Oracle® Identity Governance

Configuring the Fusion Apps Connector

12c (12.2.1.3.0)

G17201-01

May 2025

Oracle Identity Governance Configuring the Fusion Apps Connector, 12c (12.2.1.3.0)

G17201-01

Primary Author: Oracle Corporation

Contents

Preface

1 Introduction to the Connector

2 Creating an Application by Using the Connector

Abstract

Documentation for resource administrators and target system integration teams that describes how to on board Microsoft SharePoint applications to Oracle Identity Governance.

List of Figures

List of Tables

Preface

This guide describes the connector that is used to onboard Microsoft SharePoint 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.

Legal Disclaimer

This Software may enable You to link to, transfer Your Content or Third Party Content to, or otherwise access, third parties' websites, platforms, content, products, services, and information ("Third Party Services"). Oracle does not control and is not responsible for Third Party Services.

ORACLE PROVIDES ACCESS TO THE THIRD PARTY SERVICES "AS IS". ORACLE DOES NOT MAKE ANY COMMITMENTS OR PROVIDE WARRANTIES OR REPRESENTATIONS ABOUT THE THIRD PARTY SERVICES, THE FUNCTIONS OF THE THIRD PARTY SERVICES, OR THE RELIABILITY, AVAILABILITY, OR ABILITY OF THE THIRD PARTY SERVICES. TO THE EXTENT PERMITTED BY LAW, ORACLE EXCLUDES ALL WARRANTIES WITH REGARD TO THE THIRD PARTY SERVICES.

Your use of the Third Party Services are governed by Your agreement with the Third Party. You are solely responsible for: (a) complying with the terms of access and use of Third Party Services, including any Third Party Privacy Policy; and (b) ensuring that such access and use, including through passwords, credentials or tokens issued or otherwise made available to You, is authorized by the terms of access and use for such Third Party Services.

You agree to continue to comply with the terms of the Agreement for the Software and that Oracle may discontinue Your access to the Third Party Services at any time without liability to You.

1 Introduction to the Connector

This chapter introduces the Fusion Apps connector.

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

The Fusion Apps Connector lets you create and onboard Fusion Apps 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 connector:

1. Certified Components
2. Usage Recommendation
3. Certified Languages
4. Supported Connector Operations
5. Connector Architecture
6. Use Cases Supported by the Connector
7. Connector Features

1.1 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based connector
Fusion Applications	You can use any one of the following releases: • Oracle Identity Governance 12c PS4 (12.2.1.4.0) or later. • Oracle Identity Governance 12*c* PS3 (12.2.1.3.0) or later. • Oracle Identity Governance 14c (14.1.2.1.0)	You can use any one of the following releases: • Oracle Identity Governance 12c PS4 (12.2.1.4.0) or later. • Oracle Identity Governance 12*c* PS3 (12.2.1.3.0) or later. • Oracle Identity Governance 14c (14.1.2.1.0)
Oracle Identity Governance or Oracle Identity Manager JDK	JDK 1.8 and later	JDK 1.8 and later
Target systems	Oracle Fusion Cloud Applications 24C (11.13.24.07.0) or later	Oracle Fusion Cloud Applications 24C (11.13.24.07.0) or later
Connector Server	11.1.2.1.0 or 12.2.1.3.0	11.1.2.1.0 or 12.2.1.3.0
Connector Server JDK	JDK 1.8 and later	JDK 1.8 and later

1.2 Usage Recommendation

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.

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 for User

Operation	Supported?
User Management	
Create user	Yes
Update user	Yes
Enable user	Yes
Disable user	Yes
Delete user	Yes
Reset Password	Yes
Role Grant Management	
Assign and Revoke Roles	Yes

Table 1-3 Supported Connector Operations for Worker

Operation	Supported?
Worker Management	

Table 1-3 (Cont.) Supported Connector Operations for Worker

Operation	Supported?
Create worker	Yes
Update worker	Yes
Enable worker	No
Disable worker	No
Delete worker	No
Reset Password	No
Phone Numbers Grant Management	
Assign and Revoke Phone Numbers	Yes
Secondary Emails Grant Management	
Assign and Revoke Secondary Emails	Yes

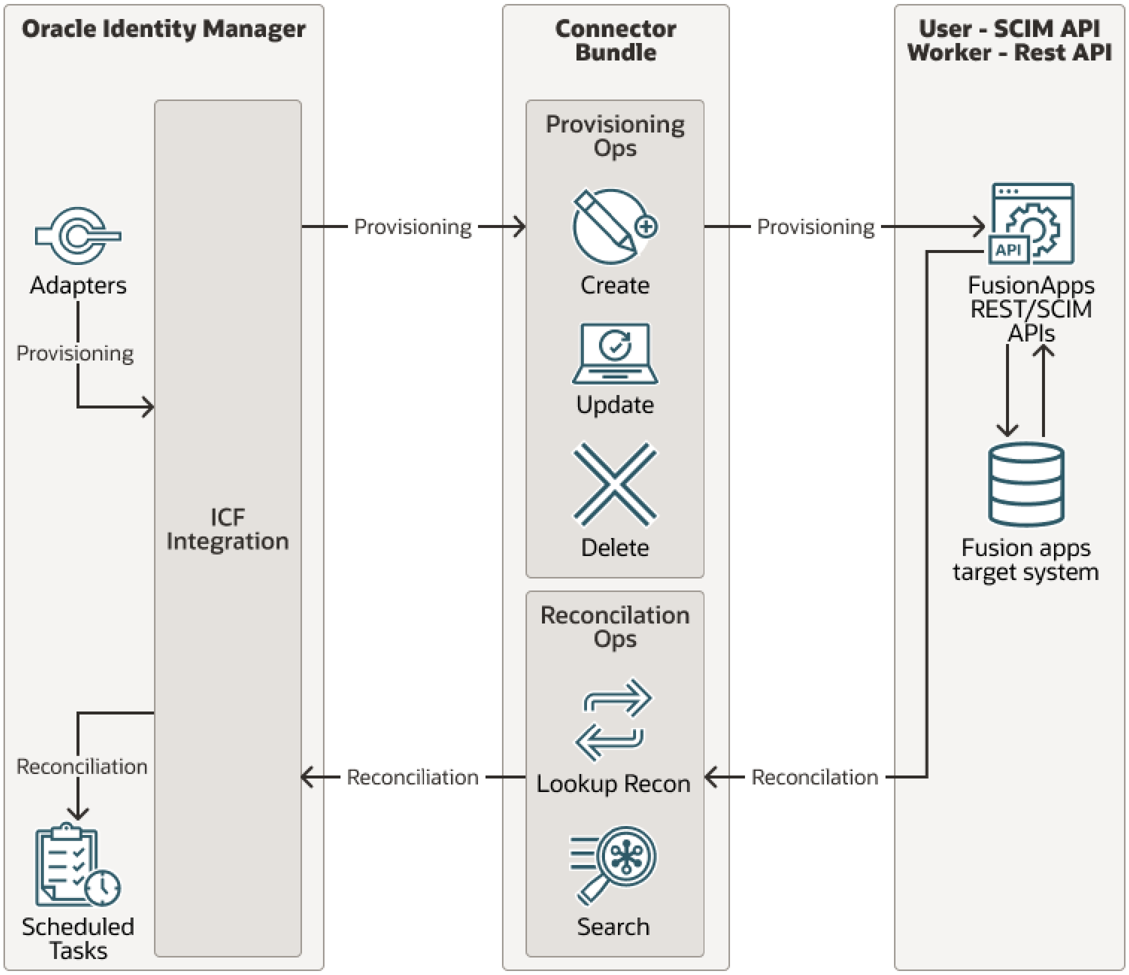
1.5 Connector Architecture

The Fusion Apps 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.

The following figure shows the architecture of the Fusion Apps.

Figure 1-1   Fusion Apps Connector Architecture



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

- **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 and workers and deleting users on the target system through Oracle Identity Governance. During provisioning, the adapters invoke the ICF operation; ICF in turn invokes the create operation on the Fusion Apps Identity Connector Bundle, and then the bundle calls the target system API (Fusion Apps 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 initiates an ICF operation, which involves searching the Fusion Apps Identity Connector Bundle. This bundle interfaces with the Fusion Apps API to retrieve user and worker records that meet specific criteria. These records are then returned via the bundle and ICF to the scheduled task, where they are integrated into Oracle Identity Governance.

Each record from the target system is compared to existing Fusion Apps resources provisioned in OIM. When a match is found, updates from the target system's Fusion Apps record are copied to the corresponding Fusion Apps resource in Oracle Identity Governance. If there's no match, the record's name is compared with OIM user logins. In the event of a match, the data from the target system's record is utilized to provision a Fusion Apps resource for the OIM user.

The Fusion Apps Identity Connector Bundle communicates with the Fusion Apps API using the HTTPS protocol. The Fusion Apps API provides programmatic access to Fusion Apps through SCIM/REST API endpoints. SCIM APIs are used to manage users' information and REST APIs are used to manage workers' information. Fusion Apps APIs are used to perform create, read, update, and delete (CRUD) operations on Fusion Apps target application.

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

1.6 Use Cases Supported by the Connector

Fusion Apps can be integrated with Oracle Identity Governance to ensure synchronized lifecycle management of privileged accounts within your enterprise, aligning with other identity-aware applications. Fusion Apps offers identity management for various models, including Cloud Identity, Synchronized Identity, and Federated Identity, making it a valuable choice for organizations seeking consistent management of accounts and roles. The following is the most common scenarios in which this connector can be used:

- **Fusion Apps User and Worker Management**:

An organization using Fusion Apps aims to integrate it with Oracle Identity Governance for efficient identity management. This integration enables user identity creation within the target system via Oracle Identity Governance. It also facilitates the synchronization of user identity changes made directly in the target system with Oracle Identity Governance

To achieve this, you need to configure the Fusion Apps connector application with your target system, providing the necessary connection details. When you wish to create a new user or worker in the target system, you can complete and submit the OIM process form to initiate the provisioning operation. The connector will execute the CreateOp operation in the target system, resulting in the user's creation upon successful execution. Updates can be performed in a similar manner.

For searching and retrieving user identities, a scheduled task from Oracle Identity Governance must be run. The connector will execute the corresponding SearchOp operation within the target system, capturing all changes and syncing them with Oracle Identity Governance.

1.7 Connector Features

The features of the connector include support for connector server, user provisioning, full reconciliation, limited reconciliation and so on.

The following table provides the list of features supported by the AOB application.

Table 1-4   Supported Connector Features Matrix

Feature	AOB Application	CI-Based Application
User Provisioning	Yes	Yes
Full reconciliation	Yes	Yes
Incremental reconciliation	Yes	Yes
Limited (Filtered)reconciliation	Yes	Yes
Delete reconciliation for users	Yes	Yes
Use connector server	Yes	Yes
Transformation and validation of account data	Yes	Yes
Clone applications or create new application instances	Yes	Yes
Provide secure communication to the target system through SSL	Yes	Yes
Support for pagination	Yes	Yes
Test connection	Yes	Yes
Reset password Note: Supported only for user	Yes	Yes

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

1. User Provisioning
2. Full Reconciliation and Incremental Reconciliation
3. Limited (Filtered)Reconciliation
4. Support for the Connector Server
5. Transformation and Validation of Account Data
6. Support for Cloning Applications and Creating Instance Applications
7. Secure Communication to the Target System

1.7.1 User Provisioning

User provisioning involves creating or modifying the account data on the target system through Oracle Identity Governance.

Note:

For more information, see Performing Provisioning Operations.

1.7.2 Full Reconciliation and Incremental Reconciliation

You can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance.

In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Governance.

For more information, see Performing Full Reconciliation and Performing Incremental Reconciliation.

1.7.3 Limited (Filtered)Reconciliation

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

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

For more information, see Performing Limited (Filtered) Reconciliation.

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 want to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements if the bundle works faster when deployed on the same host as the native managed resource.

See Also:

Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installing and configuring connector server and running the connector server

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*.

1.7.6 Support for Cloning Applications and Creating Instance Applications

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

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

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

1.7.7 Secure Communication to the Target System

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

For more information, see Configuring SSL.

2

Creating an Application by Using the Connector

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

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

2.1 Prerequisites for Creating an Application by Using the Connector

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

- Configuring the Target System
- Downloading the Connector Installation Package

2.1.1 Configuring the Target System

This is a high-level summary about the tasks to be performed on the target system before you create the application.

Create a user account on the target system and assign the necessary privileges to the same user to perform the connector operations. Follow below steps to do so.

1. Sign in to Oracle Fusion Cloud Applications
2. Navigate to **Tools** and select **Security Console**.
3. Click on **Users** and Click on **Add User Account**.
4. Create a user account with a username and password.
5. Grant the following permissions for created user account:

Table - Role/Permissions for User Account

Role Name	Role Code
IT Security Manager	ORA_FND_IT_SECURITY_MANAGER_JOB
Integration Specialist	ORA_FND_INTEGRATION_SPECIALIST_JOB
Human Resource Specialist	ORA_PER_HUMAN_RESOURCE_SPECIALIST_JOB
Application Implementation Consultant	ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB

Role Name	Role Code
Access Request Security Administrator	ORA_GTG_ACCESS_REQUEST_SECURITY_ADMINISTRATOR_JOB

Note:

The third privilege, ORA_PER_HUMAN_RESOURCE_SPECIALIST_JOB, is specifically required to view Person's information in the target system.

2.1.2 Downloading the Connector Installation Package

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

To download the connector installation package:

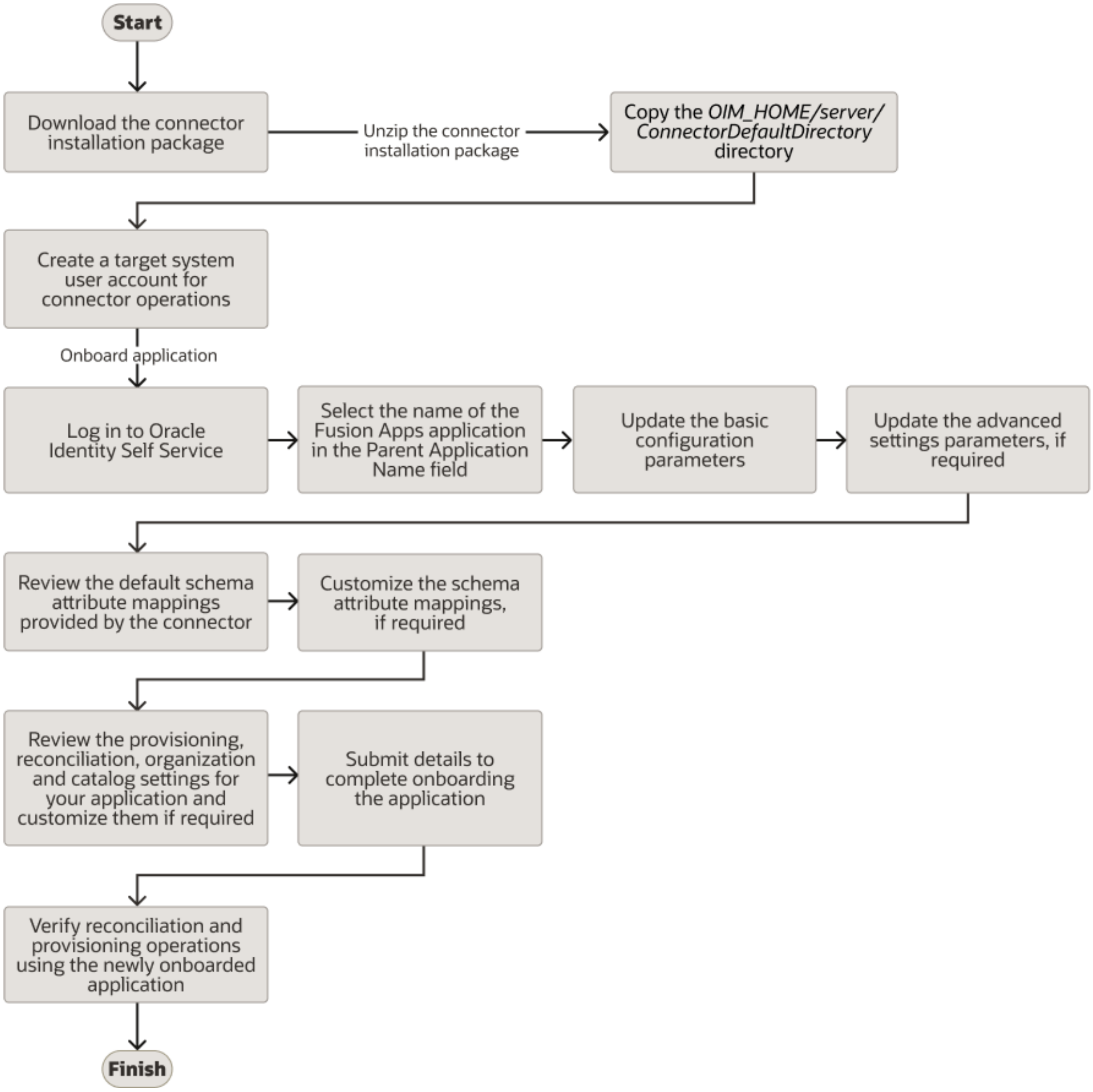
1. Navigate to the OTN website at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html .
2. Click **OTN License Agreement** and read the license agreement.
3. Select the **Accept License Agreement** option.
   You must accept the license agreement before you can download the installation package.
4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

2.2 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.

The following figure 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 the *OIM_HOME/server/ ConnectorDefaultDirectory* directory
Create a target system user account for connector operations
Onboard application
Log in to Oracle Identity Self Service
Select the name of the Fusion Apps application in the Parent Application Name field
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
Finish

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

3

Configuring the Fusion Apps Connector Target Application

While creating a target 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 attributes, predefined correlation rules, situations and responses, and reconciliation jobs.

3.1 Basic Configuration Parameters for Fusion Apps Target Application

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

Table 3-1 Basic Configuration Parameters for Fusion Apps Target Application

Parameter	Mandatory?	Description
username	Yes	Enter the user name of the target system that you create for performing connector operations. **Sample Value:** johnsmith
password	Yes	Enter the password of the target system user account that you create for connector operations. **Sample value:** password
host	Yes	Enter the host name of the machine hosting your target system. This is a mandatory attribute while creating an application. **Sample value:** fa-host.com
userSchemaEndPoint	Yes	This specifies the API endpoint of the user schema resource used to view the user SCIM resources' attribute definitions. **Sample value:**/hcmRestApi/scim/Schemas/urn:scim:schemas:core:2.0:User
userEndPoint	Yes	This specifies the API endpoint for interacting with user data. **Sample value:** /hcmRestApi/scim/Users
roleEndpoint	Yes	This specifies the API endpoint for interacting with role data. **Sample value:** /hcmRestApi/scim/Roles

Table 3-1 (Cont.) Basic Configuration Parameters for Fusion Apps Target Application

Parameter	Mandatory?	Description
workerBaseUrl	Yes	This provides the foundation for accessing various resources within the HCM REST API. **Sample value:** /hcmRestApi/resources/11.13.18.05/
workerEndPoint	Yes	This defines a specific resource path within the API that focuses on worker-related data and operations. **Sample value:** workers
Connector Server Name	No	The name of the IT resource of the type "Connector Server." **Note:** Enter a value for this parameter only if you have deployed the Fusion Apps connector in the Connector Server.
port	No	Enter the port number at which the target system is listening. **Sample value:** 123
proxyHost	No	Enter the proxy host name. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator **Sample value:** www.proxyhost.com
proxyPassword	No	Enter the proxy password. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator
proxyPort	No	Enter the proxy port number. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator for more information about proxy configuration. **Sample value:** 1106
proxyUser	No	Enter the proxy user name.This is useful when a connector is to be used in the network protected by the web proxy. Check with your network administrator for more.
SSL	No	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. **Sample value**: true

3.2 Advanced Settings Parameters for Fusion Apps Target Application

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

Table 3-2 Advanced Settings Parameters for Fusion Apps Target Application

Parameter	Mandatory?	Description
Bundle Name	Yes	This parameter holds the name of the connector bundle package. **Default value:** org.identityconnectors.faidentityservice

Table 3-2 (Cont.) Advanced Settings Parameters for Fusion Apps Target Application

Parameter	Mandatory?	Description
Bundle Version	Yes	This parameter hods the version of the connector bundle class. **Default value:**12.3.0
Connector Name	Yes	This parameter holds the name of the connector class. **Default value:**org.identityconnectors.faidentityservice.FAIdentityServiceConnector
httpHeaderContentType	No	This entry holds the content type expected by the target system in the header. **Default value:** application/json
httpHeaderAccept	No	This entry holds the accept type expected from the target system in the header. **Default value:** application/json
connectionTimeOut	No	Connection timeout occurs when a client fails to establish a connection with a server within a predetermined amount of time. **Default value:** 80000
socketTimeOut	No	The socket timeout is a setting that specifies how long a socket will wait for a response before it is considered timed out. **Default value:** 90000
requiredWorkerAttributes	Yes	Specify the necessary attributes to provision a worker, tailored to their specific worker type. **Default value:** E:familyName,LegislationCode,LegalEmployerName,WorkerType,ActionCode,BusinessUnitId#N:familyName,LegislationCode,LegalEmployerName,WorkerType,ActionCode,BusinessUnitId#C:familyName,LegislationCode,LegalEmployerName,WorkerType,ActionCode,BusinessUnitId#P:familyName,LegislationCode,LegalEmployerName,WorkerType,ActionCode,BusinessUnitId,ProposedUserPersonType,ProjectedStartDate
lookupEndPoints	Yes	A lookup endpoint is designed to retrieve specific data or information based on the provided API. **Default value:** Country:hcmCountriesLov#Department:departmentsLov#Jobs:jobsLov#BusinessUnit:hcmBusinessUnitsLOV#LegalEmployerName:legalEmployersLov#LegislationCode:legalEmployersLov#Grades:grades#AddressType:/fscmRestApi/resources/11.13.18.05/commonLookupsLOV?finder=LookupTypeAllRowsFinder;LookupType=ADDRESS_TYPE#PhoneTypes:/fscmRestApi/resources/11.13.18.05/commonLookupsLOV?finder=LookupTypeAllRowsFinder;LookupType=PHONE_TYPE#ActionCode:actionsLOV#WorkerType:/fscmRestApi/resources/11.13.18.05/commonLookupsLOV?finder=LookupTypeFinder;LookupType=PER_PERIOD_TYPE
applicationType	Yes	The application type determines if it is AOB or CI application. 'true' indicates AOB, and 'false' indicates CI. **Default value:** true
defaultBatchSize	No	This entry holds how many resources appear on a page for a search operation. **Default value:** 500

3.3 Attribute Mappings for Fusion Apps 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 attributes. The connector uses these mappings during reconciliation and provisioning operations.

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

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

Table 3-3 Default Attribute Mappings for Fusion Apps Target User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Account Type	userType	String	Yes	Yes	Yes	No	Not applicable
Id	__UID__	String	No	No	Yes	Yes	No
UserName	__NAME__	String	No	Yes	Yes	No	Not applicable
Password	password	String	No	Yes	No	No	Not applicable
Display Name	displayName	String	No	Yes	Yes	No	Not applicable
External Id	externalId	String	No	Yes	Yes	No	Not applicable
Work Email Address	emails.value	String	No	Yes	Yes	No	Not applicable
Emails Address Id	emails.EmailAddressId	String	No	Yes	Yes	No	Not applicable
Email Type	emails.type	String	No	Yes	Yes	No	Not applicable
Active	__ENABLE__	String	No	No	Yes	No	Not applicable
Last Name	name.familyName	String	Yes	Yes	Yes	No	Not applicable
First Name	name.givenName	String	No	Yes	Yes	No	Not applicable
Gender	legislativeInfo.Gender	String	No	No	Yes	No	Not applicable

Table 3-3 (Cont.) Default Attribute Mappings for Fusion Apps Target User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Preferred Language	preferredLanguage	String	No	No	Yes	No	Not applicable
Last Modified	meta.lastModified	String	No	No	Yes	No	Not applicable
Created	meta.created	String	No	No	Yes	No	Not applicable
Hire Date	workRelationships.StartDate	String	No	No	Yes	No	Not applicable
Person Id	PersonId	String	No	No	Yes	No	Not applicable
Person Number	workerInformation.personNumber	String	No	No	Yes	No	Not applicable
Manager	workerInformation.manager	String	No	No	Yes	No	Not applicable
Worker Type	workRelationships.WorkerType	String	No	Yes	Yes	No	Not applicable
Action Code	workRelationships.assignments.ActionCode	String	No	Yes	Yes	No	Not applicable
Person Name Id	names.PersonNameId	String	No	Yes	Yes	No	Not applicable
Legal Employer Name	workRelationships.LegalEmployerName	String	No	Yes	Yes	No	Not applicable
Legislation Code	names.LegislationCode	String	No	Yes	Yes	No	Not applicable
Primary Phone Id	phones.PhoneId	String	No	Yes	Yes	No	Not applicable
Primary Phone Type	phones.PhoneType	String	No	Yes	Yes	No	Not applicable
Primary Phone Number	phones.PhoneNumber	String	No	Yes	Yes	No	Not applicable
Person Address Usage Id	addresses.PersonAddrUsageId	String	No	Yes	Yes	No	Not applicable
Address Id	addresses.AddressId	String	No	Yes	Yes	No	Not applicable
Address Type	addresses.AddressType	String	No	Yes	Yes	No	Not applicable
Address Line1	addresses.AddressLine1	String	No	Yes	Yes	No	Not applicable
Address Line2	addresses.AddressLine2	String	No	Yes	Yes	No	Not applicable

Table 3-3 (Cont.) Default Attribute Mappings for Fusion Apps Target User Account

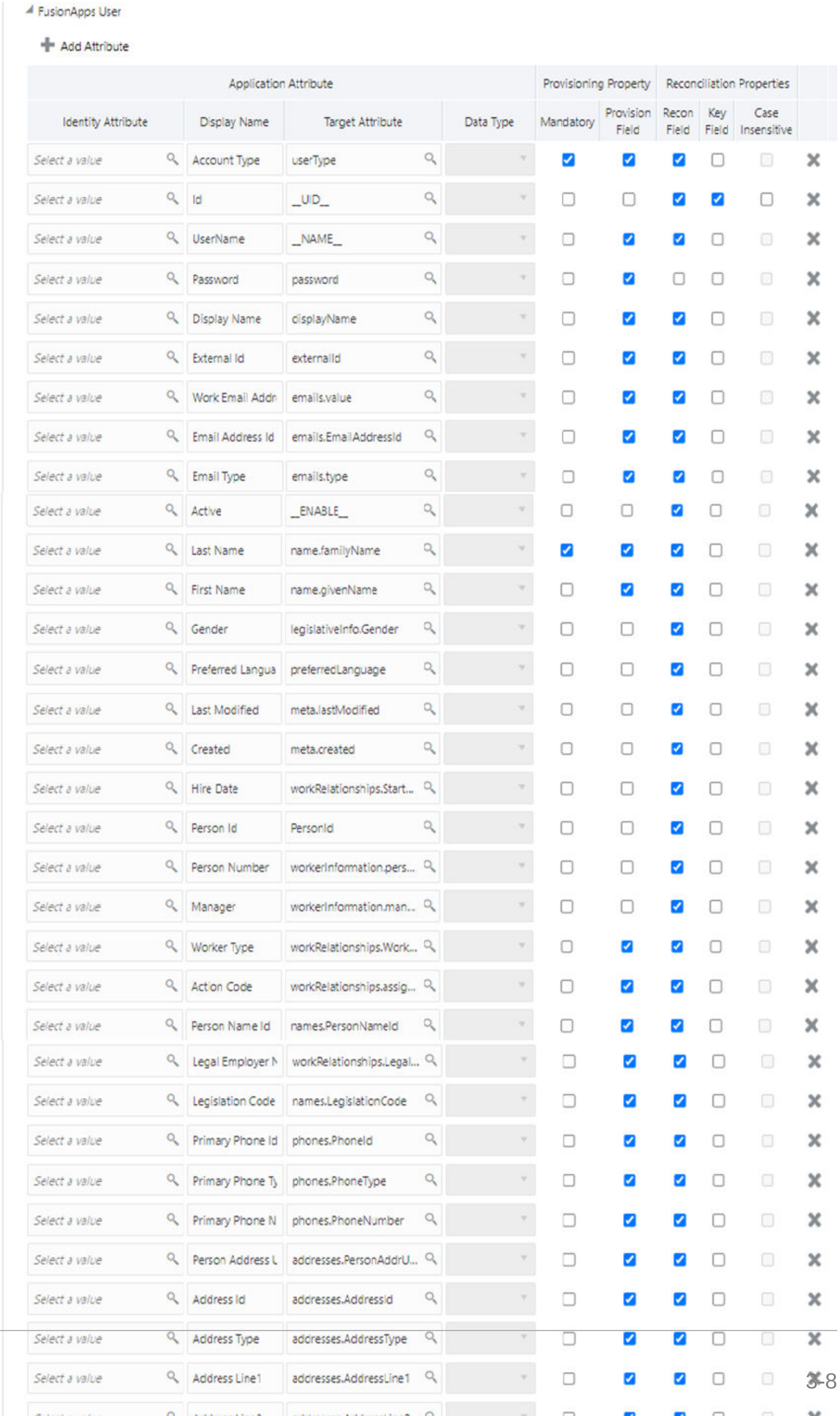
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Floor	addresses.FloorNumber	String	No	Yes	Yes	No	Not applicable
Town Or City	addresses.TownOrCity	String	No	Yes	Yes	No	Not applicable
Region1	addresses.Region1	String	No	Yes	Yes	No	Not applicable
Region2	addresses.Region2	String	No	Yes	Yes	No	Not applicable
Region3	addresses.Region3	String	No	Yes	Yes	No	Not applicable
Postal Code	addresses.PostalCode	String	No	Yes	Yes	No	Not applicable
Country	addresses.Country	String	No	Yes	Yes	No	Not applicable
Period Of Service Id	workRelationships.PeriodOfServiceId	String	No	Yes	Yes	No	Not applicable
Job	workerInformation.job	String	No	No	Yes	No	Not applicable
Start Date	workRelationships.assignments.EffectiveStartDate	String	No	No	Yes	No	Not applicable
End Date	workRelationships.assignments.EffectiveEndDate	String	No	No	Yes	No	Not applicable
Business Unit Id	workRelationships.assignments.BusinessUnitId	String	No	Yes	Yes	No	Not Applicable
Business Unit	workRelationships.assignments.BusinessUnit	String	No	No	Yes	No	Not applicable
Department	workerInformation.department	String	No	No	Yes	No	Not applicable
Grade	workRelationships.assignments.GradeCode	String	No	No	Yes	No	Not applicable
Position	workRelationships.assignments.PositionCode	String	No	No	Yes	No	Not applicable
Location	workRelationships.assignments.LocationCode	String	No	No	Yes	No	Not applicable
Termination Date	workRelationships.TerminationDate	String	No	No	Yes	No	Not applicable
Projected Start Date	workRelationships.assignments.ProjectedStartDate	String	No	Yes	Yes	No	Not applicable
Proposed User Person Type	workRelationships.assignments.ProposedUserPersonType	String	No	Yes	Yes	No	Not applicable

Table 3-3 (Cont.) Default Attribute Mappings for Fusion Apps Target User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Worker Id	workerId	String	No	Yes	Yes	No	Not applicable
IT Resource Name		Long	No	No	Yes	No	Not applicable

The following figure shows the default User account attribute mappings.

Figure 3-1   Default User Account Attribute Mappings



◢ FusionApps User

➕ Add Attribute

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	Account Type	userType		☑	☑	☑	□	□	✖
Select a value	Id	__UID__		□	□	☑	☑	□	✖
Select a value	UserName	__NAME__		□	☑	☑	□	□	✖
Select a value	Password	password		□	☑	□	□	□	✖
Select a value	Display Name	displayName		□	☑	☑	□	□	✖
Select a value	External Id	externalId		□	☑	☑	□	□	✖
Select a value	Work Email Addr	emails.value		□	☑	☑	□	□	✖
Select a value	Email Address Id	emails.EmailAddressId		□	☑	☑	□	□	✖
Select a value	Email Type	emails.type		□	☑	☑	□	□	✖
Select a value	Active	__ENABLE__		□	□	☑	□	□	✖
Select a value	Last Name	name.familyName		☑	☑	☑	□	□	✖
Select a value	First Name	name.givenName		□	☑	☑	□	□	✖
Select a value	Gender	legislativeInfo.Gender		□	□	☑	□	□	✖
Select a value	Preferred Langua	preferredLanguage		□	□	☑	□	□	✖
Select a value	Last Modified	meta.lastModified		□	□	☑	□	□	✖
Select a value	Created	meta.created		□	□	☑	□	□	✖
Select a value	Hire Date	workRelationships.Start...		□	□	☑	□	□	✖
Select a value	Person Id	PersonId		□	□	☑	□	□	✖
Select a value	Person Number	workerInformation.pers...		□	□	☑	□	□	✖
Select a value	Manager	workerInformation.man...		□	□	☑	□	□	✖
Select a value	Worker Type	workRelationships.Work...		□	☑	☑	□	□	✖
Select a value	Action Code	workRelationships.assig...		□	☑	☑	□	□	✖
Select a value	Person Name Id	names.PersonNameId		□	☑	☑	□	□	✖
Select a value	Legal Employer N	workRelationships.Legal...		□	☑	☑	□	□	✖
Select a value	Legislation Code	names.LegislationCode		□	☑	☑	□	□	✖
Select a value	Primary Phone Id	phones.PhoneId		□	☑	☑	□	□	✖
Select a value	Primary Phone Ty	phones.PhoneType		□	☑	☑	□	□	✖
Select a value	Primary Phone N	phones.PhoneNumber		□	☑	☑	□	□	✖
Select a value	Person Address L	addresses.PersonAddrU...		□	☑	☑	□	□	✖
Select a value	Address Id	addresses.AddressId		□	☑	☑	□	□	✖
Select a value	Address Type	addresses.AddressType		□	☑	☑	□	□	✖
Select a value	Address Line1	addresses.AddressLine1		□	☑	☑	□	□	✖

Fusion Apps Roles Entitlement

Below table lists the Roles form attribute mappings between the process form fields in Oracle Identity Governance and Fusion Apps Connector attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

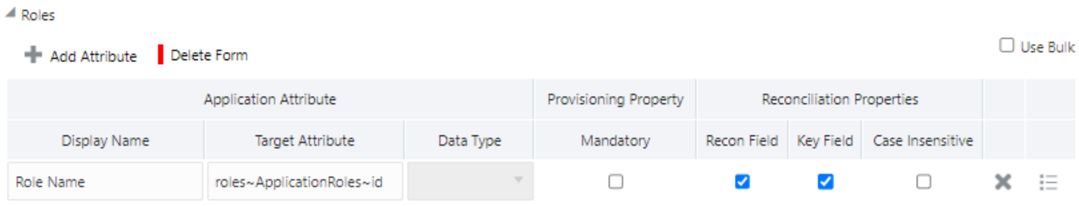
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for Roles

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Role Name	roles~ApplicationRoles~id	String	No	Yes	Yes	No

The following figure shows the default Roles entitlement mapping.

Figure 3-2 Default Attribute Mappings for the Roles



Roles

Add Attribute | Delete Form

□ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Role Name	roles~ApplicationRoles~id		□	☑	☑	□	✖	☰

Fusion Apps Phone Numbers Attribute

Below table lists the Phone numbers form attribute mappings between the process form fields in *Oracle Identity Governance* and Fusion Apps Connector attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

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

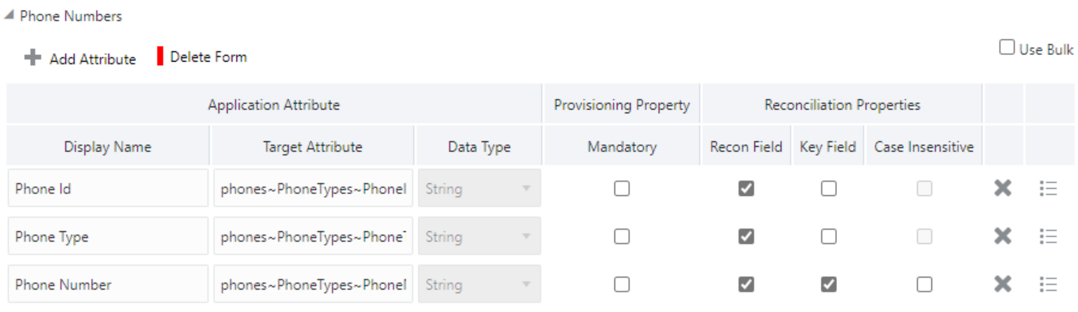
Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Phone Id	phones~PhoneTypes~PhoneId	String	No	Yes	No	Not applicable
Phone Type	phones~PhoneTypes~PhoneType	String	No	Yes	No	Not applicable

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

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Phone Number	phones~PhoneTypes~PhoneNumber	String	No	Yes	Yes	No

The following figure shows the default Phone Numbers child attribute mapping.

Figure 3-3 Default Attribute Mappings for Phone Numbers



Phone Numbers

Add Attribute | Delete Form | □ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Phone Id	phones~PhoneTypes~PhoneI	String	□	☑	□	□	✖	☰
Phone Type	phones~PhoneTypes~Phone`	String	□	☑	□	□	✖	☰
Phone Number	phones~PhoneTypes~PhoneI	String	□	☑	☑	□	✖	☰

Fusion Apps Secondary Emails Attribute

Below table lists the Secondary Emails form attribute mappings between the process form fields in Oracle Identity Governance and Fusion Apps Connector attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

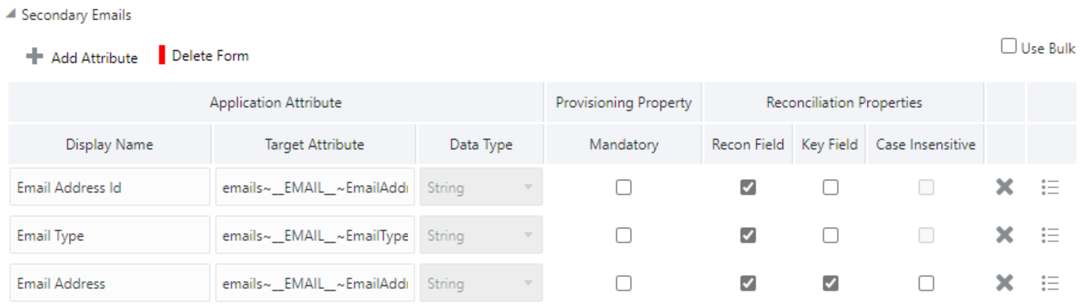
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6 Default Attribute Mappings for Secondary Emails Child Attribute

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field	Key Field?	Case Insensitive?
Email Address Id	emails~__EMAIL__~EmailAddressId	String	No	Yes	No	Not applicable
Email Type	emails~__EMAIL__~EmailType	String	No	Yes	No	Not applicable
Email Address	emails~__EMAIL__~EmailAddress	String	No	Yes	Yes	No

The following figure shows the default Secondary Emails child Attribute mapping.

Figure 3-4   Default Attribute Mappings for Secondary Emails



Secondary Emails

Add Attribute   Delete Form   □ Use Bulk

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Email Address Id	emails~__EMAIL__~EmailAddı	String	□	☑	□	□	✖	☰
Email Type	emails~__EMAIL__~EmailType	String	□	☑	□	□	✖	☰
Email Address	emails~__EMAIL__~EmailAddı	String	□	☑	☑	□	✖	☰

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

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

Table 3-7   Predefined Identity Correlation Rule for Fusion Apps Target Application

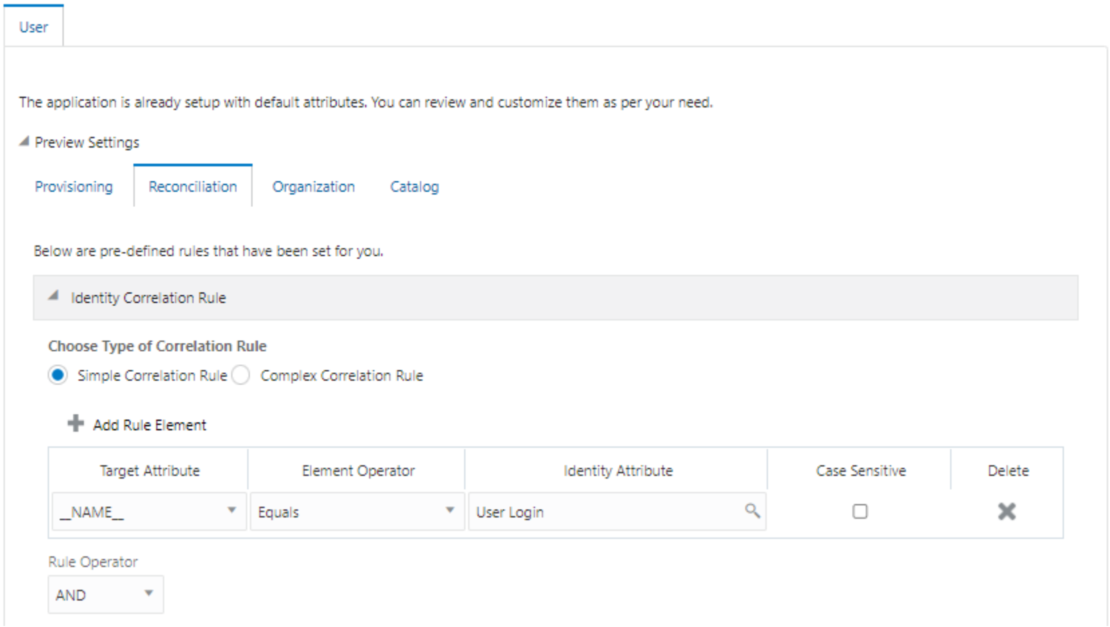
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

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

Following figure shows the Simple Correlation Rule for Fusion Apps Target Application

Figure 3-5 Simple Correlation Rule for Fusion Apps Target Application



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

The Fusion Apps 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.

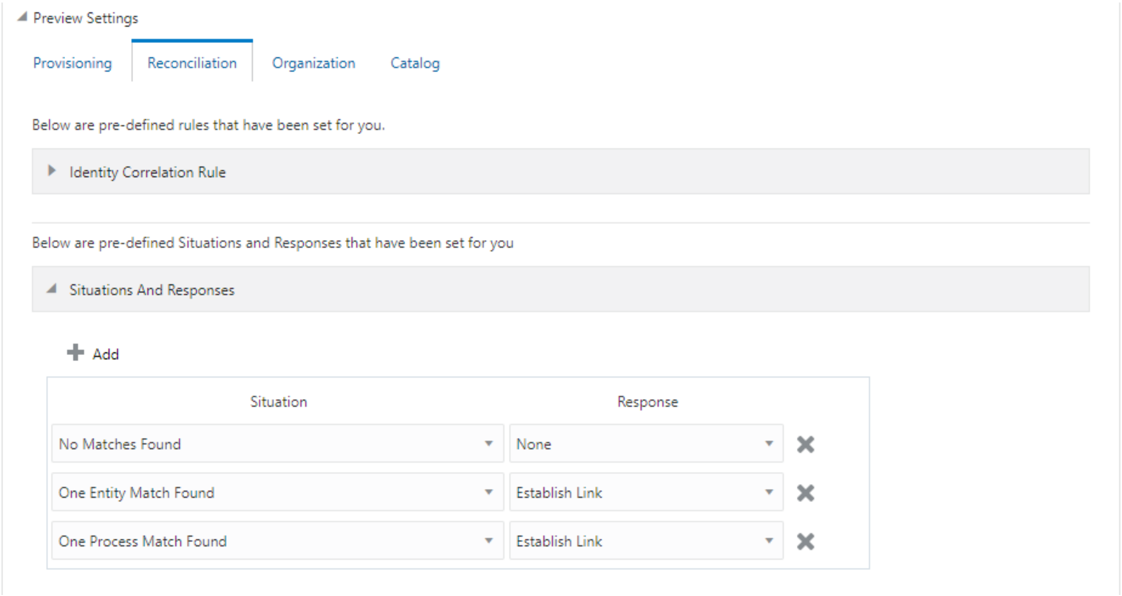
Below table lists the default situations and responses for the Fusion Apps Target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 3-8 Predefined Situations and Responses for Fusion Apps Target Application

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

The following figure shows the situations and responses for the Fusion Apps provided by default.

Figure 3-6 Predefined Situations and Responses for Fusion Apps Target Application



◢ Preview Settings

Provisioning | Reconciliation | Organization | Catalog

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

▸ Identity Correlation Rule

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

◢ Situations And Responses

✚ Add

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

3.5 Reconciliation Jobs for the Fusion Apps Target Connector

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

Fusion Apps Target User Reconciliation Job

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

The following reconciliation jobs are available for reconciling user data:

FA Identity Service User Reconciliation: The Fusion Apps Connector Target Resource User Reconciliation job is used to reconcile user data from a target application.

FA Identity Service Incremental User Reconciliation: FA Identity Service Incremental User Reconciliation job is used to fetch the records that are added or modified after the last reconciliation run.

FA Identity Service Delete User Reconciliation

The FA Identity Service Delete User Reconciliation job is used to reconcile data about deleted users from a target application. During a reconciliation run, for each deleted user account on the target system, the Fusion Apps resource is revoked for the corresponding OIM User.

> **Note:**
>
> Make sure to run Full User Reconciliation job before running Delete User Reconciliation.

Table 3-9 Parameters of the Fusion Apps Target Resource User Reconciliation

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. **Note:** Do not modify this value.
Filter	Enter the search filter for fetching user records from the target system during a reconciliation run. See Performing Limited (Filtered) Reconciliation for more information about this attribute.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: User **Note:** Do not modify this parameter.
Resource Object Name	Name of the Resource object used for reconciliation Default value: FA User **Note:** Do *not* modify the value of this parameter.
Scheduled Task Name	Name of the Scheduled task used for reconciliation **Note:** Do not modify this value parameter.

Table 3-10 Parameters of the FA Identity Service Incremental User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. **Note:** Do not modify this value.
Sync Token	This parameter holds the value of the target system attribute 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. Note: Do not enter a value for this parameter. The reconciliation engine automatically enters a value in this parameter. Sample value: <String> 2024-07-10 08:07:32.023 </String>
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: User **Note:** Do not change the default value.
Resource Object Name	Name of the Resource object used for reconciliation Default value: FA User **Note:** Do *not* modify the value of this parameter.
Scheduled Task Name	Name of the Scheduled task used for reconciliation **Note:** Do *not* modify the value of this parameter.

Table 3-11 Parameters of the FA Identity Service Delete User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. **Note:** Do not modify this value.
Object Type	This attribute holds the name of the object type for the reconciliation run. Default value: User **Note:** Do not change the default value.
Resource Object Name	Name of the Resource object used for reconciliation Default value: FA User **Note:** Do *not* modify the value of this parameter.
Scheduled Task Name	Name of the Scheduled task used for reconciliation **Note:** Do *not* modify the value of this parameter.

Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- FA Identity Service Application Roles Lookup Reconciliation
- FA Identity Service Application Country Lookup Reconciliation
- FA Identity Service BusinessUnit Lookup Reconciliation
- FA Identity Service LegalEmployerName Lookup Reconciliation
- FA Identity Service LegislationCode Lookup Reconciliation
- FA Identity Service Application AddressType Lookup Reconciliation
- FA Identity Service Application PhoneTypes Lookup Reconciliation
- FA Identity Service Application ActionCode Lookup Reconciliation
- FA Identity Service Application WorkerType Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

Table 3-12 Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: __UID__ **Note:** Do not change the value of this attribute.
Decode Attribute	Name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: __NAME__ **Note:** Do not change the value of this attribute.

Table 3-12 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system. Depending on the Reconciliation job that you are using, the default values are as follows: • For FA Identity Service Application Roles Lookup Reconciliation: Lookup.FAIdentityService.ApplicationRoles • For FA Identity Service Application Country Lookup Reconciliation: Lookup.FAIdentityService.Country • For FA Identity Service BusinessUnit Lookup Reconciliation: Lookup.FAIdentityService.BusinessUnit • For FA Identity Service LegalEmployerName Lookup Reconciliation: Lookup.FAIdentityService.LegalEmployerName • For FA Identity Service LegislationCode Lookup Reconciliation: Lookup.FAIdentityService.LegislationCode • For FA Identity Service Application AddressType Lookup Reconciliation: Lookup.FAIdentityService.AddressType • For FA Identity Service Application PhoneTypes Lookup Reconciliation: Lookup.FAIdentityService.PhoneTypes • For FA Identity Service Application ActionCode Lookup Reconciliation: Lookup.FAIdentityService.ActionCode • For FA Identity Service Application WorkerType Lookup Reconciliation: Lookup.FAIdentityService.WorkerType If you create a copy of any of these lookup definitions, then enter the name of that new lookup definition as the value of the Lookup Name attribute.
Object Type	Enter the type of object you want to reconcile. Depending on the reconciliation job that you are using, the default values are as follows: • For FA Identity Service Application Roles Lookup Reconciliation: ApplicationRole • For FA Identity Service Application Country Lookup Reconciliation: Country • For FA Identity Service BusinessUnit Lookup Reconciliation: BusinessUnit • For FA Identity Service LegalEmployerName Lookup Reconciliation: LegalEmployerName • For FA Identity Service LegislationCode Lookup Reconciliation: LegislationCode • For FA Identity Service Application AddressType Lookup Reconciliation: AddressType • For FA Identity Service Application PhoneTypes Lookup Reconciliation: PhoneTypes • For FA Identity Service Application ActionCode Lookup Reconciliation: ActionCode • For FA Identity Service Application WorkerType Lookup Reconciliation: WorkerType **Note**: Do not change the value of this parameter

4

Configuring the Fusion Apps Connector Authoritative Application

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

4.1 Basic Configuration Parameters for Fusion Apps Authoritative Application

These are the connection-related parameters that Oracle Identity Governance requires to connect to Fusion Apps Connector. These parameters are applicable for authoritative applications only.

Table 4-1 Basic Configuration Parameters for Fusion Apps Authoritative Application

Parameter	Mandatory?	Description
username	Yes	Enter the user name of the account that you created to log in to the client application. **Sample value**: johnsmith
password	Yes	Enter the password of the target system user account that you created for connector operations. **Sample value:** password
host	Yes	Enter the host name of the machine hosting your target system. This is a mandatory attribute while creating an application. **Sample value:** fa-host.com
userEndPoint	Yes	This specifies the API endpoint for interacting with user data. **Sample value:** /hcmRestApi/scim/Users
workerEndPoint	Yes	This specifies the API endpoint for interacting with worker data. **Sample value:** /hcmRestApi/resources/11.13.18.05/workers
Connector Server Name	No	The name of the IT resource of the type "Connector Server." **Note:** Enter a value for this parameter only if you have deployed the Fusion Apps connector in the Connector Server.

Table 4-1 (Cont.) Basic Configuration Parameters for Fusion Apps Authoritative Application

Parameter	Mandatory?	Description
port	No	Enter the port number at which the target system is listening. **Sample value**: 123
proxyHost	No	Enter the proxy host name. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator **Sample value**: www.example.com
proxyPassword	No	Enter the proxy password. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator
proxyPort	No	Enter the proxy port number. This is useful when a connector must be used in the network protected by the web proxy. Check with your network administrator for more information about proxy configuration. **Sample value**: 1105
proxyUsername	No	Enter the proxy user name. This is useful when a connector is to be used in the network protected by the web proxy. Check with your network administrator for more
SSL	No	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. **Default value**: true

4.2 Advanced Settings Parameters for Fusion Apps Authoritative Application

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

Table 4-2 Advanced Settings Parameters for Fusion Apps Authoritative Application

Parameter	Mandatory?	Description
Bundle Name	Yes	This parameter holds the name of the connector bundle package. **Default value:** org.identityconnectors.fauserrequestservice
Bundle version	Yes	This parameter hods the version of the connector bundle class. **Default value:** 12.3.0
Connector Name	Yes	This parameter holds the name of the connector class. **Default value:** org.identityconnectors.fauserrequestservice.FAUserRequestServiceConnector

Table 4-2 (Cont.) Advanced Settings Parameters for Fusion Apps Authoritative Application

Parameter	Mandatory?	Description
httpHeaderContentType	No	This entry holds the content type expected by the target system in the header. **Default value:** application/json
httpHeaderAccept	No	This entry holds the accept type expected from the target system in the header. **Default value:** application/json
connectionTimeOut	No	Connection timeout occurs when a client fails to establish a connection with a server within a predetermined amount of time. **Default value:** 80000
socketTimeOut	No	The socket timeout is a setting that specifies how long a socket will wait for a response before it is considered timed out. **Default value:** 90000
pageSize	Yes	This entry holds how many resources appear on a page for a search operation. **Default value:** 500

4.3 Attribute Mappings for Fusion Apps 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 attributes. The connector uses these mappings during reconciliation.

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

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

Table 4-3 Default Attribute Mappings for Fusion Apps User Account in Authoritative Application

Display Name	Target Attribute	Data Type	Mandatory?	Recon Field?	Default Value for Identity Display Name
FAAccountID	__UID__	String	No	Yes	Not Applicable
User Login	__NAME__	String	Yes	Yes	Not Applicable

Table 4-3 (Cont.) Default Attribute Mappings for Fusion Apps User Account in Authoritative Application

Display Name	Target Attribute	Data Type	Mandatory?	Recon Field?	Default Value for Identity Display Name
Email	emails.value	String	No	Yes	Not Applicable
Status	__ENABLE__	String	No	Yes	Not Applicable
Last Name	name.familyName	String	No	Yes	Not Applicable
First Name	name.givenName	String	No	Yes	Not Applicable
Display Name	displayName	String	No	Yes	Not Applicable
Preferred Language	preferredLanguage	String	No	Yes	Not Applicable
Gender	legislativeInfo.Gender	String	No	Yes	Not Applicable
PersonID	PersonId	String	No	Yes	Not Applicable
Employee Number	workerInformation.personNumber	String	No	Yes	Not Applicable
Manager Login	workerInformation.manager	String	No	Yes	Not Applicable
Job	workerInformation.job	String	No	Yes	Not Applicable
Common Name	workerInformation.businessUnit	String	No	Yes	Not Applicable
Department Number	workerInformation.department	String	No	Yes	Not Applicable
Mobile	phones.PhoneNumber	String	No	Yes	Not Applicable
Telephone Number	phones.Extension	String	No	Yes	Not Applicable

Table 4-3 (Cont.) Default Attribute Mappings for Fusion Apps User Account in Authoritative Application

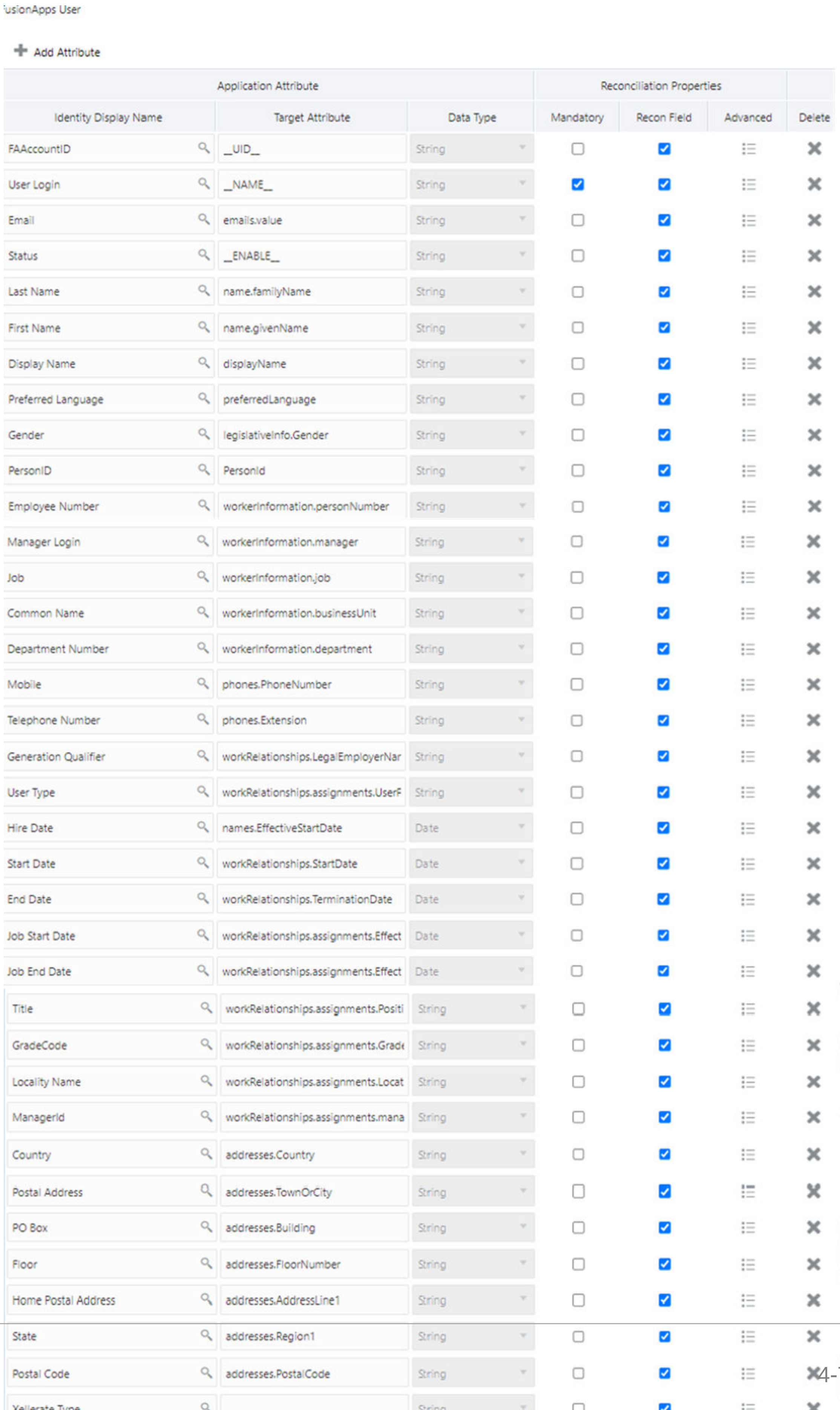
Display Name	Target Attribute	Data Type	Mandatory?	Recon Field?	Default Value for Identity Display Name
Generation Qualifier	workRelationships.LegalEmployerName	String	No	Yes	Not Applicable
User Type	workRelationships.assignments.UserPersonType	String	No	Yes	Not Applicable
Hire Date	names.EffectiveStartDate	String	No	Yes	Not Applicable
Start Date	workRelationships.StartDate	String	No	Yes	Not Applicable
End Date	workRelationships.TerminationDate	String	No	Yes	Not Applicable
Job Start Date	workRelationships.assignments.EffectiveStartDate	String	No	Yes	Not Applicable
Job End Date	workRelationships.assignments.EffectiveEndDate	String	No	Yes	Not Applicable
Title	workRelationships.assignments.PositionCode	String	No	Yes	Not Applicable
GradeCode	workRelationships.assignments.GradeCode	String	No	Yes	Not Applicable
Locality Name	workRelationships.assignments.LocationCode	String	No	Yes	Not Applicable
ManagerId	workRelationships.assignments.managers.ManagerAssignmentNumber	String	No	Yes	Not Applicable
Country	addresses.Country	String	No	Yes	Not Applicable
Postal Address	addresses.TownOrCity	String	No	Yes	Not Applicable
PO Box	addresses.Building	String	No	Yes	Not Applicable
Floor	addresses.FloorNumber	String	No	Yes	Not Applicable

Table 4-3 (Cont.) Default Attribute Mappings for Fusion Apps User Account in Authoritative Application

Display Name	Target Attribute	Data Type	Mandatory?	Recon Field?	Default Value for Identity Display Name
Home Postal Address	addresses.AddressLine1	String	No	Yes	Not Applicable
State	addresses.Region1	String	No	Yes	Not Applicable
Postal Code	addresses.PostalCode	String	No	Yes	Not Applicable
Xellerate Type		String	No	Yes	End-User
Organization Name		String	No	Yes	Xellerate Users
Role		String	No	Yes	Full-Time

Following figure shows the default User account attribute mappings.

Figure 4-1 Default Attribute Mappings for Fusion Apps User Account in Authoritative Application



usionApps User

Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
FAAccountID	__UID__	String	□	☑	☰	✖
User Login	__NAME__	String	☑	☑	☰	✖
Email	emails.value	String	□	☑	☰	✖
Status	__ENABLE__	String	□	☑	☰	✖
Last Name	name.familyName	String	□	☑	☰	✖
First Name	name.givenName	String	□	☑	☰	✖
Display Name	displayName	String	□	☑	☰	✖
Preferred Language	preferredLanguage	String	□	☑	☰	✖
Gender	legislativeInfo.Gender	String	□	☑	☰	✖
PersonID	PersonId	String	□	☑	☰	✖
Employee Number	workerInformation.personNumber	String	□	☑	☰	✖
Manager Login	workerInformation.manager	String	□	☑	☰	✖
Job	workerInformation.job	String	□	☑	☰	✖
Common Name	workerInformation.businessUnit	String	□	☑	☰	✖
Department Number	workerInformation.department	String	□	☑	☰	✖
Mobile	phones.PhoneNumber	String	□	☑	☰	✖
Telephone Number	phones.Extension	String	□	☑	☰	✖
Generation Qualifier	workRelationships.LegalEmployerNar	String	□	☑	☰	✖
User Type	workRelationships.assignments.UserF	String	□	☑	☰	✖
Hire Date	names.EffectiveStartDate	Date	□	☑	☰	✖
Start Date	workRelationships.StartDate	Date	□	☑	☰	✖
End Date	workRelationships.TerminationDate	Date	□	☑	☰	✖
Job Start Date	workRelationships.assignments.Effect	Date	□	☑	☰	✖
Job End Date	workRelationships.assignments.Effect	Date	□	☑	☰	✖
Title	workRelationships.assignments.Positi	String	□	☑	☰	✖
GradeCode	workRelationships.assignments.Grade	String	□	☑	☰	✖
Locality Name	workRelationships.assignments.Locat	String	□	☑	☰	✖
ManagerId	workRelationships.assignments.mana	String	□	☑	☰	✖
Country	addresses.Country	String	□	☑	☰	✖
Postal Address	addresses.TownOrCity	String	□	☑	☰	✖
PO Box	addresses.Building	String	□	☑	☰	✖
Floor	addresses.FloorNumber	String	□	☑	☰	✖
Home Postal Address	addresses.AddressLine1	String	□	☑	☰	✖
State	addresses.Region1	String	□	☑	☰	✖
Postal Code	addresses.PostalCode	String	□	☑	☰	✖
Xellerate Type		String	□	☑	☰	✖

4.4 Correlation Rules for the 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 Fusion Apps Connector provides a simple correlation rule when you create an Authoritative application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the target system repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

Below table lists the default simple correlation rule for a Fusion Apps 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 Updating Identity Correlation Rule in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 4-4   Predefined Identity Correlation Rule for Fusion Apps Authoritative Application

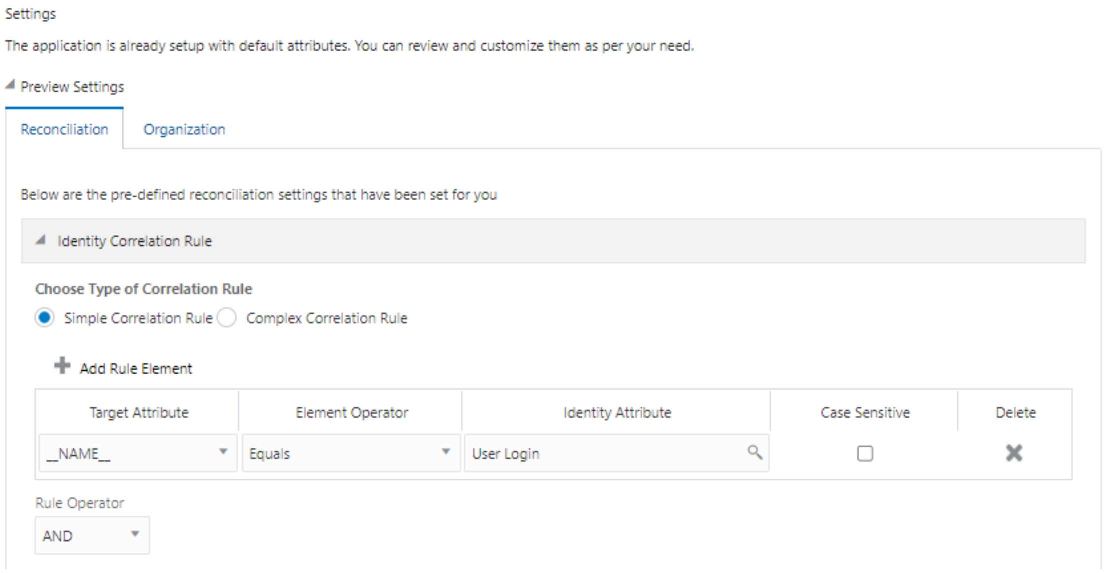
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	User Login	No

In this identity rule:

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

Following figure shows the Simple Correlation Rule for Fusion Apps Authoritative Application

Figure 4-2   Simple Correlation Rule for Fusion Apps 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

The Fusion Apps Authoritative Application 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.

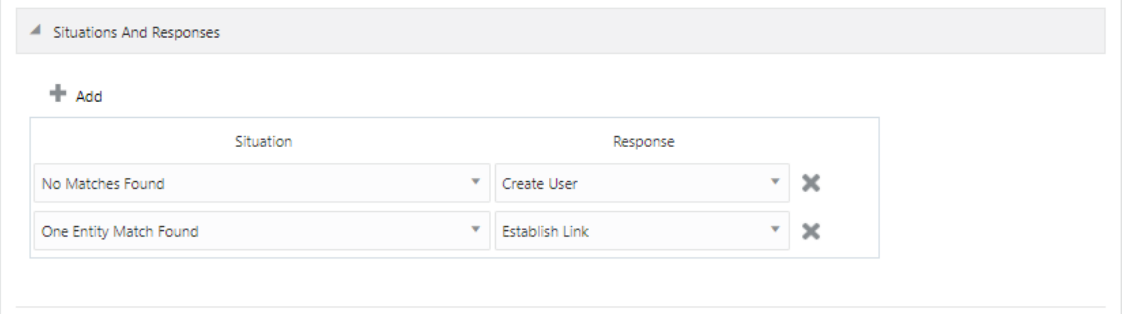
The following table lists the default situations and responses for the Fusion Apps authoritative application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*

Table 4-5 Predefined Situations and Responses for Fusion Apps Authoritative Application

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

Following figure shows the situations and responses for the Fusion Apps Authoritative Application provided by default.

Figure 4-3 Predefined Situations and Responses for Fusion Apps Authoritative Application



Situations And Responses

Add

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

4.5 Reconciliation Jobs for Fusion Apps Authoritative Application

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

Fusion Apps User Reconciliation Job

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

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

FAUserRequestService Incremental User Reconciliation: This is Fusion Apps Connector Trusted User Reconciliation job which is used to fetch all the users and workers from the target system.

Table 4-6 Parameters of the FAUserRequestService Incremental User Reconciliation Job

Parameter	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. **Note:** Do not modify this value.
Sync Token	This parameter holds the value of the target system attribute 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. **Note**: Provide the value as <String>0</String>. Then At the end of the reconciliation run, the connector automatically updates the timestamp in this parameter. **Sample value:** <String> 2024-07-10 08:07:32.023 </String>
Object Type	This attribute holds the name of the object type for the reconciliation run. **Default value**: User **Note:** Do not change the default value.
Resource Object Name	Name of the Resource object used for reconciliation **Default value:** FA User **Note:** Do *not* modify the value of this parameter.
Scheduled Task Name	Name of the Scheduled task used for reconciliation **Default value:** <Application Name> FAUserRequestService Incremental User Reconciliation **Note:** Do *not* modify the value of this parameter.

5

Performing Post configuration Tasks for the Fusion Apps Connector

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

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

5.1 Configuring Oracle Identity Governance

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

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

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

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

5.1.1 Creating and Activating a Sandbox

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

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

5.1.2 Creating a New UI Form

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

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

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

5.1.3 Publishing a Sandbox

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

1. In Identity System Administration, deactivate the sandbox.
2. Log out of Identity System Administration.
3. Log in to Identity Self Service 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*.

5.1.4 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

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

See Also:

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

5.2 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 listed in Reconciliation Jobs for the Fusion Apps Target Connector.
2. Run the Catalog Synchronization Job scheduled job.

See Also:

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

5.3 Managing Logging for the Connector

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 Logging on the Connector Server
- Enabling Logging for the Connector Server
- Understanding Log Levels
- Enabling Logging

5.3.1 Understanding Logging on the Connector Server

When you enable logging, the connector server stores in a log file information about events that occur during the course of provisioning and reconciliation operations for different statuses. By default, the connector server logs are set at INFO level, and you can change this level to any one of these.

- Error

This level enables logging of information about errors that might allow connector server 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 operation.

- FINE, FINER, FINEST

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

5.3.2 Enabling Logging for the Connector Server

Edit the logging properties file located in the CONNECTOR_SERVER_HOME/Conf directory to enable logging.

To do so:

1. Navigate to the *CONNECTOR_SERVER_HOME*/Conf directory.
2. Open the logging.properties file in a text editor.
3. Edit the following entry by replacing INFO with the required level of logging:

```
.level=INFO
```

4. Save and close the file.
5. Restart the connector server.

5.3.3 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 5-1 Log Levels and ODL Message Type:Level Combinations

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

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

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

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

5.3.4 Enabling Logging

Perform this procedure to enable logging in Oracle WebLogic Server.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:
   a. Add the following blocks in the file:

      ```
      <log_handler name='FusionApps-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='5252880'/> <property
      name='maxLogSize' value='52528800'/> <property name='encoding'
      value='UTF-8'/></log_handler> <logger name=
      'ORG.IDENTITYCONNECTORS.FAUSERREQUESTSERVICE' level="[LOG_LEVEL]"
      useParentHandlers="false"> <handler name=" FusionApps-handler"/>
      <handler name="console-handler"/> </logger><logger name=
      'ORG.IDENTITYCONNECTORS.FAIDENTITYSERVICE'level="[LOG_LEVEL]"
      useParentHandlers="false"> <handler name=" FusionApps-handler"/>
      <handler name="console-handler"/> </logger>
      ```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 5-1 lists the supported message type and level combinations. Similarly, replace [FILE_NAME] with the full path and name of the log file in which you want log messages to be recorded. The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]:**

      ```
      <log_handler name= ‘FusionApps -handler’
      level='NOTIFICATION:1'class='oracle.core.ojdl.logging.ODLHandlerFactory'
      > <property name='logreader:' value='off'/> <property name='path'
      value='F:\MyMachine\middleware\user_projects\domains\base_domain1\server
      s\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='5252880'/> <property name='maxLogSize'
      value='52528800'/> <property name='encoding' value='UTF-8'/></
      log_handler>  <logger
      name='ORG.IDENTITYCONNECTORS.FAUSERREQUESTSERVICE'level="NOTIFICATION:1"
       useParentHandlers="false"> <handler name=" FusionApps -handler"/>
      <handler name="console-handler"/> </logger><logger
      name='ORG.IDENTITYCONNECTORS.FAIDENTITYSERVICE'level="NOTIFICATION:1"
      useParentHandlers="false"> <handler name=" FusionApps -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:
   a. For Microsoft Windows: set WLS_REDIRECT_LOG= ***FILENAME***
   b. For UNIX: export WLS_REDIRECT_LOG= ***FILENAME***
      Replace ***FILENAME*** with the location and name of the file to which you want to redirect the output.
4. Restart the application server.

5.4 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, you must create an IT resource for the Connector Server as described in Creating IT Resources of *Oracle Fusion Middleware Administering Oracle Identity Governance.* While creating the IT resource, ensure to select Connector Server from the IT Resource Type list. In addition, specify values for the parameters of IT resource for the Connector Server listed in the following table.

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 5-2 Parameters of the IT Resource for the Oracle 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 Configuring the Java Connector Server with SSL for OIG in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

5.5 Localizing Field Labels in UI Forms

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

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

1. Log in to Oracle Enterprise Manager.

2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive (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 file 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 Fusion Apps Application instance. The original code is:

   ```
   <trans-unit id="$
   {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBund
   le']
   ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO
   . UD_FAUSER_USERNAME__c_description']}"><source>User ID </
   source><target/></trans-unit><trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.FusionApps.entity.userEO
   . UD_FAUSER_USERNAME__c_LABEL"><source>User ID</source><target/> </
   trans-unit>
   ```

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

```
global.udf. UD_FAUSER_USERNAME = \u30E6\u30FC\u30B6\u30FC\u540D
```

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

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO
. UD_FAUSER_USERNAME__c_description']}"><source>User ID</source>
<target> \u30E6\u30FC\u30B6\u30FC\u540D</target></trans-unit> <trans-
unitid="sessiondef.oracle.iam.ui.runtime.form.model.FusionApps.entitysEO
. UD_FAUSER_USERNAME__c_LABEL"><source>Account Name</source> <target>
\u30E6\u30FC\u30B6\u30FC\u540D</target></trans-unit>
```

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

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

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

See Also:

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

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

5.6 Configuring SSL

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

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

To configure SSL:

1. Obtain the SSL public key certificate of Fusion Apps.
2. Copy the public key certificate of Fusion Apps to the computer hosting Oracle Identity Governance.
3. Run the following `keytool` command to import the public key certificate into the identity key store in Oracle Identity Governance:

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

In this command:

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

The following are sample values for this command:

```
keytool -import -keystore <JAVA_HOME>/jre/lib/security/cacerts -file
<Cert_Location>/fileName.crt -storepass changeit -alias FusionApps01
```

```
keytool -import -keystore <WL_HOME>/server/lib/DemoTrust.jks -file
<Cert_Location>/fileName.crt -storepass DemoTrustKeyStorePassPhrase -alias
FusionApps02
```

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.
- In the Oracle Identity Governance cluster, perform this procedure on each node of the cluster and then restart each node.
- 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.

6

Using the Fusion Apps Connector

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

- Configuring Reconciliation
- Configuring Reconciliation Jobs
- Configuring Provisioning
- Uninstalling the Connector

6.1 Configuring Reconciliation

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

This section discusses the following topics related to configuring reconciliation:

- Performing Full Reconciliation
- Performing Incremental Reconciliation
- Performing Limited (Filtered) Reconciliation

6.1.1 Performing Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

To perform a full reconciliation run, ensure that no value is specified for the Filter Suffix parameter in User Reconciliation job for reconciling users.

6.1.2 Performing Incremental Reconciliation

After you deploy the connector, you must first perform full reconciliation. At the end of the reconciliation run, the connector automatically sets the Sync Token parameter of the job for user record reconciliation to the time stamp at which the run ended. From the next run onward, the connector considers only records created or modified after this time stamp for reconciliation. This is incremental reconciliation.

6.1.3 Performing Limited (Filtered) Reconciliation

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

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

This connector provides a Filter attribute that supports ICF filters (a scheduled task attribute) allowing you to use any of the Fusion Apps resource attributes to filter the target system records.

You can perform limited reconciliation by creating filters for the reconciliation module. This connector only supports *Id* filter. Below is the example for the filter:

Filter Suffix Value: equalTo('__UID__','<Id>')

Example: equalTo('__UID__','093A2592109708D1E06372431FAC584D')

In this example, the record whose Id is 093A2592109708D1E06372431FAC585D is reconciled.

6.2 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.

   > **Note:**
   >
   > If you are using OIG 12cPS4 with 2022OCTBP or later version, log in to Identity Console, click **Manage**, under **System Configuration**, 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:
   a. **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.
   b. **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

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

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

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

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

6.3 Configuring Provisioning

You can configure the provisioning operation for the Fusion Apps connector.

This section provides information on the following topics:

- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations

6.3.1 Guidelines on Performing Provisioning Operations

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

Provisioning attributes required to create User account.

To create User provisioning operation, following values are required:

- Account Type: : This will specify the Account Type (User)
- UserName: The user’s Username.
- First Name: The user's first name.
- Last Name: The user's last name.

Attributes required to be updated in the parent form of User account.

- UserName: The user’s Username
- Display Name: The user’s Display name
- External Id: The user’s External Id
- Work Email Address: The user’s work email address
- First Name: The user's first name.
- Last Name: The user's last name.

Provisioning attributes required to create Worker account.

To create Worker provisioning operation, following values are required:

- Account Type: This will specify the Account Type (Worker)
- Last Name: The worker’s Last name
- Worker Type: Worker type of worker account

- Action Code: Action Code Specifies the action performed on the record. For example: HIRE, ADD PENDING WORKER, and so on.
- Legal Employer Name: A legal employer is a legal entity that employs workers.
- Legislation Code: The LegislationCode is an attribute used to specify the legislative data group for a particular country or region.
- BusinessUnitId: A business unit is a unit of an enterprise that performs one or many business functions that can be rolled up in a management hierarchy.
- Projected Start Date: This field indicates the anticipated start date for the new employee. (This is required to provision Pending Worker)
- Proposed User Person Type: This field specifies the intended user person type for the new employee. (This is required to provision Pending Worker)

Attributes required to be updated in the parent form of Worker account.

- Last Name: Worker’s Last name.
- First Name: Worker’s First name.
- Work Email Address: Worker’s work email address
- Primary Phone Type: This will specify the phone type of worker’s primary phone number.
- Primary Phone Number: This will specify the primary phone number of worker.
- Address Line1: This will be first line of worker’s address.
- Address Line2: This will be second line of worker’s address.
- Floor: This will specify floor number of worker's address.
- Town Or City: This will specify the City or Town of workers' address.
- Region1: This will specify the Region 1 of workers' address.
- Region2: This will specify the Region 2 of workers' address.
- Region3: This will specify the Region 3 of workers' address.
- Postal Code: This will specify the postal code of workers' address.

> **Note:**
>
> 1. Upon provisioning, immediate reconciliation is necessary to obtain the ‘workerId’. This ‘workerId’ is required for all update operations on worker accounts.
> 2. Reconciliation is needed after modifying child data to fetch phoneId and emailId for each update operation of Phone and Email.
> 3. Manager, Job and departments are not reconciling to OIM for pending worker type.

6.3.2 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance, perform the following steps:

1. Log in to **Identity Self Service**.

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

6.4 Uninstalling the Connector

Uninstalling the Fusion Apps 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: Fusion Apps User; Fusion Apps Role

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

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

7 Extending the Functionality of the Connector

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

This section discusses the following topics:

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

7.1 Configuring Transformation and Validation of Data

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

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

7.2 Configuring Action Scripts

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

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

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

7.3 Configuring the Connector for Multiple 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*.

8 Upgrading the Fusion Apps Connector

If you have already deployed the 11.1.1.5.0 version of this 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.

You can upgrade the Fusion Apps Connector while in production, and with no downtime. Your customizations remain intact, and the upgrade will be transparent to your users. All form field names are preserved from the legacy connector.

> **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, first perform the upgrade procedure in a test environment.

The following sections discuss the procedure to upgrade the connector:

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

See Also:

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

8.1 Preupgrade Steps

Preupgrade steps involve performing a reconciliation run, defining the source, running the Delete JARs utility and connector preupgrade utility.

Before you perform an upgrade operation or any of the upgrade procedures, you must perform the following actions:

- Perform the preupgrade procedure documented in Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
- Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
- Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector.
- If required, create the connector XML file for a clone of the source connector.
- Disable all scheduled tasks.

- Run the Oracle Identity Manager Delete JARs utility to delete the old connector bundle to the Oracle Identity Manager database.
- Run the connector preupgrade utility.

See Also:

- – Delete JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for detailed information about the Delete JARs utility
  – Managing Connector Lifecycle of *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about the preupgrade utility

8.2 Upgrade Steps

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

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

- Staging Environment

Perform the upgrade procedure by using the wizard mode.

Note: Do not upgrade IT resource type definition. In order to retain the

default setting, you must map the IT resource definition to 'None'.

- Production Environment

Perform the upgrade procedure by using the silent mode.

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

8.3 Postupgrade Steps

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

> **Note:**
>
> If you have not retained the customizations, you must reapply them after you upgrade the connector.

Perform the following procedure:

1. Run the Oracle Identity Manager Upload JARs utility to post the new connector bundle and lib JARs to the Oracle Identity Manager database.

> **Note:**
>
> You can download the JARs from Oracle Technology Network Website (OTN) website. See Downloading the Connector Installation Package for more information.
>
> - Upload bundle/org.identityconnectors.faidentityservice-12.3.0.jar as an ICFBundle
> - Upload bundle/ org.identityconnectors.fauserrequestservice-12.3.0.jar as an ICFBundle

See Also: Upload JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for detailed information about the Upload JARs utility

2. If the connector is deployed on a Connector Server, then:
   - Stop the Connector Server.
   - Replace the existing connector bundle and lib JARs located in the *CONNECTOR_SERVER_HOME*/bundles directories respectively with the new connector bundles (bundle/org.identityconnectors.faidentityservice-12.3.0.jar and bundle/org.identityconnectors.fauserrequestservice-12.3.0.jar) from the connector installation media.
   - Start the Connector Server.
3. Reconfigure the IT resource of the connector if the IT resource details are updated.
4. Replicate all changes as in the previous version of the connector process form in a new UI form as follows:
   - Log in to Oracle Identity System Administration.
   - Create and activate a sandbox.
   - Create a new UI form to view the upgraded fields.
   - Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource from the form field, select the form (created in Step 4 c), and then save the application instance.
   - Publish the sandbox and perform full reconciliation.
5. Delete the duplicated lookup entries that are generated while upgrading the connector. The following are the list of lookup definitions.
   - Lookup.FAIdentityService.Configuration
   - Lookup.FAIdentityService.UM.ProvAttrMap
   - Lookup.FAIdentityService.UM.ReconAttrMap
   - Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted
   - Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults
   - Lookup.FAUserRequestService.Configuration.Trusted
     Perform the postupgrade procedure in Managing Connector Lifecycle of *Oracle Fusion Middlware Administering Oracle Identity Governance*.
6. Perform full reconciliation or delete reconciliation.

See Also:

- Configuring Oracle Identity Governance for information about creating, activating, and publishing a sandbox and creating a new UI form
- Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for information about deploying the Connector Server

9 Known Issues and Limitations of the Fusion Apps Connector

Updating a worker attribute that is not directly linked to user information will not automatically update the lastModified value in the corresponding user record. As a result, incremental synchronization may not capture these changes unless the user information is also modified.

10

Files and Directories in the Connector Installation Package

These are the components of the connector installation package that comprise the Fusion Apps connector.

Table 10-1 Files and Directories in the Fusion Apps Connector Installation Package

File in the Installation Package	Description
/bundle/ org.identityconnectors.faidentityservice-12.3.0.jar	This JAR is the ICF connector bundle for Target Application.
/bundle/ org.identityconnectors.fauserrequestservice-12.3.0.jar	This JAR is the ICF connector bundle for Authoritative Application.
configuration/FUSION-APPS-CI.xml	This XML file contains configuration information.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to Oracle Identity database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
xml/FusionApps-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.

File in the Installation Package	Description
xml/FusionApps-ConnectorConfig.xml	This XML file contains definitions for the following connector components: • IT resource definition • Process forms • Process task and adapters • Lookup definition • Resource objects • Process definition • Scheduled tasks • Reconciliation rules
xml/FusionApps-pre-config.xml	This XML file contains definitions for the connector objects associated with any non-User objects . Also, it contains definitions of Lookups and schedule tasks.
xml/FusionApps-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.

A

Connector Objects Used During Provisioning

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

- Provisioning Functions
- User Fields for Provisioning

A.1 Provisioning Functions

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

The Adapter column in the below table gives the name of the adapter that is used when the function is performed.

Table A-1 Provisioning Functions

Function	Adapter
Add Email to User	adpFAIDENTITYSERVICEADDROLE
Add Phone to User	adpFAIDENTITYSERVICEADDROLE
Address Line1 Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Address Line2 Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Address Type Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Add Role To User	adpFAIDENTITYSERVICEADDROLE
Business Unit Id Updated	adpFAIDENTITYSERVICEUPDATEUSER
Country Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Create FA Account	adpFAIDENTITYSERVICECREATEUSER
DeleteUser	adpFAIDENTITYSERVICEDELETEUSER
Department Updated	adpFAIDENTITYSERVICEUPDATEUSER
Disable User	adpFAIDENTITYSERVICEDISABLEUSER
Display Name Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Email Updated	adpFAIDENTITYSERVICEUPDATEROLE
Enable User	adpFAIDENTITYSERVICEENABLEUSER
External ID Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
First Name Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Floor Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Gender Updated	adpFAIDENTITYSERVICEUPDATEUSER
Grade Updated	adpFAIDENTITYSERVICEUPDATEUSER

Table A-1 (Cont.) Provisioning Functions

Function	Adapter
Job Updated	adpFAIDENTITYSERVICEUPDATEUSER
Last Name Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Link FA Account	adpFATCCOMPLETETASK
Password Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Phone Updated	adpFAIDENTITYSERVICEUPDATEROLE
Postal Code Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Preferred Language Updated	adpFAIDENTITYSERVICEUPDATEUSER
Primary Phone Number Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Primary Phone Type Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Projected Start Date Updated	adpFAIDENTITYSERVICEUPDATEUSER
Proposed User Person Type Updated	adpFAIDENTITYSERVICEUPDATEUSER
Region1 Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Region2 Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Region3 Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Remove Email From User	adpFAIDENTITYSERVICEREMOVEROLE
Remove Phone From User	adpFAIDENTITYSERVICEREMOVEROLE
Remove Role From User	adpFAIDENTITYSERVICEREMOVEROLE
Role Updated	adpFAIDENTITYSERVICEUPDATEROLE
Town Or City Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Trigger Create or Link FA Account	adpTRIGGERCREATEORLINKFAACCOUNT
UD_FAUSER Updated	adpFAIDENTITYSERVICEMULTIUPDATE
Update ExternalID	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
User Name Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE
Work Email Address Updated	adpUPDATESINGLEATTRIBUTEVALUEWITHOLDVALUE

A.2 User Fields for Provisioning

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

The below table lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Postupgrade Issue

Before upgrading the connector, the following lookup default decode values are upgraded with target configuration values.

1. Lookup.FAIdentityService.Configuration
2. Lookup.FAIdentityService.UM.ProvAttrMap
3. Lookup.FAIdentityService.UM.ReconAttrMap
4. Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted
5. Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults
6. Lookup.FAUserRequestService.Configuration.Trusted

Once the connector is upgraded, it generates duplicate entries with decode default values. Delete those duplicated lookup entries and keep values as shown in the following tables:

Lookup.FAIdentityService.Configuration

The following table lists the entries in theLookup.FAIdentityService.Configurationlookup definition.

Table A-2 Entries in the Lookup.FAIdentityService.Configuration Lookup Definition

Code Key	Decode
User Configuration Lookup	Lookup.FAIdentityService.UM.Configuration
Connector Name	org.identityconnectors.faidentityservice.FAIdentityServiceConnector
Bundle Version	12.3.0
Bundle Name	org.identityconnectors.faidentityservice
defaultBatchSize	500
applicationType	false
requiredWorkerAttributes	E:familyName,LegislationCode,LegalEmployerName,WorkerType,ActionCode,BusinessUnitId#N:familyName,LegislationCode,LegalEmployerName,WorkerType,ActionCode,BusinessUnitId#C:familyName,LegislationCode,LegalEmployerName,WorkerType,ActionCode,BusinessUnitId#P:familyName,LegislationCode,LegalEmployerName,WorkerType,ActionCode,BusinessUnitId,ProposedUserPersonType,ProjectedStartDate
lookupEndPoints	Country:hcmCountriesLov#Department:departmentsLov#Jobs:jobsLov#BusinessUnit:hcmBusinessUnitsLOV#LegalEmployerName:legalEmployersLov#LegislationCode:legalEmployersLov#Grades:grades#AddressType:/fscmRestApi/resources/11.13.18.05/commonLookupsLOV?finder=LookupTypeAllRowsFinder;LookupType=ADDRESS_TYPE#PhoneTypes:/fscmRestApi/resources/11.13.18.05/commonLookupsLOV?finder=LookupTypeAllRowsFinder;LookupType=PHONE_TYPE#ActionCode:actionsLOV#WorkerType:/fscmRestApi/resources/11.13.18.05/commonLookupsLOV?finder=LookupTypeFinder;LookupType=PER_PERIOD_TYPE

Lookup.FAIdentityService.UM.Configuration

The following table lists the entries in theLookup.FAIdentityService.UM.Configuration lookup definition.

Table A-3   Entries in the Lookup.FAIdentityService.UM.Configuration Lookup Definition

Code Key	Decode
Recon Attribute Map	Lookup.FAIdentityService.UM.ReconAttrMap
Provisioning Attribute Map	Lookup.FAIdentityService.UM.ProvAttrMap

Lookup.FAIdentityService.UM.ProvAttrMap

The following table lists the entries in theLookup.FAIdentityService.UM.ProvAttrMap lookup definition.

Table A-4   Entries in the Lookup.FAIdentityService.UM.ProvAttrMap*Lookup Definition*

Code Key	Decode
Preferred Language	preferredLanguage
External ID	externalId
Last Name	name.familyName
Display Name	displayName
UD_FAROLE~Role Name[LOOKUP]	roles
First Name	name.givenName
User Name	__NAME__
Work Email Address	emails.value
Id	__UID__
Account Type	userType
Password	password
Email Address Id	emails.EmailAddressId
Email Type	emails.type
Action Code	workRelationships.assignments.ActionCode
Person Name Id	names.PersonNameId
Worker Type	workRelationships.WorkerType
Legal Employer Name	workRelationships.LegalEmployerName
Legislation Code	names.LegislationCode
Primary Phone Id	phones.PhoneId
Primary Phone Type	phones.PhoneType
Primary Phone Number	phones.PhoneNumber
Person Address Usage Id	addresses.PersonAddrUsageId
Address Id	addresses.AddressId
Address Type	addresses.AddressType
Address Line1	addresses.AddressLine1
Address Line2	addresses.AddressLine2
Floor	addresses.FloorNumber
Town Or City	addresses.TownOrCity
Region1	addresses.Region1
Region2	addresses.Region2
Region3	addresses.Region3
Postal Code	addresses.PostalCode

Table A-4 (Cont.) Entries in the Lookup.FAIdentityService.UM.ProvAttrMap*Lookup Definition*

Code Key	Decode
Country	addresses.Country
Period Of Service Id	workRelationships.PeriodOfServiceId
Business Unit Id	workRelationships.assignments.BusinessUnitId
Business Unit	workerInformation.businessUnit
Projected Start Date	workRelationships.assignments.ProjectedStartDate
Proposed User Person Type	workRelationships.assignments.ProposedUserPersonType
Worker Id	workerId
UD_FAPHONE~Phone Id	phones~PhoneTypes~PhoneId
UD_FAPHONE~Phone Type[LOOKUP]	phones~PhoneTypes~PhoneType
UD_FAPHONE~Phone Number	phones~PhoneTypes~PhoneNumber
UD_FAEMAIL~Email Address Id	emails~__EMAIL__~EmailAddressId
UD_FAEMAIL~Email Type[LOOKUP]	emails~__EMAIL__~EmailType
UD_FAEMAIL~Email Address	emails~__EMAIL__~EmailAddress

Lookup.FAIdentityService.UM.ReconAttrMap

The following table lists the entries in theLookup.FAIdentityService.UM.ReconAttrMap lookup definition.

Table A-5 Entries in the Lookup.FAIdentityService.UM.ReconAttrMap*Lookup Definition*

Code Key	Decode
Preferred Language	preferredLanguage
Id	__UID__
First Name	name.givenName
User Name	__NAME__
Display Name	displayName
Roles~Role Name[LOOKUP]	roles~ApplicationRoles~id
Work Email Address	emails.value
Last Name	name.familyName
External ID	externalId
Status	__ENABLE__
Account Type	userType
Email Address Id	emails.EmailAddressId
Email Type	emails.type
Gender	legislativeInfo.Gender
Last Modified	meta.lastModified
Created	meta.created
Hire Date	workRelationships.StartDate
Person Id	PersonId
Person Number	workerInformation.personNumber
Manager	workerInformation.manager
Worker Type	workRelationships.WorkerType

Table A-5 (Cont.) Entries in the Lookup.FAIdentityService.UM.ReconAttrMap*Lookup Definition*

Code Key	Decode
Action Code	workRelationships.assignments.ActionCode
Person Name Id	names.PersonNameId
Legal Employer Name	workRelationships.LegalEmployerName
Legislation Code	names.LegislationCode
Primary Phone Id	phones.PhoneId
Primary Phone Type	phones.PhoneType
Primary Phone Number	phones.PhoneNumber
Person Address Usage Id	addresses.PersonAddrUsageId
Address Id	addresses.AddressId
Address Type	addresses.AddressType
Address Line1	addresses.AddressLine1
Address Line2	addresses.AddressLine2
Floor	addresses.FloorNumber
Town Or City	addresses.TownOrCity
Region1	addresses.Region1
Region2	addresses.Region2
Region3	addresses.Region3
Postal Code	addresses.PostalCode
Country	addresses.Country
Period Of Service Id	workRelationships.PeriodOfServiceId
Job	workerInformation.job
Start Date	workRelationships.assignments.EffectiveStartDate
End Date	workRelationships.assignments.EffectiveEndDate
Business Unit Id	workRelationships.assignments.BusinessUnitId
Business Unit	workerInformation.businessUnit
Department	workerInformation.department
Grade	workRelationships.assignments.GradeCode
Position	workRelationships.assignments.PositionCode
Location	workRelationships.assignments.LocationCode
Termination Date	workRelationships.TerminationDate
Projected Start Date	workRelationships.assignments.ProjectedStartDate
Proposed User Person Type	workRelationships.assignments.ProposedUserPersonType
Worker Id	workerId
Phone Numbers~Phone Id	phones~PhoneTypes~PhoneId
Phone Numbers~Phone Type[LOOKUP]	phones~PhoneTypes~PhoneType
Phone Numbers~Phone Number	phones~PhoneTypes~PhoneNumber
Secondary Emails~Email Address Id	emails~__EMAIL__~EmailAddressId
Secondary Emails~Email Type[LOOKUP]	emails~__EMAIL__~EmailType
Secondary Emails~Email Address	emails~__EMAIL__~EmailAddress

Lookup.FAUserRequestService.Configuration.Trusted

The following table lists the entries in theLookup.FAUserRequestService.Configuration.Trustedlookup definition.

Table A-6 Entries in the Lookup.FAUserRequestService.Configuration.Trusted Lookup Definition

Code Key	Decode
Bundle Version	12.3.0
Connector Name	org.identityconnectors.fauserrequestservice.FAUserRequestServiceConnector
User Configuration Lookup	Lookup.FAUserRequestService.UM.Configuration.Trusted
Bundle Name	org.identityconnectors.fauserrequestservice
defaultBatchSize	500
socketTimeOut	90000
connectionTimeOut	80000
httpHeaderContentType	application/json
httpHeaderAccept	application/json

Lookup.FAUserRequestService.UM.Configuration.Trusted

The following table lists the entries in theLookup.FAUserRequestService.UM.Configuration.Trusted lookup definition.

Table A-7 Entries in the Lookup.FAUserRequestService.UM.Configuration.Trusted Lookup Definition

Code Key	Decode
Recon Attribute Defaults	Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults
Recon Attribute Map	Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted

Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults

The following table lists the entries in theLookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaultslookup definition.

Table A-8 Entries in the Lookup.FAUserRequestService.UM.ReconAttrMap.TrustedDefaults Lookup Definition

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

Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted

The following table lists the entries in theLookup.FAUserRequestService.UM.ReconAttrMap.Trustedlookup definition.

Table A-9 Entries in the Lookup.FAUserRequestService.UM.ReconAttrMap.Trusted Lookup Definition

Code Key	Decode
FA Account Status[TRUSTED]	__ENABLE__
Locality Name	workRelationships.assignments.LocationCode
FAAccountID	__UID__
GradeCode	workRelationships.assignments.GradeCode
Country	addresses.Country
Postal Address	addresses.TownOrCity
Email	emails.value
Postal Code	addresses.PostalCode
Generation Qualifier	workRelationships.LegalEmployerName
State	addresses.Region1
Telephone Number	phones.Extension
First Name	name.givenName
User Login	__NAME__
Manager Login	workerInformation.manager
Employee Number	workerInformation.personNumber
Preferred Language	preferredLanguage
Last Name	name.familyName
Display Name	displayName
Gender	legislativeInfo.Gender
PersonID	PersonId
Job	workerInformation.job
Common Name	workerInformation.businessUnit
Hire Date	names.EffectiveStartDate
Department Number	workerInformation.department
Mobile	phones.PhoneNumber
Start Date	workRelationships.StartDate
End Date	workRelationships.TerminationDate
Job Start Date	workRelationships.assignments.EffectiveStartDate
Job End Date	workRelationships.assignments.EffectiveEndDate
Title	workRelationships.assignments.PositionCode
ManagerId	workRelationships.assignments.managers.ManagerAssignmentNumber
PO Box	addresses.Building
Floor	addresses.FloorNumber
Home Postal Address	addresses.AddressLine1

See More:

See Extending the Functionality of the Fusion Apps Connector (oracle.com) for information on addressing your specific business requirements.