

Oracle® Identity Governance

Configuring the DocuSign Connector



12c (12.2.1.3.0)

F74162-01

December 2022

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

ORACLE®

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

F74162-01

Copyright © 2022, Oracle and/or its affiliates.

Primary Author: Lakshmipathy Krishnan

Contributors:

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

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

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

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

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

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 About the DocuSign Connector

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

2 Creating an Application by Using DocuSign Connector

2.1	Process Flow for Creating an Application By Using the Connector	2-1
2.2	Prerequisites for Creating an Application By Using the Connector	2-2
2.2.1	Downloading the Connector Installation Package	2-3
2.2.2	Creating a Target System User Account for DocuSign Connector	2-3
2.2.3	Configuring the Target System	2-3
2.2.4	OAuth Flow to Generate the User-Level Tokens	2-4
2.3	Creating an Application By Using the Connector	2-6
2.4	Deploying the Connector Bundle in a Connector Server	2-7

3 Configuring the DocuSign Connector

3.1	Basic Configuration Parameters	3-1
3.2	Advanced Settings Parameters	3-2
3.2.1	Advanced Settings Parameters	3-3
3.3	Attribute Mappings	3-5

3.3.1	Attribute Mappings for a Target Application	3-5
3.4	Correlation Rules	3-8
3.4.1	Correlation Rules, Situations, and Responses for a Target Application	3-8
3.5	Reconciliation Jobs	3-10
3.5.1	User Reconciliation Job	3-10
4	Performing the Post-Configuration Tasks for DocuSign Connector	
4.1	Configuring Oracle Identity Governance	4-1
4.1.1	Creating and Activating a Sandbox	4-1
4.1.2	Creating a New UI Form	4-2
4.1.3	Publishing a Sandbox	4-2
4.1.4	Updating an Existing Application Instance with a New Form	4-2
4.2	Harvesting Entitlements and Sync Catalog	4-3
4.3	Managing Logging for the Connector	4-3
4.3.1	Understanding Log Levels	4-3
4.3.2	Enabling Logging	4-4
4.4	Configuring the IT Resource for the Connector Server	4-6
4.5	Localizing Field Labels in UI Forms	4-6
4.6	Configuring SSL	4-8
5	Using the DocuSign Connector	
5.1	Configuring Reconciliation	5-1
5.1.1	Performing Full Reconciliation	5-1
5.1.2	Performing Limited Reconciliation	5-1
5.2	Configuring Reconciliation Jobs	5-2
5.3	Performing Provisioning Operations	5-3
5.4	Uninstalling the Connector	5-3
6	Extending the Functionality of the Connector	
6.1	Adding New Attributes for Reconciliation	6-1
6.2	Adding New Attributes for Provisioning	6-1
6.3	Configuring Transformation and Validation of Data	6-2
6.4	Configuring Action Scripts	6-2
6.5	Configuring the Connector for Multiple Tenants	6-2
A	Appendix	
A.1	Known Issues and Limitations	A-1
A.2	Frequently Asked Questions for the DocuSign Connector	A-1

List of Figures

1-1	Connector Architecture	1-5
2-1	Overall Flow of the Process for Creating an Application By Using the Connector	2-2
3-1	Default Attribute Mappings for DocuSign Connector User Account	3-7
3-2	Default Attribute Mappings for the Group Names	3-8
3-3	Correlation Rule	3-9
3-4	Predefined Situations and Responses for DocuSign Connector	3-10

List of Tables

1-1	Certified Components	1-2
1-2	Supported Connector Operations	1-3
1-3	Supported Connector Features Matrix	1-7
2-1	Elements	2-5
2-2	Elements	2-6
3-1	Basic Configuration Parameters for DocuSign Connector	3-1
3-2	Advanced Settings Parameters	3-3
3-3	Default Attribute Mappings for DocuSign Connector User Account	3-6
3-4	Default Attribute Mappings for DocuSign Connector Group Names	3-7
3-5	Predefined Identity Correlation Rule for DocuSign Target Application	3-8
3-6	Predefined Situations and Responses for DocuSign Connector	3-9
3-7	Parameters of the DocuSign Full User Reconciliation	3-11
3-8	Parameters of the Reconciliation Jobs for Entitlements	3-12
3-9	DocuSign Update Access Token Job	3-14
4-1	Log Levels and ODL Message Type:Level Combinations	4-4
4-2	Parameters of the IT Resource for the Connector Server	4-6
6-1	New Attributes and the Sample Values	6-1
A-1	Files and Directories in the Connector Installation Package	A-2

Preface

This guide describes the connector that is used to onboard the DocuSign application to Oracle Identity Governance.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

Conventions

The following text conventions are used in this document:

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

1

About the DocuSign Connector

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

The DocuSign connector lets you create and onboard DocuSign 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**.

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 DocuSign connector:

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

**Note:**

In this guide, the term Oracle Identity Governance server refers to the computer on which Oracle Identity Governance is installed.

1.1 Certified Components

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

Table 1-1 Certified Components

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

**Note:**

For version 12 c PS3 (12.2.1.3.0), ensure that you download and apply patch 27861122 from [My Oracle Support](#).

1.2 Usage Recommendation

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

- If you are using Oracle Identity Governance release 12c (12.2.1.3.0) or later version, 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

Operation	Supported
User Management	-
Create a user	Yes
Reconcile user	Yes
Update user	Yes
Delete user	Yes

Table 1-2 (Cont.) Supported Connector Operations

Operation	Supported
DocuSign Group Grant Management	-
Assign and remove groups	Yes

1.5 Connector Architecture

The connector uses DocuSign APIs to synchronize user attributes between Oracle Identity Governance and DocuSign directory services and is implemented using the Identity Connector Framework (ICF) component.

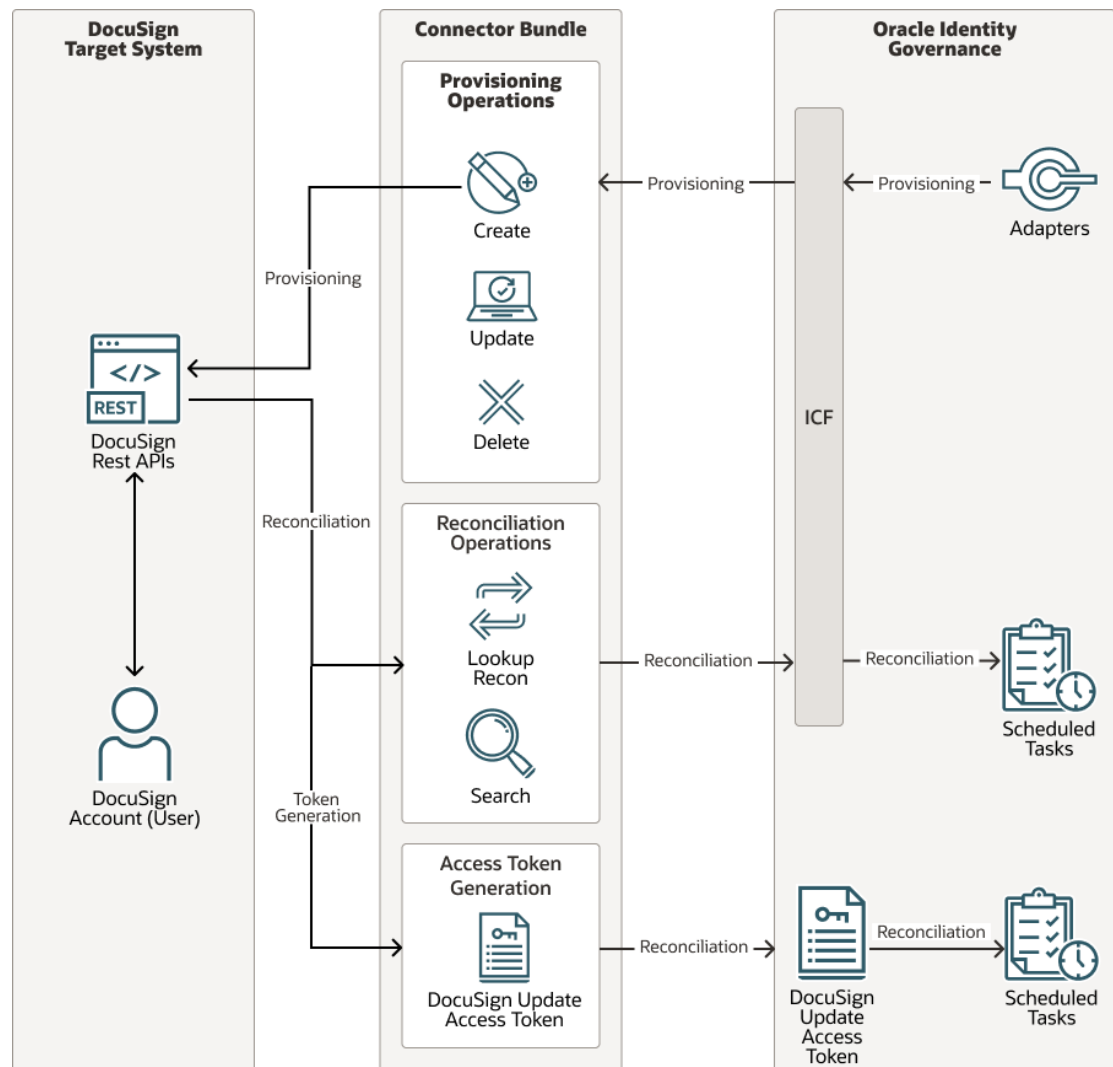
The ICF is a component that is required to use Identity Connector. ICF provides basic reconciliation and provisioning operations that are common to all Oracle Identity Governance connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such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

You can configure the connector to run in the following mode:

- **Account Management**
Account management is also known as target resource management. In this mode, the target system is used as a target resource and the connector enables the following operations:
 - **Provisioning**
Provisioning involves creating or updating users on the target system through Oracle Identity Governance. When you allocate (or provision) a DocuSign resource to the OIM User, the operation results in the creation of an account on DocuSign for that user. In the Oracle Identity Governance context, the term **provisioning** also covers updates made to the target system account through Oracle Identity Governance.
 - **Target Resource Reconciliation**
In target resource reconciliation, data related to the newly created and modified target system accounts can be reconciled and linked with existing OIM Users and provisioned resources. Use a scheduled job for performing reconciliation.

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

Figure 1-1 Connector Architecture



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

Through the provisioning operations that are performed on Oracle Identity Governance, accounts are created and updated in the target system for Oracle Identity Governance Users. During provisioning, the Adapters invoke ICF operation, ICF, in turn, invokes create operation on the DocuSign Identity Connector Bundle, and then the bundle calls the target system API for provisioning operations. The DocuSign Table 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 to the bundle, which passes it to the adapters.

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

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

The DocuSign Identity Connector Bundle communicates with the DocuSign Table API using the HTTPS protocol. The DocuSign Table API provides programmatic access through REST API endpoints. Apps can use the DocuSign API to perform create, read, update, and delete (CRUD) operations on directory data and directory objects, such as users.

 **See Also:**

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

1.6 Supported Use Cases

DocuSign connector is used to integrate OIG with a DocuSign instance. DocuSign connector ensures that all DocuSign accounts are created, updated, deleted, and deactivated on an integrated cycle with the rest of the identity-aware applications in your enterprise.

DocuSign connector standardizes service processes and implements automation to replace manual tasks. In a typical IT scenario, an organization using OIG wants to manage accounts, user association with a role or with a department across a DocuSign Cloud instance.

As a business use case, consider a leading logistics company in Australia which was using DocuSign for the ticketing system solution and OIG for Identity Management. Before using DocuSign connector, operations such as create, edit, and delete were performed manually and lacked a centralized streamlining operation. These operations can be easily automated using the DocuSign REST APIs. By integrating DocuSign connector with Oracle Identity Governance, the logistics company was able to achieve complete automation.

Following are few example scenarios which DocuSign connector facilitates:

- **DocuSign User Management**

An organization using DocuSign wants to integrate with OIG to manage identities. The organization wants to manage its user identities by creating them in the target system using OIG. The organization also wants to synchronize user identity changes performed directly in the target system with OIG. In such a scenario, a quick and easy way is to install the DocuSign connector and configure it with your target system by providing connection information in the IT resource.

DocuSign connector allows new users to self-provision on a DocuSign Cloud instance. New users can request and provision from a catalog of cloud-based resources.

To create a new user in the target system, fill in and submit the OIG process form to trigger the provisioning operation. The connector executes the create operation

against your target system and the user is created on successful execution of the operation. Similarly, operations such as delete, and update can be performed.

To search or retrieve the user identities, you must run a scheduled task from OIG. The connector will run the corresponding search operation against the user identities in the target system and fetch all the changes to OIG.

1.7 Supported Connector Features Matrix

Provides the list of features supported by the AOB application.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application
Full reconciliation	Yes
Limited (filtered) reconciliation	Yes
Delete reconciliation	Yes
Use connector server	Yes
Configure validation and transformation of account data	Yes
Perform connector operations in multiple domains	Yes
Support for pagination	Yes
Test connection	Yes
Clone applications or create new application instances	Yes
Provide secure communication to the target system through SSL	Yes

1.8 Connector Features

The features of the connector include full and incremental reconciliation, limited reconciliation, transformation and validation of account data, and others.

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

1.8.1 Support for Full Reconciliation

In full reconciliation, all records are fetched from the target system to Oracle Identity Governance.

You can switch to full reconciliation at any time after you deploy the connector. For more information on performing full reconciliation runs, see [Performing Full Reconciliation](#).

1.8.2 Support for Limited (Filtered) Reconciliation

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

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

For more information on performing limited reconciliation, see [Performing Full Reconciliation](#).

1.8.3 Support for the Connector Server

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

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

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

1.8.4 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 *Managing Application OnBoarding in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

1.8.5 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*.

1.8.6 Secure Communication to the Target System

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

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

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

2

Creating an Application by Using DocuSign Connector

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

Topics

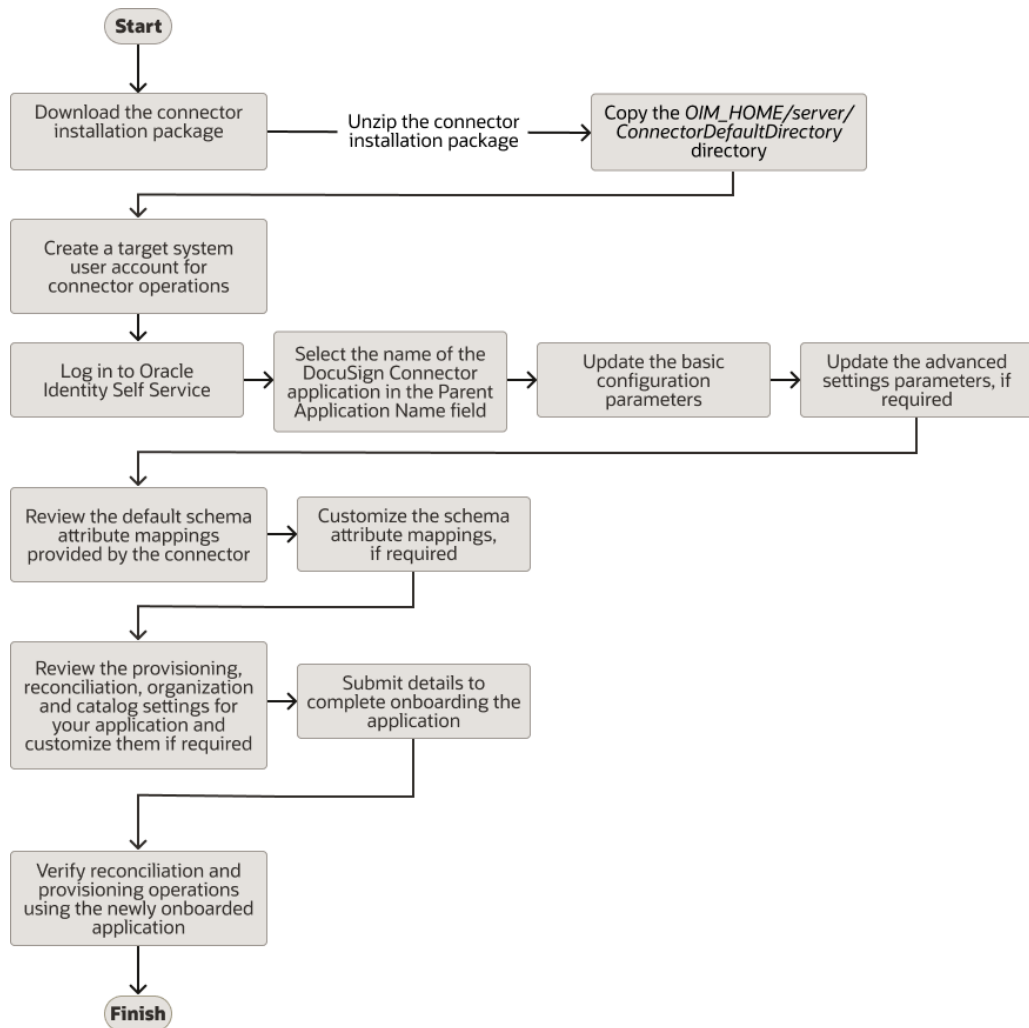
- [Process Flow for Creating an Application By Using the Connector](#)
- [Prerequisites for Creating an Application By Using the Connector](#)
- [Creating an Application By Using the Connector](#)
- [Deploying the Connector Bundle in a Connector Server](#)

2.1 Process Flow for Creating an Application By Using the Connector

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

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

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



2.2 Prerequisites for Creating an Application By Using the Connector

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

- [Downloading the Connector Installation Package](#)
- [Creating a Target System User Account for DocuSign](#)
- [Configuring the Target System](#)
- [OAuth Flow To generate the User-Level tokens](#)

2.2.1 Downloading the Connector Installation Package

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

To download the connector installation package:

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

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

4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER*.
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME/server/ConnectorDefaultDirectory* directory.

2.2.2 Creating a Target System User Account for DocuSign Connector

The user must have created a developer account to build an internal environment in DocuSign as it is required for the app to install and interact with the DocuSign API's and requests.

Make sure to create the account as an administrator to have full privilege and control over the users and visibility for viewing the user's entitlements.

2.2.3 Configuring the Target System

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

Preinstallation for the DocuSign connector involves performing a series of tasks on the target system.

Preinstallation involves the following tasks:

1. Log in to [DocuSign](#) with your account.
2. Create a basic app setup in the DocuSign target system for Auth2.0 authentication with an Authorization Code Grant.
 - Under Integrations Section, open **Apps and Keys** in your developer account **Settings** page, select **ADD APP AND INTEGRATION KEY** and create the application with an appropriate name. For example, DemoTest1..
3. Use or copy the Integration Key value, which is automatically generated once you create the application. For example, *7c2b8d7e-xxxx-xxxx-xxxx-cda8a50dd73f*.
4. Under Authentication:

- a. Under the **User Application** section, select the **Authorization Code Grant**.
 - b. To get the Secret Key, select **ADD SECRET KEY**.
 - c. Save/copy the value of the secret key to a secure place. You will need it later.
5. In the **Additional Settings** section, select **Add URI** and enter the new redirect URI (this can be a localhost address). For example, `http://example.com/callback`.

After performing these steps, you will get an Integration Key (Client Id) and the Secret Key (Client Secret). For more information about configuring target system, see <https://api.DocuSign.com/authentication/basics>.

2.2.4 OAuth Flow to Generate the User-Level Tokens

To generate the user-level access and refresh tokens, there are three steps you must complete manually and these values should be provided in `customAuthHeaders` in DocuSign Connector basic configuration for authentication.

The following steps must be completed by users who are opting in for Authorization Code Grant:

You must enter the oauth API by pass for these URL in the internet browser or use Postman to generate the tokens.

1. Requesting the Authorization Code

 **Note:**

The token URI for the developer environment is `https://account-d.docusign.com/oauth/token`.

- a. Enter the following URL in a browser as provided in the example.
Example:

```
https://accountd.docusign.com/oauth/auth?
response_type=code&scope=signature&client_id={iKey}&redirect_uri={c
allback}
```

Replace **{iKey}** with your integration key and **{callback}** with your redirect URI. The URL above includes the signature scope required for the eSignature REST API.

This URL opens the DocuSign authentication screen.

- b. After you enter your DocuSign developer account email address and password and give consent for the requested scopes. The browser will redirect to your redirect URI with a long string returned for the code parameter embedded in the URL.

Examples

Request:

```
https://account-d.docusign.com/oauth/auth?
response_type=code&scope=signature&client_id=7c2b8d7e-xxxx-
xxxx-xxxx-cda8a50dd73f&redirect_uri=http://example.com/
callback/
```

Response:

`http://example.com/callback/?code=eyJ0eXAi....81QFsje43QVZ_gw`

2. Generating Refresh and Access Tokens Using the Code Generated in Step 1.

- a. To request an access token, send a POST request containing your authorization code to the DocuSign authentication service.
- b. Paste the values of integration and secret key as Username and Password respectively under Authorization in the access token request with the type **Basic Auth** in Postman.
- c. In addition, the access token request contains a set of body parameters namely **grant_type** and **code**.
 - i. Update the key as code with value **<code>**.

 **Note:**

<code> is nothing but the authorization code that you received from the callback in step 1. For example, `code=eyJ0eXAi....QFsje43QVZ_gw`.

- ii. Likewise, update one more body parameter with the key as **grant_type** and value as **authorization_code**.
- d. Execute the Authorize Code Grant Access Token request to generate an access token and a refresh token.
 - i. In the response, you will get elements, namely, `access_token`, `token_type`, `refresh_token`, and `expires_in`.
 - ii. Copy/save the values of `access_token` and `refresh_token`.
For more information about how to get an access token with Auth Code Grant, see <https://developers.docusign.com/platform/auth/authcode/authcode-get-token/>.

Examples

Request:

```
curl --header "Authorization: Basic NWMYyjhkN....FhODg2MQ=="  
--data "grant_type=authorization_code&code=eyJ0eXAi....QFsje43QVZ_gw"  
--request POST https://account-d.docusign.com/oauth/token
```

Response:

```
{  
  "access_token": "eyJ0eXAi....mX9f7klg",  
  "token_type": "Bearer",  
  "refresh_token": "eyJ0eXAi....mruC5c3A",  
  "expires_in": 28800  
}
```

Table 2-1 Elements

Elements	Description
<code>access_token</code>	The value of the access token. Use this token in the Authorization header of all DocuSign API calls.

Table 2-1 (Cont.) Elements

Elements	Description
token_type	The type of token. For access tokens, the value of this is Bearer.
refresh_token	A token that is used to obtain a new access token without requiring user consent. The lifetime of a refresh token is typically around 30 days.
expires_in	The number of seconds before the access token expires.
grant_type	The type of grant being used to exchange an authorization code for an access token using authorization_code.

3. Providing Values for DocuSign Connector Basic Configuration.

After you have obtained the access_token and refresh_token values, you must provide these values in **customAuthHeaders** under DocuSign Connector basic configuration. For information about configuration, see [Configuring the DocuSign Connector](#). For example,
 access_token="eyJ0eXAi....mX9f7k1g","refresh_token=eyJ0eXAi....mruc5c3A "

Table 2-2 Elements

Elements	Description
refresh_token	The full refresh token value that is received from authentication.

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

2.4 Deploying the Connector Bundle in a Connector Server

You can deploy the connector either locally in Oracle Identity Manager or remotely in the Connector Server. A Connector Server is an application that enables remote execution of an Identity Connector, such as the DocuSign connector.

To deploy the connector bundle remotely in a Connector Server, follow the instructions at [Creating an Application By Using the Connector](#).

 **Note:**

- You can download the Connector Server from the Oracle Technology Network web page.
- See Configuring the IT Resource for the Connector Server for related information.
- See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installing, configuring, and running the Connector Server.

To install the connector into the Connector Server:

1. Stop the Connector Server.
2. Copy the DocuSign connector bundle into the `CONNECTOR_SERVER_HOME/bundles` directory.
3. Copy the DocuSign connector lib into the `CONNECTOR_SERVER_HOME/lib` directory.

 **Note:**

Except `docuSign-update-accesstoken.jar`, you can copy all jars in `CONNECTOR_SERVER_HOME/lib` directory.

4. Start the Connector Server. See Running the Connector Server for information about starting the Connector Server.

3

Configuring the DocuSign Connector

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.

- [Basic Configuration Parameters](#)
- [Advanced Settings Parameters](#)
- [Attribute Mappings](#)
- [Correlation Rules](#)
- [Reconciliation Jobs](#)

3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to DocuSign Connector.

Table 3-1 Basic Configuration Parameters for DocuSign Connector

Parameter	Mandatory?	Description
authenticationType	Yes	Type of authentication that is used by your target system. This connector supports Authenticating the target system by using Authorization Code Grant. Default value: other
clientId	Yes	Enter the client identifier (a unique string) issued by the authorization server to your client application during the registration process. This client ID is obtained while performing the procedure described in Configuring the Newly Added Application.
clientSecret	Yes	Enter the user namesecret key used to authenticate the identity of the target system that you create for your client application. The secret key is obtained while performing connector operations.the procedure described in ConfiguringSample value: johnsmith the Newly Added Application.
host	Yes	Enter the hostname of the machine hosting your target system (mandatory attribute). Sample value: demo.docusign.net/restapi/v2.1/accounts/5d7179f9-9e25-4232-9200-b254aa49c805
Connector Server Name	Yes	If you are using DocuSign Connector with the Java Connector Server, then provide the name of the Connector Server IT Resource .

Table 3-1 (Cont.) Basic Configuration Parameters for DocuSign Connector

Parameter	Mandatory?	Description
customAuthHeaders	Yes	<p>Enter the Access Token and Refresh Token Values. These values will get updated with running DocuSign Update Access Token Job.</p> <p>Sample value:</p> <pre>"access_token=eyJ0eXAiOiJVNCIsImFsZyI6IiJTMjU2Iiwia2lkIjoInjgxODVmZjEtNGU1MS00Y2U5LWFmMWMtNjg5ODEyMjAzMzE3In0.AQoAAAABAAUABwCA8Kx7sbjaSAGAgDDQifs42kgCAGcjU3expKxCttt3-7XOG08VAAEAAAAYAAEAAAFAAAADQakAAAANDdhZWE4OWQtNWViYy00NmMyLWI0YmYtNjE5MDRhMjE0MTE1IgakAAAANDdhZWE4OWQtNWViYy00NmMyLWI0YmYtNjE5MDRhMjE0MTE1MACABwhGsbjaSDcAC1hTwTsYB0GKF0Qif6kfLg.Lk45d4mcBPIrBghYun1S2pVa0EE0XHYTU66cqWpEuPMgSieVTRgwF3wyTOSgyPuiJNf18QTJcG6js4LvVL7sPw8IJwQ6bd-4KEKejCDusGKWIGH49P7ImV0AdaTAZ7v-OHyI-DRlGwKR8AI-UdpDKfJYV7twe6i_XlombJmXLPervSK0Ywz4ssDwDvF7g0xFvE-qEfsy-DOWX5Dbp9uYjYyqvwTrmROWGIAjcl43WnK6fMZDP9W1qeJysJ_fmVAXvXSDEoHiSJXsrGtXw9DAR4vQ4goAeqNplwmUBtJfivBnm3Fe40HkZw6YcbV4-luzOpHy0rn0e_Qr7UVo9rPQ", "refresh_token=eyJ0eXAiOiJVNCIsImFsZyI6IiJTMjU2Iiwia2lkIjoInjgxODVmZjEtNGU1MS00Y2U5LWFmMWMtNjg5ODEyMjAzMzE3In0.AQoAAAABAAAgABwCA8Kx7sbjaSAGAgHARdETQ2kgCAGcjU3expKxCttt3-7XOG08VAAEAAAAYAAEAAAFAAAADQakAAAANDdhZWE4OWQtNWViYy00NmMyLWI0YmYtNjE5MDRhMjE0MTE1IgakAAAANDdhZWE4OWQtNWViYy00NmMyLWI0YmYtNjE5MDRhMjE0MTE1MACABwhGsbjaSDcAC1hTwTsYB0GKF0Qif6kfLg.J-3Htv7CWVIZx8aAVp8vRx_4mVAEN8zm599NHI-oGKVO8OZlAMqP0-2foAGkKQoc5L5WNwWPzADNM4ls5LEJTSvo4BiqIm2jzmaJzJCvo-xixX8_qEASa5lmo6aKPop7awsKac5aBnu5IELA36XVr0fDirAtswRPsYk039pkwSGNUcZYC0hMCO-uIYpUf5Op0oTzGP3PH2TKqLexh0P43TqohGsKBTMqW3qGw38krYC1a04h7wnpxznR8OnkPOIHy9NHVwCeFNH6xxMry653cBsf50-Csd9ATCfen62420U6ZwvVQTIS8LRdepLjlxZLgNbZ6e8Iif2F7o7449S1lQ"</pre>
proxyHost	Yes	<p>Enter the name of the proxy host used to connect to an external target.</p> <p>Sample value: www.example.com</p>
proxyPassword	Yes	<p>Enter the password of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.</p>
proxyPort	Yes	<p>Enter the proxy port number.</p> <p>Sample value: 1105</p>
proxyUser	Yes	<p>Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system.</p>
sslEnabled	Yes	<p>If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false.</p> <p>Sample value: true</p>

3.2 Advanced Settings Parameters

Advanced configuration parameters vary depending on whether you are creating a target application or an authoritative application.

- [Advanced Settings Parameters](#)

3.2.1 Advanced Settings Parameters

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

Table 3-2 Advanced Settings Parameters

Parameter	Mandatory?	Description
relURIs	Yes	<p>This entry holds the relative URL of every object class supported by this connector and the connector operations that can be performed on these object classes.</p> <p>Sample value:</p> <pre>"__ACCOUNT__.CREATEOP=/users", "__ACCOUNT__.UPDATEOP=/users/\$ (__UID__\$)", "__ACCOUNT__.TESTOP=/users", "__ACCOUNT__.SEARCHOP=/ users?\$(Filter Suffix)\$&additional_info=true&count=\$ (PAGE_SIZE)\$&status=Active,ActivationRequired,ActivationSent", "__ACCO UNT__.DELETEOP=/users", "__PROFILE__.SEARCHOP=/ permission_profiles", "groupList.SEARCHOP=/ groups", "__SIGNING__.SEARCHOP=/ signing_groups", "__ACCOUNT__.groupList.UPDATEOP=/groups/\$ (groupList.groupId)\$/users", "__ACCOUNT__.signingGroupId.UPDATEOP=/ signing_groups/\$(signingGroupId)\$/ users", "__ACCOUNT__.groupList.REMOVEATTRIBUTE=/groups/\$ (groupList~groupList~groupId)\$/ users", "__ACCOUNT__.signingGroupId.REMOVEATTRIBUTE=/signing_groups/\$ (signingGroupId)\$/users", "__ACCOUNT__.signingGroupId.SEARCHOP=/ signing_groups/\$(signingGroupId)\$/ users", "__ACCOUNT__.groupList.SEARCHOP=/users/\$(__UID__\$)"</pre>
nameAttributes	No	<p>This entry holds the namehelpText="Target attribute for all the objects that are handled by this connector. For example, __NAME__ for the __ACCOUNT__ each object class that it used for User accounts, the name attribute is user_name."</p> <p>Sample value:</p> <pre>"__ACCOUNT__.email", "groupList.groupName", "__PROFILE__.permissionProf ileName", "__SIGNING__.groupName"</pre>
uidAttributes	No	<p>This entry holds the uidhelpText="Target attribute for all the objects that are handled by this connector. For example, __UID__ for each object class.</p> <p>Sample value:</p> <pre>"__ACCOUNT__.userId", "groupList.groupId", "__PROFILE__.permissionProfi leId", "__SIGNING__.signingGroupId"</pre>
Bundle Name	Yes	<p>This entry holds the name of the connector bundle.</p> <p>Sample value:</p> <pre>org.identityconnectors.genericrest</pre>

 **Note:**

Do not modify this entry.

Table 3-2 (Cont.) Advanced Settings Parameters


Parameter	Mandatory?	Description
Bundle Version	Yes	This entry holds the version of the connector bundle. Sample value: 12.3.0
 Note: Do not modify this entry.		
Connector Name	No	This entry holds the name of the connector. Sample value: org.identityconnectors.genericrest.GenericRESTConnector
opTypes	No	This entry specifies the HTTP operation type for each object class supported by the connector. Values are comma separated and are in the following format: <i>OBJ_CLASS.OP=HTTP_OP</i> In this format, <i>OBJ_CLASS</i> is the connector object class, <i>OP</i> is the connector operation (for example, CreateOp, UpdateOp, SearchOp), and <i>HTTP_OP</i> is the HTTP operation (GET, PUT, or POST). Sample value: "__ACCOUNT__.CREATEOP=POST", "__ACCOUNT__.UPDATEOP=PUT", "__ACCOUNT__.DELETEOP=DELETE", "groupList.SEARCHOP=GET", "__PROFILE__.SEARCHOP=GET", "__SIGNING__.SEARCHOP=GET", "__ACCOUNT__.SEARCHOP=GET", "__ACCOUNT__.TESTOP=GET", "__ACCOUNT__.groupList.UPDATEOP=PUT", "__ACCOUNT__.signingGroupId.UPDATEOP=PUT", "__ACCOUNT__.groupList.REMOVEATTRIBUTE=DELETE", "__ACCOUNT__.signingGroupId.REMOVEATTRIBUTE=DELETE", "__ACCOUNT__.signingGroupId.SEARCHOP=GET", "__ACCOUNT__.groupList.SEARCHOP=GET"
pageSize	No	This entry holds how many resources appears on a page for a search operation. Sample value: 100
jsonResourcesTag	No	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload. Sample value: "__ACCOUNT__=users;newUsers", "groupList=groups", "__SIGNING__=groups", "__PROFILE__=permissionProfiles"
httpHeaderContent	No	This entry holds the content type expected by the target system in the header. Sample value: application/json
httpHeaderAccept	No	This entry holds the accept type expected from the target system in the header. Sample value: application/json
specialAttributeTargetFor	No	This entry lists the format in which an attribute is present in the target system endpoint. Values are comma separated and are presented in the following format: <i>OBJ_CLASS.ATTR_NAME= TARGET_FORMAT</i> . Sample value: "__ACCOUNT__.groupList=groupList"

Table 3-2 (Cont.) Advanced Settings Parameters

Parameter	Mandatory?	Description
Special AttributeHandling	No	This entry lists the special attributes whose values should be sent to the target one by one ("SINGLE"). Values are comma separated and are in the following format: OBJ_CLASS.ATTR_NAME.PROV_OP=SINGLE . Sample value: "__ACCOUNT__.groupList.SEARCHOP=SINGLE", "__ACCOUNT__.groupList.ADDATTRIBUTE=SINGLE"
Custompayload	No	This entry lists the payloads for all operations that are not in the standard format. Sample value: "__ACCOUNT__.CREATEOP={\"newUsers\": [{\"userName\": \"\$(userName) \$\", \"email\": \"\$(__NAME__) \$\", \"password\": \"\$(__PASSWORD__) \$\", \"firstName\": \"\$(firstName) \$\", \"lastName\": \"\$(lastName) \$\", \"company\": \"\$(company) \$\", \"permissionProfileId\": \"\$(permissionProfileId) \$\"}] }\", \"__ACCOUNT__.DELETEOP={\"users\": [{\"userId\": \"\$(__UID__) \$\"}] }\", \"__ACCOUNT__.groupList.UPDATEOP={\"users\": [{\"userId\": \"\$(__UID__) \$\"}] }\", \"__ACCOUNT__.signingGroupId.UPDATEOP={\"users\": [{\"userName\": \"\$(userName) \$\", \"email\": \"\$(__NAME__) \$\"}] }\", \"__ACCOUNT__.groupId.REMOVEATTRIBUTE={\"users\": [{\"userId\": \"\$(__UID__) \$\"}] }\", \"__ACCOUNT__.signingGroupId.REMOVEATTRIBUTE={\"users\": [{\"userName\": \"\$(userName) \$\", \"email\": \"\$(__NAME__) \$\"}] }"
passwordAttribute	No	This entry holds the name of the target system attribute that is mapped to the __PASSWORD__ attribute . Sample value: password
childFieldsWithSingleEnd	No	This entry specifies special attribute data coming in from a single end-point response. Sample value: "__ACCOUNT__.groupList"
pageUrlAttribute	No	This entry specifies the JSON response attribute, which is used to paginate to the next set of records. Sample value: nextUri

3.3 Attribute Mappings

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

- [Attribute Mappings for a Target Application](#)

3.3.1 Attribute Mappings for a Target Application

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

DocuSign Connector User Account Attributes

[Table 3-3](#) lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and DocuSign 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 DocuSign Connector User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User Id	__UID__	String	No	No	Yes	Yes	Yes
Full Name	username	String	Yes	Yes	Yes	No	NA
Email	__NAME_	String	Yes	Yes	Yes	No	NA
Created Date Time	createdDate	String	No	No	Yes	No	NA
password	PASSWORD	String	No	Yes	No	No	NA
Country	workAddress.country	String	No	Yes	Yes	No	NA
User Type	userType	String	No	No	Yes	No	NA
Permission Profile	permissionProfileId	String	No	Yes	Yes	No	NA
Company	company	String	No	Yes	Yes	No	NA
Language	userSettings.locale	String	No	Yes	Yes	No	NA
Can Send Envelope	userSettings.canSendEnvelope	String	No	Yes	Yes	No	NA
Status	userStatus	String	No	No	Yes	No	NA
IT Resource Name	-	Long	No	No	Yes	No	NA

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

Figure 3-2 Default Attribute Mappings for the Group Names

Application Attribute			Provisioning Property	Reconciliation Properties				
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive		
Group Name	groupList~groupList~groupId	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

3.4 Correlation Rules

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

Topics

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

3.4.1 Correlation Rules, Situations, and Responses for a 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 DocuSign connector provides a simple correlation rule when you create an Target application. The connector uses this correlation rule to compare the entries in Oracle Identity Governance repository and the authoritative application repository, determine the difference between the two repositories, and apply the latest changes to Oracle Identity Governance.

[Table 3-5](#) lists the default simple correlation rule for DocuSign Connector application. If required, you can edit the default correlation rule or add new rules. For more information about adding or editing simple or complex correlation rules, see *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Predefined Identity Correlation Rule for DocuSign Target Application

Authoritative Attribute	Element Operator	Identity Attribute	Case Sensitive?
__NAME__	Equals	Email	No

In the identity rule:

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

Figure 3-3 Correlation Rule

User

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

Preview Settings

Provisioning Reconciliation Organization Catalog

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

+ Add Rule Element

Target Attribute	Element Operator	Identity Attribute	Case Sensitive	Delete
UID	Equals	Email	<input type="checkbox"/>	X

Rule Operator

AND

Predefined Situations and Responses

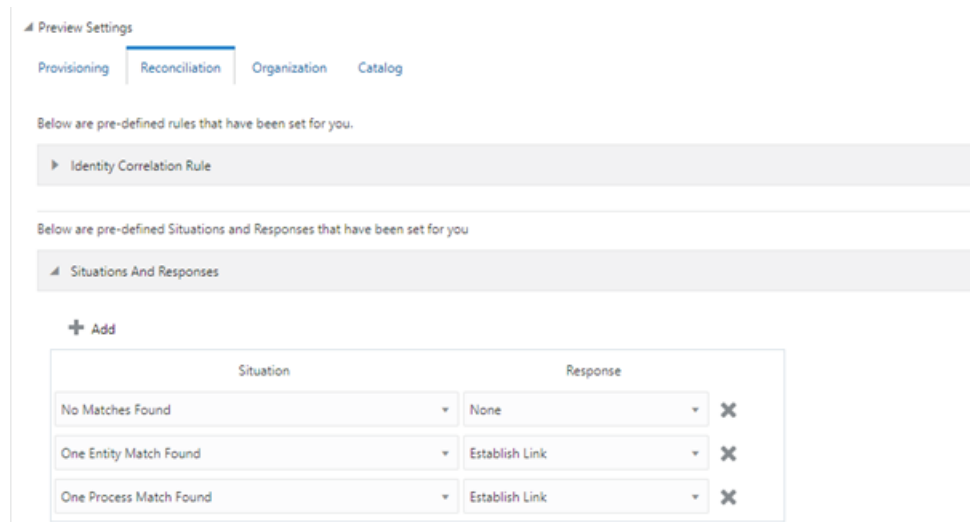
The DocuSign connector provides a default set of situations and responses when you create a target application. These situations and responses specify the action that Oracle Identity Governance must take based on the result of a reconciliation event.

[Table 3-6](#) lists the default situations and responses for the DocuSign Connector application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see *Creating a Target Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6 Predefined Situations and Responses for DocuSign Connector

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

[Figure 3-4](#) shows the situations and responses that the connector provides by default.

Figure 3-4 Predefined Situations and Responses for DocuSign Connector

3.5 Reconciliation Jobs

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

- [User Reconciliation Job](#)

3.5.1 User Reconciliation Job

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




User Reconciliation Job

The DocuSign Provisioned Status Reconciliation job is used to fetch and monitor all Service Requests which are in Provisioning Status.

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 DocuSign Full User Reconciliation is used to reconcile user data from a target application.

Table 3-7 Parameters of the DocuSign Full 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.
	<div style="border: 1px solid #0070C0; padding: 5px; background-color: #E6F2FF;">  Note: Do not modify this value. </div>
Filter	Enter the search filter for fetching user records from the target system during a reconciliation run. See Performing Limited 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
	<div style="border: 1px solid #0070C0; padding: 5px; background-color: #E6F2FF;">  Note: Do not change the default value. </div>
Scheduled Task Name	Name of the scheduled task used for reconciliation.
	<div style="border: 1px solid #0070C0; padding: 5px; background-color: #E6F2FF;">  Note: Do not modify this value. </div>

Reconciliation Job for Entitlements

The following jobs are available for reconciling entitlements:

- DocuSign Group Lookup Reconciliation
- DocuSign Permission Profile Lookup Reconciliation

The parameters for all the reconciliation jobs are the same.

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

Table 3-8 describes the parameters of the reconciliation Jobs for entitlements.

Table 3-8 Parameters of the Reconciliation Jobs for Entitlements





Parameter	Description
Application Name	<p>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.</p> <div data-bbox="1084 550 1380 724" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Note: Do not modify this value. </div>
Lookup Name	<p>This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched.</p> <p>Depending on the Reconciliation job that you are using, the default values are as follows:</p> <ul style="list-style-type: none"> For DocuSign Group Lookup Reconciliation: Lookup.DocuSign.Groups For DocuSign Permission Profile Lookup Reconciliation: Lookup.DocuSign.PermissionProfile
Object Type	<p>Enter the type of object whose values must be synchronized.</p> <p>Depending on the scheduled job that you are using, the default values are as follows:</p> <ul style="list-style-type: none"> For DocuSign Group Lookup Reconciliation : groupList For DocuSign Permission Profile Lookup Reconciliation : __PROFILE__ <div data-bbox="1084 1381 1380 1585" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Note: Do not change the value of this attribute. </div>

Table 3-8 (Cont.) Parameters of the Reconciliation Jobs for Entitlements

Parameter	Description
Code Key Attribute	<p>Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute).</p> <p>Default value:</p> <ul style="list-style-type: none"> For DocuSign Group Lookup Reconciliation: __UID__ For DocuSign Permission Profile Lookup Reconciliation: __UID__ <div data-bbox="1084 674 1378 846" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Note:</p> <p>Do not modify this value.</p> </div>
Decode Attribute	<p>Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute).</p> <p>Default value:</p> <ul style="list-style-type: none"> For DocuSign Group Lookup Reconciliation: __NAME__ For DocuSign Permission Profile Lookup Reconciliation: __NAME__ <div data-bbox="1084 1224 1378 1423" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Note:</p> <p>Do not change the value of this attribute.</p> </div>

DocuSign Update Access Token Job

The following job is available for updating Access and Refresh Token in customAuthHeaders under Basic Configuration.

**Note:**

Access Tokens received through the OAuth Authorization Code Grant flow usually have an 8-hour lifetime.

Table 3-9 DocuSign Update Access Token Job

Parameter	Description
Access Token Endpoint	This parameter holds the value of the access token endpoint. For example, https://account-d.docusign.com/oauth/token
IT Resource Name	Name of the IT resource 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.
Task Name	This parameter holds the name of the scheduled job. Default value: DocuSign Update Access Token

4

Performing the Post-Configuration Tasks for DocuSign Connector

The following 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](#)

4.1 Configuring Oracle Identity Governance

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



Note:

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

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

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

4.1.1 Creating and Activating a Sandbox

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

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

4.1.2 Creating a New UI Form

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

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

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

4.1.3 Publishing a Sandbox

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

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

4.1.4 Updating an Existing Application Instance with a New Form

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

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

 **See Also:**

- *Creating a Sandbox, Activating a Sandbox, and Publishing 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*

4.2 Harvesting Entitlements and Sync Catalog

You can populate the entitlement schema from the child process form table, and harvest groups, application instances, and entitlements into a 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](#).
2. Run the Entitlement List scheduled job to populate the Entitlement Assignment schema from the child process form table.
3. Run the Catalog Synchronization Job scheduled job.

 **See Also:**

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

4.3 Managing Logging for the Connector

Oracle Identity Governance uses Oracle Java Diagnostic Logging (OJDL) for recording all types of events pertaining to the connector. OJDL is based on `java.util.logger`.

The following topics provide detailed information about logging:

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

4.3.1 Understanding Log Levels

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

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

- `SEVERE.intValue()+100`

This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

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

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

Java Level	ODL Message Type:Level
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.

4.3.2 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='DocuSign-handler' level='[LOG_LEVEL]'

class='oracle.core.ojdl.logging.ODLHandlerFactory'><property
name='logreader:' value='off'></property> <property name='path'
value='[FILE_NAME]'></property> <property name='format'
value='ODL-Text'></property> <property name='useThreadName'
value='true'></property> <property name='locale'
value='en'></property> <property name='maxFileSize'
value='5242880'></property> <property name='maxLogSize'
value='52428800'></property> <property name='encoding'
value='UTF-8'></property> </log_handler> <logger
name="ORG.IDENTITYCONNECTORS.GENERICREST" level="[LOG_LEVEL]"
useParentHandlers="false"> <handler
name="DocuSign-handler"/> <handler
name="console-handler"/> </logger> <logger
name="ORG.IDENTITYCONNECTORS.RESTCOMMON" level="[LOG_LEVEL]"
useParentHandlers="false"> <handler
name="DocuSign-handler"/> <handler
name="console-handler"/> </logger>
```

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

```
<log_handler name='DocuSign-handler' level='NOTIFICATION:1'

class='oracle.core.ojdl.logging.ODLHandlerFactory'><property
name='logreader:' value='off'></property> <property name='path'

value='F:\MyMachine\middleware\user_projects\domains\base_domain1\serv
ers\oim_server1\logs\oim_server1-diagnostic-1.log'></property>
<property name='format'
value='ODL-Text'></property> <property name='useThreadName'
value='true'></property> <property name='locale'
value='en'></property> <property name='maxFileSize'
value='5242880'></property> <property name='maxLogSize'
value='52428800'></property> <property name='encoding'
value='UTF-8'></property> </log_handler> <logger
name="ORG.IDENTITYCONNECTORS.GENERICREST" level="NOTIFICATION:1"
useParentHandlers="false"> <handler
name="DocuSign-handler"/> <handler
name="console-handler"/> </logger> <logger
name="ORG.IDENTITYCONNECTORS.RESTCOMMON" level="NOTIFICATION:1"
useParentHandlers="false"> <handler
name="DocuSign-handler"/> <handler
name="console-handler"/>
</logger>
```

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

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

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

4. Restart the application server.

4.4 Configuring the IT Resource for the Connector Server

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

After you create the application for your target system, 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 use to select **Connector Server** from the **IT Resource Type** list.

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

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: 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 <code>true</code> to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter <code>false</code> . Default value: <code>false</code> Note: It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see <i>Configuring the Java Connector Server with SSL in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance</i> .

4.5 Localizing Field Labels in UI Forms

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

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

1. Log in to Oracle Enterprise Manager.

2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive (**oracle.iam.console.identity.sysadmin.ear_V2.0_metadata.zip**) to the local computer.
5. Extract the contents of the archive, and open one of the following file in a text editor if you are using Oracle Identity Governance 12c (12.2.1.3.0) or later version:

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

6. Edit the BizEditorBundle.xlf file in the following manner:
 - a. Search for the following text:

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

- b. Replace with the following text:

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

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

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

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

```
<trans-unit
  id="$
  {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
  ndle']}
  ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.user
  EO.UJ_DOCUSIGN_USER_ID__c_description']}>
  <source>User Id</source><target/>
</trans-unit>
<trans-unit

  id="sessiondef.oracle.iam.ui.runtime.form.model.DocuSign30.entity.Docu
  Sign30EO.UJ_DOCUSIGN_USER_ID__c_LABEL">
  <source>User Id</source><target/><target/>
</trans-unit>
```

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

```
global.udf.UD_DOCUSIGN_USR_USER_ID=\u30E6\u30FC\u30B6\u30FCID
```

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

```
</trans-unit><trans-unit
  id="$
  {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']}
  ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_DOCUSIGN_USER_ID__c_description']}>
  <source>User Id</source>
  <target/>
</trans-unit>
<trans-unit

id="sessiondef.oracle.iam.ui.runtime.form.model.DocuSign30.entity.DocuSign30EO.UD_DOCUSIGN_USER_ID__c_LABEL">
  <source>User Id</source>
  <target>\u30E6\u30FC\u30B6\u30FCID</target>
<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.

4.6 Configuring SSL

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

For example, Domains:

<https://demo.docusign.net>
<https://account-d.docusign.com>

2. Copy the public key certificate of DocuSign connector 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 DocuSign
```

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

 **Note:**

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

5

Using the DocuSign Connector

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

- [Configuring Reconciliation](#)
- [Configuring Reconciliation Jobs](#)
- [Performing Provisioning Operations](#)
- [Uninstalling the Connector](#)

5.1 Configuring Reconciliation

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

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

- [Performing Full Reconciliation](#)
- [Performing Limited Reconciliation](#)

5.1.1 Performing Full Reconciliation

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

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

After you create the application, you must first perform full reconciliation. To perform a full reconciliation run, ensure that no value is specified for the Filter parameter of the job for reconciling users.

5.1.2 Performing Limited Reconciliation

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

By default, all target system records are reconciled during the current reconciliation run. You can customize this process by specifying the subset of target system records that must be reconciled. You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a Filter attribute (a scheduled task attribute) that allows you to use DocuSign Connector resource attributes to filter the target system records.

Due to the limited functionality support of the DocuSign target system with respect to filtering queries for string data type fields, the connector only supports /userId and &email=<email_id> filters. Below are examples for both filters:

Filter Suffix value: /userId
Example: /423de2c9-6ef2-4827-8761-778556403170

In this example, the record whose userId is 423de2c9-6ef2-4827-8761-778556403170 is reconciled.

Filter Suffix value: &email=<emailId>
Example: &email=john.snow@example12.com

In this example, all records whose email is john.snow@example12.com is reconciled.

5.2 Configuring Reconciliation Jobs

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

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

To configure a reconciliation job:



Note:

If you are using OIG 12cPS4 with 2022OCTBP or later version, log in to Identity Console, click **Manage**, and then under System Configuration, click **Scheduler**.

1. Log in to Identity System Administration.
2. In the left pane, 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:
 - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
 - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type. See *Creating Jobs in Oracle Fusion Middleware Administering Oracle Identity Governance*.

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

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

 **Note:**

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

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

 **Note:**

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

5.3 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

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

 **See Also:**

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

5.4 Uninstalling the Connector

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

If you want to uninstall the connector for any reason, then run the Uninstall Connector utility. Before you run this utility, ensure that you set values for `ObjectType` and `ObjectValues` properties in the `ConnectorUninstall.properties` file. For example, if you want to delete resource objects, scheduled tasks, and scheduled jobs associated with the connector, then

enter "ResourceObject", "ScheduleTask", "ScheduleJob" as the value of the `ObjectType` property and a semicolon-separated list of object values corresponding to your connector as the value of the `ObjectValues` property.

Below are examples to uninstall ResourceObjects and ScheduleJobs respectively:

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

 **Note:**

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

For more information, see [Uninstalling a Connector](#) in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

6

Extending the Functionality of the Connector

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

The following topics describe the procedures to extend the functionality of the connector :

- [Adding New Attributes for Reconciliation](#)
- [Adding New Attributes for Provisioning](#)
- [Configuring Transformation and Validation of Data](#)
- [Configuring Action Scripts](#)
- [Configuring the Connector for Multiple Tenants](#)

6.1 Adding New Attributes for Reconciliation

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

The default attribute mappings for reconciliation are listed in [Attribute Mappings](#).

6.2 Adding New Attributes for Provisioning

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

The default attribute mappings for provisioning are listed in [Attribute Mappings](#).

Table 6-1 New Attributes and the Sample Values

New Attributes	Sample Values
Phone	workAddress.phone
Postal Code	workAddress.postalCode



Note:

The new attributes works on Update Account.

6.3 Configuring Transformation and Validation of Data

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

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

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

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

6.4 Configuring Action Scripts

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

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

Configure these scripts to run before or after 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*.

6.5 Configuring the Connector for Multiple Tenants

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

The following example illustrates this requirement:

XYZ corporation has multiple tenants including an independent schema. To meet the requirement posed by such a scenario, you must clone your application which copies all configurations of the base application into the cloned application.

For more information about cloning applications, see *Cloning Applications in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

A

Appendix

This section contains the following topics:

- [Known Issues and Limitations](#)
- [Frequently Asked Questions for the DocuSign Connector](#)
- [Files and Directories in the Connector Installation Package](#)

A.1 Known Issues and Limitations

This is a known issues and limitation associated with the DocuSign connector.

Provisioning user with the same Email ID from OIG, which already exists in the target.

The user does not create in the target, but one more new account will be provisioned in OIG for that particular user with the exiting User's ID.

Workaround: There is no workaround for this issue.

A.2 Frequently Asked Questions for the DocuSign Connector

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

1. Is Email an updatable field?

Answer: No, Email is not an updatable field as it is considered a key field in the target.

2. Provisioning user account from OIG will result in creating a user in target with default groups namely "Administrator" and "Everyone".

Answer: This is expected behavior from the target.

 **Note:**

Default Groups assignment/removal has a dependency on Permission-Profile.

For example, if a user is created with Permission-Profile as "Account Administrator" by default, the user will be assigned to "Administrators" and "Everyone" Groups. If provisioned with other than "Account Administrator" as Permission-Profile, the user will be assigned with only the "Everyone" Group.

A.3 Files and Directories in the Connector Installation Package

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

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

File in the Installation Media Directory	Description
/bundle/ org.identityconnectors.genericrest-12.3.0.jar	This JAR file is the ICF connector bundle.
configuration/DocuSign-CI.xml	This XML file contains configuration information.
lib/docuSign-update-accesstoken.jar	This jar is required to run the "DocuSign Update Access Token" Job that will update access and refresh token on a scheduled basis.
lib/commons-codec-1.16.jar	docuSign-update-accesstoken.jar has a dependency on these jars.
lib/httpclient5-5.1.3.jar	
lib/httpcore5-5.1.3.jar	
lib/jackson-annotations-2.14.0.jar	
lib/jackson-core-2.14.0.jar	
lib/jackson-databind-2.13.4.2.jar	
lib/slf4j-api-2.0.0.jar	
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the Oracle Identity 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/DocuSign-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 and also the configuration details specific to your target system, attribute mappings, correlation rules, and reconciliation jobs.
xml/DocuSign-pre-config.xml	This XML file contains definitions for lookup and schedule task.