Oracle® Identity Governance

Configuring the Dropbox Application

12c (12.2.1.3.0)
F16810-03
September 2020

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

F16810-03

Primary Author: Gowri.G.R

Contributors: Bhargav Janapati

Contents

List of Tables

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

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

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

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

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

Conventions

The following text conventions are used in this document:

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

What's New in This Guide?

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

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

Support for Onboarding Applications Using the Connector

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

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific update has been made in revision "03" of this guide:

The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to remove Oracle Identity Manager versions prior to 11g Release 2 PS3 (11.1.2.3.0).

The following documentation-specific update has been made in revision "02" of this guide:

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

1

About the Dropbox 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 Dropbox connector enables you to onboard applications in Oracle Identity Governance for Dropbox.

> **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 Dropbox connector:

- Introduction to the Connector
- Certified Components
- Usage Recommendation
- Supported Connector Operations
- Connector Architecture
- Supported Use Cases

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

1.1 Introduction to the Connector

The Dropbox connector enables Oracle Identity Governance to manage Dropbox by using Microsoft Active Directory (AD) as a middleware. Microsoft Active Directory is configured as a user source for performing all of the user management operations (create, update, delete, disable, and enable users) in Dropbox, and the user management data is directly stored in AD.

> **Note:**
>
> The Oracle Identity Governance Connector for Dropbox is referred to as **Dropbox connector** in this guide. Similarly, the Oracle Identity Governance Connector for Microsoft Active Directory User Management is referred to as **OIG AD connector**, and the Dropbox Business Active Directory Connector is referred to as **Dropbox AD connector**.

The Dropbox connector uses the following connectors to synchronize data between Oracle Identity Governance and Dropbox:

Oracle Identity Governance Connector for Microsoft Active Directory User Management

The Oracle Identity Governance Connector for Microsoft Active Directory User Management (OIG AD connector) allows synchronization of the Dropbox user and group information between Oracle Identity Governance and AD. It uses AD as a managed (target) resource of the identity data. The OIG AD connector is configured to run in the account management mode (or target resource management). This mode enables the following operations:

- **Provisioning**

  Provisioning involves creating, updating, or deleting users on AD through Oracle Identity Governance. When you allocate (or provision) a Microsoft Active Directory resource to an Oracle Identity Governance User, the operation results in the creation of an account on Microsoft Active Directory for that user. In the Oracle Identity Governance context, the term "provisioning" is also used to mean updates (for example enabling or disabling) made to the AD account through Oracle Identity Governance.

- **Target resource reconciliation**

  In target resource reconciliation, data related to newly created and modified accounts on AD can be reconciled and linked with existing Oracle Identity Governance Users and provisioned resources. To perform target resource reconciliation, the Active Directory User Target Recon scheduled job is used.

  Depending on the data that you want to reconcile, you use different scheduled jobs.

For detailed information on the OIG AD connector (such as certified languages, supported connector features, and so on), see About the Microsoft Active Directory User Management Connector in *Oracle Identity Governance Configuring the Microsoft Active Directory User Management Application*.

Dropbox Business Active Directory Connector

Dropbox uses a lightweight Dropbox Business Active Directory Connector (Dropbox AD connector) behind the firewall to synchronize the Dropbox user and group information between AD and Dropbox directory services.

The Dropbox AD connector automates provisioning of User and Group accounts in Dropbox from AD. These User and Group accounts are included as members of a Microsoft Active Directory group (specified as values of the AD Sync Group attribute of AD), which is used for synchronizing the accounts from AD to Dropbox through the Dropbox AD Connector scheduled task.

For more information on the Dropbox AD connector, visit the Dropbox website at https://www.dropbox.com/, navigate to Help Center, and search for Dropbox Active Directory Connector.

1.2 Certified Components

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

Table 1-1 Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Oracle Identity Governance or Oracle Identity Manager	You can use any one of the following releases: • Oracle Identity Governance release 12c PS4 (12.2.1.4.0) • Oracle Identity Governance 12c (12.2.1.3.0)	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance release 12c PS4 (12.2.1.4.0) • Oracle Identity Governance 12c (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0)
Target system	Dropbox **Note**: The connector uses Microsoft Active Directory (AD) as a middleware. Therefore, AD is configured as a user source for performing all of the user management operations in Dropbox.	Dropbox **Note**: The connector uses Microsoft Active Directory (AD) as a middleware. Therefore, AD is configured as a user source for performing all of the user management operations in Dropbox.
Connector Server	11.1.2.1.0 or 12.2.1.3.0	11.1.2.1.0 or 12.2.1.3.0
Oracle Identity Governance Connector for Microsoft Active Directory User Management	12.2.1.3.0	11.1.1.6.0 or 12.2.1.3.0

Table 1-1 (Cont.) Certified Components

Component	Requirement for AOB Application	Requirement for CI-Based Connector
Dropbox Business Active Directory Connector	2.0.850300	2.0.850300

1.3 Usage Recommendation

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

> **Note:**
>
> If you are using the latest 12.2.1.*x* version of this connector in the CI-based mode, then see *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management*, Release 11.1.1 for complete details on connector deployment, usage, and customization.

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

Operations	Supported?
User Management	
Create user	Yes
Update user	Yes
Delete user	Yes
Enable user	Yes
Disable user	Yes
Entitlement Grant Management	
Create Group	Yes
Update Group	Yes

Table 1-2 (Cont.) Supported Connector Operations

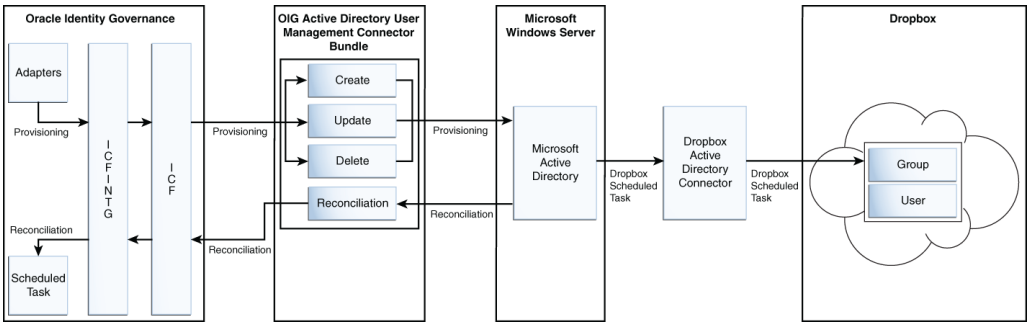
Operations	Supported?
Assign Group to User	Yes

1.5 Connector Architecture

The user management operations are implemented in Dropbox by using Microsoft Active Directory (AD) as a middleware.

As discussed earlier, the Dropbox connector uses the OIG AD connector and Dropbox AD connector to synchronize the Dropbox user and group information between Oracle Identity Governance, AD, and Dropbox directory services.

Figure 1-1 Architecture of the Dropbox Connector



As shown in Figure 1-1, AD is configured as a target resource of Oracle Identity Governance. The OIG AD connector is a .NET framework-based connector that is implemented using the Identity Connector Framework (ICF) component. The ICF component 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 connection pooling, buffering, time outs, and filtering. ICF is distributed together with Oracle Identity Governance. Therefore, you do not need to configure or modify ICF.

The Dropbox connector helps in provisioning User and Group accounts in Dropbox through the following two-step process:

1. The OIG AD connector creates or updates User and Group accounts in AD through the provisioning operations that are performed on Oracle Identity Governance.
2. The Dropbox AD connector automates provisioning of the User and Group accounts in Dropbox by fetching the attributes from AD and then synchronizing the data with Dropbox through the Dropbox AD Connector scheduled task. Based on the data fetched from AD, the User and Group accounts are automatically created or updated in Dropbox.

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

For more information on the architecture of the OIG AD connector, see Connector Architecture in *Oracle Identity Governance Configuring the Microsoft Active Directory User Management Application*.

For more information on the Dropbox AD connector, visit the Dropbox website at https://www.dropbox.com/, navigate to Help Center, and search for Dropbox Active Directory Connector.

1.6 Supported Use Cases

Dropbox is a cloud-based application that offers file-hosting services, such as cloud storage, file synchronization, personal cloud, and client software. The Dropbox connector enables Oracle Identity Governance to manage identities and access privileges for Dropbox users and groups.

The following are some of the most common scenarios in which the Dropbox connector can be used:

Dropbox User Management

The Dropbox connector automates provisioning and deprovisioning of Dropbox User accounts. Because Dropbox involves accessing and sharing content with users or groups across various locations, this connector ensures a secure access by granting it to users with appropriate access rights. For example, after a user joins an organization, a Dropbox user account is automatically provisioned to the user based on the predefined access policies in Oracle Identity Governance. Similarly, this account is deactivated after the user leaves the organization.

Dropbox Group Management

The Dropbox connector automates provisioning and deprovisioning of Dropbox Group accounts. You can configure a parent group by adding multiple users or groups (these groups may further include a set of users) in a flat group hierarchy. This configured group is then synchronized with Dropbox, and the associated user and group details are created.

This connector also helps in managing access rights for Dropbox Group accounts by ensuring specific access to various teams or departments in an organization.

2

Deploying and Using the Dropbox Connector

As a prerequisite for Oracle Identity Governance to communicate with Microsoft Active Directory and Dropbox, the OIG AD connector and Dropbox AD connector must be deployed and configured at the back end.

This chapter contains the following sections:

2.1 Deploying and Using the OIG AD Connector

Deploying the connector involves performing the preinstallation, installation, and postinstallation tasks. You can use the connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.

You deploy the OIG AD connector using the application onboarding capability of Identity Self Service. The detailed instructions for deploying and using the OIG AD connector is available in *Oracle Identity Governance Configuring the Microsoft Active Directory User Management Application*. For more information, see the following sections of the guide:

- Creating an Application By Using the Microsoft Active Directory User Management Connector for onboarding applications using the connector and the prerequisites for doing so
- Configuring the Microsoft Active Directory User Management Connector for configuring basic configuration and advanced settings parameters, attribute mappings, predefined correlation rules, situations and responses, and reconciliation jobs
- Performing the Postconfiguration Tasks for the Microsoft Active Directory User Management Connector for performing necessary tasks after creating an application
- Using the Microsoft Active Directory User Management Connector for understanding the guidelines on using the connector, performing connector operations, and uninstalling the connector
- Extending the Functionality of the Microsoft Active Directory User Management Connector for extending the functionality of the connector to address your specific requirements

2.2 Deploying and Using the Dropbox AD Connector

Deploying the connector involves performing the preinstallation, installation, and postinstallation tasks. After configuring the connector, you can use it to synchronize

the Dropbox user and group information between Microsoft Active Directory and Dropbox directory services.

The procedure for deploying and using the Dropbox AD connector is available in the Dropbox product documentation.

For the detailed instructions on deploying and using the Dropbox AD connector, visit the Dropbox website at https://www.dropbox.com/, navigate to Help Center, and search for Dropbox Active Directory Connector.