Oracle® Identity Governance

Configuring the Box Application

12c (12.2.1.3.0)
F14100-05
February 2023

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

F14100-05

Copyright © 2018, 2023, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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

List of Figures

List of Tables

Preface

This guide describes the connector that is used to onboard Box 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 Box application.

The updates discussed 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 Box target system. This helps in quicker onboarding of the applications for these targets into Oracle Identity Governance by using an intuitive UI.

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 12.2.1.3.0

The following is a documentation-specific update for revision "04" of the guide:

Logger names present in Enabling Logging have been updated.

The following is a documentation-specific update for revision "03" of the guide:

The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include information about mandatory patches that you must apply to Oracle Identity Governance release 12c PS3 (12.2.1.3.0). In addition, Oracle Identity Manager 11g Release 2 PS2 BP09 has been removed from the "Requirement for CI-Based Connector" column.

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

- The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance release 12c PS4 (12.2.1.4.0). This row has also been updated to include information about mandatory patches that you must apply to Oracle Identity Governance release 12c PS3 (12.2.1.3.0).
- The "Connector Server" and "Connector Server JDK" rows of Table 1-1 have been updated.
- Broken links have been fixed and some editorial corrections were made.

1

About the Box 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 Box connector lets you create and onboard Box applications in Oracle Identity Governance.

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

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

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

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

1.1 Certified Components

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

Table 1-1 lists the certified components for this 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) **Note**: Ensure that you download and apply the patches 26616250 and 25323654 from My Oracle Support.	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 BP06
Target System	Box	Box
Connector Server	11.1.2.1.0 and later	11.1.2.1.0 and later
Connector Server JDK	JDK 1.8 and later	JDK 1.8 and later

1.2 Usage Recommendation

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

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

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

1.3 Certified Languages

These are the languages that the connector supports.

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

1.4 Supported Connector Operations

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

Table 1-2 Supported Connector Operations

Operation	Supported?
User Management	
Create user	Yes
Update user	Yes
Delete User	Yes
Enable User	Yes
Disable User	Yes

> **Note:**
>
> All the connector artifacts required for managing groups as an object (for example groups attribute mappings, reconciliation rules, jobs, and so on) are not visible in the Applications UI in Identity Self Service. However, all the required information is available in the predefined application templates of the connector installation package.

1.5 Connector Architecture

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

The connector enables you to manage accounts on the target system. Managing accounts consists of the following processes:

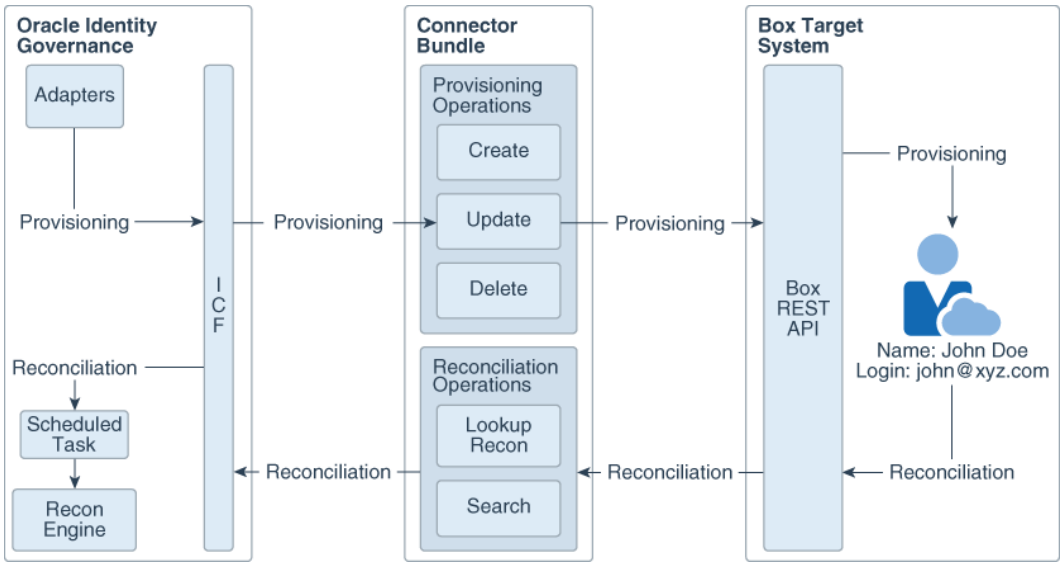
- **Provisioning**

  Provisioning involves creating or updating users on the target system through Oracle Identity Governance. When you allocate (or provision) a Box resource to an OIG User, the operation results in the creation of an account on Box 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 newly created and modified target system accounts can be reconciled and linked with existing OIG Users and provisioned resources. A scheduled job is used for reconciliation.

Figure 1-1 Connector Architecture



As shown in this figure, Box is configured as a target resource of Oracle Identity Governance. Through provisioning operations performed on Oracle Identity Governance, accounts are created and updated on the target system for OIG Users. Through reconciliation, account data that is created and updated directly on the target system is fetched into Oracle Identity Governance and stored against the corresponding OIG Users. Identity Connector Framework (ICF) is a component that is required in order to use Identity Connectors. ICF is distributed together with Oracle Identity Governance.

You do not need to configure or modify ICF. During provisioning, the Adapters invoke ICF operation, ICF in turn invokes create operation on Box Identity Connector Bundle and then the bundle calls Box REST API for Provisioning operations. The Box REST API on the target system accepts provisioning data from the bundle, carries out the required operation on the target system, and returns the response from the target system back to the bundle, which passes it to the adapters. During reconciliation, a scheduled task invokes ICF operation, ICF inturn invokes search operation on Box Identity Connector Bundle and then the bundle calls Box REST 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 Box resources that are already provisioned to OIG Users. If a match is found, then the update made to the Box record from the target system is copied to the Box 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 an Box resource to the OIG User.

The Box Identity Connector Bundle communicates with the Box REST API using the HTTPS protocol.

1.6 Supported Use Cases

Box is a cloud computing business which provides file-sharing, collaborating, and other tools for working with files that are uploaded to its servers. Box provides dynamic, flexible content

management solution which empowers users to share and access content from anywhere, while providing IT enterprise-grade security and oversight into how content moves within their organizations.

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

- Update Access Token

  Today, security is one of the biggest concerns that organizations face while accessing cloud applications. Each cloud application has its own mechanism to ensure that a security breach does not take place. Box uses automated tokens to achieve this. The administrators of the Box Connector are assigned a security token which is required to authenticate and authorize the administrators in order to perform various operations on the application. This token also gets refreshed periodically to minimize risk.

  Oracle Identity Manager Connector for Box provides automated admin token management to ensure that your administrator's security tokens are up-to-date. This functionality ensures that only authenticated and authorized administrators can perform the operations without any delay due to stale or expired tokens.

- Box User Management

  Organizations across the globe are using Box for content sharing. They want their employees to be able to access and share the most up-to-date information across different geographical locations. To achieve this, a Box administrator has to create and grant login to the concerned employees. The Box administrator must also be sure of the complete life cycle of this particular user. It must be ensured that when an employee leaves the organization, they should no longer be able to access sensitive information or content or files using their Box account. Similarly, during an employee's tenure, it has to be ensured that they have access towards files and content which they alone are entitled to use while access must be restricted towards classified files and content.

  Doing this manually for every employee is very cumbersome thus resulting in errors sometimes. Oracle Identity Manager Connector for Box provides user management functionality which enables automation of provisioning and deprovisioning of the users (employees). Whenever a new employee joins the organization, a Box account will automatically be provisioned to them along with appropriate access rights. Likewise, when they leave the organization, the same account will automatically be deactivated. This not only saves time but provides robust security as manual intervention is minimal here.

- Exempt Box User from 2-Step Login Verification

  As the need for enhanced security increases, Box provides an extra layer of security through the use of 2-step verification. This process requires the user to present the following two authenticating pieces of evidence when they log in:

  – Something they know (their Box password)

  – Something they have (an OTP code that is sent to their mobile device)

  The OTP code is sent to the users mobile device as a text message (SMS). In case the user loses their mobile device or cannot access the confirmation codes sent to the mobile device for reasons unknown, the Box Connector provides an option to exempt the user from the 2-Step Login Verification requirement. An exempted user would be able to log in successfully with only the Box password. If you would like to exempt a group of users or the administrator, you can enable the option **Exempt this user from 2-Step login verification** for that particular user.

- User Email Alias Management

  In an organization, a user may have multiple email addresses. For example, in case of acquisitions or mergers, there is a need to manage multiple email addresses for different domains. In such a situation, you may want to add a new email alias for a user who changed their name but left their primary email address the same.

  Email alias allows users to link multiple email addresses to a single Box account for easy management of their important content. Now, any user type can add multiple email addresses to their account and designate one as the primary address, where collaboration invites and Box notifications will be sent. With Oracle Identity Manager Connector for Box, you can manage email aliases and mark any one of them as primary for the user account.

- Box User's Group Membership Management

  Organizations are usually broken down into departments, project teams or other sub-units and with this systematic break-down, there comes a need to grant different teams different levels of access for different content. The group functionality of Box helps the organization to achieve this, thereby making it easy to replicate the work or resource breakdown easy in Box. It also helps in creating new teams along new lines. Groups make this division of labor easy to replicate in Box, and also give the opportunity to create new teams along new lines.

  Oracle Identity Manager Connector for Box enables an organization to manage user's group memberships. A user can be a member of one or more groups. Oracle Identity Manager Connector for Box has the capability to enable the IT group to retain visibility into how content is managed and accessed. With monitoring and granular access control capabilities, it can be ensured that only authorized users have access.

  One other benefit of collaborating using the Box User's Group Membership Management is that, as new users are added to any specific group, they are automatically eligible to gain access to the content already shared. This means that, such new users can log in and gain access to relevant content required by them to perform their job effectively.

- User and Group Reconciliation

  If a user with an existing Box application (which has other users and groups configured) wants to manage users and group membership, they must initially migrate the pre-existing Box groups into Oracle Identity Manager. The Box Connector facilitates User Reconciliation and Group Lookup Reconciliation to bulk load these users and their group memberships to Oracle Identity Manager respectively.

1.7 Supported Connector Features Matrix

Provides the list of features supported by the AOB application and CI-based connector.

Table 1-3 Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Full reconciliation	Yes	Yes
Limited reconciliation	Yes	Yes
Use connector server	Yes	Yes
Transformation and validation of account data	Yes	Yes

Table 1-3 (Cont.) Supported Connector Features Matrix

Feature	AOB Application	CI-Based Connector
Perform connector operations in multiple domains	Yes	Yes
Support for paging	Yes	Yes
Test connection	Yes	No
Reset password	Yes	Yes

1.8 Connector Features

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

- Full Reconciliation
- Limited Reconciliation
- Support for the Connector Server
- Secure Communication to the Target System
- Transformation and Validation of Account Data

1.8.1 Full Reconciliation

After you create the application, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Governance.

> **Note:**
>
> The connector cannot support incremental reconciliation because of the target system limitation. The target system does not provide a way to filter user records based on the attribute which stores the time at which the account data is created or modified.

You can perform a full reconciliation run at any time. See Configuring Reconciliation .

1.8.2 Limited Reconciliation

You can set a reconciliation filter as the value of the Filter attribute of a reconciliation scheduled job. This filter specifies the subset of added and modified target system records that must be reconciled.

For more information, see Performing Limited 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 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.

1.8.5 Transformation and Validation of Account Data

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

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

2

Creating an Application by Using the Box Connector

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

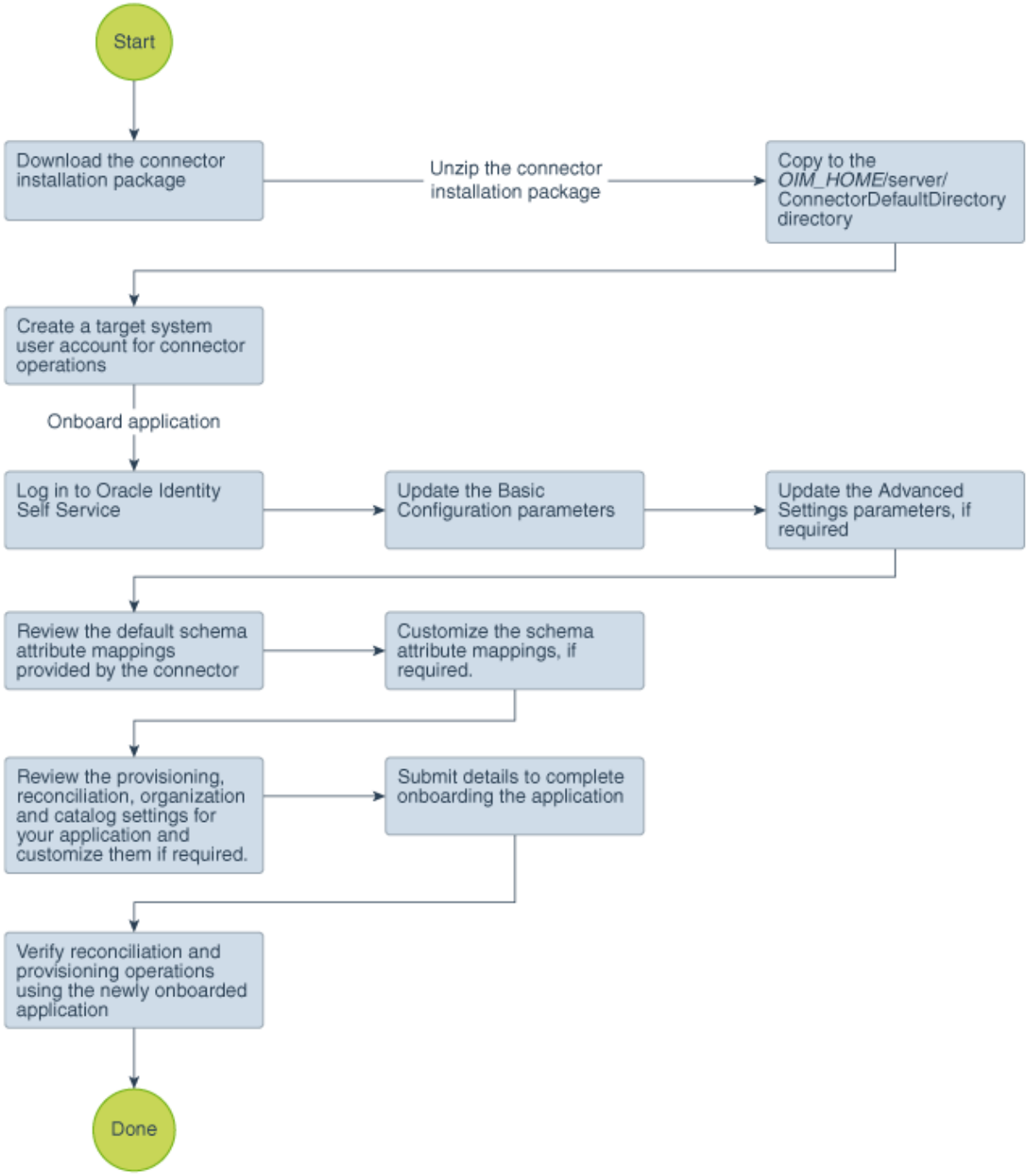
Topics

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.

- Configuring the Target System
- Downloading the Connector Installation Package

2.2.1 Configuring the Target System

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

Preinstallation involves the following tasks:

1. Create a Box service account on the target system to manage users on Box through Oracle Identity Governance.

   Ensure that the account is created with the **Co-Admin** role and **Manage Users** and **Manage Groups** administrative privileges.
2. Register the client application of the connector to provide a secure sign-in and authorization for your services.
3. On successful registration of the client application, configure your newly registered application to obtain the Client ID and Client Secret values.

   These values are required to generate access and refresh tokens for your application.
4. Generate access and refresh tokens using the Box service account created in Step 1 and the Client ID and Client Secret values obtained in Step 3.

   Access and refresh tokens must be generated manually for the first time. You provide these values for the customAuthHeaders parameter while configuring the IT Resource in Basic Configuration Parameters . Access and refresh tokens expire in 60 minutes and 60 days respectively. To avoid this, the Box Update Access Token scheduled job runs a scheduler to renew these values in a periodic manner. This scheduled job is discussed later.

> **Note:**
>
> If the Box Update Access Token scheduled job fails to run as expected and both access and refresh tokens expire, you must perform this procedure to generate a new pair of access and refresh tokens. After these values are obtained, configure the customAuthHeaders parameter in Basic Configuration Parameters .

The detailed instructions for performing these preinstallation tasks are available in the Box product documentation. For more information, visit the Box website at https://docs.box.com/docs.

2.2.2 Downloading the Connector Installation Package

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

To download the connector installation package:

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

   You must accept the license agreement before you can download the installation package.
4. Download and save the installation package to any directory on the computer hosting Oracle Identity Governance.
5. Extract the contents of the installation package to any directory on the computer hosting Oracle Identity Governance. This creates a directory named *CONNECTOR_NAME-RELEASE_NUMBER.*
6. Copy the *CONNECTOR_NAME-RELEASE_NUMBER* directory to the *OIG_HOME*/server/ConnectorDefaultDirectory directory.

2.3 Creating an Application By Using the Connector

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

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

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

1. Create an application in Identity Self Service. The high-level steps are as follows:
   a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
   b. Ensure that the **Connector Package** option is selected when creating an application.
   c. Update the basic configuration parameters to include connectivity-related information.
   d. If required, update the advanced setting parameters to update configuration entries related to connector operations.

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

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

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

   The application is created in Oracle Identity Governance.

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

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

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

See Also:

- Basic Configuration Parameters for more information about basic configuration parameters and their descriptions
- Advanced Settings Parameters for more information about advanced settings parameters and their descriptions

3
Configuring the Box Connector

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

This section contains the following topics:

3.1 Basic Configuration Parameters

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

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

Table 3-1 Basic Configuration Parameters for the Box Connector

Parameter	Mandatory?	Description
authenticationType	Yes	Enter the type of authentication used by your target system. The Box target system uses manual input of access token and refresh token for OAuth2.0 authentication. **Default value :** `Other`
Host	Yes	Enter the host name of the computer hosting your target system. **Sample value**: `api.box.com/2.0`

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

Parameter	Mandatory?	Description
clientId	Yes	Enter the client identifier (a unique string) issued by the authorization server to your client application during the registration process. You would have obtained the client ID while configuring the newly registered application. **Sample value**: `83b-88onw9ddvgy9nnbworruf0x4nre9`
clientSecret	Yes	Enter the secret key used to authenticate the identity of your client application. You obtained the secret key while performing the procedure described in Configuring the Newly Added Application. **Sample value**: `5Zi1PivsZDd00iHwK1GcZmvv5qNFCvuI`
customAuthHeaders	Yes	Takes access token and refresh token values. **Sample value**: `"access_token=fjvf0ghwpm3H1gSnWec3NcSVkgUFLIaQ","refresh_token=V1P163HMIC52RDxVE8rwlWHas0w71QWAJ2AXSivEpr6LluxGsQtDB34nxuKHhFJd"`
sslEnabled	Yes	If the target system requires SSL connectivity, then set the value of this parameter to true. Otherwise set the value to false. **Default value**: `true`
Connector Server Name	No	If you are using Box Connector together with the Java Connector Server, then provide the name of Connector Server.
Port	No	Enter the port number at which the target system is listening. **Sample value**: `443`
proxyHost	No	Enter the name of the proxy host used to connect to an external target.
proxyPassword	No	Password of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.

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

Parameter	Mandatory?	Description
proxyPort	No	Proxy port number.
proxyUser	No	Proxy user name of the target system user account that Oracle Identity Manager uses to connect to the target system.

3.2 Advanced Settings Parameters

The advanced settings parameters are the configuration-related entries that the connector uses during reconciliation and provisioning operations.

> **Note:**
>
> All parameters in the below table are mandatory

Table 3-2 Advanced Settings Parameters for the Box Connector

Parameter	Description
Bundle Name	This entry holds the name of the connector bundle. **Default value:** `org.identityconnectors.genericrest`
Bundle Version	This entry holds the version of the connector bundle. **Default value:** `12.3.0`
Connector Name	This entry holds the name of the connector. **Default value:** `org.identityconnectors.genericrest.GenericRESTConnector`
httpHeaderAccept	This holds the accept-type expected from the target system in the header. **Default value**: `application/json`
customPayload	This entry lists the payloads for all operations that are not in the standard format. **Default value**: `"__ACCOUNT__.__GROUP__.UPDATEOP={ \"user\": { \"id\": \"$(__UID__)$\"}, \"group\": { \"id\": \"$(id)$ \" } }","__ACCOUNT__.__GROUP__.CREATEOP={ \"user\": { \"id\": \"$(__UID__)$ \"}, \"group\": { \"id\": \"$(id)$ \" } }"`

Table 3-2 (Cont.) Advanced Settings Parameters for the Box Connector

Parameter	Description
nameAttributes	This entry holds the name attribute for all the objects that are handled by this connector. **Default value**: `"__ACCOUNT__.login","__GROUP__.name"`
jsonResourcesTagspecialAttributeHandling	This entry holds the json tag value that is used during reconciliation for parsing multiple entries in a single payload. **Default value**: `"__ACCOUNT__=entries","__GROUP__=entries","__ACCOUNT__.__GROUP__=entries","__ACCOUNT__.email=entries","__ACCOUNT__.__MEMBERSHIP__.__GROUP__=entries","__ACCOUNT__.__MEMBERSHIP__.email=entries"`
specialAttributeHandling	Enter the list of special attributes whose values must be sent to the target system in separate calls, one at a time. If you do not specify a value for this parameter, then the connector will send all values for a given special attribute in a single call. **Default value**: `"__ACCOUNT__.__GROUP__.CREATEOP=SINGLE","__ACCOUNT__.__GROUP__.UPDATEOP=SINGLE","__ACCOUNT__.email.CREATEOP=SINGLE","__ACCOUNT__.email.UPDATEOP=SINGLE","__ACCOUNT__.role.SEARCHOP=SINGLE","__ACCOUNT__.is_exempt_from_login_verification.SEARCHOP=SINGLE","__ACCOUNT__.is_sync_enabled.SEARCHOP=SINGLE"`
httpHeaderContentType	This holds the content-type expected by the target system in the header. **Default value**: `application/json`

Table 3-2 (Cont.) Advanced Settings Parameters for the Box Connector

Parameter	Description
relURIs (Box)	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. **Default value**: `"__ACCOUNT__.CREATEOP=/users","__ACCOUNT__.UPDATEOP=/users/$(__UID__)$","__ACCOUNT__.SEARCHOP=/users?$(Filter Suffix)$&limit=$(PAGE_SIZE)$&offset=$(PAGE_OFFSET)$","__ACCOUNT__.DELETEOP=/users/$(__UID__)$","__GROUP__.SEARCHOP=/groups?$(Filter Suffix)$&limit=$(PAGE_SIZE)$&offset=$(PAGE_OFFSET)$","__ACCOUNT__.__GROUP__.CREATEOP=/group_memberships","__ACCOUNT__.__GROUP__.UPDATEOP=/group_memberships","__ACCOUNT__.__GROUP__.SEARCHOP=/users/$(__UID__)$/memberships?limit=$(PAGE_SIZE)$&offset=$(PAGE_OFFSET)$","__ACCOUNT__.__GROUP__.DELETEOP=/group_memberships/$(__MEMBERSHIP__.id)$","__ACCOUNT__.__MEMBERSHIP__.__GROUP__.SEARCHOP=/users/$(__UID__)$/memberships","__ACCOUNT__.email.UPDATEOP=/users/$(__UID__)$/email_aliases","__ACCOUNT__.email.SEARCHOP=/users/$(__UID__)$/email_aliases?limit=$(PAGE_SIZE)$&offset=$(PAGE_OFFSET)$","__ACCOUNT__.email.DELETEOP=/users/$(__UID__)$/email_aliases/$(__MEMBERSHIP__.id)$","__ACCOUNT__.__MEMBERSHIP__.email.SEARCHOP=/users/$(__UID__)$/email_aliases?limit=$(PAGE_SIZE)$&offset=$(PAGE_OFFSET)$","__ACCOUNT__.role.SEARCHOP=/users/$(__UID__)$?fields=role","__ACCOUNT__.is_sync_enabled.SEARCHOP=/users/$(__UID__)$?fields=is_sync_enabled","__ACCOUNT__.is_exempt_from_login_verification.SEARCHOP=/users/$(__UID__)$?fields=is_exempt_from_login_verification"`
statusEnableValue	This entry holds the value of the status attribute in the target system which represents the enable value. **Default value**: `active`

Table 3-2 (Cont.) Advanced Settings Parameters for the Box Connector

Parameter	Description
enableEmptyString	This entry holds the configuration value. If this configuration is set to `true`, the connector will send an empty string instead of null to the target system when any attribute of the Box account of Oracle Identity Governance user is updated with a blank value. **Default value**: `true`
specialAttributeTargetFormat	This entry lists the format in which a special attribute is present in the target system endpoint. **Default value**:`"__ACCOUNT__.__GROUP__=group","__ACCOUNT__.__MEMBERSHIP__.__GROUP__=group.id"`
statusAttributes	This entry lists the name of the target system attribute that holds the status of an account. For example, for the __ACCOUNT__ object class that it used for User accounts, the status attribute is accountEnabled. **Default value**: `__ACCOUNT__.status`
uidAttributes	This entry holds the uid attribute for all the objects that are handled by this connector. **Default value**: `"__ACCOUNT__.id","__GROUP__.id"`
opTypes	This entry specifies the HTTP operation type for each object class supported by the connector. **Default value**: `"__ACCOUNT__.CREATEOP=POST","__ACCOUNT__.UPDATEOP=PUT","__ACCOUNT__.DELETEOP=DELETE","__ACCOUNT__.__GROUP__.UPDATEOP=POST","__ACCOUNT__.__GROUP__.DELETEOP=DELETE","__ACCOUNT__.email.UPDATEOP=POST","__ACCOUNT__.email.DELETEOP=DELETE"`
statusDisableValue	This entry holds the value of the status attribute in the target system which represents the disable value. **Default value**: `inactive`

3.3 Attribute Mappings

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

Box User Account Attributes

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

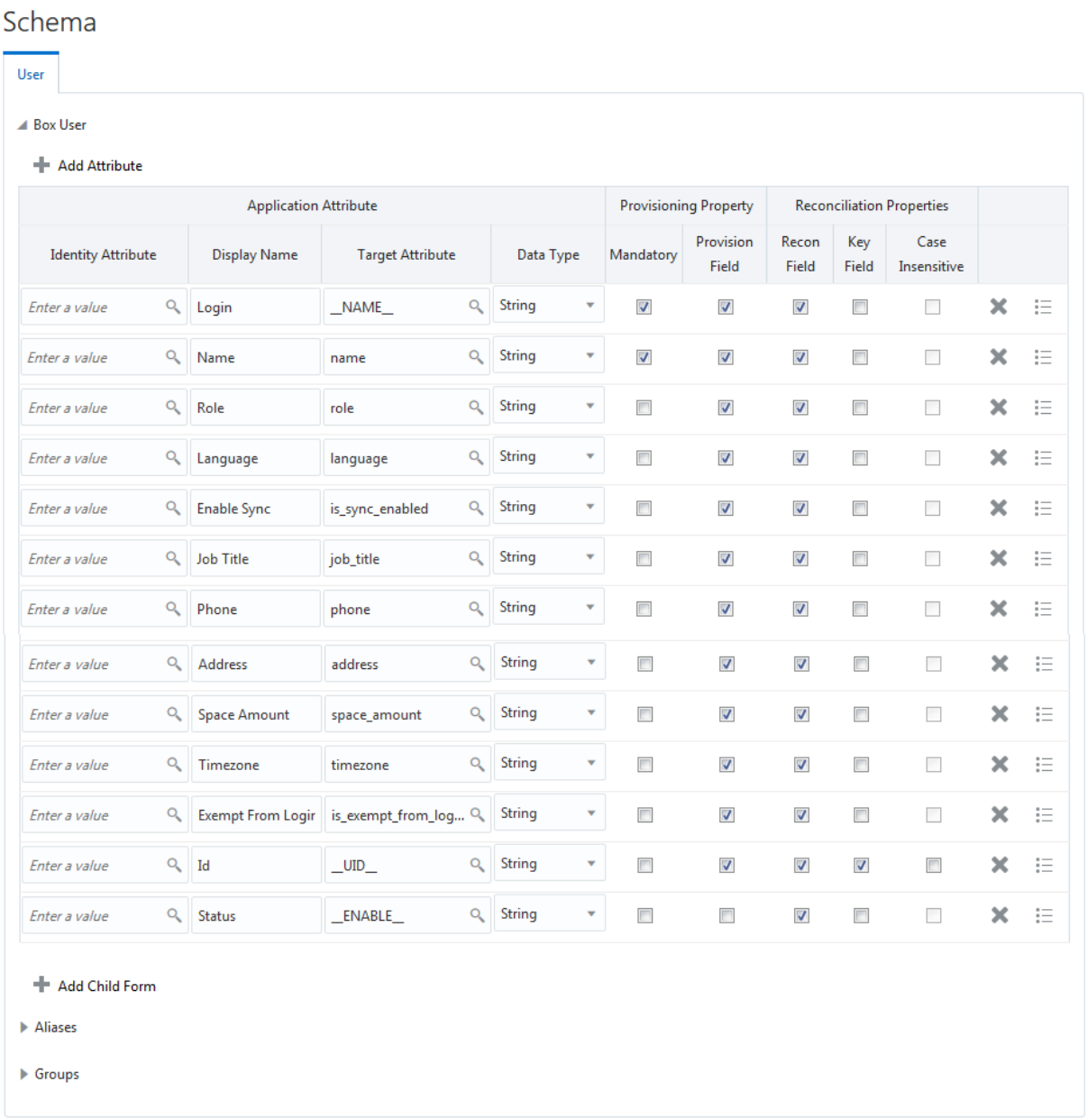
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attribute Mappings for Box User Account

Identity Attribute	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Login	__NAME__	String	Yes	Yes	Yes	No	No
Name	name	String	Yes	Yes	Yes	Yes	No
Role	role	String	No	Yes	Yes	No	No
Language	language	String	No	Yes	Yes	No	No
Enable Sync	is_sync_enabled	String	No	Yes	Yes	No	No
Job Title	job_title	String	No	Yes	Yes	No	No
Phone	_ENABLE_	String	No	Yes	Yes	No	No
Address	address	String	No	Yes	Yes	No	No
Space Amount	space_amount	String	No	Yes	Yes	No	No
Timezone	timezone	String	No	Yes	Yes	No	No
Exempt From Login	is_exempt_from_login	String	No	Yes	Yes	No	No
Id	_UID_	String	No	Yes	Yes	No	No
Status	_ENABLE_	String	No	No	Yes	No	No

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

Figure 3-1 Default Attribute Mappings for Box User Account



Groups Entitlement

Table 3-4 lists the group forms attribute mappings between the process form fields in Oracle Identity Governance and Box target application attributes. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

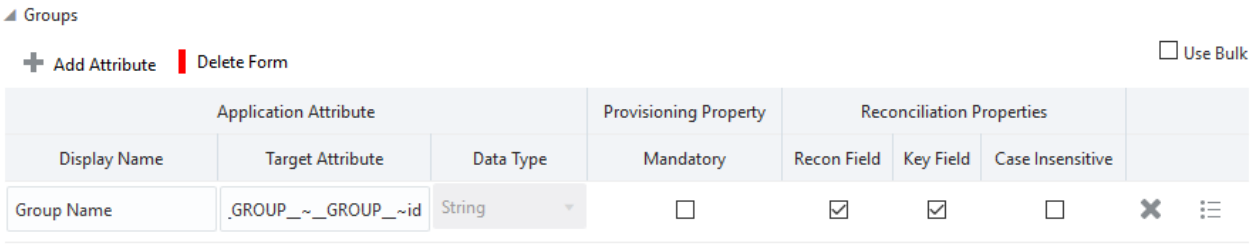
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for Groups Entitlement

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

Figure 3-1 shows the default attribute groups mapping.

Figure 3-2 Default Attribute Mappings for Groups Entitlement



3.4 Correlation Rules

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

Predefined Identity Correlation Rules

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

Table 3-5 lists the default simple correlation rule for Box connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-5 Predefined Identity Correlation Rule for a Box Target Application

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

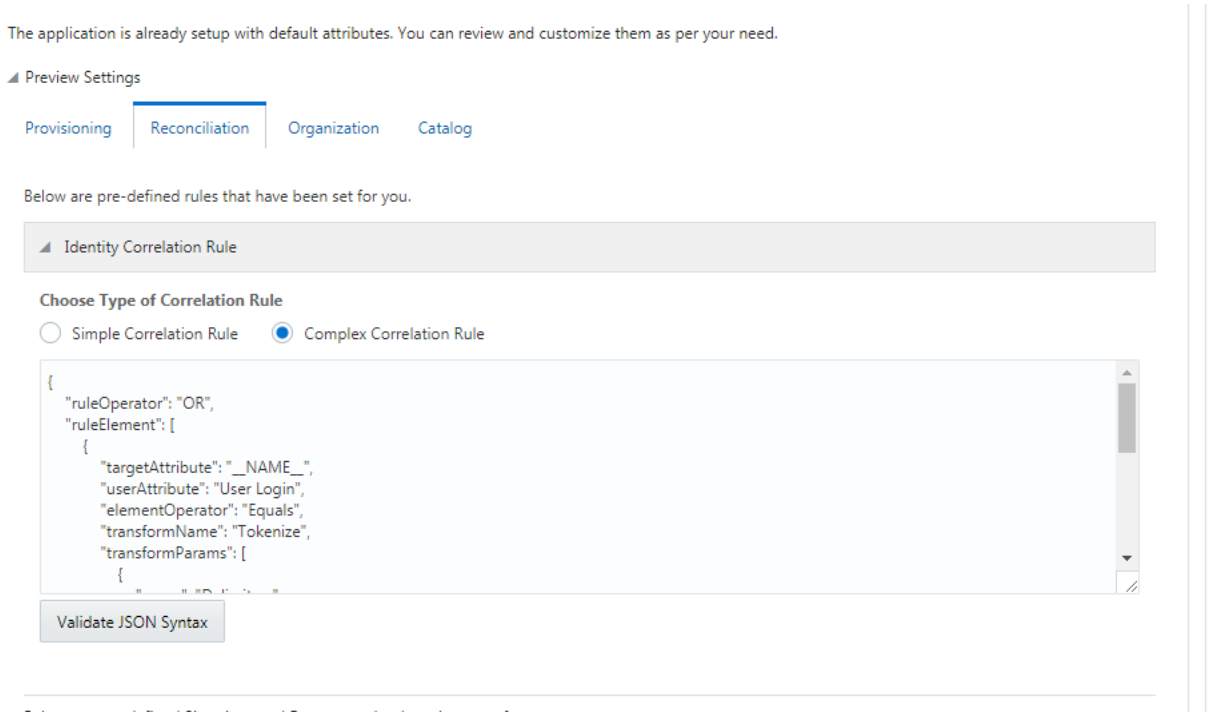
In this identity rule:

- __NAME__ is a single-valued attribute on the target system that identifies the user account.

- User Login is the field on the OIG User form.

Figure 3-3 shows the complex correlation rule for Box target application.

Figure 3-3 Complex Correlation Rule for a Box Target Application



Predefined Situations and Responses

The Box 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.

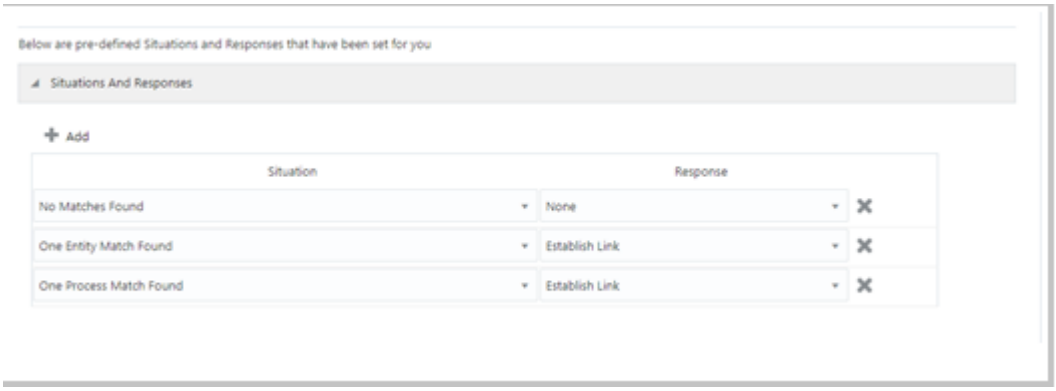
Table 3-5 lists the default situations and responses for Box target application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-6 Predefined Situations and Responses for a Box Target Application

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 for Box that the connector provides by default.

Figure 3-4 Predefined Situations and Responses for a Box Target Application



3.5 Reconciliation Jobs

Learn about reconciliation jobs that are automatically created in Oracle Identity Governance after you create a target application for your target system.

User Reconciliation Job

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

The Box Target User Reconciliation job is used to fetch all user records from the target system.

Table 3-7 Parameters of the Box Target User Reconciliation Job

Attribute	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do not modify this value.
Filter Suffix	Enter the search filter for fetching records from the target system during a reconciliation run. **Sample value**: `/0e220301db039a00b88df7a0cf9619` See Configuring Reconciliation Jobs for more information about filtered reconciliation.
Object Type	Type of object you want to reconcile. Default value: `User`

Reconciliation Jobs for Lookup Field Synchronization

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

The Box Group Lookup Reconciliation Scheduled job is used for lookup fields synchronization.

Table 3-8 Parameters of the Box Group Lookup Reconciliation Scheduled Job

Attribute	Description
Application Name	Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application. Do *not* modify this value.
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system. **Default value**: `Lookup.box.groups`
Object Type	Type of object you want to reconcile. **Default value**: `_Group_`
Code Key Attribute	Name of the connector attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). **Default value**: `__UID__`
Decode Attribute	Name of the connector attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). **Default value** : `__NAME__`

Box Update Access Token Job

Access token configured as part of IT resource will expire in 60 minutes and refresh token will expire in 60 days. Box Update Access Token Job is used to keep the value of the access token (in the IT resource) always valid. Every 50 minutes, this job is scheduled to run periodically.

> **Note:**
>
> If for some reason this scheduler is not run for more than 60 days, then the refresh token value in IT resource would have expired due to which if you run the Box Update Access Token Job after 60 days, it will fail. In such cases, a new access token and refresh token has to be generated manually.

Table 3-9 Attributes of the Box Update Access Token Job

Attribute	Description
Access Token Endpoint	This attribute holds the Box REST endpoint to get the new access token. Default value: `https://app.box.com/api/oauth2/token`
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `Box`

Table 3-9 (Cont.) Attributes of the Box Update Access Token Job

Attribute	Description
Task Name	This attribute holds the name of the scheduled task. Default value: `Box Update Access Token` You must *not* change the default value.
Start Date	This attribute holds the Start Date and time of job. Select current time and date from the Calender drop-down.

4

Performing the Postconfiguration Tasks for the Box Connector

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

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

4.1 Configuring Oracle Identity Governance

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

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

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

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

4.1.1 Creating and Activating a Sandbox

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

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

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 Manager*.

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

4.1.3 Publishing a Sandbox

Before you publish a sandbox, perform the following procedure as a best practice to validate all sandbox changes made till this stage as it is hard to revert changes once a sandbox is published:

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

4.1.4 Updating an Existing Application Instance with a New Form

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

1. Create a sandbox and activate it. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
2. Create a new UI form for the resource. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
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 Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

4.2 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Reconciliation Jobs for Lookup Field Synchronization.

2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

> **See Also:**
>
> Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for a description of the Entitlement List and Catalog Synchronization Job scheduled jobs

4.3 Managing Logging

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

4.3.1 Understanding Log Levels

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

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

- SEVERE.intValue()+100

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

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

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

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

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

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

These 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	TRACE16
FINEST	TRACE32

The configuration file for OJDL is logging.xml is located at the following path:
DOMAIN_HOME/config/fmwconfig/servers/OIM_SERVER/logging.xml

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

4.3.2 Enabling Logging

To enable logging in Oracle WebLogic Server:

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

```
<log_handler name='BOX-handler'
level='[LOG_LEVEL]'class='oracle.core.ojdl.logging.ODLHandlerFact
ory'>
<property name='logreader:' value='off'/>
<property name='path' value='[FILE_NAME]'/>
<property name='format' value='ODL-Text'/>
<property name='useThreadName' value='true'/>
<property name='locale' value='en'/> <property
name='maxFileSize' value='5242880'/>
<property name='maxLogSize' value='52428800'/>
<property name='encoding' value='UTF-8'/>
</log_handler>


<logger name="ORG.IDENTITYCONNECTORS.GENERICREST"
level="[LOG_LEVEL]" useParentHandlers="false">
<handler name="BOX-handler"/>
<handler name="console-handler"/>
</logger>


<logger name="ORG.IDENTITYCONNECTORS.RESTCOMMON"
level="[LOG_LEVEL]" useParentHandlers="false">
```

```
<handler name="BOX-handler"/>
<handler name="console-handler"/>
</logger>
```

b. Replace both occurrences of [LOG_LEVEL] with the ODL message type and level combination that you require. Table 4-1 lists the supported message type and level combinations. Similarly, replace [FILE_NAME] with the full path and name of the log file in which you want log messages to be recorded. The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]:**

```
<log_handler name='BOX-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
<property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\serv
ers\o im_server1\logs\oim_server1-diagnostic-1.log'/>
<property name='format' value='ODL-Text'/>
<property name='useThreadName' value='true'/>
<property name='locale' value='en'/>
<property name='maxFileSize' value='5242880'/>
<property name='maxLogSize' value='52428800'/>
<property name='encoding' value='UTF-8'/>
</log_handler>

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

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

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

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

     ```
     set WLS_REDIRECT_LOG=FILENAME
     ```

   - For UNIX:

     ```
     export WLS_REDIRECT_LOG=FILENAME
     ```

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

4.4 Configuring the IT Resource for the Connector Server

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

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

In Oracle Identity System Administration, search for and edit the Box Connector Server IT resource to specify values for the parameters of IT resource for the Connector Server listed in Table 4-2. For more information about searching for IT resources and updating its parameters, see Managing IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Governance*.

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

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

4.5 Localizing Field Labels in UI Forms

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

To localize a field label that is added to the UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand Application Deployments and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.

4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:
   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en_US.xlf
6. Edit the BizEditorBundle_en_US.xlf file in the following manner:
   a. Search for the following text:

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

   c. Search for the application instance code. This procedure shows a sample edit for Box 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.UD_BOX_LOGIN__c_description']}">
      <source>Login</source>
      <target/>
      </trans-unit>
      <trans-unit
      id="sessiondef.oracle.iam.ui.runtime.form.model.BoxForm.entity.BoxForm
      EO.UD_BOX_LOGIN__c_LABEL">
      <source>Login</source>
      <target/>
      </trans-unit>
      ```

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

      ```
      global.udf.UD_BOX_LOGIN=\u30ED\u30B0\u30A4\u30F3
      ```

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

      ```
      <trans-unit id="$
      {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
      ndle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.user
      ```

```
EO.UD_BOX_LOGIN__c_description']}">
<source>Login</source>
<target>\u30ED\u30B0\u30A4\u30F3</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.BoxForm.entity.Bo
xFormEO.UD_BOX_LOGIN__c_LABEL">
<source>Login</source>
<target>\u30ED\u30B0\u30A4\u30F3</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 Manager.

4.6 Configuring SSL

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

1. Obtain the SSL certificate by obtaining the public key certificate of the target system.
2. Copy the public key certificate of the target system 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 -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -file
   CERT_FILE_NAME -storepass PASSWORD
   ```

   In this command:

   - *CERT_FILE_NAME* is the full path and name of the certificate file
   - *PASSWORD* is the password of the keystore.

   The following is a sample value for this command:

   ```
   keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -
   file /home/target.cert -storepass example_password
   ```

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

5
Using the Box Connector

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

5.1 Configuring Reconciliation

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

This section discusses the following topics related to configuring reconciliation:

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.

To perform a full reconciliation run, remove (delete) any value currently assigned to the Filter attribute of the Full User Reconciliation job. See Reconciliation Jobs for information about this reconciliation job.

During a full reconciliation run, if you provide both batching parameters and filters, the connector processes the data in batches. Then, filters are applied to the processed data.

5.1.2 Performing Limited Reconciliation

You can perform limited reconciliation by creating filters for the reconciliation module, and reconcile records from the target system based on a specified filter criterion.

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.

The scheduled job provides a Filter Suffix parameter that allows you to use any of the Box resource attributes to filter the target system records. You can perform limited reconciliation by creating filters for the reconciliation module. For detailed information about the various filter syntax that are supported, refer to the Box documentation.

For the Filter Suffix attribute on the scheduled job, following are sample values that can be provided:

- ?filter_term=sand

  In the above sample, **sand** is specified after the **?filter_term=** syntax in the filter suffix attribute. This returns all users starting with the term sand in either the name or the login values.

  Similarly, any value specified after the **?filter_term=** syntax returns users whose name or login begins with the string value specified in the filter syntax field.

- /181216415

  In the above sample, **181216415** is specified after the **/** syntax in the filter suffix attribute. This returns all users records whose UID matches 181216415.

  Similarly, any value specified after the **/** syntax returns users whose UID attributes which is equal to the string specified in the filter syntax field.

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:

1. Log in to Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the parameters of the scheduled task:
   - **Retries**: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
   - **Schedule Type**: Depending on the frequency at which you want the job to run, select the appropriate schedule type. 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 Configuring Provisioning

You can configure the provisioning operation for the Box connector.

- Guidelines on Performing Provisioning Operations
- Performing Provisioning Operations

5.3.1 Guidelines on Performing Provisioning Operations

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

For a Create User provisioning operation, you must specify a value for the Name and Login fields. For example for the Name field, enter `John Doe` and for Login field, enter `jdoe@example.com`.

5.3.2 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.

For example: `BOX User; BOX Group`

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

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

6

Extending the Functionality of the Box Connector

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

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

6.1 Configuring Transformation and Validation of Data

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

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

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

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

Following is a sample transformation script for reference:

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

    return null;
}

def getBeneficiaryPwdFromContext() {
    return context.beneficiaryPassword;
}


if (binding.variables != null) {
    if (binding.variables.containsKey("context")) {
```

```
                        if (context.operationType != null) {

if(context.operationType.equalsIgnoreCase("create")){
                                if (context.provisionMechanism !=
null) {

if(context.provisionMechanism.equalsIgnoreCase("POLICY")) {
                                        Username =
getBeneficiaryAttrFromContext("Login");
                                        First_Name =
getBeneficiaryAttrFromContext("Name");




                                    } else if
(context.provisionMechanism.equalsIgnoreCase("REQUEST") ||
context.provisionMechanism.equalsIgnoreCase("ADMIN")) {
                                        if (Username == null ||
Username == "") {
                                             Username =
getBeneficiaryAttrFromContext("Login");
                                        }

                                        if (Name == null || First_Name
== "") {
                                             First_Name =
getBeneficiaryAttrFromContext("Name");
                                        }


                                    }
                                }
                            }

                        }
                    }
                }
```

6.2 Configuring Action Scripts

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

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

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

6.3 Configuring the Connector for Multiple Installations of the Target System

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

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

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

7

Upgrading the Box Connector

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

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

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

7.1 Preupgrade Steps

Preupgrade steps for the connector involves performing a reconciliation run to fetch records from the target system, defining the source connector in Oracle Identity Manager, creating copies of the connector if you want to configure it for multiple installations of the target system, and disabling all the scheduled jobs.

Perform the following preupgrade steps:

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

7.2 Upgrade Steps

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

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

- Staging Environment

Perform the upgrade procedure by using the wizard mode.

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

- Production Environment

  Perform the upgrade procedure by using the silent mode.

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

7.3 Postupgrade Steps

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

Perform the following procedure:

1. Delete the old Connector JARs. Run the Oracle Identity Manager Delete JARs `($ORACLE_HOME/bin/DeleteJars.sh)` utility to delete the existing ICF bundle `org.identityconnectors.genericrest-1.0.11150.jar` from the Oracle Identity Manager database.

   When you run the Delete JARs utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being deleted, and the name of the JAR file to be removed. Specify `4` as the value of the JAR type.

2. Upload the new connector JARs:

   a. Run the Oracle Identity Manager Upload JARs `($ORACLE_HOME/bin/UploadJars.sh)` utility to upload the connector JARs.

   b. Upload the `org.identityconnectors.genericrest-12.3.0.jar` bundle as an ICF Bundle. Run the Oracle Identity Manager Upload JARs utility to post the new ICF bundle `org.identityconnectors.genericrest-12.3.0.jar` file to the Oracle Identity Manager database.

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

   c. Delete the following **Code Key** and **Decode** entries in the `Lookup.Box.Configuration` lookup definition:

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

        Decode:

```
"__ACCOUNT__.CREATEOP=/users","__ACCOUNT__.UPDATEOP=/
users/$(__UID__)$","__ACCOUNT__.SEARCHOP=/users/$(Filter
Suffix)$","__ACCOUNT__.DELETEOP=/users/$
(__UID__)$","__GROUP__.SEARCHOP=/groups/$(Filter
Suffix)$","__ACCOUNT__.__GROUP__.CREATEOP=/
group_memberships","__ACCOUNT__.__GROUP__.UPDATEOP=/
group_memberships","__ACCOUNT__.__GROUP__.SEARCHOP=/users/$
(__UID__)$/memberships","__ACCOUNT__.__GROUP__.DELETEOP=/
group_memberships/$
(__MEMBERSHIP__.id)$","__ACCOUNT__.__MEMBERSHIP__.__GROUP__
.SEARCHOP=/users/$(__UID__)$/
memberships","__ACCOUNT__.email.UPDATEOP=/users/$
(__UID__)$/email_aliases","__ACCOUNT__.email.SEARCHOP=/
users/$(__UID__)$/
email_aliases","__ACCOUNT__.email.DELETEOP=/users/$
(__UID__)$/email_aliases/$
(__MEMBERSHIP__.id)$","__ACCOUNT__.__MEMBERSHIP__.email.SEA
RCHOP=/users/$(__UID__)$/
email_aliases","__ACCOUNT__.role.SEARCHOP=/users/$
(__UID__)$?
fields=role","__ACCOUNT__.is_sync_enabled.SEARCHOP=/users/$
(__UID__)$?
fields=is_sync_enabled","__ACCOUNT__.is_exempt_from_login_v
erification.SEARCHOP=/users/$(__UID__)$?
fields=is_exempt_from_login_verification"
```

d. Delete the following **Code Key** and **Decode** entries in the `Lookup.Box.UM.ReconAttrMap.Trusted` lookup definition:

   Code Key: `Usage Location`; **Decode**: `UsageLocation`

3. Restart Oracle Identity Manager.
4. If the connector is deployed on a Connector Server, then:
   a. Stop the connector server.
   b. Replace the existing bundle JAR file `org.identityconnectors.genericrest-1.0.1115.jar` with the new bundle JAR file `org.identityconnectors.genericrest-12.3.0.jar`.
   c. Start the connector server.

> **Note:**
>
> If you have configured the connector for multiple versions of target system, see Configuring the Connector for Multiple Installations of the Target System.

8
Known Issues and Workarounds

The following is the known issue with the Box connector.

Known Issue:

Description not available for received **HTTP Status Code: 301** or **HTTP/1.1 301 Moved Permanently**

Workaround: You must enable **SSL** or set the value for **sslEnabled** as true in the basic configuration.

A

Files and Directories in the Box Connector Installation Package

These are the files and directories on the connector installation package that comprise the Box connector.

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

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