Oracle® Identity Governance

Configuring the WebEx Application

12c (12.2.1.3.0)
F12380-02
December 2019

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

F12380-02

Primary Author: Debapriya Datta

Contributing Authors: Alankrita Prakash

Contributors: Bhargav Janapati

Contents

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Governance with WebEx.

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 WebEx 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 WebEx target system. This helps in quicker onboarding of the applications for this target system 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 updates have been made in 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).
- Table 1-2 has been updated to include information about Meeting Type management.
- Creating an Application By Using the Connector has been updated to include information about adding values to the Lookup.Webex.MeetingTypes lookup.
- Table 3-2 has been updated to include new parameters.

- Table 3-3 has been updated to include Metting Type attributes.
- Known Issues and Limitations of the WebEx Connector has been added to include that the connector does not support incremental reconciliation.
- Some editorial corrections have been made.

1

About the WebEx 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 WebEx connector lets you create and onboard WebEx 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.

> **Note:**
>
> In this guide, WebEx is sometimes referred to as the **target system**.

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

- Certified Components
- Usage Recommendation
- Certified Languages
- Supported Connector Operations
- Connector Architecture

- Supported Use Cases
- Supported Connector Features Matrix
- Connector Features

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

1.1 Certified Components

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

> **Note:**
>
> If you are using Oracle Identity Manager release 11.1.*x*, then you can install and use the connector 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.

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: • 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	Cisco WebEx	Cisco WebEx
Connector Server	11.1.2.1.0 or later	11.1.2.1.0 or later
Connector Server JDK	JDK 1.8 or later	JDK 1.8 or later

1.2 Usage Recommendation

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

- If you are using Oracle Identity Governance release 12c (12.2.1.3.0) or later, 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 of Table 1-1, then use the 11.1.1.*x* version of the WebEx 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*c* (12.2.1.3.0) or later.

> **Note:**
>
> If you are using the latest 12.2.1.*x* version of the Webex connector in the CI-based mode, then see *Oracle Identity Manager Connector Guide for WebEx*, 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 (US)
- 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
Recon User	Yes
Update User	Yes
Delete User	Yes
Set Password	Yes
Reset Password	Yes
Enable User	Yes
Disable User	Yes
Meeting Type Management	
Add MeetingTypes	Yes
Add multiple MeetingTypes	Yes
Update MeetingTypes	Yes
Update multiple MeetingTypes	Yes
Remove MeetingTypes	Yes
Remove multiple MeetingTypes	Yes

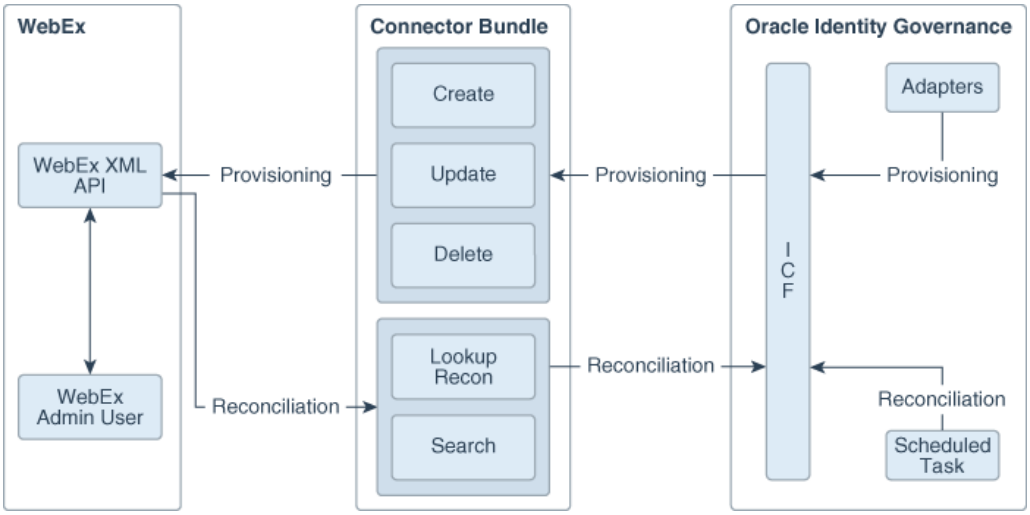
1.5 Connector Architecture

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

The ICF is a component that 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. The ICF is shipped along with Oracle Identity Governance. Therefore, you need not configure or modify the ICF.

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

Figure 1-1 Connector Architecture



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

- **Provisioning**

  Provisioning involves creating, updating, enabling, disabling or deleting users on the target system through Oracle Identity Governance. During provisioning, the Adapters invoke ICF operation, ICF inturn invokes create operation on the WebEx Connector Bundle and then the bundle calls the target system API for provisioning operations. The WebEx XML API on the target system accepts provisioning data from the bundle, carries out the required operation on the target system, and returns the response from the target system back to the bundle, which passes it to the adapters.

- **Target Resource Reconciliation**

  During reconciliation, a scheduled task invokes an ICF operation. ICF in turn invokes a search operation on the WebEx Connector Bundle and then the bundle calls WebEx XML 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 WebEx resources that are already provisioned to Oracle Identity Governance Users. If a match is found, then the update made to the WebEx record from the target system is copied to the WebEx resource in Oracle Identity Governance. If no match is found, then the user ID of the record is compared with the user ID of each Oracle Identity Governance User. If a match is found, then data in the target system record is used to provision a WebEx resource to the Oracle Identity Governance User.

The WebEx Identity Connector Bundle communicates with the WebEx XML API using the HTTPS protocol. The WebEx XML API provides programmatic access through

REST API endpoints. Apps can use the WebEx API to perform create, read, update, and delete (CRUD) operations on directory data and directory objects, such as users.

1.6 Supported Use Cases

WebEx provides on-demand collaboration, online meeting, web conferencing, and video conferencing applications. Each user should have a valid subscription for using the WebEx services. The WebEx connector is used to integrate Oracle Identity Governance with WebEx to ensure that all WebEx accounts are created, updated, and deactivated on an integrated cycle with the rest of the identity-aware applications in your enterprise.

While most of the organizations are leveraging WebEx services, a vital drawback is that an Admin user needs to manage all user identities and subscriptions manually. Since it is a time and effort consuming process for an administrator, it is advisable to use the WebEx connector. The connector automates the process of managing user identities and subscriptions and additionally reduces the burden of managing the whole life cycle of a WebEx user manually. The WebEx connector automates the process of user account provisioning, de-provisioning and subscription without any Admin intervention. Another important challenge faced is that all users are placed at a central location where the Admin can apply various organizational policies for WebEx users and generate an audit report for the same. This process is also automatically managed by the WebEx connector. To overcome these challenges, a quick and easy solution is to install the WebEx connector and configure it with your target system by providing connection information in the IT resource.

The WebEx Connector enables Oracle Identity Governance to manage all WebEx users at a single place where WebEx accounts are automatically provisioned or de-provisioned based upon the defined policies in Oracle Identity Governance respective to account users. With the help of Oracle Identity Governance, the WebEx connector Admin can perform all operations in Oracle Identity Governance and apply all Identity and Access Management features accordingly. The WebEx connector provides the ability to manage accounts and related operations across all applications without spending additional resources and time.

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
Perform full reconciliation	Yes	Yes
Perform limited reconciliation	Yes	Yes
Support for Connector Server	Yes	Yes
Configure validation and transformation of account data	Yes	Yes
Perform connector operations in multiple domains	Yes	Yes
Support for paging	Yes	Yes

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

Feature	AOB Application	CI-Based Connector
Test connection	Yes	No
Reset password	Yes	Yes
Clone applications or create new application instances	Yes	Yes
Provide secure communication to the target system through SSL	Yes	Yes

1.8 Connector Features

The features of the connector include support for provisioning user accounts, target resource reconciliation, reconciliation of all existing account data, limited reconciliation, transformation and validation of account data during reconciliation and provisioning, support for the connector server, multiple installations of the target system, secure communication to the target system through SSL, and so on.

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

1.8.1 Support for Full Reconciliation

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

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

1.8.2 Support for Limited (Filtered) Reconciliation

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

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

See Limited Reconciliation for WebEx Connector.

1.8.3 Support for the Connector Server

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

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

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

1.8.4 Transformation and Validation of Account Data

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

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

1.8.5 Support for Cloning Applications and Creating Instance Applications

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

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

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

1.8.6 Secure Communication to the Target System

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

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

See Configuring SSL for the Connector.

2

Creating an Application by Using the WebEx Connector

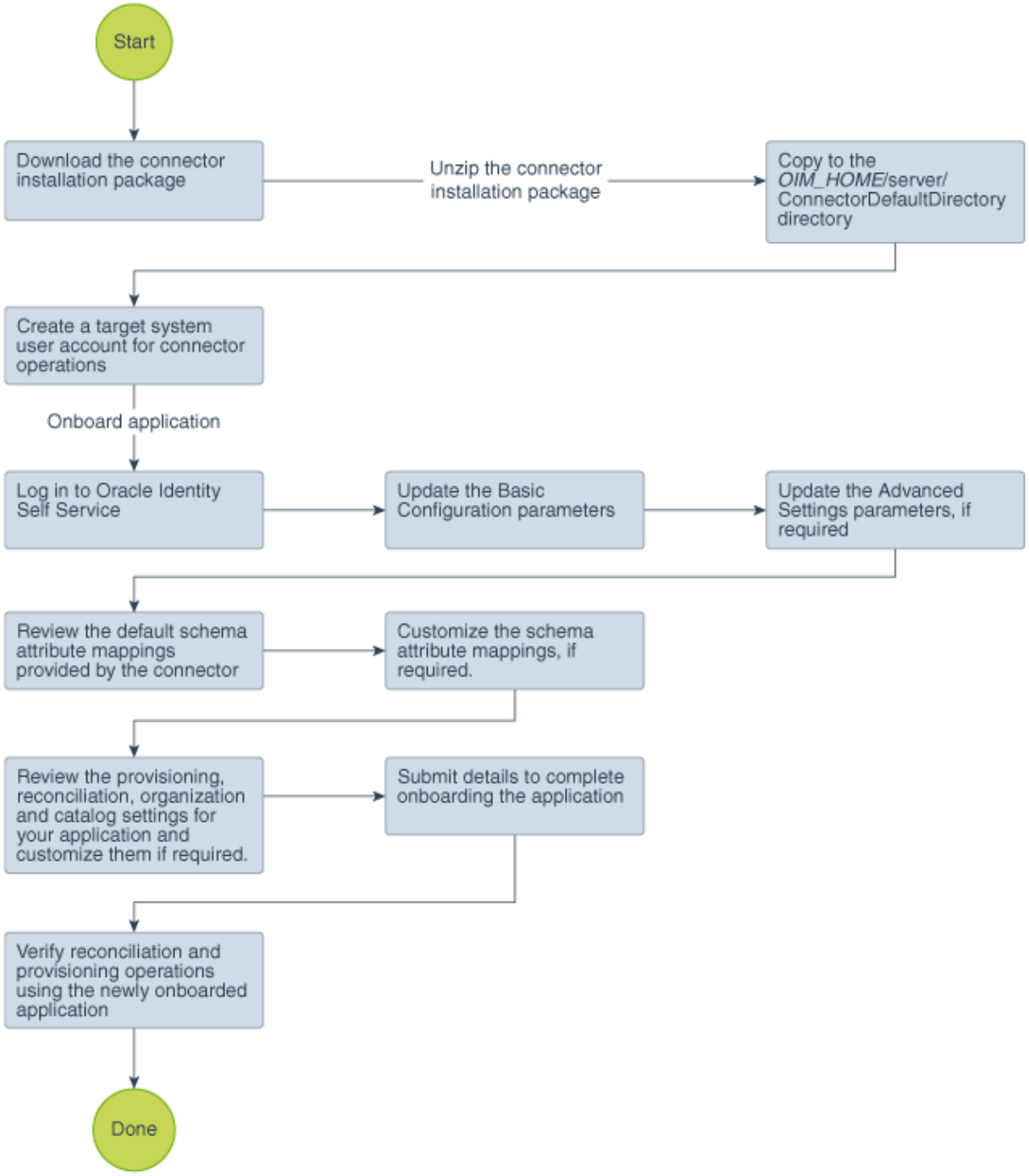
Learn about onboarding applications using the connector and the prerequisites for doing so.

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

Configuring the Target System involves creating a WebEx service account on the target system to manage users on WebEx through Oracle Identity Governance and registering a client application with the target system so that the connector can access WebEx XML APIs.
Perform the following procedure to create a service user account on the target system.

> **Note:**
>
> The detailed instructions for performing these preinstallation tasks are available in the WebEx product documentation at http://www.cisco.com/.

To configure the target system:

1. Login to the WebEx application using the Admin account.
2. Create a WebEx service user account on the target system to manage users on WebEx through Oracle Identity Manager.
3. Register the client application of the connector to provide a secure sign-in and authorization for your services.
4. From the Site Administration link, create a user with Account Type as Site **Administrator** and provide values for all the mandatory fields required for user creation.
5. Login with the new user credentials and from the Site Administration link, copy the SiteID and PartnerID values which needs to be updated in the Basic Configuration while configuring WebEx connector.

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. Add values for the Lookup.Webex.MeetingTypes lookup, as follows:

   a. Login to Identity Sytem Administration either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.

   b. Click **Lookups**, and search for `Lookup.Webex.MeetingTypes`. Click **Edit Lookup Type**, and add values for this static lookup. For example:

Meaning	Code
Webex~AUO	49~16
Webex~PRO	49~113
Webex~ONS	49~129
Webex~TRS	49~128
Webex~SC3	49~13

   Here, 49 is the IT resource key.

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

See Also:

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

3
Configuring the WebEx 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.

3.1 Basic Configuration Parameters

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

Table 3-1 Basic Configuration Parameters for the WebEx Connector

Parameter	Mandatory?	Description
webexID	Yes	Enter the Administrator ID for logging in to the WebEx application.
password	Yes	Enter the Admin password of the account for logging in to the WebEx application. **Sample value**: `password`
partnerID	Yes	Enter the partner identification generated for the admin user. See Configuring the Target System for more information on obtaining the partnerID. **Sample value**: `DU_ceBa1Qyg2nVJPNdfgILQ`
siteID	Yes	Enter the Site ID generated for the Admin user. See Configuring the Target System for more information on obtaining the siteID. **Sample value**: **12396652**
siteUrl	Yes	Enter the Site URL or the WebEx end point URL. **Sample value**: `https://example-dev.webex.com/WBXService/XMLService`
Connector Server Name	No	By default, this field is blank. If you are using this connector with the Java Connector Server, then provide the name of Connector Server IT Resource here.
proxyHost	No	Enter the name of the proxy host used to connect to an external target. **Sample value**: `www.example.com`

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

Parameter	Mandatory?	Description
proxyPort	No	Enter the proxy port number. **Sample value**: `80`
proxyUsername	No	Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system.
proxyPassword	No	Enter the password of the proxy user ID of the target system user account that Oracle Identity Governance uses to connect to the target system.

3.2 Advanced Settings Parameters

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

> **Note:**
>
> Unless specified, do not modify entries in the below table.

Table 3-2 Advanced Settings Parameters for the WebEx Connector

Parameter	Mandatory?	Description
Bundle Version	No	This entry holds the version of the connector bundle. **Default value**: `12.3.0`
Bundle Name	No	This entry holds the name of the connector bundle. **Default value**: `org.identityconnectors.webex`
Connector Name	No	This entry holds the name of the connector class. **Default value**: `org.identityconnectors.webex.WebexConnector`
startFrom	No	Enter the number to start from. **Default value**: `1`
maximumNum	No	Enter the number of records in each batch that must be fetched from the target system during a reconciliation run. **Default value**: `100`
meetingCenter	Yes	This parameter holds the Index values of Service Type Webex Meetings. **Default value**: 0 **Sample value for session codes AUO and PRO**: 16,113
trainingCenter	Yes	This parameter holds the Index values of Service Type Webex Training. **Default value**: 0 **Sample value for session codes TRS**: 128
eventCenter	Yes	This parameter holds the Index values of Service Type Webex Events. **Default value**: 0 **Sample value for session codes ONS:** 129

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

Parameter	Mandatory?	Description
supportCenter	Yes	This parameter holds the Index values of Service Type Webex Support. **Default value**: 0 **Sample value for session codes SC3**: 13

> **Note:**
>
> For Index values of Webex Service Types, login to Webex site administrative console, and navigate to Site Information.

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.

WebEx User Account Attributes

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

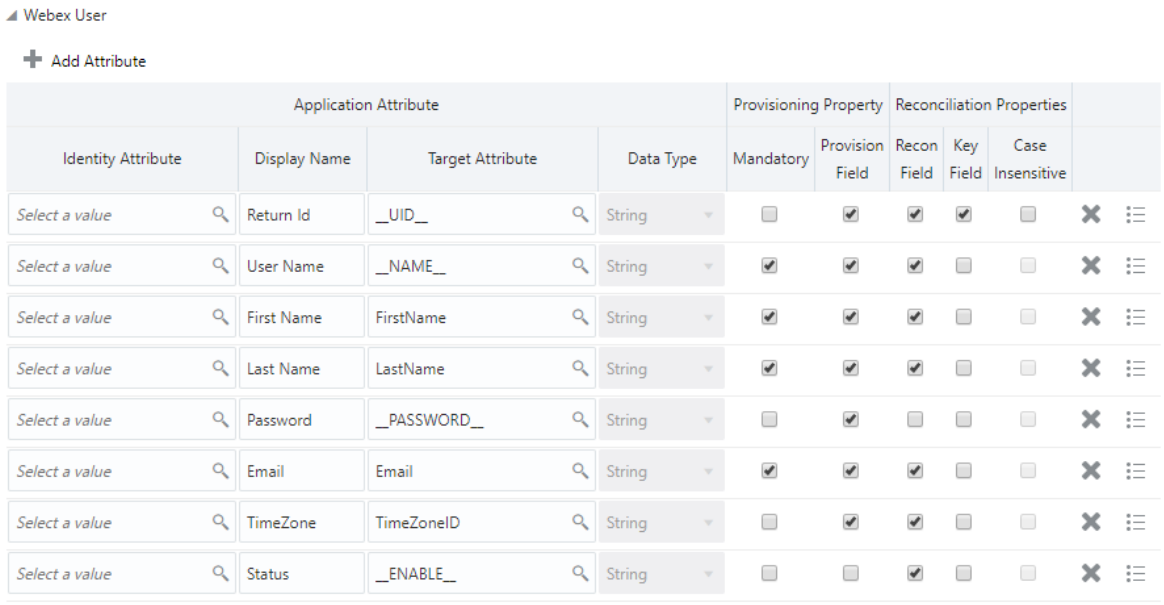
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in Creating a Target Application of *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-3 Default Attribute Mappings for WebEx User Account

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Return Id	__UID__	String	No	Yes	Yes	Yes	No
User Name	__NAME__	String	Yes	Yes	Yes	No	No
First Name	FirstName	String	Yes	Yes	Yes	No	No
Last Name	LastName	String	Yes	Yes	Yes	No	No
Email	Email	String	Yes	Yes	Yes	No	No
TimeZone	TimeZoneID	String	No	Yes	Yes	No	No
Status	__ENABLE__	String	No	No	Yes	No	No
Password	__PASSWORD__	String	No	Yes	No	No	No

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

Figure 3-1 Default Attribute Mappings for WebEx User Account



Meeting Types Attributes

Table 3-4 lists the Meeting Types-specific attribute mappings between the process form fields in Oracle Identity Governance and Webex target application attributes. The table lists whether or not 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.

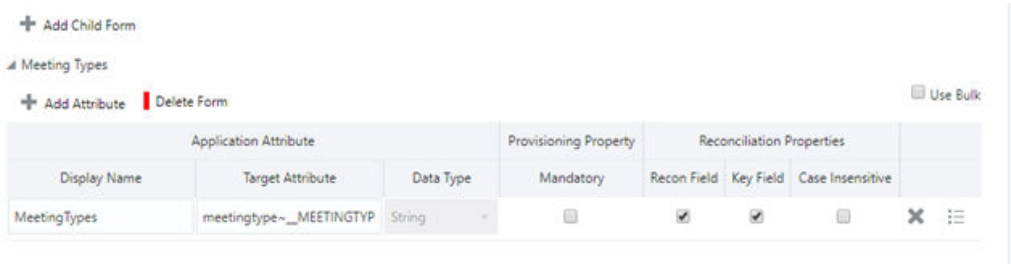
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes, as described in Creating a Target Application in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

Table 3-4 Default Attribute Mappings for Meeting Types

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
MeetingTypes	meetingtype~__MEETINGTYPES__~MeetingTypes.MeetingType	String	No	Yes	Yes	No

Figure 3-2 shows the default Meeting Types mapping.

Figure 3-2 Default Attribute Mappings for Meeting Types



3.4 Rules, Situations, and Responses

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

Predefined Identity Correlation Rules

By default, the WebEx 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.

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

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

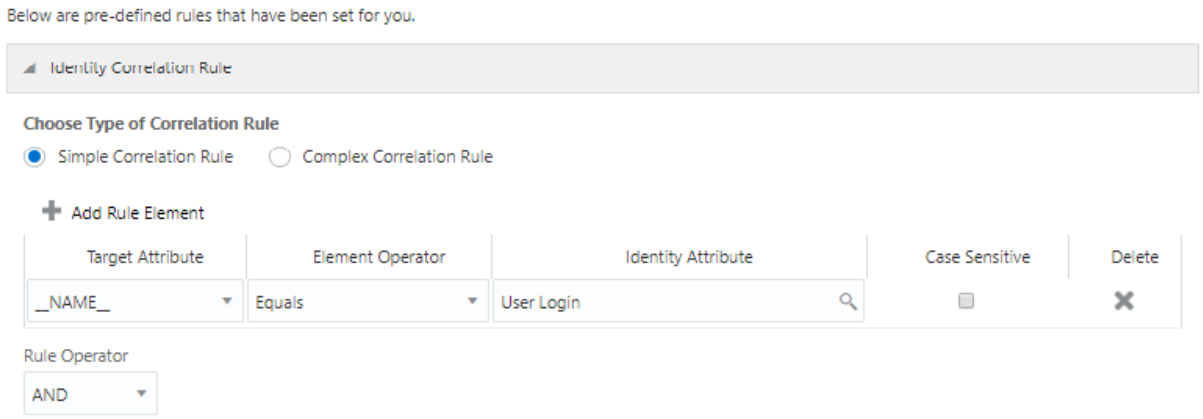
Target Attribute	Element Operator	Identity Attribute	Case Sensitive?	Rule Operator
__NAME__	Equals	User Login	No	AND

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.
- Rule Operator is AND

Figure 3-3 shows the simple correlation rule for the WebEx connector.

Figure 3-3 Predefined Identity Correlation Rules



Predefined Situations and Responses

The WebEx 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.

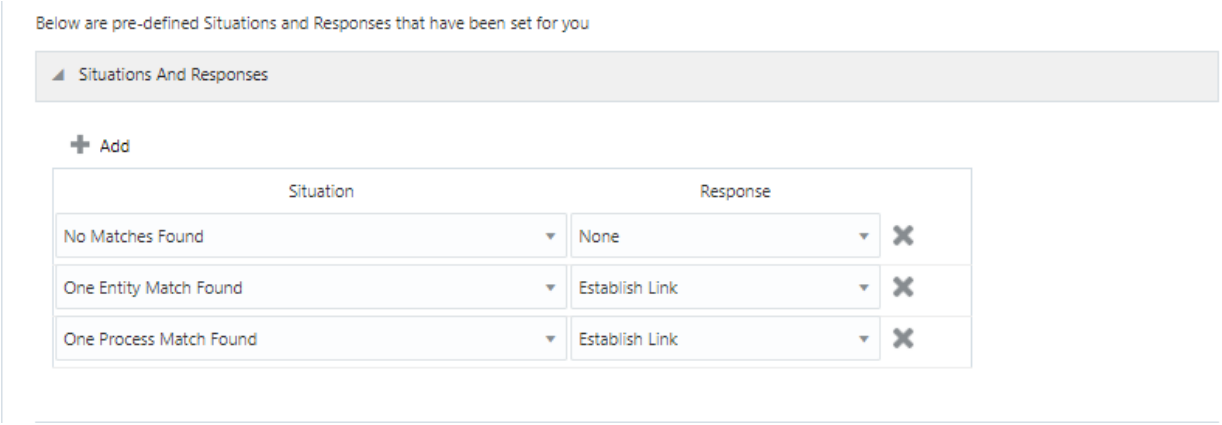
Table 3-5 lists the default situations and responses for the WebEx connector. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Creating a Target Application in *Oracle Fusion Middleware Performing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

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

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

shows the default situations and responses for the WebEx connector.

Figure 3-4 Default Situations and Responses



3.5 Reconciliation Jobs

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

Full User Reconciliation Job

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

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

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

Table 3-7 describes the parameters of the WebEx User Reconciliation job.

Table 3-7 Parameters of the WebEx 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	Enter the search filter for fetching records from the target system during a reconciliation run. **Sample value**: `equalTo('FirstName','John')` See Performing Limited Reconciliation for more information about filtered reconciliation.
Batch Size	Enter the number of batches to be reconciled. **Default value**: `0`

Table 3-7 (Cont.) Parameters of the WebEx User Reconciliation Job

Attribute	Description
No. of Batches	Type of object you want to reconcile. **Default value**: `0`
Batch Start Index	Enter the Batch start index from which point the user reconciliation has to start. **Default value**: `0`
Object Type	Type of object you want to reconcile. **Default value**: `User`

Reconciliation Jobs for Lookup Field Synchronization

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

The Webex Timezone Lookup Reconciliation Scheduled job is used to fetch data about time zones during target resource reconciliation.

Table 3-8 describes the parameters of the Webex Timezone Lookup Reconciliation Scheduled job.

Table 3-8 Parameters of the Webex Timezone 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.
Code Key Attribute	Enter the 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	Enter the 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__`
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.Webex.TimeZones`

Table 3-8 (Cont.) Parameters of the Webex Timezone Lookup Reconciliation Scheduled Job

Attribute	Description
Object Type	Enter the type of object whose values must be synchronized. **Default value** :`timeZones`

4

Performing the Postconfiguration Tasks for the WebEx 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 for the Connector
- Configuring the IT Resource for the Connector Server
- Localizing Field Labels in UI Forms
- Configuring SSL for the Connector

4.1 Configuring Oracle Identity Governance

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

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

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

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

4.1.1 Creating and Activating a Sandbox

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

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

4.1.2 Creating a New UI Form

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

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

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

4.1.3 Publishing a Sandbox

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

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

4.1.4 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

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

See Also:

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

4.2 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization discussed in Reconciliation Jobs for Lookup Field Synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about this scheduled job.

4.3 Managing Logging for the Connector

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

The following topics provide detailed information about logging:

- Understanding Log Levels
- Enabling Logging

4.3.1 Understanding Log Levels

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

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

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

These message types are mapped to ODL message type and level combinations as shown in Table 4-1.

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

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

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

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

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

4.3.2 Enabling Logging

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='WebEx-handler'
level='[LOG_LEVEL]' class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
```

```
    <property name='locale' value='en'/>
    <property name='maxFileSize' value='5242880'/>
    <property name='maxLogSize' value='52428800'/>
    <property name='encoding' value='UTF-8'/>
  </log_handler>

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

b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. .

Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages specific to connector operations to be recorded.

The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]** :

```
<log_handler name='WebEx-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
    <property name='path' value='/<%OIM_DOMAIN%>/servers/oim_server1/logs/
WebExScriptLogs.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.WebEx" level="NOTIFICATION:1"
useParentHandlers="false">
    <handler name="WebEx-handler"/>
    <handler name="console-handler"/>
  </logger>
```

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

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

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

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

4. Restart the application server.

4.4 Configuring the IT Resource for the Connector Server

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

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

In Oracle Identity System Administration, search for and edit the WebEx 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 WebEx Connector Server

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

4.5 Localizing Field Labels in UI Forms

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

To localize field label that 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.xlf

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

   a. Search for the following text:

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

   b. Replace with the following text:

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

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

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

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

   ```
   <trans-unit
   id="$
   {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResource
   Bundle']
   ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.us
   erEO.UD_SN_USR_USERNAME__c_description']}">
   <source>User Name</source>
   <target/>
   </trans-unit>
   <trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.snform.entity.snform
   EO.UD_SN_USR_USERNAME__c_LABEL">
   <source>First Name</source>
   <target/>
   </trans-unit>
   ```

   d. Open the properties file from resource folder in the connector package, for example `WebEx_ja.properties`, and get the value of the attribute from the file, for example,

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

e. Replace the original code shown in Step 7.c with the following:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResource
Bundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.us
e
rEO.UD_SN_USR_ USER_NAME __c_description']}">
<source>Account Name</source>
<target>u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.WebEx.entity
sEO.UD_SN_USR_UserName__c_LABEL">
<source>Account Name</source>
<target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>
```

f. Repeat Steps 7.a through 7.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.

h. 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

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

4.6 Configuring SSL for the Connector

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

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

To configure SSL:

1. Obtain the SSL public key certificate of WebEx.
2. Copy the public key certificate of WebEx to the computer hosting Oracle Identity Governance.

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

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

   In this command:

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

   The following is a sample value for this command:

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

   Note:

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

5
Using the WebEx Connector

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

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

5.1 Configuring Reconciliation

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

This section provides details on the following topics related to configuring reconciliation:

- Performing Full Reconciliation
- Performing Limited Reconciliation

5.1.1 Performing Full Reconciliation

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

To perform a full reconciliation run, ensure that no value is specified for the Filter attribute of the scheduled job for reconciling users.

See Configuring Reconciliation for information about this reconciliation job.

5.1.2 Performing Limited Reconciliation

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

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

The following filter operators are supported:

- equalTo
- greaterThan
- lessThan
- and
- or

You can apply the and, equalTo, and or filter parameters to the following attributes:

- User Name
- FirstName
- LastName
- Email
- Active
- __UID__
- __NAME__

You can apply the greaterThan and lessThan filter parameters to the following attributes:

- RegDateStart
- RegDateEnd

You can perform limited reconciliation using the Filter attribute (a scheduled task attribute) that allows you to use any of the WebEx resource attributes to filter the target system records. For detailed information about the various filter syntax that are supported, refer the WebEx documentation.

For detailed information about ICF Filters, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

While creating the application, follow the instructions in Configuring Reconciliation to specify attribute values.

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

Learn about performing provisioning operations in Oracle Identity Governance and the guidelines that you must apply while performing these operations.

- Guideline on Performing Provisioning Operations
- Performing Provisioning Operations

5.3.1 Guideline on Performing Provisioning Operations

This is the guideline that you must apply while performing provisioning operations.

During the Create User provisioning operation, you must specify a value for the User Name field. For example, John Doe. It is a mandatory field.

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 (for example, `WebEx User; WebEx Group`) as the value of the `ObjectValues` property.

> **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 WebEx Connector

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

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*.

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 WebEx Connector

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

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

The following sections discuss the procedure to upgrade the connector:

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

> **See Also:**
>
> 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, deleting duplicate entries for lookup definitions, verifying attribute mappings for custom attributes, and so on.

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.webex-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.webex-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.webex-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.

3. After upgrading the connector, a duplicate entry is created in the Lookup.WebEx.Configuration lookup definition for the `Bundle Version` parameter. Log in to Oracle Identity Manager Design Console and delete the following duplicate entry:

Code Key	Decode
Bundle Version	1.0.1115

4. If any attribute mappings are missing for custom attributes, log in to Oracle Identity Manager Design Console and update the mappings.
5. Restart Oracle Identity Manager.
6. If the connector is deployed on a Connector Server, then:
   a. Stop the Connector Server.
   b. Replace the existing bundle JAR file `org.identityconnectors.webex-1.0.11150.jar` with the new bundle JAR file `org.identityconnectors.webex-12.3.0.jar`.
   c. Start the Connector Server.

After upgrading the connector, you can perform either full reconciliation or limited reconciliation. This ensures that records created or modified since the last reconciliation run are fetched into Oracle Identity Manager.

See Also:

- Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about deploying the Connector Server
- Configuring Reconciliation for more information about performing full or limited reconciliation

8

Known Issues and Limitations of the WebEx Connector

These are the known issues and limitations associated with the WebEx connector.

Limitations Related to Target System Features

WebEx does not provide an API to reconcile the users based on the last modified time. Therefore, incremental reconciliation feature cannot be implemented.

A

Files and Directories in the WebEx Connector Package

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

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

File in the Installation Media Directory	Description
/bundle/ org.identityconnectors.webex-12.3.0.jar	This JAR is the ICF connector bundle.
configuration/Webex-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 Governance database. **Note:** A **resource bundle** is a file containing localized versions of the text strings that include GUI element labels and messages.
xml/Webex-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/WebEx-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.