Oracle® Identity Governance

Configuring the SAP SuccessFactors Application

Release 12c (12.2.1.3.0)
F12374-06
August 2022

Oracle Identity Governance Configuring the SAP SuccessFactors Application, Release 12c (12.2.1.3.0)

F12374-06

Primary Author: Alankrita Prakash

Contributors: Gowri.G.R

Contents

Preface

What's New in This Guide?

1 About the SAP SuccessFactors Connector

2 Creating an Application by Using the SAP SuccessFactors Connector

3 Configuring the SAP SuccessFactors Connector

4 Performing the Postconfiguration Tasks for the SAP SuccessFactors Connector

5 Using the SAP SuccessFactors Connector

6 Extending the Functionality of the SAP SuccessFactors Connector

List of Figures

List of Tables

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

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

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

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

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

Conventions

The following text conventions are used in this document:

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

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

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

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

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

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

Conventions

The following text conventions are used in this document:

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

What’s New in This Guide?

These are the updates made to the software and documentation for release 12.2.1.3.0.

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

- Software Updates

  This section provides details on the updates made to the connector software.

- Documentation-Specific Updates

  This section provides details on the major changes that are made to this guide. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

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

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following is a documentation-specific update for revision "05" of the guide:

All Oracle Identity Manager versions prior to 11*g* Release 2 PS3 (11.1.2.3.0) have been removed from Table 1-1.

The following are documentation-specific updates for revision "04" of the guide:

- A Note about Group Management has been added to Supported Connector Operations.
- Information about Proxy Server has been added to Basic Configuration Parameters .

The following are documentation-specific updates for revision "03" of the guide:

- Information about Group Management has been added to Supported Connector Operations.

- Information about Entitlement Grant Management has been added to Use Cases Supported by the Connector.
- Defalut values for parameters lookupUrl, upsertUrl, and customURIs has been updated in Table 3-2 of Advanced Setting Parameters.
- Information about child form "Groups" has been added to Attribute Mappings for the Target Application.
- A new scheduled job for Groups has been added to Reconciliation Jobs.

The following are the documentation-specific updates for revision "02" of the guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance release 12c PS4 (12.2.1.4.0).
- The "Oracle Identity Governance or Oracle Identity Manager JDK", "Connector Server", and "Connector Server JDK" rows of Table 1-1 have been updated.
- Several broken links were fixed throughout the document.

The following is a documentation-specific update for revision "01" of the guide:

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

1 About the SAP SuccessFactors Connector

Oracle Identity Governance 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 Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications.

The SAP SuccessFactors connector lets you create and onboard SAP SuccessFactors applications in Oracle Identity Governance.

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

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

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

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

- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations
- Connector Architecture
- Use Cases Supported by the Connector
- Connector Features

1.1 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Manager or Oracle Identity Governance	You can use any one of the following releases: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0)	You can use one of the following releases: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 BP06 (11.1.2.3.6)
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 or later	JDK 1.8 or later
Target systems	SAP SuccessFactors	SAP SuccessFactors
Connector Server	11.1.2.1.0 or later	11.1.2.1.0 or later
Connector Server JDK	JDK 1.8 or later	JDK 1.8 or later

1.2 Usage Recommendation

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

- If you are using Oracle Identity Governance 12c (12.2.1.3.0), then use the latest 12.2.1.x version of this connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.
- If you are using any of the Oracle Identity Manager releases listed in the “Requirement for CI-Based Connector” column in Table 1-1, then use the 11.1.*x* version of the SAP SuccessFactors connector. If you want to use the 12.1.*x* version of this connector, then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0.

1.3 Certified Languages

These are the languages that the connector supports.

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)

- Czech
- Danish
- Dutch
- English
- Finnish
- French
- French (Canadian)
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.4 Supported Connector Operations

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

Table 1-2 Supported Connector Operations

Operation	Supported
User Management	
Create user	Yes
Update user	Yes

Table 1-2 (Cont.) Supported Connector Operations

Operation	Supported
Delete User	Yes **Note**: In the current release, delete operation is not supported by the target application. When you execute a user-delete operation from the connector application, the deleted user gets disabled on the target application.
Enable User	Yes
Disable User	Yes
Test Connection	Yes
Group Management	**Note**: To obtain support for group management, apply patch SuccessFactors-12.2.1.3.0B or later.
Add group	Yes
Add multiple groups	Yes
Remove group	Yes
Remove multiple groups	Yes
Assign single or multiple groups	Yes
Remove single or multiple groups	Yes

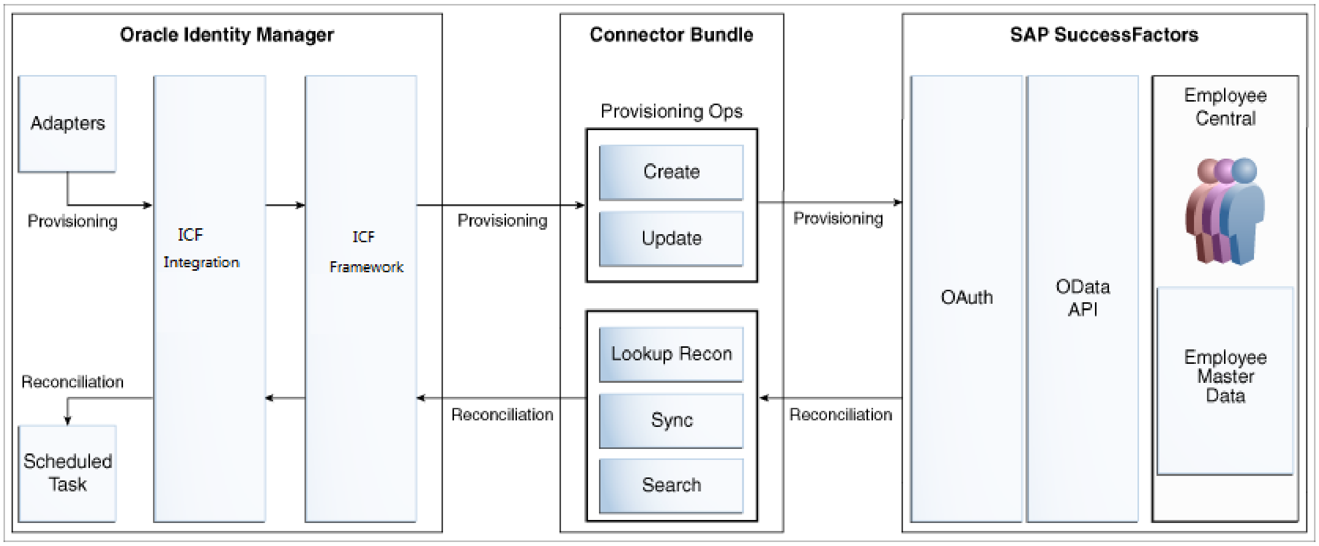
1.5 Connector Architecture

The SuccessFactors 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 Governance connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as, buffering, time outs, and filtering. ICF is distributed together with Oracle Identity Governance. Therefore, you do not need to configure or modify ICF.

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

Figure 1-1 Architecture of the SuccessFactors Connector



The connector is configured to run in one of the following modes:

- Identity reconciliation

  Identity reconciliation is also known as authoritative. In this mode, the target system is used as an authoritative source and users are directly created and modified on Oracle Identity Governance by reconciliation jobs. During reconciliation, a scheduled task invokes an ICF operation. ICF inturn invokes a search operation on the SuccessFactors Connector Bundle and then the bundle calls the OData API for reconciliation operation. The API extracts user records that match the reconciliation criteria and hands them over through the bundle and ICF back to the scheduled task, which brings the records to Oracle Identity Governance.

  Each user record fetched from the target system is compared with existing Oracle Identity Governance Users. If a match is found between the target system record and the Oracle Identity Governance User, then the Oracle Identity Governance 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 Oracle Identity Governance 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 and updating users on the target system through Oracle Identity Governance. During provisioning, the adapters invoke ICF operation, ICF inturn invokes create operation on the SuccessFactors Identity Connector Bundle and then the bundle calls the target system API for provisioning operations. The 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.

  - Target resource reconciliation

During reconciliation, a scheduled task invokes an ICF operation. ICF inturn invokes a search operation on the SuccessFactors Identity Connector Bundle and then the bundle calls the target system API for reconciliation operation. The API extracts user records that match the reconciliation criteria and hands them over through the bundle and ICF back to the scheduled task, which brings the records to Oracle Identity Governance.

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

1.6 Use Cases Supported by the Connector

The SAP SuccessFactors application uses the Software as a Service (SaaS) model and supports full human resource lifecycle functions on a single platform. The SAP SuccessFactors application allows an organization to make various data-driven people management decisions. The SAP SuccessFactors connector integrates Oracle Identity Governance with SuccessFactors application.

The SAP SuccessFactors connector standardizes service processes and implements automation to replace manual tasks. The SuccessFactors connector enables you to use SuccessFactors either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Governance. Multiple instances of SuccessFactors solution can use a single connector bundle.

User Management and Entitlement Grant Management are example scenarios which the SuccessFactors connector facilitates:

User Management

An organization using SAP SuccessFactors wants to integrate with Oracle Identity Governance to manage the employee provisioning operations. The organization wants to manage its employee information (add and update functions) by creating them in the target system using Oracle Identity Governance. The organization also wants to synchronize employee updates performed directly in the target system with Oracle Identity Governance. In such a scenario, a quick and an easy way is to install the SuccessFactors connector and configure it with your target system by providing connection information in the IT resource.

The SuccessFactors connector is used to manage various employee attributes such as email id, hire-date, and job-level.

Entitlement Grant Management

In SuccessFactors context, static permission groups are created and modified by adding individual user names to a group using an excel spreadsheet. They store a static list of users instead of a list based on dynamically generated criteria. Changing user information does not modify group members. However, you must redefine group members by importing an updated spreadsheet.

The SAP SuccessFactors Connector enables an organization to add and remove users from a static group. It also helps fetch static group memberships through reconciliation for a user. If a user with an existing SuccessFactors application wants to manage group membership, they must initially migrate the pre-existing SuccessFactors static groups into Oracle Identity Governance.

In terms of operational capability, the connector facilitates user reconciliation and group lookup reconciliation. From Oracle Identity Governance, however, connector group membership is limited to SAP SuccessFactors Static groups only. Dynamic groups are managed by SuccessFactors but READ-ONLY reconciliation of dynamic groups are possible with a change in the connector configuration.

1.7 Connector Features

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

Table 1-3 provides the list of features supported by the AOB application and CI-based connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Full reconciliation	Yes	Yes
Incremental reconciliation	Yes	Yes
Support for Trusted Source Reconciliation	Yes	Yes
Limited reconciliation	Yes	Yes
Use connector server	Yes	Yes
Clone applications or create new application instances	Yes	Yes
Transformation and validation of account data	Yes	Yes
Reconcile user account status	Yes	Yes
Test Connection	Yes	No
Perform connector operations in multiple domains	Yes	Yes
Support for paging from Release 12.2.1.3.0J	Yes	Yes

The following topics provide more information on the features of the AOB application:

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

1.7.1 Full and Incremental Reconciliation

After you create the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance. After the first full reconciliation run, you can configure your connector for incremental reconciliation. In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

See Performing Full and Incremental Reconciliation for the Connector.

> **Note:**
>
> The connector supports incremental reconciliation if the target system contains an attribute that holds the timestamp at which an object is created or modified.

1.7.2 Support for Trusted Source Reconciliation

The SuccessFactors connector can be configured as a trusted source for reconciliation of records into Oracle Identity Governance.

1.7.3 Limited Reconciliation

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

You can set a reconciliation filter as the value of the Filter Suffix attribute of the user reconciliation scheduled job. The Filter Suffix attribute helps you to assign filters to the API based on which you get a filtered response from the target system.

See Performing Limited Reconciliation for the Connector

1.7.4 Support for the Connector Server

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

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

For information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server, see Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

1.7.5 Transformation and Validation of Account Data

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

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

2 Creating an Application by Using the SAP SuccessFactors Connector

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

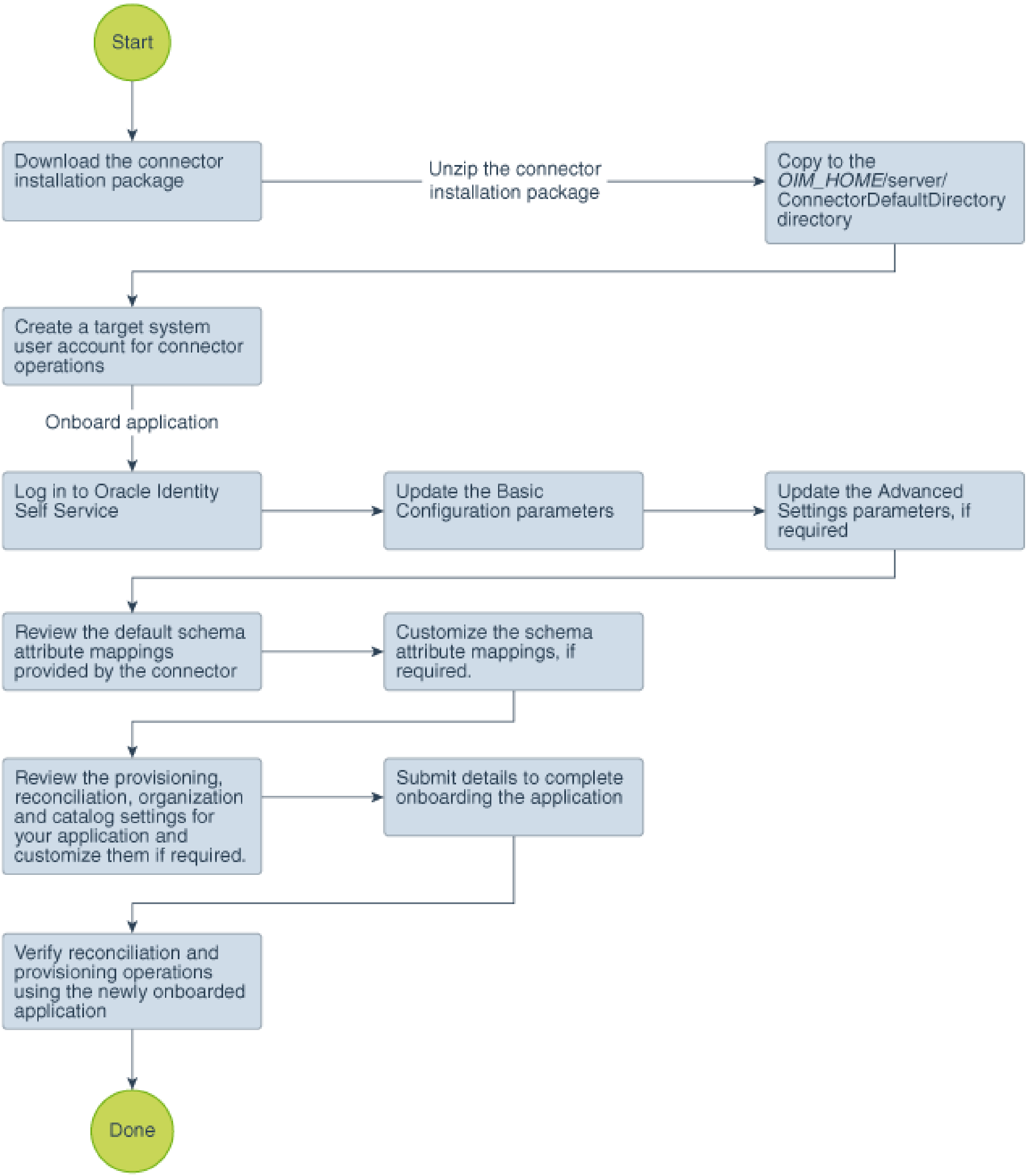
- Process Flow for Creating an Application By Using the Connector
- Prerequisites for Creating an Application By Using the Connector
- Creating an Application By Using the Connector

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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


Start
Download the connector installation package
Unzip the connector installation package
Copy to the *OIM_HOME*/server/ ConnectorDefaultDirectory directory
Create a target system user account for connector operations
Onboard application
Log in to Oracle Identity Self Service
Update the Basic Configuration parameters
Update the Advanced Settings parameters, if required
Review the default schema attribute mappings provided by the connector
Customize the schema attribute mappings, if required.
Review the provisioning, reconciliation, organization and catalog settings for your application and customize them if required.
Submit details to complete onboarding the application
Verify reconciliation and provisioning operations using the newly onboarded application
Done

2.2 Prerequisites for Creating an Application By Using the Connector

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

- Registering the Client Application
- Downloading the Connector Installation Package

2.2.1 Registering the Client Application

Registering the client application (that is, the SuccessFactors connector) with the target system is a step that is performed so that the connector can access the REST APIs. The step includes client application registration, certificate generation, and obtaining clientid and client secret attributes.

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

> **Note:**
>
> The detailed instructions for performing these preinstallation tasks are available in SuccessFactors product documentation at https://support.sap.com/documentation.html/

1. Register your client application with SuccessFactors to provide a secure sign in and authorization of your services. You can register your client application by creating an application in the SuccessFactors Manage OAuth2 Client Applications page.
2. While creating an application, ensure that you provide information in the mandatory fields. Fields such as Application Name, Description, Application URL, Common Name (CN), and Validity (Days) are mandatory fields required for the SuccessFactors connector. As a best practice, SuccessFactors recommends to use your company ID as the Common Name (CN) field information. As part of registering your client application, a `Certificate.pem` file gets generated.
3. Make a note of the clientId and client secret information. Post application registration, from the Manage OAuth2 Client Application page you can view the clientId and client secret information. The clientId and client secret info is required while configuring the Basic Configuration parameters at the time of application creation.

2.2.2 Downloading the Connector Installation Package

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

To download the connector installation package:

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

3. Select the **Accept License Agreement** option.

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

4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.

5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.* For example, successfactors-12.2.1.3.0

6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIM_HOME*/server/ConnectorDefaultDirectory directory.

2.3 Creating an Application By Using the Connector

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

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

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

1. Create an application in Identity Self Service. The high-level steps are as follows:

   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.

   b. Ensure that the **Connector Package** option is selected when creating an application.

   c. Update the basic configuration parameters to include connectivity-related information.

   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.

   e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.

   f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.

   g. Review the details of the application and click **Finish** to submit the application details.

      The application is created in Oracle Identity Governance.

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

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

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

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

3 Configuring the SAP SuccessFactors Connector

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

This section contains the following topics:

- Basic Configuration Parameters
- Advanced Setting Parameters
- Attribute Mappings
- Correlation Rules
- Reconciliation Jobs

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to the SAP SuccessFactor target application.

> **Note:**
>
> - Unless specified, the parameters in the table are applicable to both target and authoritative applications.
> - In the following table, attributes marked as mandatory are applicable only for `Basic authentication`. For `oauth_saml` authentication, all attributes are mandatory except the `password`, `port` and `Connector Server Name` attributes.
> - To use the proxy server, apply one-off patch SuccessFactors-12.2.1.3.0A or later.

Table 3-1 Parameters in the Basic Configuration

Parameter	Mandatory?	Description
authenticationType	Yes	Type of authentication used by your target system. This connector supports the target system OAuth2.0 client credentials. **Default value**: `oauth_saml` **Note**: Based on requirement, the default value can be modified to `Basic authentication`.
companyId	Yes	Enter the company ID for user provisioning. During licensing of SuccessFactors solution, a unique company ID is provided. The OData API uses the company ID attribute to validate your access token.
Host	Yes	Enter the host name of the computer hosting your target system. **Sample value**: `apisalesdemo4.successfactors.com`
sslEnabled	Yes	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. **Default value**: `true`
username	Yes	Enter the username which has permissions to perform all the Identity Management features using APIs. When you purchase a Sandbox, this username is provided by the SAP SuccessFactors organization. **Sample value**: johnsmith
authenticationServerUrl	No	Enter the URL of the authentication server that validates the client ID and client secret for your target system. **Sample** `value: https://apisalesdemo4.successfactors.com/oauth/token?`

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

Parameter	Mandatory?	Description
authorizationUrl	No	Authorization URL is the URL which returns the access token. Ensure that you provide correct parameters and their values to receive an access token. **Sample value:**`https://apisalesdemo4.successfactors.com/oauth/idp`
clientId	No	Enter the client identifier (a unique string) issued by the authorization server to your client application during the registration process. You obtained the client ID while performing.
clientUrl	No	This is the attribute that provides the Sandbox URL. This Sandbox URL needs to be registered with the target resource. **Sample value**: `https://apisalesdemo4.successfactors.com`
privateKeyLocation	No	Enter location of the certificate. During the client application creation process, a certificate gets stored.
Connector Server Name	No	If you have deployed the SuccessFactors connector in the Connector Server, then enter the name of the IT resource for the Connector Server.
grantType	No	The most important step for an application in the OAuth flow is how the application receives an access token (and optionally a refresh token). A grant type is the mechanism used to retrieve the token. OAuth defines several different access grant types that represent different authorization mechanisms. **Default value**: `urn:ietf:params:oauth:grant-type:saml2-bearer`

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

Parameter	Mandatory?	Description
Password	Yes	Enter the password of the computer hosting your target system.
Port	No	Enter the port number at which the target system is listening. **Sample value**: `443`
proxyHost	No	Enter the name of the proxy host used to connect to an external target.
proxyPassword	No	Enter the password of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.
proxyPort	No	Enter the proxy port number.
proxyUser	No	Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system. **Sample value:** `80`

3.2 Advanced Setting Parameters

The advanced setting parameters for the SAP SuccessFactors configuration vary depending on whether you are creating a target application or an authoritative application These are the configuration-related entries that the connector uses during reconciliation and provisioning operations.

> **Note:**
>
> - Unless specified, the parameters in the table are applicable to both target and authoritative applications.
> - All parameters in the below table are mandatory.

Table 3-2 Advanced Setting Parameters for the SAP SuccessFactors

Parameter	Description
lookupUrl	This the endpoint URL used to reconcile lookup data from the target system. **Default value**: `"jobLevel=/odata/v2/FOJobCode?$select=externalCode,name,jobFunction,jobLevel","groupName=/odata/v2/DynamicGroup?&$filter=staticGroup+eq+true"` **Note:** In case you want to reconcile dynamic groups from the target system as well, change the following: 1. Change the value of lookupUrl to: `"jobLevel=/odata/v2/FOJobCode?$select=externalCode,name,jobFunction,jobLevel","groupName=/odata/v2/DynamicGroup?$format=json"`. 2. Re-run the Groups schedule job after changing the above value. However, you cannot add or remove a user to dynamic groups. In case a dynamic group is provisioned or removed for an user, then an error will be automatically displayed.
upsertUrl	This entry holds the value of endpoint URL that is used for performing any upsert operation on the user account. **Default value**: `User=/odata/v2/upsert","addGroup=/odata/v2/updateStaticGroup?groupId=groupNameL&action='add'&userIds=Username","removeGroup=/odata/v2/updateStaticGroup?groupId=groupNameL&action='remove'&userIds=Username`

Table 3-2 (Cont.) Advanced Setting Parameters for the SAP SuccessFactors

Parameter	Description

reconUrl	This entry holds the value of endpoint URL that is used to reconcile users from the target resource.
	Default value:
	`/odata/v2/User?$format=JSON&$filter=status%20ne%20'p'`
	The default value supported from Release 12.2.1.3.0J:
	`/odata/v2/User?$format=json&$expand=empInfo,empInfo/jobInfoNav,empInfo/personNav/personalInfoNav&$filter=status+ne+'p'`
	For more information, see the "one-off README.txt" file.

userUrl	This entry holds the value of endpoint URL that is used to perform the create user operation. **Default value**: `/odata/v2/User`
Bundle Name	This entry holds the name of the connector bundle. **Default value:** `org.identityconnectors.successfactors`
Bundle Version	This entry holds the version of the connector bundle. **Default value:** `12.3.0`
Connector Name	This entry holds the name of the connector. **Default value:** `org.identityconnectors.successfactors.SuccessFactorsConnector`

Table 3-2 (Cont.) Advanced Setting Parameters for the SAP SuccessFactors

Parameter	Description
customURIs	This entry holds the customURIs of the connector. **Default value**: `"EmpJob=/odata/v2/EmpJob?$filter=userId+eq+'(Username)'", "PerPersonal=/odata/v2/PerPersonal?$filter=personIdExternal+eq+'(Username)'","UserEntity=/odata/v2/User?$filter=status+ne+'p'+and+userId+eq+'(Username)'","EmpEmployment=/odata/v2/EmpEmployment?$filter=userId+eq+'(Username)'","PerPerson=/odata/v2/PerPerson?$filter=personIdExternal+eq+'(Username)'","groupId=/odata/v2/getDynamicGroupsByUser?userId='(Username)'&groupSubType='permission'"` The default value supported from Release 12.2.1.3.0J: `"groupId=/odata/v2/getDynamicGroupsByUser?userId='(Username)'&groupSubType='permission'"`
objectMetadatas	This entry holds a comma separated list of object metadata information. During provisioning, each object requires a metadata entry in the payload. The metadata value is unique for each object entity. **Default value**: `"UserEntity={\"uri\":\"User('Username')\"}","PerPerson={\"uri\":\"PerPerson('Username')\"}","EmpEmployment={\"uri\":\"EmpEmployment(personIdExternal='Username',userId='Username')\"}","EmpJob={\"uri\":\"EmpJob(userId='Username',startDate=datetime'DateTime')\"}","PerPersonal={\"uri\":\"PerPersonal(personIdExternal='Username',startDate=datetime'DateTime')\"}"`

Table 3-2 (Cont.) Advanced Setting Parameters for the SAP SuccessFactors

Parameter	Description

childFields	This attribute holds child data mapping.
	Default value:
	`"groupId=groupId"`
	The default value supported from Release 12.2.1.3.0J: `"futureDatedHire=true"`
	To mask the user information that can be PII (Personal Identifiable Information) or any security data printing in logs, add a new attribute:
	`maskedAttributeList="empInfo/personNav/nationalIdNav/nationalId","empInfo/jobInfoNav"`
	For more information, see the "one-off README.txt" file.

3.3 Attribute Mappings

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

- Attribute Mappings for the Target Application
- Attribute Mappings for the Authoritative Application

3.3.1 Attribute Mappings for the Target Application

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

Default Attributes for SAP SuccessFactors Target Application

Table 3-3 lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and SAP SuccessFactors target application columns.

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

Table 3-3 Default Attributes for SAP SuccessFactors Target Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Username	__NAME__	String	Yes	Yes	Yes	Yes	Yes

Table 3-3 (Cont.) Default Attributes for SAP SuccessFactors Target Application

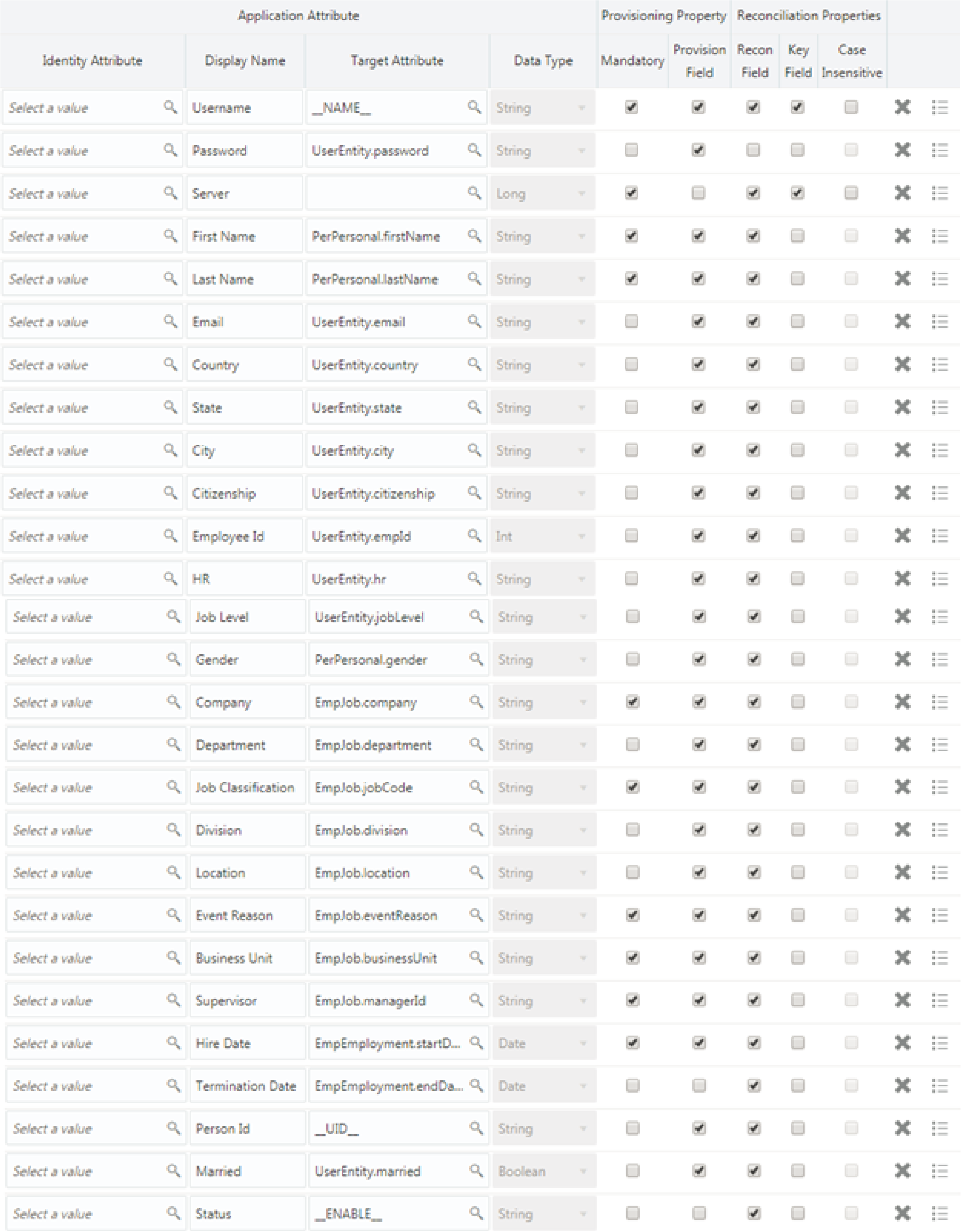
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Password	UserEntity.password	String	No	Yes	No	No	NA
Server		Long	Yes	No	Yes	Yes	NA
First Name	PerPersonal.firstName	String	Yes	Yes	Yes	No	NA
Last Name	PerPersonal.lastName	String	Yes	Yes	Yes	No	NA
Email	UserEntity.email	String	No	Yes	Yes	No	NA
Country	UserEntity.country	String	No	Yes	Yes	No	NA
State	UserEntity.state	String	No	Yes	Yes	No	NA
City	UserEntity.city	String	No	Yes	Yes	No	NA
Citizenship	UserEntity.citizenship	String	No	Yes	Yes	No	NA
Employee Id	UserEntity.empId	String	No	Yes	Yes	No	NA
HR	UserEntity.hr	String	No	Yes	Yes	No	NA
Job Level	UserEntity.jobLevel	String	No	Yes	Yes	No	NA
Gender	PerPersonal.gender	String	No	Yes	Yes	No	NA
Company	EmpJob.company	String	Yes	Yes	Yes	No	NA
Department	EmpJob.department	String	No	Yes	Yes	No	NA
JobClassification	EmpJob.jobCode	String	Yes	Yes	Yes	No	NA
Division	EmpJob.division	String	No	Yes	Yes	No	NA
Location	EmpJob.location	String	No	Yes	Yes	No	NA
Event Reason	EmpJob.eventReason	String	Yes	Yes	Yes	No	NA
Business Unit	EmpJob.businessUnit	String	Yes	Yes	Yes	No	NA

Table 3-3 (Cont.) Default Attributes for SAP SuccessFactors Target Application

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Supervisor	EmpJob.managerId	String	Yes	Yes	Yes	No	NA
Hire Date	EmpEmployment.startDate	String	Yes	Yes	Yes	No	NA
Termination Date	EmpEmployment.endDate	String	No	No	Yes	No	NA
Person Id	__UID__	String	No	Yes	Yes	No	NA
Married	UserEntity.married	String	No	Yes	Yes	No	NA
Status	__ENABLE__	String	No	No	Yes	No	NA

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

Figure 3-1   Default Attribute Mappings for SAP SuccessFactors Target User Account



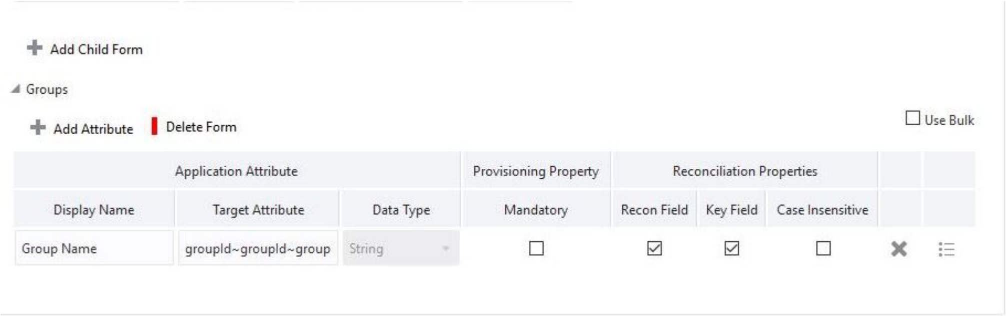
Application Attribute				Provisioning Property		Reconciliation Properties				
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive		
Select a value	Username	__NAME__	String	☑	☑	☑	☑	☐	✖	☰
Select a value	Password	UserEntity.password	String	☐	☑	☐	☐	☐	✖	☰
Select a value	Server		Long	☑	☐	☑	☑	☐	✖	☰
Select a value	First Name	PerPersonal.firstName	String	☑	☑	☑	☐	☐	✖	☰
Select a value	Last Name	PerPersonal.lastName	String	☑	☑	☑	☐	☐	✖	☰
Select a value	Email	UserEntity.email	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Country	UserEntity.country	String	☐	☑	☑	☐	☐	✖	☰
Select a value	State	UserEntity.state	String	☐	☑	☑	☐	☐	✖	☰
Select a value	City	UserEntity.city	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Citizenship	UserEntity.citizenship	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Employee Id	UserEntity.empId	Int	☐	☑	☑	☐	☐	✖	☰
Select a value	HR	UserEntity.hr	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Job Level	UserEntity.jobLevel	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Gender	PerPersonal.gender	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Company	EmpJob.company	String	☑	☑	☑	☐	☐	✖	☰
Select a value	Department	EmpJob.department	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Job Classification	EmpJob.jobCode	String	☑	☑	☑	☐	☐	✖	☰
Select a value	Division	EmpJob.division	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Location	EmpJob.location	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Event Reason	EmpJob.eventReason	String	☑	☑	☑	☐	☐	✖	☰
Select a value	Business Unit	EmpJob.businessUnit	String	☑	☑	☑	☐	☐	✖	☰
Select a value	Supervisor	EmpJob.managerId	String	☑	☑	☑	☐	☐	✖	☰
Select a value	Hire Date	EmpEmployment.startD...	Date	☑	☑	☑	☐	☐	✖	☰
Select a value	Termination Date	EmpEmployment.endDa...	Date	☐	☐	☑	☐	☐	✖	☰
Select a value	Person Id	__UID__	String	☐	☑	☑	☐	☐	✖	☰
Select a value	Married	UserEntity.married	Boolean	☐	☑	☑	☐	☐	✖	☰
Select a value	Status	__ENABLE__	String	☐	☐	☑	☐	☐	✖	☰

Table 3-4 Default Attributes for SAP SuccessFactors Group Management Child Form

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field	Case Insensitive
Group Name	gropId~groupId~groupId	String	No	Yes	Yes	No

Figure 3-2 shows the Group child form attribute mappings.

Figure 3-2 Group Child Form Attribute Mapping



Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Group Name	groupId~groupId~group	String	☐	☑	☑	☐	✖	☰

3.3.2 Attribute Mappings for the Authoritative Application

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

Table 3-5 lists the user-specific attribute mappings between the reconciliation fields in Oracle Identity Governance and SAP SuccessFactors columns. The table also lists the data type for a given attribute and specified whether it is a mandatory attribute for reconciliation.

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

You may use the default schema that has been set for you or update and change it before continuing to the next step.

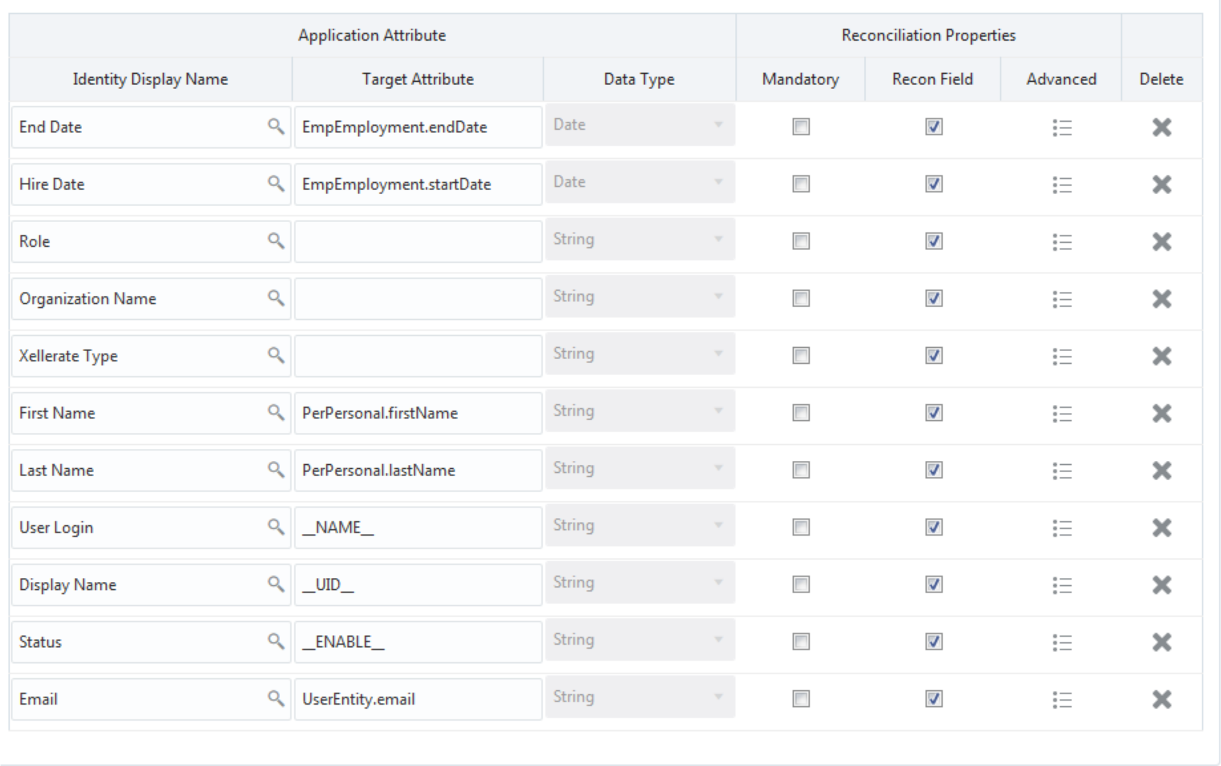
The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form. They cannot be left blank during reconciliation. The target attribute mappings for these identity attributes are empty by default because there are no corresponding columns in the target system.

Table 3-5 Default Attributes for SAP SuccessFactors Authoritative Application

Identity Display Name	Target Attribute	Data Type	Mandatory Recon Property?	Recon Field?	Default Value for Identity Display Name
End Date	EmpEmployment.endDate	Date	No	Yes	NA
Hire Date	EmpEmployment.startDate	Date	No	Yes	NA
Role		String	No	Yes	Full-Time
Organization Name		String	No	Yes	Xellerate Users
Xellerate Type		String	No	Yes	End-User
First Name	PerPersonal.firstName	String	No	Yes	NA
Last Name	PerPersonal.lastName	String	No	Yes	NA
User Login	__NAME__	String	No	Yes	NA
Display Name	__UID__	String	No	Yes	NA
Status	__ENABLE__	String	No	Yes	NA
Email	UserEntity.email	String	No	Yes	NA

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

Figure 3-3 Default Attributes for SAP SuccessFactors Authoritative Application



Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
End Date	EmpEmployment.endDate	Date	□	☑	☰	✖
Hire Date	EmpEmployment.startDate	Date	□	☑	☰	✖
Role		String	□	☑	☰	✖
Organization Name		String	□	☑	☰	✖
Xellerate Type		String	□	☑	☰	✖
First Name	PerPersonal.firstName	String	□	☑	☰	✖
Last Name	PerPersonal.lastName	String	□	☑	☰	✖
User Login	__NAME__	String	□	☑	☰	✖
Display Name	__UID__	String	□	☑	☰	✖
Status	__ENABLE__	String	□	☑	☰	✖
Email	UserEntity.email	String	□	☑	☰	✖

3.4 Correlation Rules

Learn about the predefined rules, responses and situations for Target and Trusted applications. The connector use these rules and responses for performing reconciliation.

- Correlation Rules for the Target Application
- Correlation Rules for an Authoritative Application

3.4.1 Correlation Rules for the Target Application

When you create a target application, the connector uses correlation rules to determine the identity to which Oracle Identity Governance must assign a resource.

Predefined Identity Correlation Rules

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

Table 3-6 lists the default simple correlation rule for SAP SuccessFactors connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6   Predefined Identity Correlation Rule for SAP SuccessFactors Connector

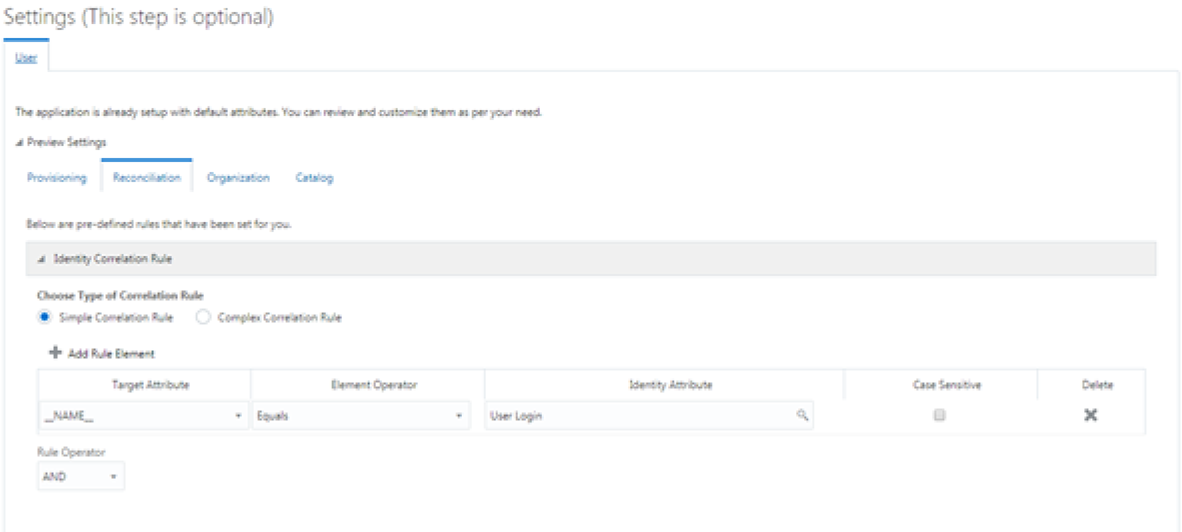
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

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

Figure 3-4 shows the simple correlation rule for SAP SuccessFactors target application.

Figure 3-4   Simple Correlation Rule for SAP SuccessFactors Application



Settings (This step is optional)

User

The application is already setup with default attributes. You can review and customize them as per your need.

Preview Settings

Below are pre-defined rules that have been set for you.

Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
__NAME__	Equals	User Login	□	✕

Rule Operator: AND

Predefined Situations and Responses

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

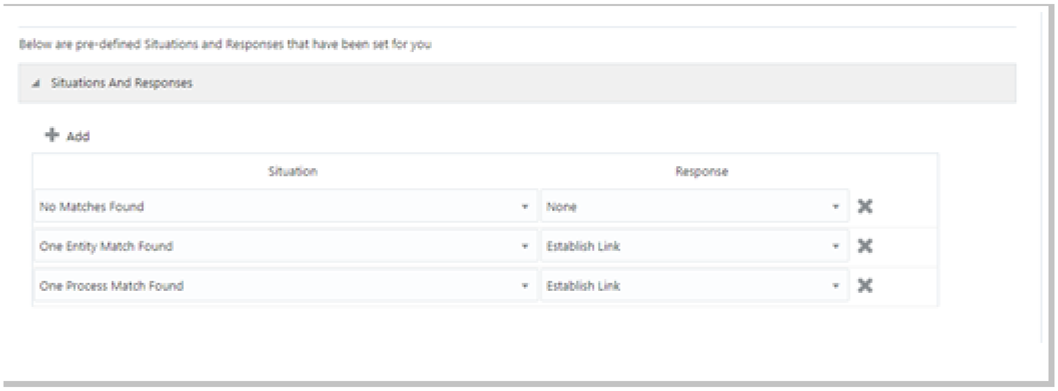
Table 3-7 lists the default situations and responses for SAP SuccessFactors target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-7 Predefined Situations and Responses for SAP SuccessFactors Target Application

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

Figure 3-5 shows the situations and responses for SAP SuccessFactors that the connector provides by default.

Figure 3-5 Predefined Situations and Responses for SAP SuccessFactors Target Application



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

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

3.4.2 Correlation Rules for an Authoritative Application

When you create an authoritative application, the connector uses correlation rules to determine the identity to which Oracle Identity Governance must assign a resource.

Predefined Identity Correlation Rules

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

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

Table 3-8   Predefined Identity Correlation Rule for SAP SuccessFactors Authoritative Application

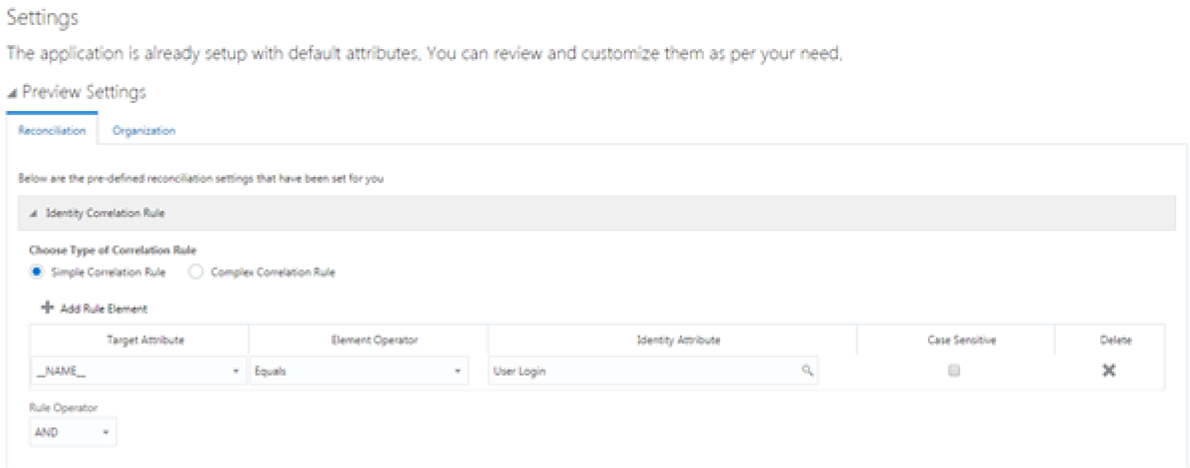
Authoritative Attribute	Element Operator	Identity Attribute	Case Sensitive?
Name	Equals	User Login	No

In the correlation rule element:

- __Name__ is an attribute on the target system that uniquely identifies the user account.
- User Login is the field on the OIM User form.
- Rule operator: AND

Figure 3-6 shows the simple correlation rule for SAP SuccessFactors Authoritative application.

Figure 3-6   Simple Correlation Rule for SAP SuccessFactors Authoritative Application



Settings

The application is already setup with default attributes. You can review and customize them as per your need.

◢ Preview Settings

Reconciliation | Organization

Below are the pre-defined reconciliation settings that have been set for you

◢ Identity Correlation Rule

Choose Type of Correlation Rule

● Simple Correlation Rule ○ Complex Correlation Rule

+ Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
NAME	Equals	User Login	□	✖

Rule Operator: AND

Predefined Situations and Responses

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

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

Table 3-9   Predefined Situations and Responses for SAP SuccessFactors Authoritative Application

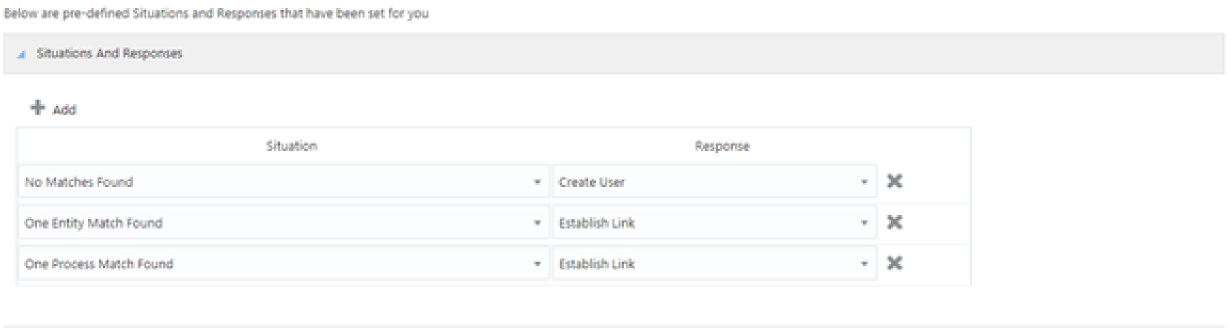
Situation	Response
No Matches Found	Create User

Table 3-9 (Cont.) Predefined Situations and Responses for SAP SuccessFactors Authoritative Application

Situation	Response
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 3-7 shows the situations and responses for SAP SuccessFactors that the connector provides by default.

Figure 3-7 Predefined Situations and Responses for the SAP SuccessFactors Authoritative Application



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

Situations And Responses

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

3.5 Reconciliation Jobs

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

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

- SAP SuccessFactors Target Resource User Reconciliation

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

- SAP SuccessFactors Authoritative User Reconciliation

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

User Reconciliation Job

Table 3-11 describes the parameters of Target User Reconciliation job.

Table 3-10   Parameters of the Scheduled Job for Target User Reconciliation

Attribute	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Object Type	Type of object you want to reconcile. Default value: `User`
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. **Sample value**: `userId eq 'personId'` **Note**: This sample value is not mandatory and is used for limited reconciliation.
Scheduled Task Name	Name of the scheduled job. **Note:** For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.
Incremental Recon Attribute	Name of the target system column that holds holds the timestamp at which the user record was modified. **Default value**: `lastModifiedDateTime`
Latest Token	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute parameter. The Latest Token parameter is used for internal purposes. By default, this value is empty.

Table 3-11 describes the parameters of Authoritative User Reconciliation job.

Table 3-11   Parameters of the Scheduled Job for Authoritative User Reconciliation

Attribute	Description
Application Name	Name of the application you created for your trusted application. This value is the same as the value that you provided for the Application Name field while creating your trusted application. Do not modify this value.
Scheduled Task Name	This parameter holds the name of the scheduled task. **Default value**: `<Application Name> Trusted User Reconciliation`
Filter Suffix	Enter the search filter for fetching user records from the target system during a reconciliation run. **Sample value**: `0`

Table 3-11 (Cont.) Parameters of the Scheduled Job for Authoritative User Reconciliation

Attribute	Description
Object Type	Type of object you want to reconcile. Default value: `User`
Incremental Recon Attribute	Name of the target system column that holds holds the timestamp at which the user record was modified. **Default value**: `lastModifiedDateTime`
Latest Token	The parameter holds the value of the target system column that is specified as the value of the Incremental Recon Attribute. The Latest Token parameter is used for internal purposes. By default, this value is empty.

Reconciliation Jobs for Lookup Field Synchronization

These lookup definitions are used as an input source for lookup fields in Oracle Identity Governance.

The following scheduled jobs are used for lookup fields synchronization:

- SuccessFactors HR Lookup Reconciliation Scheduled Job
- SuccessFactors JobLevel Lookup Reconciliation Scheduled Job
- SuccessFactors Supervisor Lookup Reconciliation Scheduled Job
- SuccessFactors Group Lookup Reconciliation Scheduled Job

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

The parameters for all the scheduled jobs for lookup field synchronization are the same. Table 3-12 describes the parameters of the scheduled jobs.

Table 3-12 Parameters of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system.
Object Type	Type of object you want to reconcile. **Sample values**: `HR, JobLevel, Supervisor, groupName`

Table 3-12 (Cont.) Parameters of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Name of the connector 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	Name of the connector 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__`

4 Performing the Postconfiguration Tasks for the SAP SuccessFactors Connector

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

The following topics discuss the Postconfiguration procedures:

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

4.1 Configuring Oracle Identity Governance

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

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

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

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

4.1.1 Creating and Activating a Sandbox

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

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

4.1.2 Creating a New UI Form

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

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

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

4.1.3 Publishing a Sandbox

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

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

4.1.4 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

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

See Also:

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

4.2 Harvesting Entitlements and Sync Catalog

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

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

See Also:

- Reconciliation Jobs for more information on lookup field synchronization list
- Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Goverance* for information about the Entitlement List and Catalog Synchronization Job scheduled jobs

4.3 Managing Logging

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

4.3.1 Understanding Log Levels

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

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

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.
- SEVERE

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

  This level enables logging of information about potentially harmful situations.
- INFO

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

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

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

These message types are mapped to ODL message type and level combinations as shown in Table 4-2.

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

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

Table 4-2 Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1

Table 4-2 (Cont.) Log Levels and ODL Message Type:Level Combinations

Java Level	ODL Message Type:Level
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

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

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

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

4.3.2 Enabling Logging

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

    a. Add the following blocks in the file:

```
<log_handler name='SuccessFactors-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.SuccessFactors"
level="[LOG_LEVEL]" useParentHandlers="false">
    <handler name="SuccessFactors-handler"/>
    <handler name="console-handler"/>
</logger>
```

    b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 4-2 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='SuccessFactors-handler'
level='NOTIFICATION:1'class='oracle.core.ojdl.logging.ODLHandlerF
actory'>
    <property name='logreader:' value='off'/>
    <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1
\servers\oim_server1\logs\oim_server1-diagnostic-1.log'/>
    <property name='format' value='ODL-Text'/>
    <property name='useThreadName' value='true'/>
    <property name='locale' value='en'/>
    <property name='maxFileSize' value='5242880'/>
    <property name='maxLogSize' value='52428800'/>
    <property name='encoding' value='UTF-8'/>
</log_handler>

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

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

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

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

4.4 Configuring the IT Resource for the Connector Server

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

After you create the application for your target system, the connector creates a default IT resource for the Connector Server. The name of this default IT resource is `SuccessFactors Connector Server`.

In Oracle Identity System Administration, search for and edit the SuccessFactors Connector Server IT resource to specify values for the parameters of IT resource for the Connector Server listed in Table 4-3. For more information about searching for IT resources and updating its parameters, see Managing IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

Table 4-3 Parameters of the IT Resource for the SAP SuccessFactors Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. **Sample value**: `HostName`
Key	Enter the key for the Connector Server.
Port	Enter the number of the port at which the Connector Server is listening. **Sample value**: `8763`
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Governance times out. If the value is zero or if no value is specified, the timeout is unlimited. **Sample value**: `0` (recommended value)
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter `false.` **Default value**: `false` **Note**: It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see Setting SSL for Connector Server and OIM in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance.*

4.5 Localizing Field Labels in UI Forms

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

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive (oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip) to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:

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

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

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

a. Search for the following text:

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

b. Replace with the following text:

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

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

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

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

```
 <trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_USER_NAME__c_description']}
"><source>User Name</source><target/></trans-unit><trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.
RSAForm.entity.SuccessFactorsFormEO.UD_USER_NAME
__c_LABEL"><source>First Name</source><target/></trans-unit>
```

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

```
global.udf.UD_GA_USR_ USER_NAME =\u30A2\u30AB\u30A6\u30F3
\u30C8\u540D.
```

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBu ndle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.use rEO.UD_GA_USR_ USER_NAME __c_description']}
"><source>Account Name</source>
<target>u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target></trans-
unit>
<trans-
unitid="sessiondef.oracle.iam.ui.runtime.form.model.SuccessFactor
s.entity sEO.UD_GA_USR_ACCOUNT_NAME__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.

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

4.6 Configuring SSL

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

To configure SSL:

1. Obtain the SSL public key certificate of SuccessFactors.

2. Copy the public key certificate of SuccessFactors to the computer hosting Oracle Identity Governance.

3. Run the following `keytool` command to import the public key certificate into the identity key store in Oracle Identity Governance:

   ```
   keytool -import -alias ALIAS -trustcacerts -file CERT_FILE_NAME -keystore
   KEYSTORE_NAME -storepass PASSWORD
   ```

   In this command:

   - *ALIAS* is the public key certificate alias.
   - *CERT_FILE_NAME* is the full path and name of the certificate store (the default is cacerts).
   - *KEYSTORE_NAME* is the name of the keystore.
   - *PASSWORD* is the password of the keystore.

   The following is a sample value for this command:

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

   > **Note:**
   >
   > - Change the parameter values passed to the `keytool` command according to your requirements. Ensure that there is no line break in the keytool arguments.
   > - Ensure that the system date for Oracle Identity Governance is in sync with the validity date of the SSL certificate to avoid any errors during SSL communication.

5
Using the SAP SuccessFactors Connector

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

The following topics are discussed in this chapter:

> **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.

- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations
- Uninstalling the Connector

5.1 Configuring Reconciliation

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

The following topics related to configuring reconciliation are discussed in this section:

- Performing Full and Incremental Reconciliation for the Connector
- Performing Limited Reconciliation for the Connector

5.1.1 Performing Full and Incremental Reconciliation for the Connector

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Governance. After you create the application, you must first perform full reconciliation.

At the end of the reconciliation run, the `Latest Token` parameter of the reconciliation job for user record reconciliation is automatically updated. From the next reconciliation run onward, only records created after this time stamp are considered for reconciliation. This is incremental reconciliation.

You can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Governance. To perform a full reconciliation run, remove (delete) any value currently assigned to the Latest Token and Filter parameters and run one of the reconciliation jobs listed in the Reconciliation Jobs section.

For example, consider `lastModifiedDateTime` as a sample Incremental Recon Attribute associated with the SAP SuccessFactors Target Resource User Reconciliation. After the first full reconciliation run, the `Latest Token` parameter gets populated accordingly. In subsequent reconciliation runs, the connector fetches only the user records that are created or updated after the timestamp.

5.1.2 Performing Limited Reconciliation for the Connector

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

Consider a filter suffix value: `userId eq ‘JohnSmith’`

In this example, the connector performs filter reconciliation and only reconciles the user information whose `PersonID` is JohnSmith

> **Note:**
>
> If the target system contains more number of records than what it can return in a single response, then use the Flat File connector to perform limited reconciliation.

5.2 Configuring Reconciliation Jobs

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

You can apply this procedure to configure the 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 job as follows:
    a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

   b. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. On the Job Details tab, you can modify the parameters of the scheduled task:

   - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

   > **Note:**
   >
   > See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance* 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:**
   >
   > See Reconciliation Jobs for the list of scheduled tasks and their attributes.

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

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

5.3 Guidelines on Performing Provisioning Operations

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

For a Create User Provisioning operation, you must specify a value for the User Name field along with the domain name. For example, jdoe@example.com. The User Name is a mandatory field, other mandatory fields are Business Unit, Company, Hire Date, Username, Event Reason, First Name, Last Name, Supervisor and Job Classification.

5.4 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

1. Log in to Identity Self Service.

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

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

5.5 Uninstalling the Connector

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

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

For example: `SuccessFactors User`

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

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

6

Extending the Functionality of the SAP SuccessFactors Connector

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

The following topics are discussed in this section:

- Configuring Transformation and Validation of Data
- Configuring Action Scripts
- Configuring the Connector for Multiple Installations of the Target System
- Understanding OData API Dictionary

6.1 Configuring Transformation and Validation of Data

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

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

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

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

Following is a sample transformation script for reference:

```
def getBeneficiaryAttrFromContext(attrName) {
    if (context.beneficiary != null) {
        return context.beneficiary.getAttribute(attrName);
    }

    return null;
}

def getBeneficiaryPwdFromContext() {
    return context.beneficiaryPassword;
}
```

```
    if (binding.variables != null)
    {
        if (binding.variables.containsKey("context"))
        {
            if (context.operationType != null)
            {
                if(context.operationType.equalsIgnoreCase("create"))
                {
                    if (context.provisionMechanism != null)
                    {

if(context.provisionMechanism.equalsIgnoreCase("POLICY"))
                        {
                            Username = 
getBeneficiaryAttrFromContext("User Login");
                            First_Name = 
getBeneficiaryAttrFromContext("First Name");
                            Last_Name = 
getBeneficiaryAttrFromContext("Last Name");
                            Password = getBeneficiaryPwdFromContext();
                            Company = "ACE_USA";
                            Job_Classification = "ADMIN-1";
                            Event_Reason    = "HIRNEW";
                            Business_Unit = "ACE_IND";
                            Supervisor = "JDOE";
                            Hire_Date = (new java.util.Date()-1);
                        } //if
                        else if 
(context.provisionMechanism.equalsIgnoreCase("REQUEST") || 
context.provisionMechanism.equalsIgnoreCase("ADMIN"))
                        {

                            if (Username == null || Username == "")
                            {
                                Username = 
getBeneficiaryAttrFromContext("User Login");
                            }
                            if (First_Name == null || First_Name == "")
                            {
                                First_Name = 
getBeneficiaryAttrFromContext("First Name");
                            }
                            if (Last_Name == null || Last_Name == "")
                            {
                                Last_Name = 
getBeneficiaryAttrFromContext("Last Name");
                            }
                            if (Password == null || Password == "")
                            {
                                Password = 
getBeneficiaryPwdFromContext();
                            }
                            if (Company == null || Company == "") {
                                Company = "ACE_USA";
                            }
                            if (Job_Classification== null ||
Job_Classification == "")
                            {
                                Job_Classification = "ADMIN-1";
                            }
                            if (Event_Reason== null || Event_Reason == "")
                            {
                                Event_Reason = "HIRNEW";
                            }
                            if (Business_Unit== null || Business_Unit == "")
                            {
                                Business_Unit    = "ACE_IND";
                            }
                            if (Supervisor== null || Supervisor == "")
                            {
                                Supervisor = "JDOE";
                            }
                            Hire_Date = (new java.util.Date()-1);
                            }//else if
                    }
                }

            }
        }
    }
```

6.2 Configuring Action Scripts

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

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

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

6.3 Configuring the Connector for Multiple Installations of the Target System

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

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

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

6.4 Understanding OData API Dictionary

The OData API Dictionary component stores a bundle of object entities. Each SuccessFactors instance contains ready-to-use object entities. The object entities in the OData API Dictionary can also be customized as per requirement.

The following topics are discussed in this appendix:

- About OData API Dictionary
- Viewing OData API Dictionary in the SAP SuccessFactors Connector
- Adding Custom Attributes and Object Entities in Oracle Identity Governance
- Providing Values in Static Lookups

6.4.1 About OData API Dictionary

Every SuccessFactors instance has several object entities. The OData API Dictionary bundles these object entities and presents them in a tabular format. The SuccessFactors object entities contain information such as allowed operations, attributes (also referred to as property name) and labels.

6.4.2 Viewing OData API Dictionary in the SAP SuccessFactors Connector

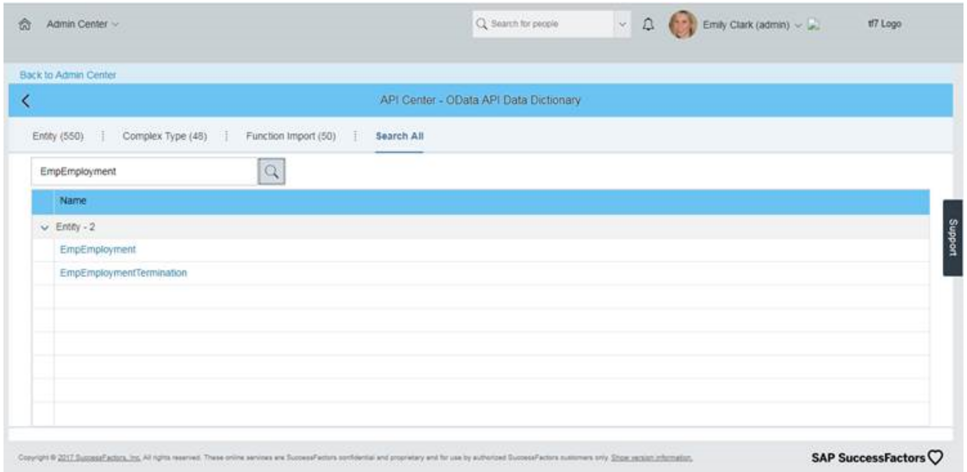
SAP SuccessFactors provides an option to view existing object entities listed under the OData API Dictionary link.

To view an existing OData API Dictionary:

1. Log in to your SuccessFactors instance.
2. Search for OData API Dictionary in the **Tool Search** text field on the Admin Center page. The OData API Dictionary link listed under **My Favorites** link category.
3. Click **OData API Dictionary** link. The OData API Entities list appears.

   The displayed list includes both ready-to-use object entities along with your customized object entities.
   Figure 6-1 shows a list of OData API Entities.

Figure 6-1 OData API Entities



EmpEmployment

Name
Entity - 2
EmpEmployment
EmpEmploymentTermination

Copyright © 2017 SuccessFactors, Inc. All rights reserved. These online services are SuccessFactors confidential and proprietary and for use by authorized SuccessFactors customers only. Show version information.

Note:

- In the current release, User Interface for the OData API Data Dictionary is enhanced. The `OData API Data Dictionary` link is available in the `Admin Center` console. If this link is not visible, verify your access grant permissions.
- In the OData API Data Dictionary, you can use the `Search All` functionality. However for a filtered search, you can either use specific search terms such as `Entity`, `Complex Type`, or `Function Import`, or you can use objects such as `PerPersonal`, `EmpEmployment` and `Attributes`. associated with them.

6.4.3 Adding Custom Attributes and Object Entities in Oracle Identity Governance

SAP SuccessFactors provides a ready-to-use OData API Dictionary. Apart from the ready-to-use object entities present in the OData API Dictionary, if you require a new attribute and a new object entity, then you need to customize the OData API Dictionary. Using the OData API Dictionary component, all customized object entities are mapped to their corresponding attributes in the target system.

Adding custom attributes and object entities to Oracle Identity Governance is a two-step operation as follows:

- Firstly in your SuccessFactors instance, you need to search for the custom attribute that is present in the OData API Dictionary. Make a note of the custom attribute and the entity object below which this custom attribute is listed. For more information about customizing the OData API Dictionary, contact SAP SuccessFactors support.

- After obtaining the required information about custom attribute and object entity, you need to add this new attribute to Oracle Identity Governance. This new attribute provides a mapping between the custom attribute and the target system.

To associate the attribute with an object entity:

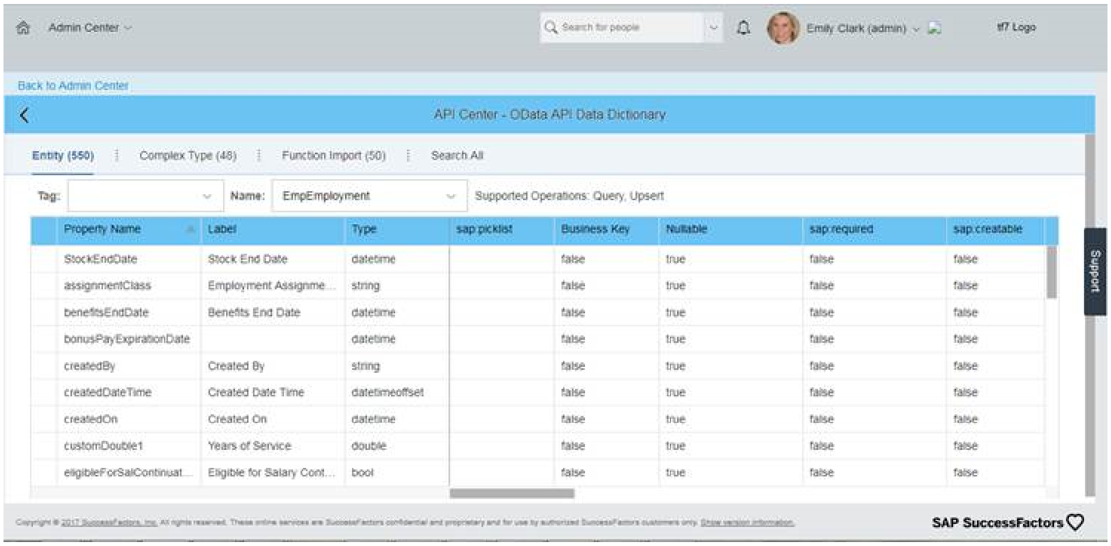
1. Log in to Identity Self Service by using the System Administration account.
2. Go to the **Manage** tab and click the **Applications** box. The **Applications** page appears.
3. From the **Applications** page, from the **Actions** menu, click **Create**, and then select **Target**. The **Application Template** page appears.
4. From the **Application Template** page, navigate to **Schema Attribute** page.
5. From the **Schema Attribute**, click **Add Attribute** to add a new row to the table. Provide the following **Application Attribute** details:
   a. **Display Name**: Enter the display name for the attribute in Oracle Identity Governance.
   b. **Target Attribute**: Enter the target attribute name. For SuccessFactors, enter PerPersonal.formalName.
   c. **Data Type**: Select the String data type from the list.
   d. **Mandatory**: Select if the attribute is mandatory for target provisioning.
   e. **Provision Field**: Select Yes from the list.
   f. **Recon Field**: Select Yes from the list.
   g. **Key Field**: Select No from the list.
   h. **Case Insensitive**: Do not make any modifications to this attribute.
6. Click **Save** to save your changes.

6.4.4 Providing Values in Static Lookups

SuccessFactors provides an option to add values to the static lookup definition. Adding values is a requirement to associate code and the meaning values in the target system. To add values in the static lookups for SuccessFactors, first you need to check if any code value is present for the attribute under consideration. If a code value is present, then the same needs to be added to the corresponding lookup definition in Oracle Identity Governance.

Consider the below illustration shown in Figure 6-2. In the illustration, observe that the value in the location field is `San Mateo (US_SFO)`. The `US_SFO` is the value which needs to be provided as the `Code` and the value `San Mateo (US_SFO)` or just the name of the location `San Mateo` as the `Meaning` value for the static Lookup Location. These two values need to be present under `Lookup.Location` in Oracle Identity Manager Process Form page.

Figure 6-2   Providing Values in a Static Lookup


Admin Center
Search for people
Emily Clark (admin)
tf7 Logo
Back to Admin Center
API Center - OData API Data Dictionary
Entity (550)
Complex Type (48)
Function Import (50)
Search All
Support
Copyright © 2017 SuccessFactors, Inc. All rights reserved. These online services are SuccessFactors confidential and proprietary and for use by authorized SuccessFactors customers only. Show version information.
SAP SuccessFactors

Tag: Name: EmpEmployment Supported Operations: Query, Upsert

Property Name	Label	Type	sap:picklist	Business Key	Nullable	sap:required	sap:creatable
StockEndDate	Stock End Date	datetime		false	true	false	false
assignmentClass	Employment Assignme...	string		false	true	false	false
benefitsEndDate	Benefits End Date	datetime		false	true	false	false
bonusPayExpirationDate		datetime		false	true	false	false
createdBy	Created By	string		false	true	false	false
createdDateTime	Created Date Time	datetimeoffset		false	true	false	false
createdOn	Created On	datetime		false	true	false	false
customDouble1	Years of Service	double		false	true	false	false
eligibleForSalContinuat...	Eligible for Salary Cont...	bool		false	true	false	false

To provide values for the **Lookup.SuccessFactors.Location** static lookup:

1. Log in to Oracle Identity System Administration.
2. Click **Lookups** from the left navigation pane. The **Search and Select Lookup Type** window appears.
3. From the **Search and Select Lookup Type** window, search and open the lookup for which the new static value needs to be added, and click **Search**.
4. From the search results, select the Lookup for which the new static value needs to be added and click the **edit** icon. The **Edit Lookup Type** window appears.
5. In the **Edit Lookup Type** window, click the **create Lookup** icon and enter values for Code and Meaning attributes. For the Code attribute, provide the target attribute name and for the meaning attribute, provide the process form name.
6. Click **Save** to save your changes.

7 Upgrading the SAP SuccessFactors Connector

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

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

The following sections discuss the procedure to upgrade the connector:

- Upgrade Steps
- Postupgrade Steps

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

7.1 Upgrade Steps

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

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

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.

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

- Production Environment

  Perform the upgrade procedure by using the silent mode.

7.2 Postupgrade Steps

Upgrade steps involve uploading new connector JAR to the Oracle Identity Manager database.

Perform the following procedure:

1. If the connector is deployed on a Connector Server, then:
   a. Stop the connector server.
   b. Replace the existing jar `org.identityconnectors.successfactors-1.0.11150.jar` with `org.identityconnectors.successfactors-12.3.0.jar`.

      > **Note:**
      >
      > Replace the existing bundle with new bundle in the Connector Server and also in the database bundle folder of Oracle Identity Manager.

   c. Start the connector server.
2. If the connector is not deployed on a Connector Server, then:
   a. Run the Oracle Identity Manager Delete JARs utility to delete the existing ICF bundle `org.identityconnectors.successfactors-1.0.11150.jar` from the Oracle Identity Manager database.

      When you run the Delete JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being deleted, and the name of the JAR file to be removed. Specify `4` as the value of the JAR type.
   b. Run the Oracle Identity Manager Upload JARs utility to post the ICF bundle `org.identityconnectors.successfactors-12.3.0.jar.` file to the Oracle Identity Manager database.

      When you run the Upload JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify `4` as the value of the JAR type.

Note:

After completing the connector upgrade steps, ensure to delete the following Code Key and Decode entries in `Lookup.SuccessFactors.Configuration` and `Lookup.SuccessFactors.Configuration.Trusted` lookup definitions:

- `Code Key`: Bundle Version
- `Decode`: 1.0.1115

Additionally, after completing the artifact level upgrade steps, ensure that you delete any attribute which reflects previous version of the connector from both target and trusted lookup configuration tables.

3. Restart Oracle Identity Manager.

See Also:

If you have configured the connector for multiple versions of target system, then refer to Configuring the Connector for Multiple Installations of the Target System for more information

8

Known Issues and Workarounds for the SAP SuccessFactors Connector

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

The following are issues associated with the target system:

- Support for Delete User Operation
- Support for Translation of Termination Date

8.1 Support for Delete User Operation

This connector does not support delete user operation. When you initiate a delete user operation in Oracle Identity Governance, since the delete operation is not supported, the target system disables the user.

Workaround:

There is no workaround available for this issue.

8.2 Support for Translation of Termination Date

The SuccessFactors connector bundle supports 28 different languages. In this release, the translation for the attribute `Termination Date` is not supported across different languages.

Workaround:

There is no workaround available for this issue.

A

Files and Directories on the SAP SuccessFactors Connector Installation Package

This appendix provides the list of files and directories in the connector installation package and their descriptions.

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

File in the Installation Media Directory	Description
org.identityconnectors.successfactors-12.3.0.jar	This JAR is the ICF connector bundle.
configuration/SuccessFactors-CI.xml	This file is used for installing a CI-based connector. This XML file contains configuration information that is used by the Connector Installer during connector installation.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied to the Oracle Identity Governance database. **Note**: A resource bundle is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/SuccessFactors-ConnectorConfig.xml	This XML file contains definitions for the following connector objects • IT resource definition • Process forms • Process tasks and adapters • Lookup definitions • Resource objects • Process definition • Scheduled tasks • Reconciliation rules **Note**: This file is applicable only for a CI-based connector.
xml/SuccessFactors-auth-template.xml	This file contains definitions for the connector objects required for creating an Authoritative application. It includes certain details required to connect Oracle Identity Governance with the target system . It also includes configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/SuccessFactors-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User objects such as Roles.

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

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