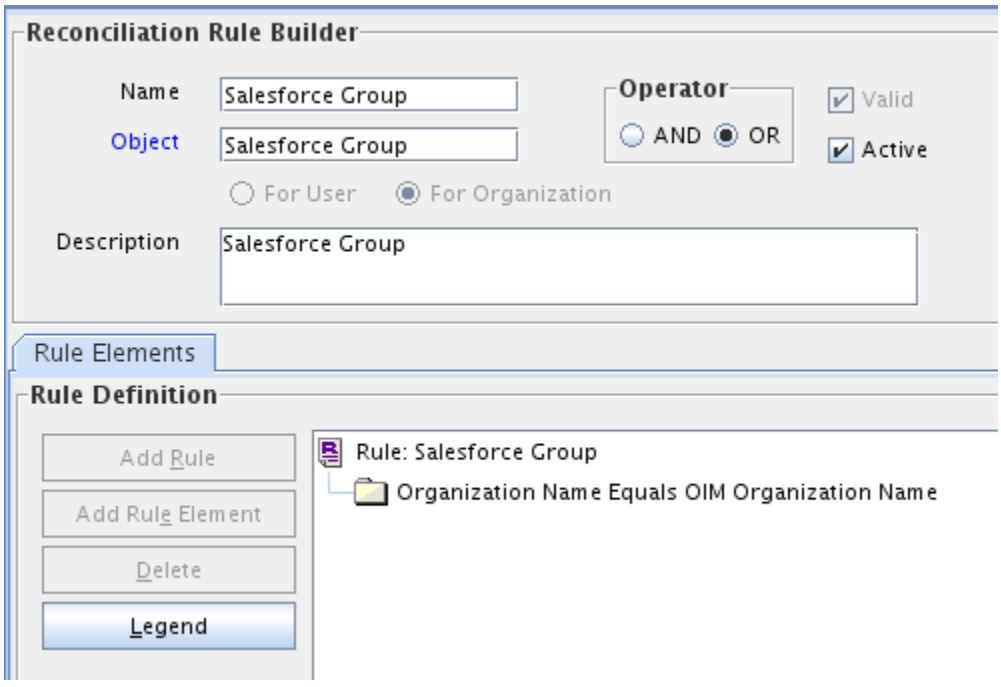
1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools.**
3. Double-click **Reconciliation Rules.**
4. Search for and open one of the following reconciliation rules:
   - For Users: `Salesforce User Recon Rule`
     Figure 1-3 shows the target resource reconciliation rule for users.

Figure 1-3 Reconciliation Rule for Target Resource Reconciliation of Users



- For Groups: `Salesforce Groups Recon Rule`
  Figure 1-4 shows the target resource reconciliation rule for groups.

Figure 1-4 Reconciliation Rule for Target Resource Reconciliation of Groups



1.8.5 Reconciliation Action Rules for Target Resource Reconciliation

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

Table 1-15 Action Rules for Target Resource Reconciliation

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

1.8.6 Viewing Reconciliation Action Rules for Target Resource Reconciliation

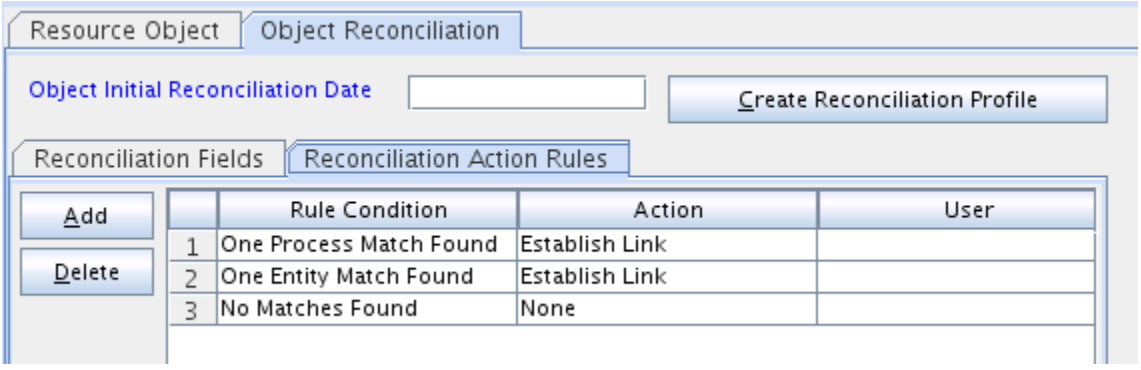
You can view reconciliation action rules on the Object Reconciliation tab of a resource object in Oracle Identity Manager Design Console.

To view reconciliation action rules for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management.**
3. Double-click **Resource Objects.**
4. Search for and open one of the following resource objects:
   - For Users: **Salesforce User**
   - For Groups: **Salesforce Group**
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab.

   The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1-5 shows the reconciliation action rule for target resource reconciliation.

Figure 1-5 Reconciliation Action Rule for Target Resource Reconciliation



1.9 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

This section confers the following topics:

- Provisioning Functions
- User Fields for Provisioning
- Group Fields for Provisioning

1.9.1 Provisioning Functions

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

The Adapter column in Table 1-16 gives the name of the adapter that is used when the function is performed.

Table 1-16 User provisioning functions

Function	Adapter
Create User	adpSALESFORCECREATEOBJECT
Update User	adpSALESFORCEUPDATEATTRIBUTEVALUE
Delete user	adpSALESFORCEDELETEOBJECT
Enable user	adpSALESFORCEENABLETASK
Disable user	adpSALESFORCEDISABLETASK
Change or reset password	adpSALESFORCEUPDATEATTRIBUTEVALUE
Update child table values	adpSALESFORCEUPDATECHILDTABLEVALUE
Add child table values	adpSALESFORCEADDCHILDATA
Remove child table values for a user	adpSALESFORCEREMOVECHILDATA

Note:

Delete user is not supported in Salesforce.com. Deleting the user through SCIM API results in disabling the user on the target system.

1.9.2 User Fields for Provisioning

The Lookup.Salesforce.UM.ProvAttrMap lookup definition maps process form fields with target system fields. This lookup definition is used for performing user provisioning operations.

Table 1-17 Entries in the Lookup.Salesforce.UM.ProvAttrMap Lookup Definitions

Code Key (Process Form Field)	Decode (Salesforce Field)
Role	__ACCOUNT__.roles.value
UD_SF_UGP~Group Name[LOOKUP]	ACCOUNT__.groups~__ACCOUNT__.groups~value
UD_SF_PHONE~Phone Number	__ACCOUNT__.phoneNumbers~__ACCOUNT__.phoneNumbers~value
UD_SF_PHONE~Type	__ACCOUNT__.phoneNumbers~__ACCOUNT__.phoneNumbers~type
User Name	__NAME__
Last Name	name.familyName
First Name	name.givenName
Preferred Language	preferredLanguage
Title	Country
Nick Name	Nickname
Locale	Locale
Profile[LOOKUP]	__ACCOUNT__.entitlements.value,primary:true
ID	__UID__
Email	__ACCOUNT__.emails.value,type:work
Password	___PASSWORD___

1.9.3 Group Fields for Provisioning

The Lookup.Salesforce.GM.ProvAttrMap lookup definition maps user resource object fields and target system attributes. This lookup definition is used for performing group provisioning operations.

While assigning multiple groups with the same name, the target 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 target and OIM in synchronization. Table 1-18 lists the group fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-18 Entries in the Lookup.Salesforce.GM.ProvAttrMap Lookup Definition

Group Field on Oracle Identity Manager	Salesforce Field
Display Name	__NAME__
ID	__UID__

1.10 Connector Objects Used During Trusted Source Reconciliation

Trusted source reconciliation involves fetching data about newly created or modified accounts on the target system and using that data to create or update OIM Users.

The Salesforce Trusted User Recon and Salesforce Trusted User Reconciliation scheduled jobs are used to initiate trusted source reconciliation runs.

This section discusses the following topics:

- User Fields for Trusted Source Reconciliation
- Reconciliation Rules for Trusted Source Reconciliation
- Reconciliation Action Rules for Trusted Source Reconciliation

1.10.1 User Fields for Trusted Source Reconciliation

The Lookup.Salesforce.UM.ReconAttrMap.Trusted lookup definition maps user fields of the OIM User form with corresponding field names in the target system. This lookup definition is used for performing trusted source reconciliation runs.

Table 1-19 Entries in the Lookup.Salesforce.UM.ReconAttrMap.Trusted Lookup Definition

Code Key (OIM User Form Field)	Decode (Target System Field)
Preferred Language	preferredLanguage
Email	__ACCOUNT__.emails.value,type:wor k
Status[TRUSTED]	__ENABLE__
ID	__UID__
User Name	__NAME__
First Name	name.givenName
Last Name	name.familyName
Display Name	displayName

1.10.2 Reconciliation Rules for Trusted Source Reconciliation

Reconciliation rules for trusted source reconciliation are used by the reconciliation engine to determine the OIM User identity that must be created or updated for the corresponding account in the target system.

In the reconciliation rule, Salesforce GUID on OIM should match the Account ID on target or User Login on OIM should match the UserName on the target system.

Reconciliation Rule for Users

The following is the process-matching rule for users:

Rule name: Salesforce User Trusted Recon Rule

Rule element: Salesforce GUID Equals ID or User Login Equals User Name

In this rule element:

- Salesforce GUID is the UDF Field for Salesforce Connector on OIM
- ID is the Account ID of Salesforec User on the target.
- User Login is the User ID field of the OIM User form.
- User Name is the name attribute which is unique field of the Salesforce account.

1.10.3 Reconciliation Action Rules for Trusted Source Reconciliation

Reconciliation action rules define the actions that must be performed based on the reconciliation rules.

Table 1-20 Action Rules for Trusted Source Reconciliation

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

1.11 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Deploying the Salesforce Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the Salesforce Connector describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Extending the Functionality of the Salesforce Connector describes the procedures to perform if you want to extend the functionality of the connector.
- Files and Directories on the Installation Media lists the files and directories in the installation media.

2
Deploying the Salesforce Connector

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

The following topics discuss these stages:

- Preinstallation
- Installation
- Postinstallation

2.1 Preinstallation

Preinstallation for the Salesforce connector involves registering a client application (that is, the Salesforce connector) with the target system and obtaining 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.

Preinstallation 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.

2.2 Installation

You must install the Salesforce connector in Oracle Identity Manager and if required, place the connector code bundle in the Connector Server.

The following topics discuss installing the Salesforce connector:

- Understanding Installation of the Salesforce Connector
- Running the Connector Installer
- Configuring the IT Resource for the Target System

2.2.1 Understanding Installation of the Salesforce Connector

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

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

- Run the connector code locally in Oracle Identity Manager.

  In this scenario, you deploy the connector in Oracle Identity Manager. Deploying the connector in Oracle Identity Manager involves performing the procedures described in Running the Connector Installer and Configuring the IT Resource for the Target System.

- Run the connector code remotely in a Connector Server.

  In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server.

2.2.2 Running the Connector Installer

> **Note:**
>
> In this guide, the term Connector Installer has been used to refer to the Install Connectors feature of Oracle Identity System Administration.

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory: `OIM_HOME/server/ConnectorDefaultDirectory`
2. If you have not already done so, create a directory in `OIM_HOME/ConnectorDefaultDirectory/targetsystems-lib` with the same name as the installer package. For example: `OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/Salesforce-11.1.1.5.0`

   > **Note:**
   >
   > If you are doing it for the first time place the bundle in the connector server bundle directory.

3. Log in to Oracle Identity System Administration.
4. In the left pane, under System Management, click **Manage Connector**.
5. In the Manage Connector page, click **Install**.
6. From the Connector List list, select **Salesforce Connector*RELEASE NUMBER***. This list displays the names and release numbers of connectors whose installation

files you copy into the default connector installation directory: `OIM_HOME/server/ConnectorDefaultDirectory`

If you have copied the installation files into a different directory, then:

a. In the **Alternative Directory** field, enter the full path and name of that directory.

b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

c. From the Connector List list, select **Salesforce Connector *RELEASE NUMBER.***

7. Click **Load**.

8. To start the installation process, click **Continue**. The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (by using the Deployment Manager)

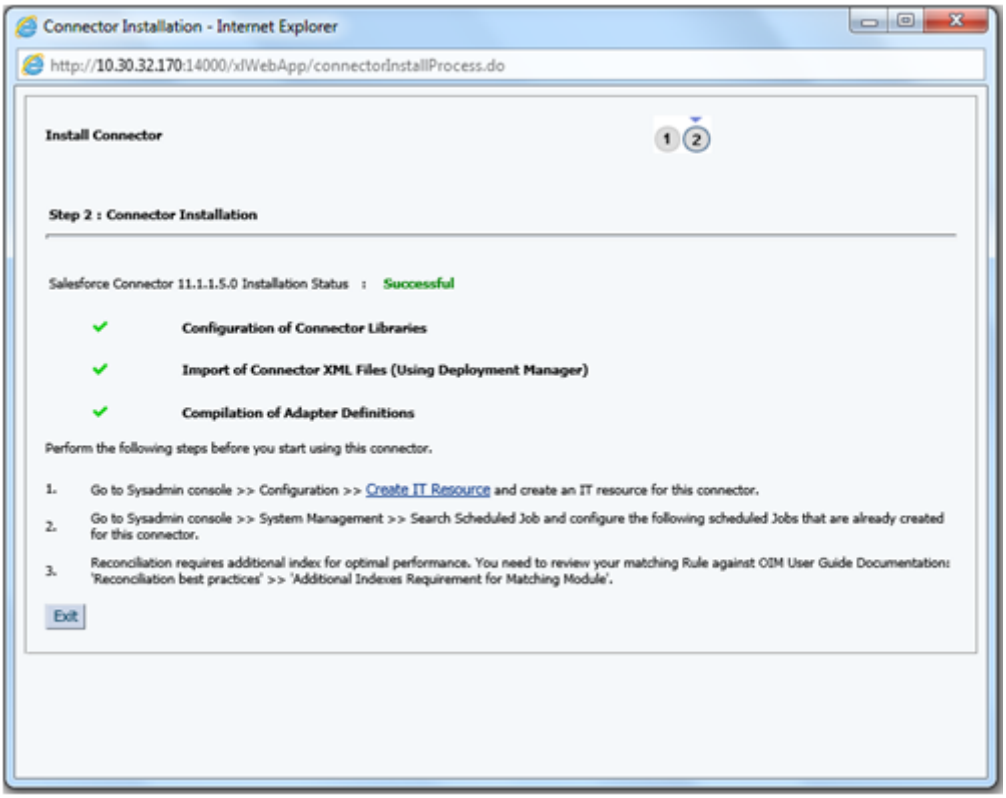
   c. Compilation of adapters

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

   a. Retry the installation by clicking **Retry**.

   b. Cancel the installation and begin again from step 3.

Figure 2-1 Installation Status



9. If all three tasks of the connector installation process are successful, then a message indicating successful installation appears.

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

   a. Ensuring that the prerequisites for using the connector are addressed

   > **Note:**
   >
   > At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. There are no prerequisites for some predefined connectors. See Clearing Content Related to Connector Resource Bundles from the Server Cache for information about running the PurgeCache utility. There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector

      Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

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

2.2.3 Configuring the IT Resource for the Target System

The IT resource for the target system is created during connector installation. This IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

The Salesforce IT resource is automatically created when you run the Connector Installer. You must specify values for the parameters of the IT resource.

To specify values for the parameters of the IT resource:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox.
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**.
5. Click **Edit** for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2-1 describes each parameter.

> **Note:**
>
> Entries in this table are sorted in alphabetical order of parameter names.

Table 2-1 Parameters of the IT Resource

Parameter	Description
acceptType	Accept type for the header that denotes how the request body must be parsed. The request body should only be parsed as JSON if the Content-Type header is application/json.
authenticationServerUrl	URL of the authentication server that validates the client ID and client secret. Sample value: `https://$HOTSNAME$.salesforce.com/services/oauth2/token?`
baseURI	Base relative URI of your target system. For example, if you are using version1 (v1), then the baseURI will be `/services/scim/v1`. Similarly, if you are using version2 (v2), then the baseURI will be `/services/scim/v2.`
clientId	The client identifier (a unique string) issued by the authorization server to your domain during the registration process performed in Preinstallation. Sample Value: `3MVG9Z8h6Bxz0zc6gU3lDg8zQflDLyyydUdH151g9VVT7O.ys_WFNz5q0EDkFWDAjDeavV5.XWVP6Hyhdg6zS`
clientSecret	Value used to authenticate the identity of your domain. This value is obtained while performing the procedure described in Preinstallation. Sample Value: `6551799938364196225`
Configuration Lookup	Name of the lookup definition that stores configuration information used during reconciliation and provisioning. Default value: `Lookup.Salesforce.Configuration`
ConnectorServer Name	If you are using Salesforce Connector together with the Java Connector Server, then provide the name of Connector Server IT Resource here.
contentType	This entry holds the content type expected by the target system in the header. Default Value : `application/json`

Table 2-1 (Cont.) Parameters of the IT Resource

Parameter	Description
grantType	Type of authentication used by your target system. grantTypes supported by the SCIM code are `basic`, `jwt`,`client_credentials`, `password`, and `custom`. However, the grantType supported by Salesforce is `password` only. Default value: `password`
Host	Salesforce Host name or IP address of the computer hosting the target system. Sample value: `www.*****.salesforce.com`
Password	Enter the password of the target system user account that you created (for connector operations) while performing the procedure described in Preinstallation.
sslEnabled	If the target system requires SSL connectivity, set the value of this parameter to `true`. Otherwise set the value to `false`.
proxyHost	Name of the proxy host used to connect to an external target. Sample value: `www.example.com`
proxyPassword	Password of the proxy user ID of the target system user account that Oracle Identity Manager uses to connect to the target system.
proxyPort	Proxy port number. Sample value: `80`
proxyUser	Proxy user name of the target system user account that Oracle Identity Manager uses to connect to the target system.
Username	Enter the user name of the target system that you created (for performing connector operations) while performing the procedure described in Preinstallation.

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

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Configuring Oracle Identity Manager
- Localizing Field Labels in UI Forms
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Managing Logging for the Salesforce Connector
- Obtaining GUID of Roles

2.3.1 Configuring Oracle Identity Manager

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

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

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

2.3.1.1 Creating and Activating a Sandbox

See Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for instructions on creating and activating a sandbox.

2.3.1.2 Creating a New UI Form

See Managing Forms in *Oracle Fusion Middleware Administering Oracle Identity Manager* for instructions on creating a new UI form. While creating the UI form, ensure that you select the resource object corresponding to the Salesforce connector that you want to associate the form with.

2.3.1.3 Creating an Application Instance

Create an application instance as follows.

For detailed instructions, see Managing Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

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 Manager* for detailed instructions.

2.3.1.4 Publishing a Sandbox

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

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

2.3.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Jobs for Lookup Field Synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.3.1.6 Updating an Existing Application Instance with a New Form

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

1. Create a sandbox and activate it as described in Creating and Activating a Sandbox.
2. Create a new UI form for the resource as described in Creating a New UI Form.
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 as described in Publishing a Sandbox.

2.3.2 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. 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-unitid="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']['persdef.sessiondef.oracle.iam.ui.
runtime.form.model.user.entity.userEO.UD_SF_USR_USERNAME__c_descr
iption']}">

<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*.xlf. In this file name, replace *LANG_CODE* with the code of the language to which you are localizing. Sample file name: BizEditorBundle_ja.xlf

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

> **See Also:**
>
> Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about exporting and importing metadata files.

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

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

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

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

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

> **Note:**
>
> You can use the PurgeCache utility to purge the cache for any content category. Run PurgeCache.bat *CATEGORY_NAME* on Microsoft Windows or PurgeCache.sh *CATEGORY_NAME* on UNIX. The *CATEGORY_NAME* argument represents the name of the content category that must be purged.
> For example, the following commands purge Metadata entries from the server cache:
>
> - `PurgeCache.bat MetaData`
> - `PurgeCache.sh MetaData`
>
> Before running the PurgeCache utility, ensure the WL_HOME and JAVA_HOME environment variables are set.

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

t3://*OIM_HOST_NAME*:*OIM_PORT_NUMBER*

In this format:

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

2.3.4 Managing Logging for the Salesforce Connector

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

2.3.4.1 Understanding Log Levels

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. ODL is the principle logging service used by Oracle Identity Manager and is based on java.util.Logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

These log levels are mapped to ODL message type and level combinations as shown in Table 2-2.

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

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

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

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

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

2.3.4.2 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.GENERICSCIM" 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 2-2 lists the supported message type and level combinations.

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

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

```
<log_handler name='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_server1\logs\
     oim_server1-diagnostic-1.log'/>
    <property name='format' value='ODL-Text'/>
    <property name='useThreadName' value='true'/>
    <property name='locale' value='en'/>
    <property name='maxFileSize' value='5242880'/>
    <property name='maxLogSize' value='52428800'/>
    <property name='encoding' value='UTF-8'/>
  </log_handler>

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

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

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

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

   For UNIX: export WLS_REDIRECT_LOG=***FILENAME***

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

2.3.5 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 SCIM services exposed by Salesforce.com do not provide any endpoint to fetch the Role GUIDs programatically. 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
```

2.3.6 Configuring SSL for connector

Configure SSL to secure data communication between Oracle Identity Manager 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 Manager.

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

In this example, the certificate file `supportcert.pem` is imported to the identity keystore `client_store.jks` with password `weblogic1`:

```
keytool -import -alias serverwl -trustcacerts -file supportcert.pem -
keystore client_store.jks -storepass weblogic1
```

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

3
Using the Salesforce Connector

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

This chapter discusses the following topics:

> **Note:**
>
> These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

3.1 Scheduled Jobs for Lookup Field Synchronization

Scheduled jobs for lookup field synchronization fetch the most recent values from specific fields in the target system to lookup definitions in Oracle Identity Manager. These lookup definitions are used as an input source for lookup fields in Oracle Identity Manager.

The following scheduled jobs are used for lookup field synchronization:

- Salesforce Group Lookup Reconciliation Scheduled Job
- Salesforce Profile Lookup Reconciliation Scheduled Job

Table 3-1 describes the attributes of both scheduled jobs. The procedure to configure scheduled tasks is described later in this guide.

> **Note:**
>
> The target system allows you to use special characters in lookup fields. However, in Oracle Identity Manager, special characters are not supported in lookup definitions.

Table 3-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Enter the name of the attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default Value: `__UID__`
Decode Attribute	Enter the name of the attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default Value: `__NAME__`
IT Resource Name	Name of the IT resource for the target system installation from which you reconcile user records. Default value: `Salesforce`
Lookup Name	Name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Depending on the scheduled job you are using, the default values are as follows: • For Salesforce Group Lookup Reconciliation Scheduled Job: `Lookup.Salesforce.Groups` • For Salesforce Profile Lookup Reconciliation Scheduled Job: `Lookup.Salesforce.Profiles`
Object Type	Name of the type of object you want to reconcile. Depending on the scheduled job you are using, the default values are as follows: • For Salesforce Group Lookup Reconciliation Scheduled Job: `Group` • For Salesforce Profile Lookup Reconciliation Scheduled Job: `Entitlement`

3.2 Configuring Reconciliation for Salesforce Connector

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

This section discusses the following topics related to configuring reconciliation:

- Full Reconciliation
- Limited Reconciliation
- Reconciling Large Number of Records
- Reconciliation Scheduled Jobs

3.2.1 Full Reconciliation

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

> **Note:**
>
> To eliminate the Automated Process User that the Salesforce sandbox has and to get all the users successfully during full reconciliation, you must add the following filter, `greaterThan('userType','AutomatedProcest')|lessThan('userType','AutomatedProcess')`

To perform a full reconciliation run, remove or delete any value assigned to the Filter and run the scheduled job for user reconciliation.

> **Note:**
>
> - 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.

3.2.2 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.

> **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.

For detailed information about Filters, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

3.2.3 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 Manager.

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

1. Export all users in the target system to a flat file.
2. Copy the flat file to a location that is accessible from Oracle Identity Manager.
3. Create a schema file representing the structure of the flat file.
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`.

3.2.4 Reconciliation Scheduled Jobs

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

This section discusses the following scheduled jobs that you can configure for reconciliation:

- Scheduled Jobs for Reconciliation of User Records
- Scheduled Job for Reconciliation of Groups

3.2.4.1 Scheduled Jobs for Reconciliation of User Records

The scheduled jobs for user reconciliation include Salesforce Target Resource User Reconciliation and Salesforce Trusted User Reconciliation that are used when you want to run the connector in the target resource and trusted source modes respectively.

Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled jobs:

- Salesforce Target Resource User Reconciliation

  This scheduled job is used to reconcile user data in the target resource (account management) mode of the connector.

- Salesforce Trusted User Reconciliation

  This scheduled job is used to reconcile user data in the trusted source (identity management) mode of the connector.

Table 3-2 describes the attributes of both scheduled jobs.

Table 3-2 Attributes of the Scheduled Job for User Reconciliation

Attribute	Description
Filter	Enter the search filter for fetching user records from the target system during a reconciliation run. See ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for sample values.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. The default value of this attribute in the Salesforce Target Resource User Reconciliation scheduled job is `Salesforce`. The default value of this attribute in the Salesforce Trusted User Reconciliation scheduled job is `Salesforce Trusted`.
Object Type	Type of object you want to reconcile. Default value: `User` Do *not* change the value of the attribute.

Table 3-2 (Cont.) Attributes of the Scheduled Job for User Reconciliation

Attribute	Description
Resource Object Name	Name of the resource object against which reconciliation runs must be performed. The default value of this attribute in the Salesforce Target Resource User Reconciliation scheduled job is `Salesforce User`. The default value of this attribute in the Salesforce Trusted User Reconciliation scheduled job is `Salesforce User Trusted`. Do *not* change the value of this attribute.

3.2.4.2 Scheduled Job for Reconciliation of Groups

The Salesforce Group Recon scheduled job is used to reconcile group data from the target system.

Table 3-3 Attributes of the Salesforce Group Recon Scheduled Job

Attribute	Description
Filter	Enter the search filter for fetching group records from the target system during a reconciliation run. See ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for sample values.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group data. Default value: `Salesforce`
Object Type	Type of object you want to reconcile. Default value: `Group` Do *not* change the value of the attribute.
OIM Organization Name	Enter the name of the Oracle Identity Manager organization in which reconciled groups must be created or updated. Sample Value: Xellerate Users.
Resource Object Name	Name of the resource object against which reconciliation runs must be performed. Default value: `Salesforce Group` Do *not* change the value of this attribute.
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `Salesforce Group Recon`

3.3 Configuring Scheduled Jobs

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

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

To configure a scheduled job:

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

   > **Note:**
   >
   > See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

   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:**
   >
   > - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
   > - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
   > - See Reconciliation Scheduled Jobs for the list of scheduled tasks and their attributes.

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

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

3.4 Guidelines on Performing Provisioning Operations

These guidelines provide information on what to do when performing provisioning operations.

You must apply the following guideline while performing a provisioning operation:

- 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 Manager in synchronization.

3.5 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Manager:

1. Log in to Oracle Identity Self Service.
2. Create a user. See Managing Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts**.
4. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit.**
7. If you want to provision entitlements, then:
   - On the Entitlements tab, click **Request Entitlements**.
   - In the Catalog page, search for and add to cart the entitlement, and then click **Checkout**.
   - Click **Submit**.

3.6 Uninstalling the Salesforce Connector

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

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the Salesforce Connector

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

This chapter discusses the following topics:

> **Note:**
>
> From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* for information about managing lookups by using the Form Designer in the Oracle Identity System Administration.

- Adding New User or Group Attributes for Reconciliation
- Adding New User or Group Attributes for Provisioning
- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During User Reconciliation
- Configuring the Connector for Multiple Installations of the Target System
- Defining the Connector

4.1 Adding New User or Group Attributes for Reconciliation

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

The default attribute mappings for reconciliation are listed in Table 1-13 and Table 1-14.

- Adding New Attributes on the Process Form
- Adding Attributes to Reconciliation Fields
- Creating Reconciliation Field Mapping
- Creating Entries in Lookup Definitions
- Performing Changes in a New UI Form

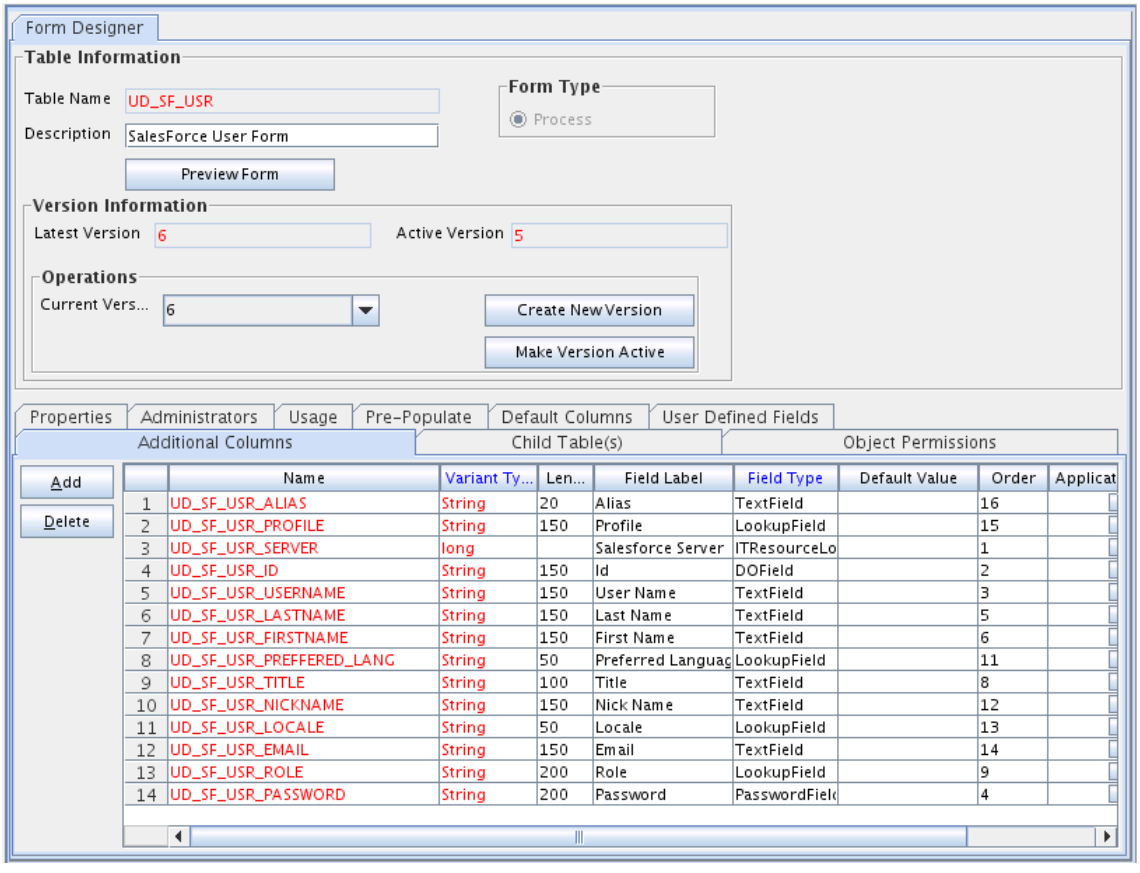
4.1.1 Adding New Attributes on the Process Form

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

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
   a. Expand **Development Tools**, and then double-click **Form Designer**.
   b. Search for and open one of the following process forms:
      - For Users: **UD_SF_USR**
      - For Groups: **UD_SF_GRP**
   c. Click **Create New Version**, and then click **Add**.
   d. Enter the details of the field.

      For example, if you are adding the ALIAS field, enter `UD_SF_USR_ALIAS` in the Name field and then enter other details such as Variable Type, Length, Field Label, and Field Type.
   e. Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form.

Figure 4-1 Form Designer



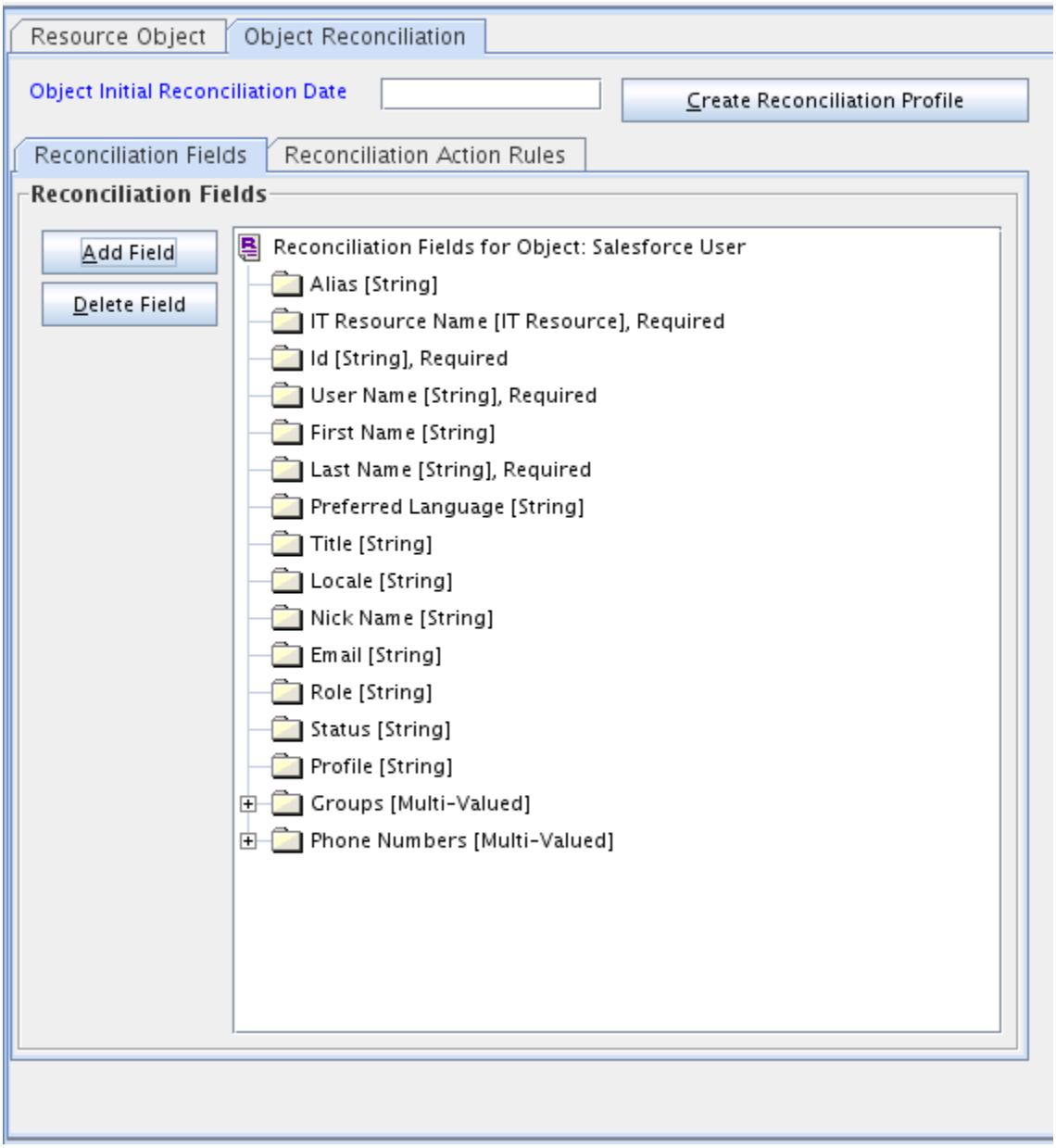
4.1.2 Adding Attributes to Reconciliation Fields

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

1. Expand **Resource Management**, and double-click **Resource Objects**.
2. Search for and open one of the following resource objects:
   - For Users: **Salesforce User**
   - For Groups: **Salesforce Groups**
3. On the Object Reconciliation tab, click **Add Field**.
4. Enter the details of the field.

   For example, enter `ALIAS` in the **Field Name** field and select **String** from the Field Type list.
5. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:

Figure 4-2 Object Reconciliation Tab

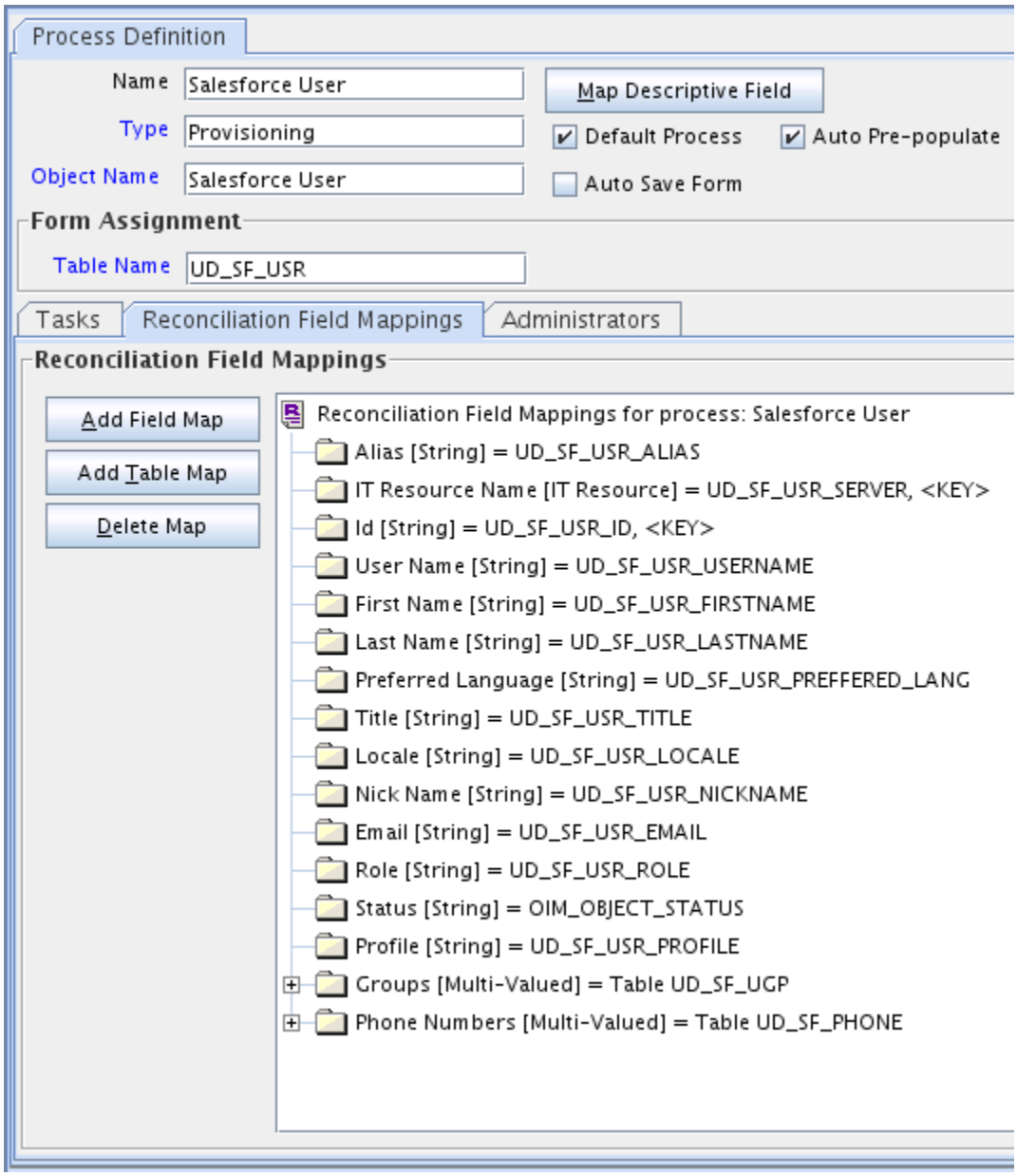


4.1.3 Creating Reconciliation Field Mapping

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

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

Figure 4-3 Process Definition Tab



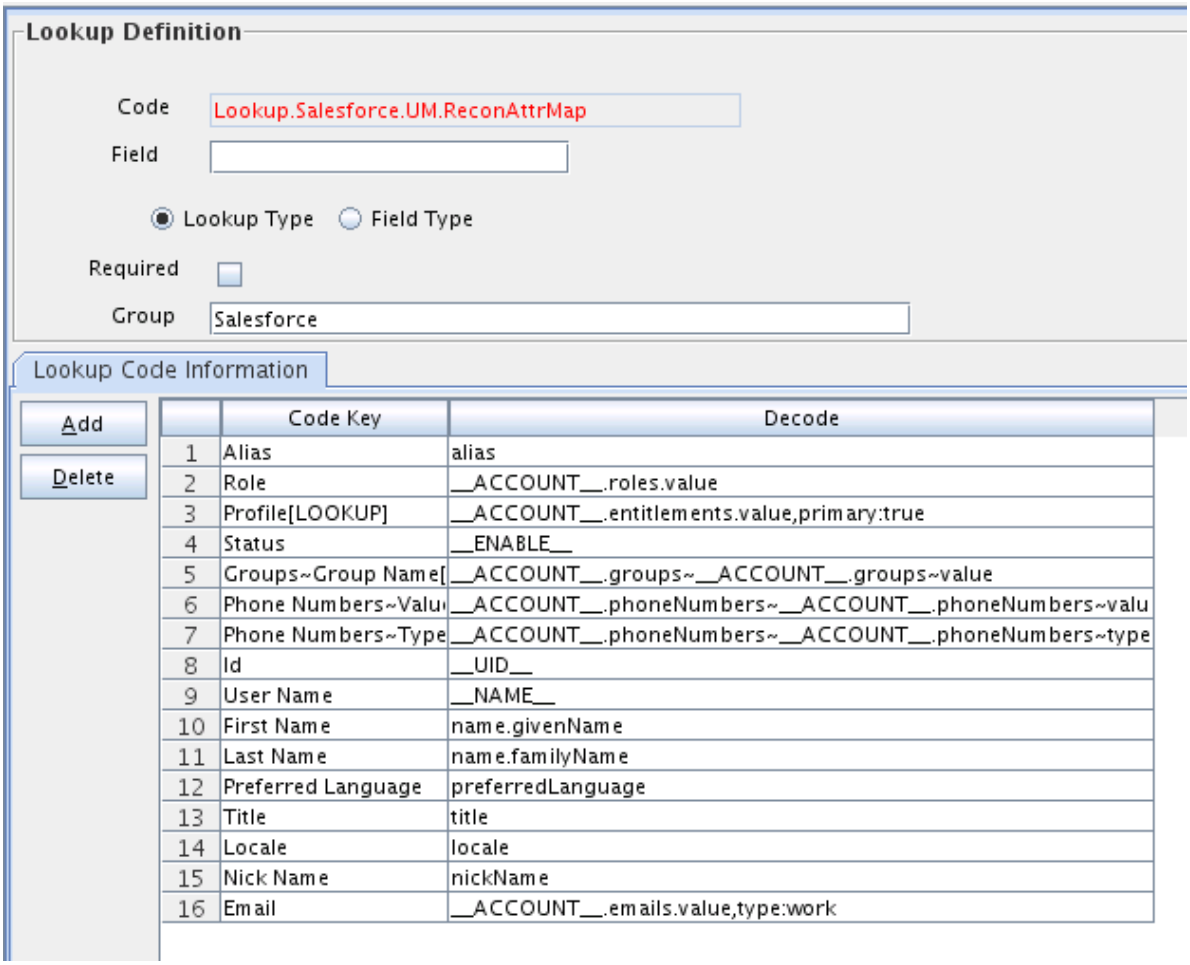
4.1.4 Creating Entries in Lookup Definitions

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

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open one of the following lookup definitions:
   - For Users: **Lookup.Salesforce.UM.ReconAttrMap**
   - For Groups: **Lookup.Salesforce.GM.Recon.AttrMap**

4. Click **Add** and enter the Code Key and Decode values for the field. The Code Key value must be the name of the field in the resource object.
5. Click the Save icon. The following screenshot shows the entry added to the lookup definition:

Figure 4-4 Lookup Definition Page



4.1.5 Performing Changes in a New UI Form

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

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

5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

4.2 Adding New User or Group Attributes for Provisioning

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

The default attribute mappings for provisioning are listed in Table 1-13 and Table 1-17. The following topics discuss the procedure to add new user or group attributes for provisioning:

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

4.2.1 Adding New Attributes for Provisioning

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

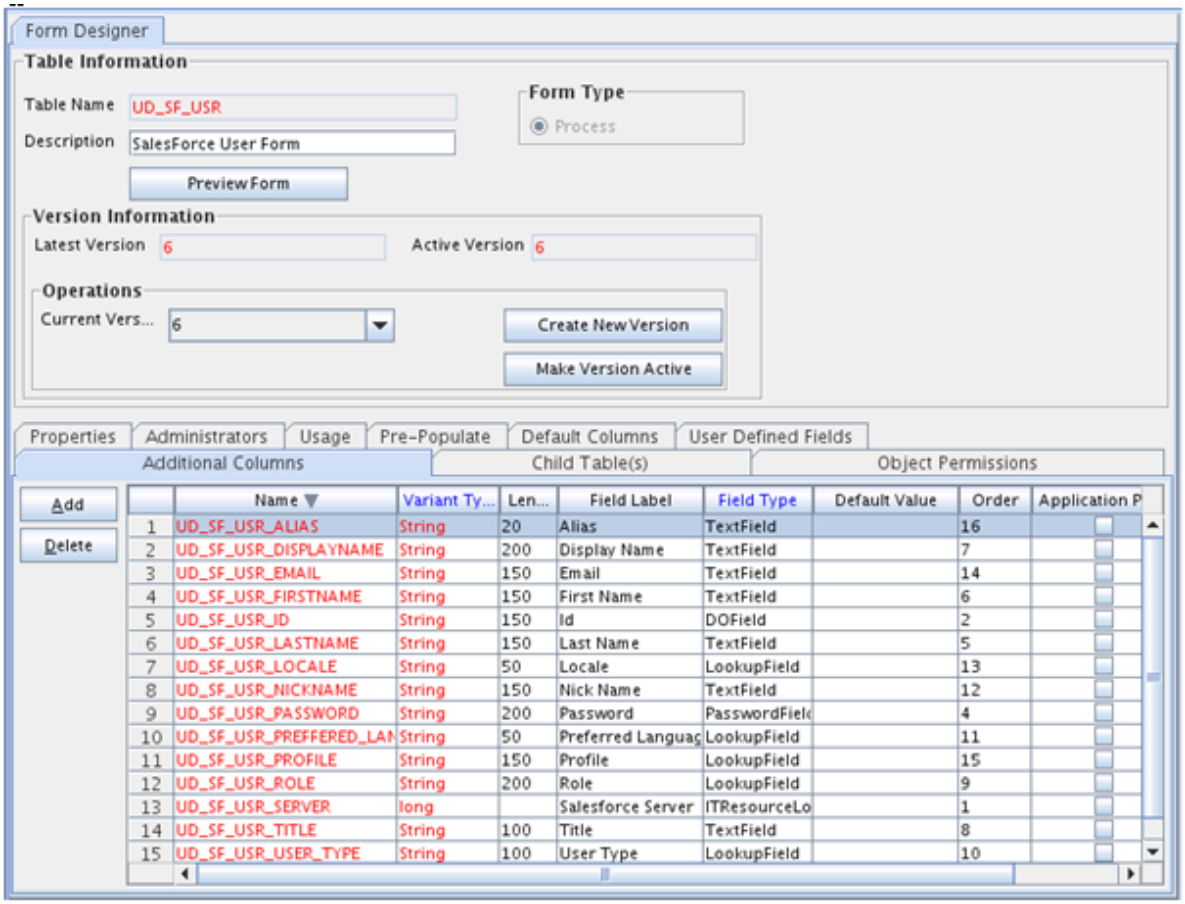
> **Note:**
>
> If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

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

   For example, if you are adding the ALIAS field, enter `UD_SF_USR_ALIAS` in the Name field, and then enter the rest of the details of this field.
6. Click the Save icon, and then click **Make Version Active**.

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

Figure 4-5 New Field Added to the Process Form



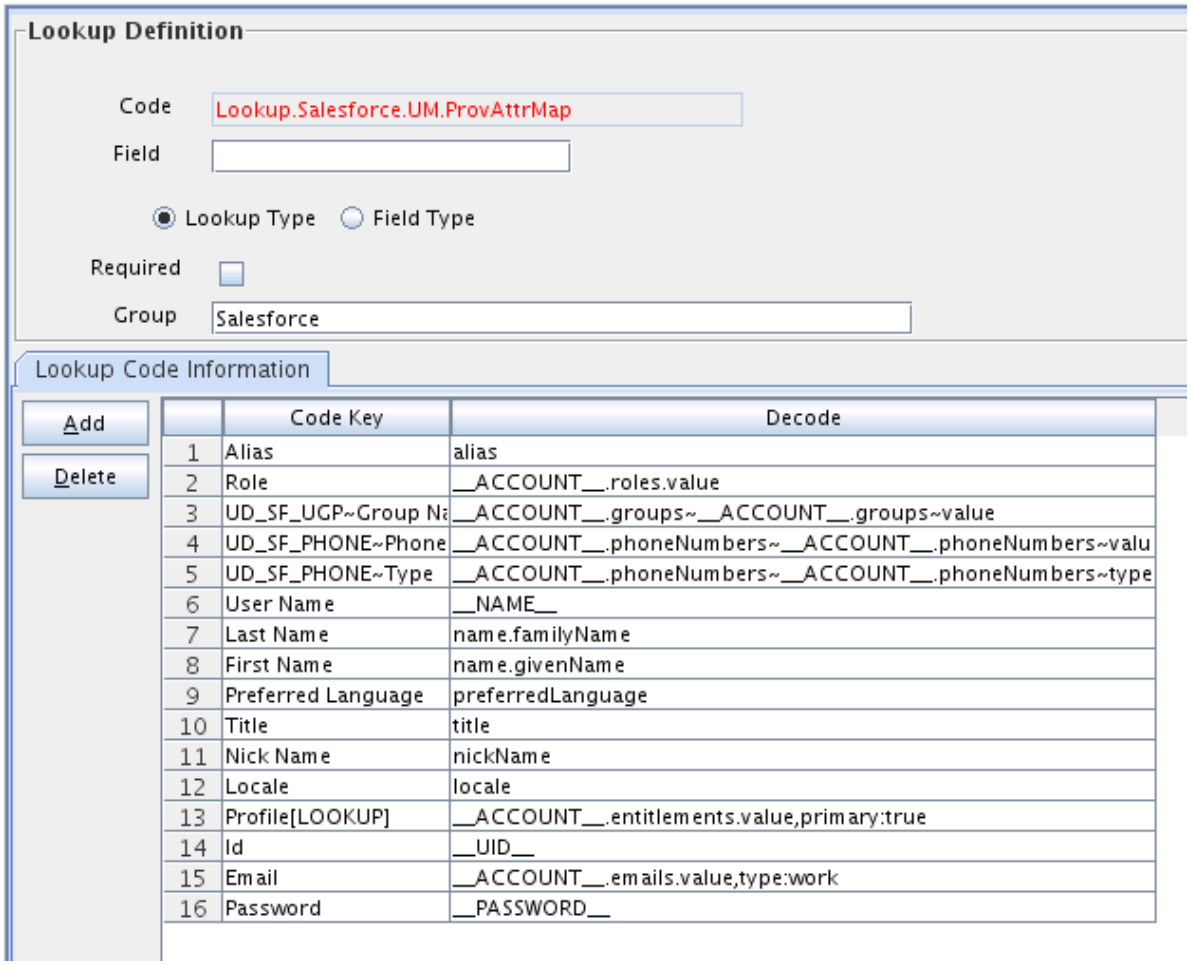
4.2.2 Creating Entries in Lookup Definitions for Provisioning

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

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open one of the following lookup definitions:
   - For Users: **Lookup.Salesforce.UM.ProvAttrMap**
   - For Groups: **Lookup.Salesforce.GM.ProvAttrMap**
4. Click **Add** and then enter the Code Key and Decode values for the attribute.

   For example, enter `Alias` in the Code Key column and then enter `alias` in the Decode column. The following screenshot shows the entry added to the lookup definition:

Figure 4-6 Entry Added to the Lookup Definition



4.2.3 Creating a Task to Enable Update Operations

Create a task to enable updates on the new user or group attribute during provisioning operations.

If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

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

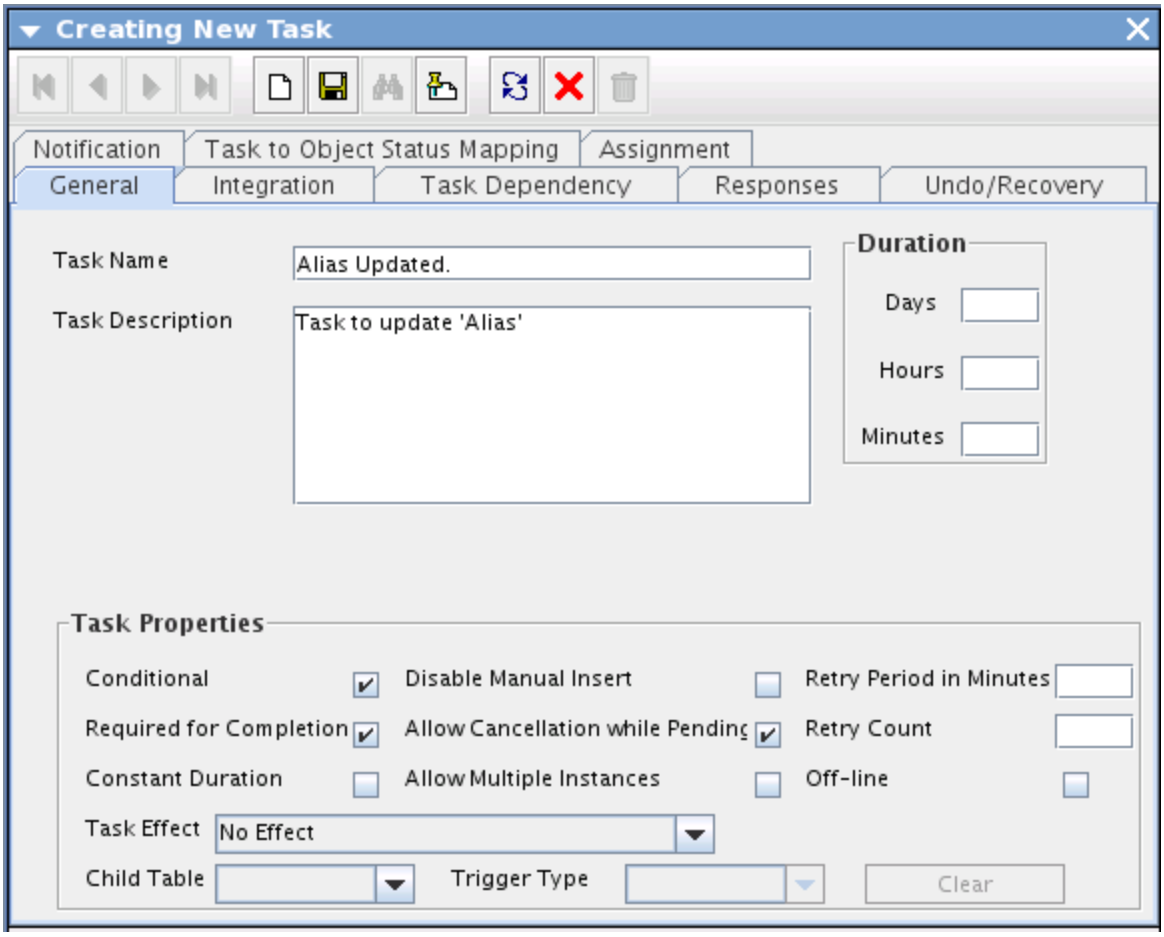
1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open one of the following process definitions:
   - For Users: **Salesforce User**
   - For Groups: **Salesforce Group**
3. Click **Add**.
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
   - Conditional

- Required for Completion
- Allow Cancellation while Pending
- Allow Multiple Instances

5. Click the Save icon.

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

Figure 4-7 New Task Added to the Process Definition



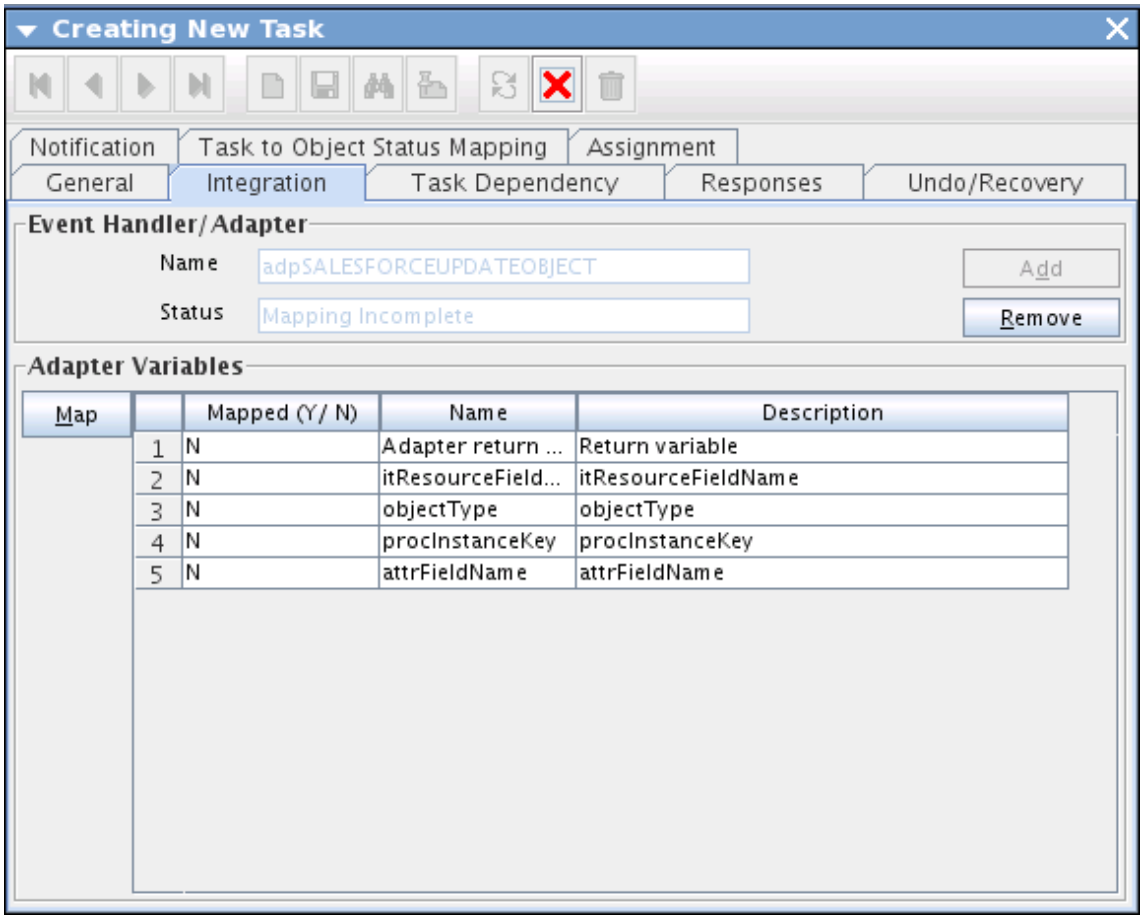
6. In the provisioning process, select the adapter name in the Handler Type section as follows:

   a. On the Integration tab of the Creating New Task dialog box, click **Add**.

   b. In the Handler Selection dialog box, select **Adapter**, click **adpSALESFORCEUPDATEOBJECT**, and then click the Save icon.

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

Figure 4-8 List of Adapter Variables



7. In the Adapter Variables region, click the **ParentFormProcessInstanceKey** variable.
8. In the dialog box that is displayed, create the following mapping:
   - Variable Name: **ParentFormProcessInstanceKey**
   - Map To: **Process Data**
   - Qualifier:**Process Instance**
9. Click **Save** and close the dialog box.
10. If you are enabling update provisioning operations for a User attribute, then repeat Steps 7 through 9 for the remaining variables listed in the Adapter Variables region.

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

Variable	Map To	Qualifier	Literal Value
Adapter Return Value	Response Code	NA	NA
Object Type	Literal	String	User
itResourceFieldName	Literal	String	UD_SF_USR_SERVER

Variable	Map To	Qualifier	Literal Value
attributeFieldName	Literal	String	Alias

11. If you are enabling update provisioning operations for a Group attribute, then repeat Steps 7 through 9 for the remaining variables listed in the Adapter Variables region.

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

Variable	Map To	Qualifier	Literal Value
ParentFormProcessInstanceKey	Process Data	Process Instance	NA
Adapter Return Value	Response Code	NA	NA
Object Type	Literal	String	Group
itResourceFieldName	Literal	String	UD_SF_GRP_SERVER
attributeFieldName	Literal	String	NAME_OF_THE_NEW_GROUP_ATTRIBUTE

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

4.2.4 Replicating Form Designer Changes to a New UI Form

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

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

4.3 Configuring Validation of Data During Reconciliation and Provisioning

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

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

For data that fails the validation check, the following message appears or recorded in the log file:

```
Validation failed for attribute ATTRIBUTE_NAME.
```

> **Note:**
>
> This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

To configure validation of data:

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

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

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

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

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

```
"true"
       is
       *    returned.
        */
           boolean valid=true;
           String sUserName=(String) hmUserDetails.get(field);
for(int
   i=0;i<sUserName.length();i++){
     if (sUserName.charAt(i) == '#'){
         valid=false;
         break;
                }
                }
          return valid;
            }
```

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

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

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

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

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

4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.Salesforce.UM.ReconValidation.**
   c. Save the changes to the lookup definition.
   d. Search for and open the **Lookup.Salesforce.UM.Configuration** lookup definition.
   e. Save the changes to the lookup definition.
5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.Salesforce.UM.ProvValidation.**

c. In the Code Key column, enter the process form field name. For example, `User Name`. In the Decode column, enter the class name. For example, `org.identityconnectors.Salesforce.extension`.

d. Save the changes to the lookup definition.

e. Search for and open the **Lookup.Salesforce.UM.Configuration** lookup definition.

f. Save the changes to the lookup definition.

4.4 Configuring Transformation of Data During User Reconciliation

You can configure transformation of reconciled single-valued account data according to your requirements.

For example, you can use User Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

> **Note:**
>
> This feature cannot be applied to the Locked/Unlocked status attribute of the target system.

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

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

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

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

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

   ```
   package oracle.iam.connectors.common.transform;
   import java.util.HashMap;
   public class TransformAttribute {
       /*
       Description:Abstract method for transforming the attributes
       param hmUserDetails<String,Object>
       HashMap containing parent data details
       param hmEntitlementDetails<String,Object>
       HashMap containing child data details
       */
            public Object transform(HashMap hmUserDetails, HashMap
       hmEntitlementDetails,String sField) {
   /*
   *    You must write code to transform the attributes.
   Parent data attribute values can be fetched by using
   ```

```
   hmUserDetails.get("Field Name").
   *To fetch child data values, loop through the
 *    ArrayList/Vector fetched by hmEntitlementDetails.get("Child
Table")
 *    Return the transformed attribute.
   */
      String sUserName= (String)hmUserDetails.get("User Name");
      String sLastName= (String)hmUserDetails.get("Last Name");
      String sFullName=sUserName+"."+sLastName;
      return sFullName;
      }
   }
```

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

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

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

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

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

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.
4. If you created the Java class for transforming a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.Salesforce.UM.ReconTransformation.**
   c. In the Code Key column, enter the resource object field name on which you want to apply transformation. For example, `User Name`. In the Decode column, enter the name of the class that implements the transformation logic. For example, `oracle.iam.connectors.common.transform.TransformAttribute`.
   d. Save the changes to the lookup definition.
5. Add an entry in the Lookup.Salesforce.UM.Configuration lookup definition to enable transformation as follows:
   a. Expand Administration, and then double-click **Lookup Definition.**
   b. Search for and open the **Lookup.Salesforce.UM.Configuration** lookup definition.

c. In the Code Key column, enter `Recon Transformation Lookup`. In the Decode column, enter `Lookup.Salesforce.UM.ReconTransformation`.

d. Save the changes to the lookup definition.

4.5 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system.

The following example illustrates this requirement:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

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

4.6 Defining the Connector

By using the Identity System Administration, you can define a customized or reconfigured connector. Defining a connector is equivalent to registering the connector with Oracle Identity Manager.

A connector is automatically defined when you install it using the Install Connectors feature or when you upgrade it using the Upgrade Connectors feature. You must manually define a connector if:

- You import the connector by using the Deployment Manager.
- You customize or reconfigure the connector.
- You upgrade Oracle Identity Manager.

The following events take place when you define a connector:

- A record representing the connector is created in the Oracle Identity Manager database. If this record already exists, then it is updated:
- The status of the newly defined connector is set to Active. In addition, the status of a previously installed release of the same connector automatically is set to Inactive.

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

5

Known Issues and Workarounds for the Salesforce Connector

There are no known issues associated with this release of the connector.

A

Files and Directories on the Installation Media

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

Table A-1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
bundle/ org.identityconnectors.genericscim-1.0.1115	This JAR is the Identity Connector bundle.
configuration/Salesforce-CI.xml	This XML file contains configuration information that is used during connector installation
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the Oracle Identity Manager database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/Salesforce-ConnectorConfig.xml	This XML file contains definitions for the following connector objects: • IT resource definition • Process forms • Process tasks and adapters • Lookup definitions • Resource objects • Process definitions • Scheduled tasks