Oracle® Identity Manager
Connector Guide for WebEx

Release 11.1.1
E79077-02
May 2020

ORACLE

Oracle Identity Manager Connector Guide for WebEx, Release 11.1.1

E79077-02

Primary Author: Gowri GR

Contributors: Mike Howlett

Contents

2 Deploying the WebEx Connector

3 Using the WebEx Connector

List of Figures

List of Tables

Preface

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

Audience

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

Related Documents

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

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

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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 Oracle Identity Manager Connector for WebEx?

This chapter provides an overview of the updates made to the software and documentation for the WebEx connector in release 11.1.1.5.0.

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

- Software Updates

  This section provides information on the updates made to the connector software. This section also provides information on the sections of this guide that have changes in response to each software update.

- Documentation-Specific Updates

  This section provides information on the major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager connector for WebEx. Therefore, there are no software-specific updates in this release.

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 11.1.1.5.0

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

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

1

About the WebEx Connector

The WebEx connector integrates Oracle Identity Manager with WebEx.

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

1.1 Introduction to the WebEx Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. The WebEx connector enables you to use WebEx as a managed (target) resource for Oracle Identity Manager.

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

> **Note:**
>
> At some places in this guide, the term **target system** has been used to refer to WebEx.

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. This data is used to add or modify resources (that is, accounts) allocated to Oracle Identity Manager Users. In addition, you can use Oracle Identity Manager to provision or update WebEx resources (accounts) assigned to Oracle Identity Manager Users. These provisioning operations performed on Oracle Identity Manager translate into the creation or updates to target system accounts.

1.2 Certified Components for the WebEx Connector

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

Table 1-1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 12c (12.2.1.4.0) • Oracle Identity Governance 12c (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS2 BP09 (11.1.2.2.9) • Oracle Identity Manager 11*g* Release 2 PS3 BP06 (11.1.2.3.6)
Target System	Cisco WebEx
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 or later

1.3 Certified Languages for the WebEx Connector

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

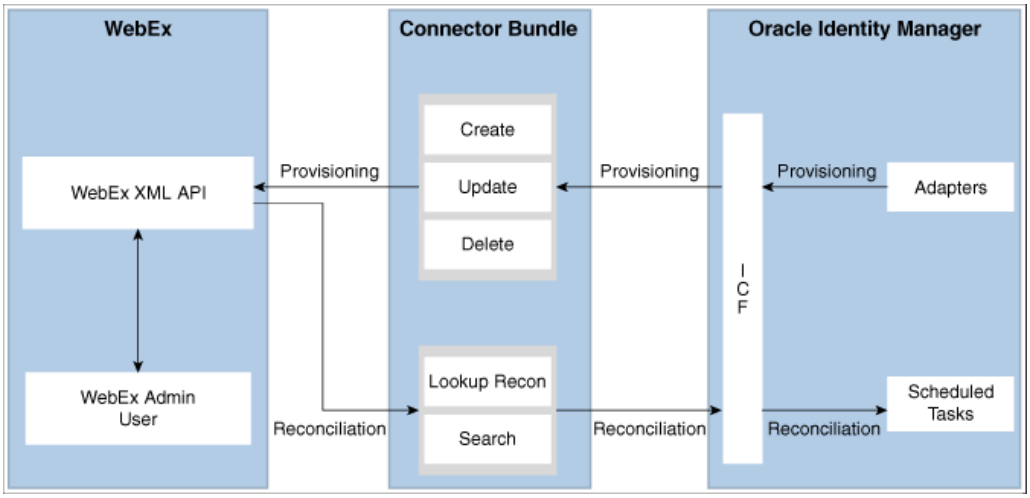
1.4 Architecture of the WebEx Connector

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

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

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

Figure 1-1 Connector Architecture



The connector can be configured to run in the Account Management mode. Account management is also known as target resource management. In this mode, the target

system is used as a target resource and the connector enables the following operations:

- **Provisioning**

  Provisioning involves creating, updating, enabling, disabling or deleting users on the target system through Oracle Identity Manager. 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 Manager.

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

1.5 Use Cases Supported by the WebEx Connector

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 Manager 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 Manager 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 Manager respective to account users. With the help of Oracle Identity Manager, the WebEx connector Admin can perform all operations in Oracle Identity Manager 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.

1.6 Features of the WebEx Connector

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

- Full Reconciliation
- Limited (Filtered) Reconciliation
- Support for the Connector Server
- Transformation and Validation of Account Data

1.6.1 Full Reconciliation

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

You can perform a full reconciliation any time. See Full Reconciliation for the WebEx Connector.

1.6.2 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.

See Limited Reconciliation for WebEx Connector.

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

> **See Also:**
>
> Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installation options for this connector.

1.6.4 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning.

In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

- Configuring Transformation of Data During User Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning

1.7 Lookup Definitions Used During Connector Operations

Lookup definitions used during reconciliation and provisioning are either preconfigured or can be synchronized with the target system.

Lookup definitions used during connector operations can be categorized as follows:

- Lookup Definition Synchronized with the Target System
- Preconfigured Lookup Definitions for the WebEx Connector

1.7.1 Lookup Definition Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to select a single value from a set of values. For example, you may want to select a timezone from the Time Zone lookup field to specify the timezone preference for a user. Lookup field synchronization of the Lookup.Webex.TimeZones lookup definition involves copying additions or changes made to specific fields in the target system to lookup definitions in Oracle Identity Manager.

When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization populates these lookup fields with values from the corresponding lookup definitions.

After you deploy the connector, the Lookup.Webex.TimeZones lookup definition, which is used as an input source for a lookup field, is automatically created in Oracle Identity Manager.

This lookup definition is empty by default and is populated with values fetched from the target system when you run the scheduled job for lookup field synchronization. For example, when you run the scheduled job for time zones lookup field synchronization, all time zones on the target system are fetched to Oracle Identity Manager and populated in the Lookup.Webex.TimeZones lookup definition.

The following is the format in which data is stored in the Lookup.Webex.TimeZones lookup definition after lookup field synchronization:

- **Code Key:**

  <IT_RESOURCE_KEY>~<FIELD_VALUE_ID>

  In this format:

  – *IT_RESOURCE_KEY* is the numeric code assigned to an IT resource in Oracle Identity Manager.

  – *FIELD_VALUE_ID* is the ID of the timezone in the target system.

  Sample value: `188~21`

  In this sample value, `188` is the numeric code assigned to the IT resource associated with the target system and `21` is the ID of the timezone in the target system.

- **Decode:**

  <IT_RESOURCE_NAME>~<LOOKUP_FIELD_VALUE>

  In this format:

  – *IT_RESOURCE_NAME* is the name assigned to an IT resource in Oracle Identity Manager.

  – *LOOKUP_FIELD_VALUE* is the value of the timezone in the target system.

  Sample value: `Webex~GMT+02:00,Central European(Paris)`

  In this sample value, `Webex` is the name assigned to the IT resource in Oracle Identity Manager and `GMT+02:00,Central European(Paris)` is the value of the timezone in the target system

Table 1-2 shows sample entries in the Lookup.Webex.TimeZones lookup definition.

Table 1-2 Sample Entries in the Lookup.Webex.TimeZones Lookup Definition.

Code Key	Decode
44~22	Webex~GMT+01:00, GMT(London)
44~128	Webex~GMT+02:00, Central European (Paris)
44~4	Webex~GMT-07:00, Pacific(San Francisco)

1.7.2 Preconfigured Lookup Definitions for the WebEx Connector

Preconfigured lookup definitions are the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

The other lookup definitions are as follows:

- Lookup.Webex.Configuration
- Lookup.Webex.UM.Configuration

- Lookup.Webex.UM.ProvAttrMap
- Lookup.Webex.UM.ReconAttrMap

1.7.2.1 Lookup.Webex.Configuration

The Lookup.Webex.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

Table 1-3 lists the default entries in the Lookup.Webex.Configuration values lookup definition.

> **Note:**
>
> Do not modify the entries in this lookup definition

Table 1-3 Entries in the Lookup.Webex.Configuration Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.webex	This entry holds the name of the connector bundle.
Bundle Version	1.0.11150	This entry holds the version of the connector bundle.
Connector Name	org.identityconnectors.webex.WebexConnector	This entry holds the name of the connector class.
User Configuration Lookup	Lookup.Webex.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties.
startFrom	1	This entry holds the number of already retrieved users to be skipped before the next user matches the query criteria in the database which is retrieved. Default value: 1
maximumNum	100	This entry holds the integer value for the maximum number of records to return from a search. Default value: 100

1.7.2.2 Lookup.Webex.UM.Configuration

The Lookup.Webex.UM.Configuration lookup definition contains entries specific to the user object type. This lookup definition is preconfigured and is used during user management operations.

Table 1-4 Entries in the Lookup.Webex.UM.Configuration Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.Webex.UM.ProvAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during user provisioning operations.
Recon Attribute Map	Lookup.Webex.UM.ReconAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during user reconciliation.

1.7.2.3 Lookup.Webex.UM.ProvAttrMap

The Lookup.Webex.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attribute names.

This lookup definition is preconfigured and used during target resource provisioning. Table 1-8 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for target resource provisioning. See Adding New User Attributes for Provisioning.

1.7.2.4 Lookup.Webex.UM.ReconAttrMap

This lookup definition is preconfigured and used during target resource reconciliation.

The Lookup.Webex.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. Table 1-5 lists default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for target resource reconciliation. See Adding New User Attributes for Provisioning.

1.8 Connector Objects Used During Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to Oracle Identity Manager Users.

The WebEx Resource User Reconciliation scheduled job is used to initiate a reconciliation run. This scheduled job is discussed in Reconciliation Scheduled Job.

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for generic information about connector reconciliation

This section contains the following topics related to connector objects:

- User Fields for Target Resource Reconciliation
- Reconciliation Rule for User Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation

1.8.1 User Fields for Target Resource Reconciliation

The Lookup.Webex.UM.ReconAttrMap lookup definition maps resource object fields with target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, entries are in the following format:

- **Code Key**: Reconciliation field of the resource object
- **Decode**: Name of the target system attribute

Table 1-5 lists the entries in this lookup definition.

Table 1-5 Entries in the Lookup.Webex.UM.ReconAttrMap Definition

Code Key (Resource Object Field)	Decode (Webex Field)
Return Id	__UID__
User Name	__NAME__
First Name	FirstName
Last Name	LastName
Email	Email
TimeZone[LOOKUP]	TimeZoneID
Status	__ENABLE__

1.8.2 Reconciliation Rule for User Target Resource Reconciliation

Reconciliation rules for user target resource reconciliation are used by the reconciliation engine to determine the identity to which Oracle Identity Manager must assign a newly discovered account on the target system.

This section contains the following topics related to user reconciliation rule for target resource reconciliation:

- Target Resource Reconciliation Rule for Users
- Viewing Reconciliation Rules for Target Resource Reconciliation

1.8.2.1 Target Resource Reconciliation Rule for Users

The following is the process-matching rule for users:

Rule name: Webex User Recon Rule

Rule element: User Login Equals User Name

In this rule:

- `User Login` is the User ID field of the Oracle Identity Manager User form.
- `User Name` is the unique login name for user in target system.

1.8.2.2 Viewing Reconciliation Rules for Target Resource Reconciliation

After you deploy the connector, you can view the reconciliation rules on the Reconciliation Rule Builder form in Oracle Identity Manager Design Console. To view reconciliation rules for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools.**
3. Double-click **Reconciliation Rules.**
4. Search for and open the **Webex User** reconciliation rule.

Figure 1-2 Reconciliation Rule for Target Resource Reconciliation of Users

1.8.3 Reconciliation Action Rules for Target Resource Reconciliation

Reconciliation action rules define that actions the connector must perform based on the reconciliation rules defined for users.

This section provides information related to reconciliation action rules for target resource reconciliation:

- Target Resource Reconciliation Action Rules for Users
- Viewing Reconciliation Action Rules for Target Resource Reconciliation

1.8.3.1 Target Resource Reconciliation Action Rules for Users

Table 1-6 lists the action rules for target resource reconciliation.

Table 1-6 Action Rules for Reconciliation for Target System

Rule Condition	Action
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

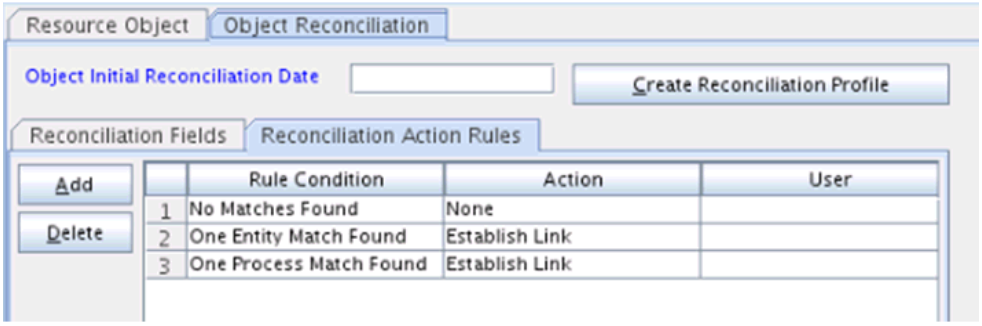
1.8.3.2 Viewing Reconciliation Action Rules for Target Resource Reconciliation

You can view reconciliation action rules on the Object Reconciliation tab of a resource object in Oracle Identity Manager Design Console. To view reconciliation action rules for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management.**
3. Double-click **Resource Objects.**
4. Search for and open the **Webex User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab.

   The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1-3 shows the reconciliation action rule for target resource reconciliation.

Figure 1-3 Reconciliation Action Rule for Target Resource Reconciliation



1.9 Connector Objects Used During Provisioning

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

This section provides information related to connector objects used during a provisioning operation:

- Provisioning Functions
- User Fields for Provisioning

1.9.1 Provisioning Functions

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

The Adapter column in Table 1-7 provides the name of the adapter that is used when the function is performed.

> **See Also:**
>
> Types of Adapters in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about process tasks and adapters for generic information about process tasks and adapters

Table 1-7 User Provisioning Functions

Function	Adapter
Create User	adpWEBEXCREATEUSER
Update User	adpWEBEXUPDATEUSER
Delete user	adpWEBEXDELETEUSER
Enable user	adpWEBEXENABLETASK
Disable user	adpWEBEXDISABLETASK

1.9.2 User Fields for Provisioning

The Lookup.Webex.UM.ProvAttrMap lookup definition maps process form fields with WebEx fields. This lookup definition is used for performing user provisioning operations.

In this lookup definition, entries are in the following format:

Code Key: Name of the process form field.

Decode: Name of the target system attribute.

Table 1-8 lists the default entries in this lookup definition.

Table 1-8 Entries in the Lookup.Webex.UM.ProvAttrMap Lookup Definition

Code Key	Decode
Email	Email
First Name	FirstName
Last Name	LastName
Password	__PASSWORD__
Return Id	__UID__
Status	__ENABLE__
TimeZone[LOOKUP]	TimeZoneID
User Name	__NAME__

1.10 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Deploying the WebEx Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the WebEx Connector describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Extending the Functionality of the WebEx Connector describes procedures that you can perform if you want to extend the functionality of the connector.
- Known Issues and Workarounds for the WebEx Connector lists known issues and limitations associated with this release of the connector.
- Files and Directories on the WebEx Connector Installation Media lists the files and directories that comprise the connector installation media.

2
Deploying the WebEx Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, and postinstallation.

The following topics provide details on these stages:

- Preinstallation
- Installation
- Postinstallation

2.1 Preinstallation

Preinstallation for the WebEx connector involves creating a WebEx service account on the target system to manage users on WebEx through Oracle Identity Manager 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/.

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 IT Resource after connector installation.

2.2 Installation

Installing the connector requires you to run the connector installer and then configure the IT resource.

- Understanding Installation of the WebEx Connector
- Running the Connector Installer

- Configuring the IT Resource for the Target System

2.2.1 Understanding Installation of the WebEx Connector

You can run the connector code either locally in Oracle Identity Manager or remotely in a Connector Server.

Depending on where you want to run the connector code (bundle), the connector provides the following installation options:

- Run the connector code locally in Oracle Identity Manager. In this scenario, you deploy the connector in Oracle Identity Manager. Deploying the connector in Oracle Identity Manager involves performing the procedures described in Running the Connector Installer and Configuring the IT Resource for the Target System.
- Run the connector code remotely in a Connector Server. In this scenario, you deploy the connector in Oracle Identity Manager, and then, deploy the connector bundle in a Connector Server. See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing, configuring, and running the Connector Server, and then installing the connector in a Connector Server.

2.2.2 Running the Connector Installer

When you run the Connector Installer, it automatically copies the connector files to directories in Oracle Identity Manager, imports connector XML files, and compiles adapters used for provisioning.

To run the Connector Installer, perform the following procedure:

1. Copy the contents of the connector installation media into the following directory:

   OIM_HOME`/server/ConnectorDefaultDirectory`
2. Log in to Oracle Identity System Administration.
3. In the left pane, under Provisioning Configuration, click **Manage Connector.**
4. In the Manage Connector page, click **Install.**
5. From the **Connector List** list, select **Webex Connector *RELEASE_NUMBER*.**

   This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory: *OIM_HOME*`/server/ConnectorDefaultDirectory`. If you have copied the installation files into a different directory, then:

   a. In the Alternative Directory field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh.**

   c. From the Connector List list, select **Webex Connector *RELEASE_NUMBER*.**
6. Click **Load**.
7. To start the installation process, click **Continue.** In a sequence, the following tasks are automatically performed:

   a. Connector library configuration.

   b. Import of the connector XML files (by using the Deployment Manager).

   c. Adapter compilation.

On successful completion of a task, a check mark is displayed for the task. If a task fails, then an *X* mark along with a message stating the reason for failure is displayed. If a task fails, then make the required correction and perform one of the following steps:

a. Retry the installation by clicking **Retry.**

b. Cancel the installation and begin the procedure from Step 3.

8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed.

   Click **Exit** to finish the installation procedure.

2.2.3 Configuring the IT Resource for the Target System

An IT resource for your target system is created after you install the connector. You configure this IT resource to let the connector connect Oracle Identity Manager with your target system.

This section contains the following topics:

- IT Resource Parameters
- Specifying Values for the IT Resource Parameters

2.2.3.1 IT Resource Parameters

An IT resource is composed of parameters that store connection and other generic information about a target system. Oracle Identity Manager uses this information to connect to a specific installation or instance of your target system.

Table 2-1 IT Resource Parameters

Parameter	Description
WebexID	Enter the WebEx Site Administrator ID.
SiteUrl	Enter the Site URL or the WebEx end point URL.
siteID	Enter the Site ID generated for the Admin user.
partnerID	Enter the partner identification generated for the admin user.
password	Enter the Admin password of the account used to login to the WebEx Site.
proxyHost	Name of the proxy host used to connect to an external target. Sample value: `www.example.com`
proxyPassword	Password of the proxy user ID of the target system user account that Oracle Identity Manager uses to connect to the target.
proxyPort	Proxy port number at which the target system is listening. Sample value: `80`

Table 2-1 (Cont.) IT Resource Parameters

Parameter	Description
proxyUser	Proxy user name of the target system user account that Oracle Identity Manager uses to connect to the target system.
Configuration Lookup	Name of the lookup definition that stores configuration information used during reconciliation and provisioning. Default value: `Lookup.Webex.Configuration`
Connector Server Name	If you have deployed the WebEx connector in the Connector Server, then enter the name of the IT resource for the Connector Server.

2.2.3.2 Specifying Values for the IT Resource Parameters

The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information during provisioning and reconciliation.

The WebEx IT resource is automatically created when you run the Connector Installer. You must specify values for the parameters as follows:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **IT Resource.**
3. In the IT Resource Name field on the Manage IT Resource page, enter `Webex` and then click **Search.**
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource, WebEx. See IT Resource Parameters.
7. To save the values, click **Update**.

2.3 Postinstallation

Postinstallation for the WebEx connector involves configuring Oracle Identity Manager, enabling logging to track information about all connector events, and configuring SSL. It also involves performing some optional configurations such as localizing the user interface.

- Configuring Oracle Identity Manager
- Localizing Field Labels in UI Forms
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Managing Logging for the WebEx Connector
- Configuring SSL for WebEx

2.3.1 Configuring Oracle Identity Manager

You must create a UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations. In addition, you must run entitlement and catalog synchronization jobs.

These procedures are described in the following sections:

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

2.3.1.1 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*.

2.3.1.2 Creating a New UI Form

See Creating Forms by Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager* for instructions on creating a new UI form. While creating the UI form, ensure that you select the resource object corresponding to the Generic SCIM connector that you want to associate the form with. In addition, select the **Generate Entitlement Forms** check box.

2.3.1.3 Associating the Form with the Application Instance

By default, an application instance named WebEx Application Instance is automatically created after you install the connector. You must associate this application instance with the form created in Creating a New UI Form.

After updating the application instance, you must publish it to an organization to make the application instance available for requesting and subsequent provisioning to users. However, as a best practice, perform the following procedure before publishing the application instance:

1. In Oracle Identity System Administration, deactivate the sandbox.
2. Log out of Oracle Identity System Administration.
3. Log in to the Oracle Identity Self Service and activate the sandbox that you deactivated in Step 1.
4. In the Catalog page, search for and add to cart the application instance updated in and then click **Checkout**.
5. Publish the application instance only if everything appears correctly. Otherwise, fix the issues and then publish the application instance. See Publishing an Application Instance to Organizations in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

2.3.1.4 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 Oracle Identity System Administration, deactivate the sandbox.
2. Log out of the Oracle Identity System Administration.
3. Log in to the Oracle 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 WebEx 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*.

2.3.1.5 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*.

2.3.2 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_WEBEX_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_WEBEX_FIRSTNAME__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_WEBEX_USERNAME =\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_WEBEX_USERNAME__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_WEBEX_USERNAME__c_LABEL">
<source>Account Name</source>
<target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>
```

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

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

   Sample file name: BizEditorBundle_ja.xlf.

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

> **Note:**
>
> See Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about exporting and importing metadata files

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

2.3.3 Clearing Content Related to Connector Resource Bundles from the Server Cache

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache you can either restart Oracle Identity Manager or run the PurgeCache utility. The following is the procedure to clear the server cache by running the PurgeCache utility:

1. In a command window, switch to the *OIM_HOME*/server/bin directory.
2. Enter one of the following commands:
   - On Microsoft Windows: `PurgeCache.bat All`
   - On UNIX: `PurgeCache.sh All`

   When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

   `t3://`*`OIM_HOST_NAME`*`:`*`OIM_PORT_NUMBER`*

   In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

You can use the PurgeCache utility to purge the cache for any content category.

2.3.4 Managing Logging for the WebEx Connector

Oracle Identity Manager uses (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

2.3.4.1 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 2-2.

Table 2-2 Log Levels and ODL Message Type:Level Combinations

Log 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.

2.3.4.2 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 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='F:\MyMachine\middleware\user_projects
\domains\base_domain1\servers\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.WEBEX" level="NOTIFICATION:
1"useParentHandlers="false">
<handler name="Webex-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.

2.3.5 Configuring SSL for WebEx

Configure SSL to secure data communication between Oracle Identity Manager and WebEx.

To configure SSL:

1. Obtain the SSL certificate by obtaining the public key certificate of WebEx.
2. Copy the public key certificate of WebEx to the computer hosting Oracle Identity Manager.
3. Run the following keytool command to import the public key certificate into the identity key store in Oracle Identity Manager:

```
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 DemoTrustKeyStorePassPhrase
```

> **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

4. From the left hand pane of the Weblogic console, select **Servers**.
5. From the customize this table region, select **AdminServer [admin]** and **oim_server**.
6. Select **Configuration**, **SSL**, and **Advanced**.
7. Set Host Verification to **None** and select the **Use JSSE SSL** checkbox.
8. Click **Save.**
9. Restart the servers to apply the above setting.

3
Using the WebEx Connector

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

The following topics provide details on using the connector:

3.1 Scheduled Job for Lookup Field Synchronization

The WebEx TimeZones Lookup Reconciliation scheduled job is used for lookup field synchronization. Values fetched by this scheduled job from the target system are populated in the Lookup.Webex.TimeZones lookup definition.

Table 3-1 Attributes of the Scheduled Job for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Enter the name of the 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 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__`
IT Resource Name	Name of the IT resource for the target system installation from which you reconcile user records. Default value: `Webex`
Lookup Name	Name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Default value: `Lookup.Webex.TimeZones`
Object Type	Name of the type of object you want to reconcile. Default value: `TimeZones`

3.2 Configuring Reconciliation for WebEx Connector

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:

- Full Reconciliation for the WebEx Connector
- Limited Reconciliation for WebEx Connector
- Reconciliation Scheduled Job

3.2.1 Full Reconciliation for the WebEx Connector

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

After you deploy the connector, you must first perform full reconciliation. To perform a full reconciliation run, ensure that no value is specified for the Filter attribute of the scheduled job for reconciling users.

3.2.2 Limited Reconciliation for WebEx Connector

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.

3.2.3 Reconciliation Scheduled Job

Scheduled jobs for reconciliation are created when you run the Connector Installer. The Webex User Reconciliation scheduled job is used to reconcile user account data from the target system in the target resource (account management) mode of the connector.

Table 3-2 Attributes of the User Reconciliation Scheduled Job

Attribute	Description
Filter	Enter the search filter for fetching records from the target system during a reconciliation run. Sample value: `equalTo('FirstName','john.doe')` See Limited Reconciliation for WebEx Connector.
IT Resource Name	Name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `Webex`
Object Type	Type of object you want to reconcile. Default value: `User` **Note:** User is the only object that is supported. Therefore, do not change the value of this attribute.
Resource Object Name	Name of the resource object that is used for reconciliation. Default value: `Webex User` **Note**: Do not change the value of this attribute.
Scheduled Task Name	Name of the scheduled task that is used for reconciliation. Default value: `Webex User Reconciliation`

3.3 Configuring Scheduled Jobs

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

To configure a scheduled job:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Scheduler.**
3. Search for and open the scheduled task as follows:

a. On the left pane, 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 following parameters:

   - **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.

> **Note:**
>
> See Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the scheduled types.

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:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - 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.
> - Attributes of the scheduled job are discussed in Reconciliation Scheduled Job.

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.

3.4 Guidelines on Performing Provisioning Operations

You must apply the below guideline while performing a provisioning operation:

For a Create User provisioning operation, you must specify a value for the Username field. For example, John Doe. It is a mandatory field, other mandatory fields are First name, Last name, Email, and Password.

3.5 Performing Provisioning Operations

You create a new user in Oracle 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 Manager:

1. Log in to Oracle Identity Self Service.
2. Create a user. See Creating a User in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager*.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance created for the IT resource (in Associating the Form with the Application Instance), and then click **Checkout**.

> **Note:**
>
> Ensure to select proper values for lookup type fields as there are a few dependent fields. Selecting a wrong value for such fields may result in provisioning failure.

5. Click Ready to **Submit.**
6. Click **Submit.**

3.6 Uninstalling the WebEx Connector

Uninstalling the connector involves deleting data related to the connector from Oracle Identity Manager Database. You use the Uninstall Connectors utility to uninstall a connector.

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

4

Extending the Functionality of the WebEx Connector

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

The following topics provide details on extending the functionality of the connector:

> **Note:**
>
> From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups of *Oracle Fusion Middleware Administering Oracle Identity Manager* for information about managing lookups by using the Form Designer in Oracle Identity System Administration.

- Adding New User Attributes for Reconciliation
- Adding New User Attributes for Provisioning
- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During User Reconciliation
- Configuring the Connector for Multiple Installations of the Target System
- Defining the Connector

4.1 Adding New User Attributes for Reconciliation

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

The default attribute mappings for reconciliation are listed in Table 1-5.

> **Note:**
>
> This connector supports configuration of already existing (standard) attributes of WebEx for reconciliation.

This section contains the following topics related to adding new attributes for users:

- Adding New Attributes on the Process Form
- Adding Attributes to the Resource Object

- Creating Reconciliation Field Mapping
- Creating Entries in Lookup Definition for Reconciliation
- Performing Changes in a New UI Form

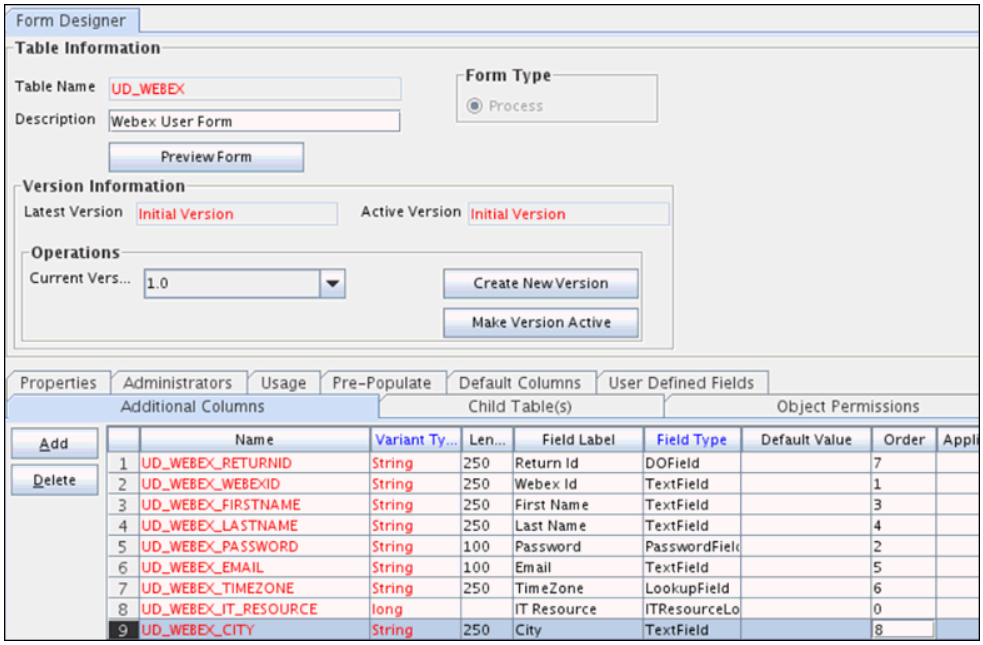
4.1.1 Adding New Attributes on the Process Form

You add a new attribute on the process form in the Form Designer section of Oracle Identity Manager Design Console.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_Webex_USR** process form.
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the field.

   For example, if you are adding the City field, enter `UD_WEBEX_CITY` in the Name field and then enter other details such as Variable Type, Length, Field Label, and Field Type.
6. Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form.

Figure 4-1 New Field Added to the Process Form



4.1.2 Adding Attributes to the Resource Object

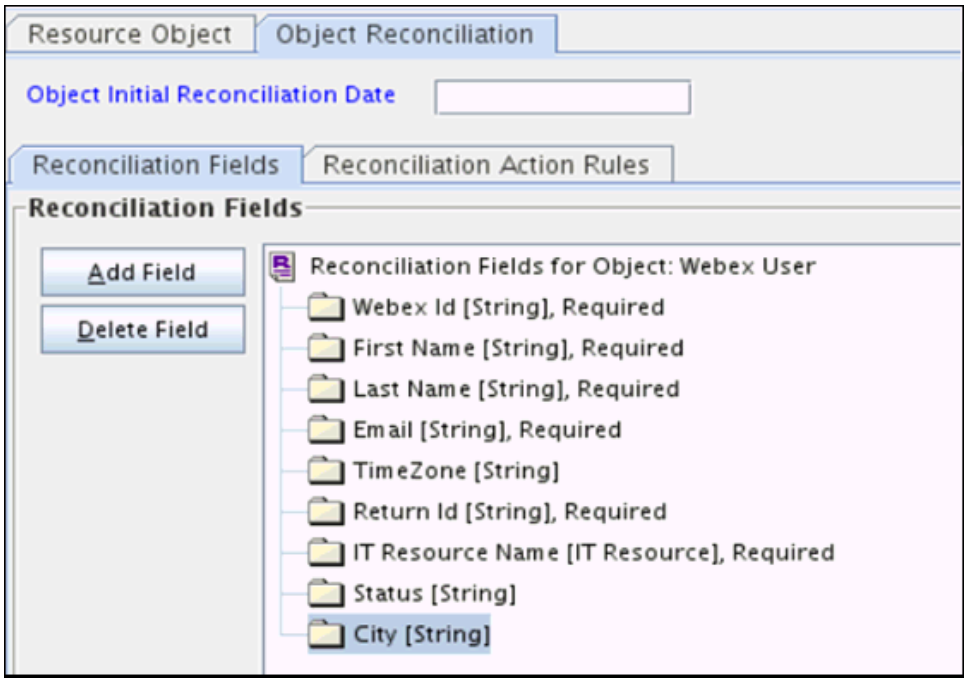
You can add the new attribute to the resource object in the Resource Objects section of Oracle Identity Manager Design Console.

1. Expand **Resource Management**, and double-click **Resource Objects**.

2. Search for and open the **Webex User** resource object.
3. On the Object Reconciliation tab, click **Add Field**.
4. Enter the details of the field.

   For example, enter `CITY` in the **Field Name** field and select **String** from the **Field Type** list. Later in this procedure, you enter the field name as the Code value of the entry that you create in the lookup definition for reconciliation.
5. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:

Figure 4-2 New Reconciliation Field Added to the Resource Object



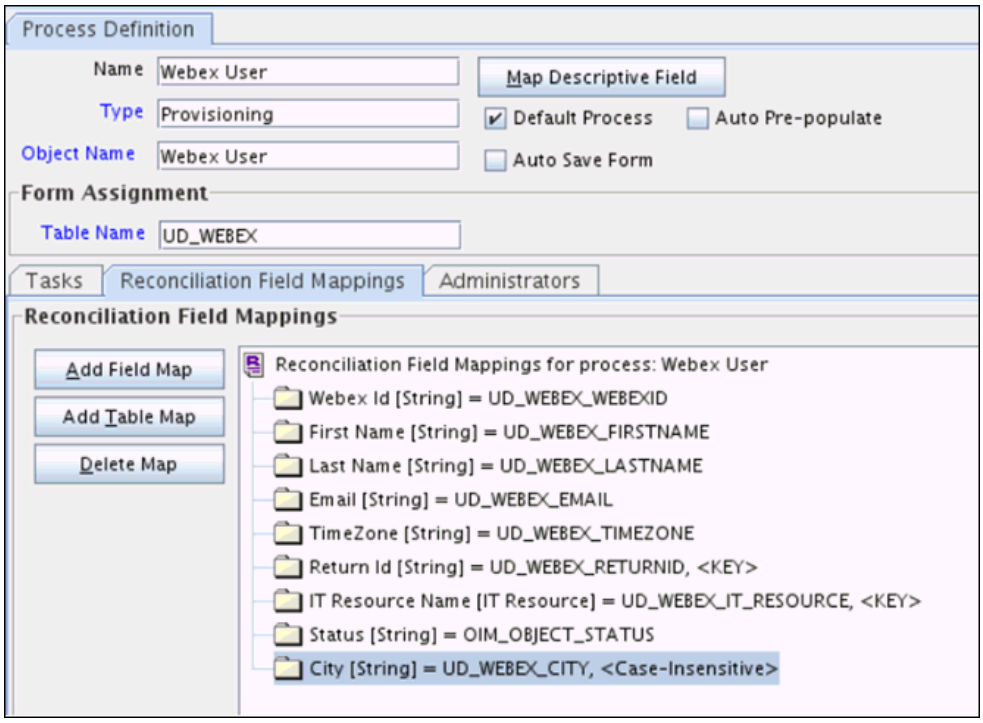
6. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

4.1.3 Creating Reconciliation Field Mapping

You create a reconciliation field mapping for the new attribute in the Process Definition section of Oracle Identity Manager Design Console.

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the **Webex User** process definition.
3. On the Reconciliation Field Mappings tab of the process definition, click **Add Field Map**.
4. From the Field Name list, select the field that you want to map.
5. Double-click the **Process Data Field** field, and then select the column for the attribute. For example, select **UD_WEBEX_CITY**.
6. Click the **Save** icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:

Figure 4-3 New Reconciliation Field Mapped to a Process Data Field in the Process Definition



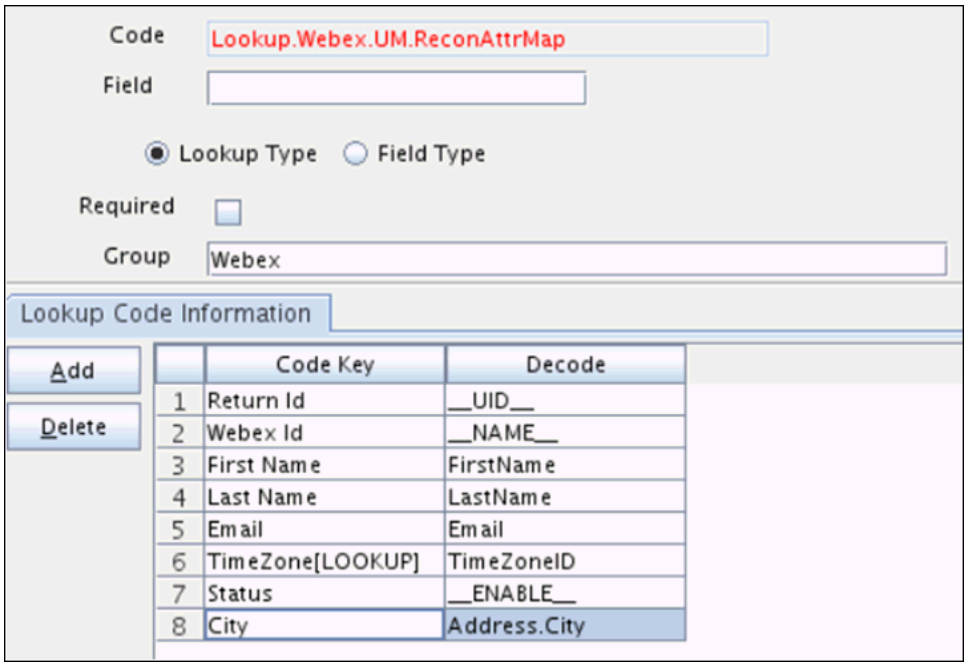
4.1.4 Creating Entries in Lookup Definition for Reconciliation

You create an entry for the newly added attribute in the lookup definition that holds attribute mappings for reconciliation.

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open the **Lookup.Webex.UM.ReconAttrMap** lookup definition.
4. Click **Add** and enter the Code Key and Decode values for the field.
5. Click the Save icon.

   The following screenshot shows the entry added to the lookup definition:

Figure 4-4 Entry Added to the Lookup Definition



4.1.5 Performing Changes in a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

4.2 Adding New User Attributes for Provisioning

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

The default attribute mappings for provisioning are listed in Table 1-8.

This section provides information related to adding new user or group attributes for provisioning:

4.2.1 Adding New Attributes for Provisioning

You add a new attribute on the process form in the Form Designer section of Oracle Identity Manager Design Console.

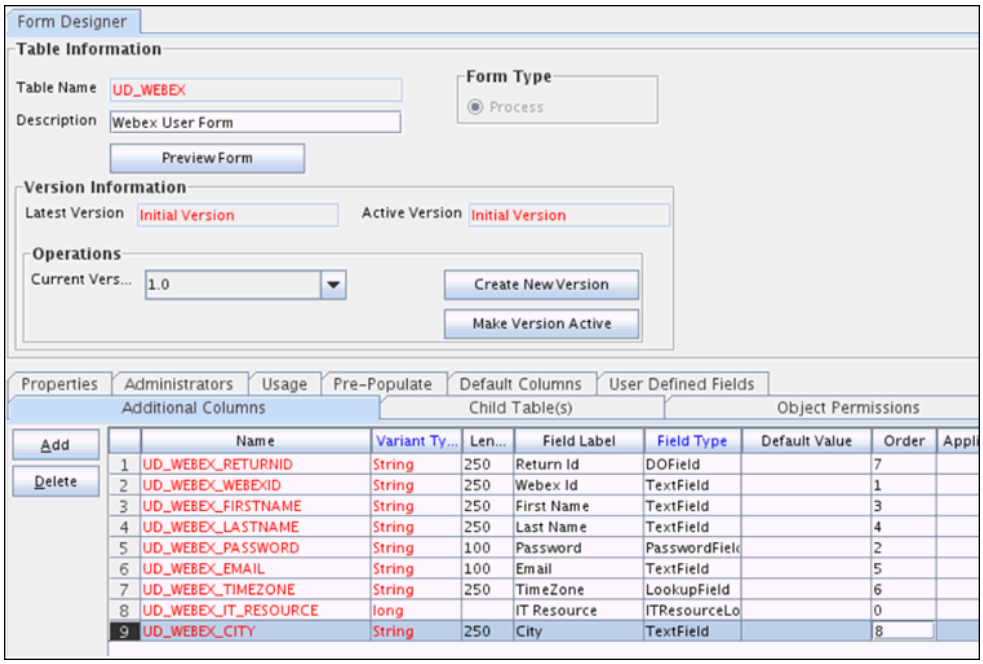
> **Note:**
>
> If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_Webex_USR** process form.
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the attribute.

   For example, if you are adding the CITY field, enter `UD_WEBEX_CITY` in the Name field, and then enter the rest of the details of this field.
6. Click the Save icon, and then click **Make Version Active**.

   The following screenshot shows the new field added to the process form:

Figure 4-5 New Field Added to the Process Form



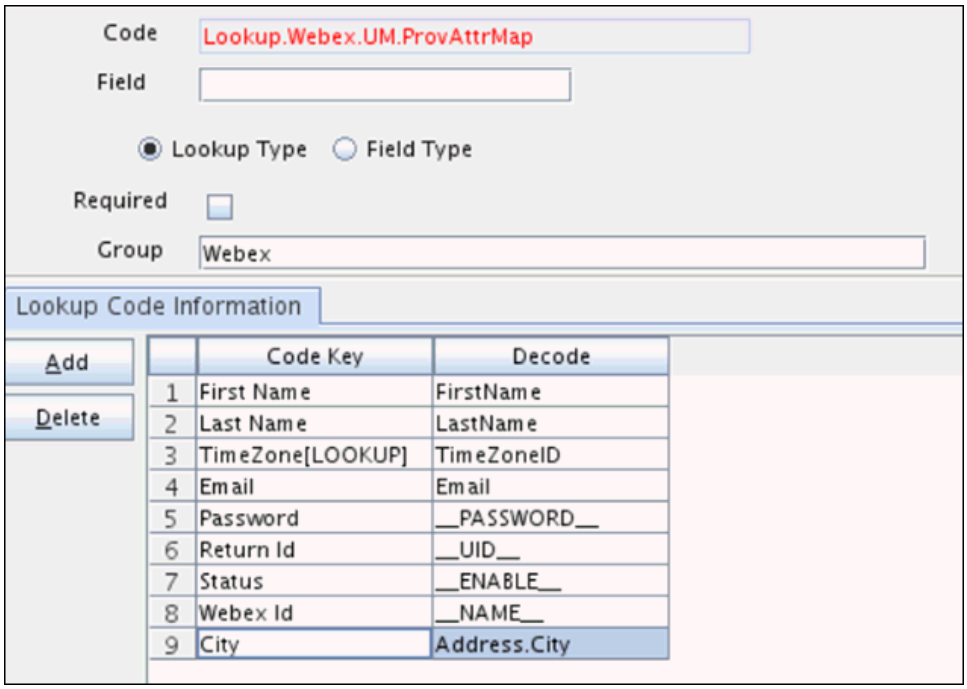
4.2.2 Creating Entries in Lookup Definition for Provisioning

You create an entry for the newly added attribute in the lookup definition that holds attribute mappings for provisioning.

1. Expand **Administration**.
2. Double-click **Lookup Definition**.
3. Search for and open the **Lookup.Webex.UM.ProvAttrMap** lookup definition.
4. Click **Add** and enter the Code Key and Decode values for the field.
5. Click the Save icon.

   The following screenshot shows the entry added to the lookup definition:

Figure 4-6 Entry Added to the Lookup Definition



4.2.3 Creating a Task to Enable Update Operations

Create a task to enable updates on the new user attribute during provisioning operations.

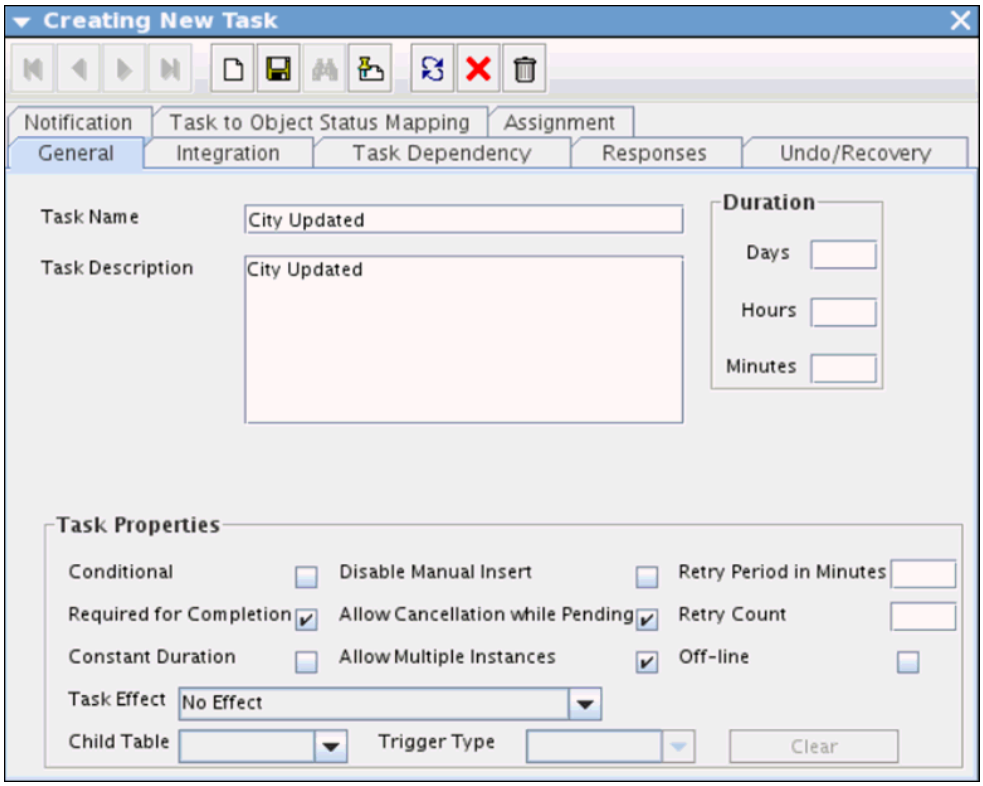
If you do not perform this procedure, then you will not be able to modify values of any attributes that were specified as part of the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the new user attribute as follows:

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open the **Webex User** process definition.
3. Click **Add.**
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
   - Conditional
   - Allow Cancellation while Pending
   - Allow Multiple Instances
5. Click the Save icon.

   The following screenshot shows the new task added to the process definition:

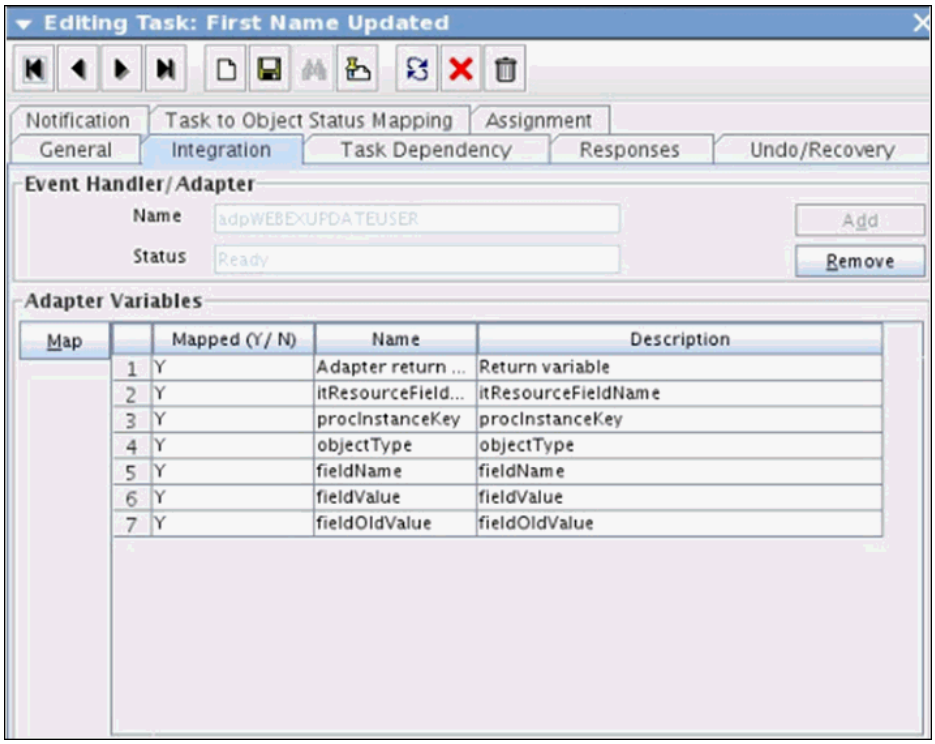
Figure 4-7 New task Added to the Process Definition



6. In the provisioning process, select the adapter name in the Handler Type section as follows:
   a. Go to the Integration tab, click **Add.**
   b. In the Handler Selection dialog box, select **Adapter**.
   c. From the Handler Name column, select **adpWebexUPDATEUSER**.
   d. Click Save and close the dialog box.

      The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:

Figure 4-8 List of Adapter Variables



7. In the Adapter Variables region, click the **ParentFormProcessInstanceKey** variable.
8. In the dialog box that is displayed, create the following mapping:
   - **Variable Name:** ParentFormProcessInstanceKey
   - **Map To:** Process Data
   - **Qualifier:**Process Instance
9. Click **Save** and close the dialog box.
10. If you are enabling update provisioning operations for a User attribute, then repeat Steps 7 through 9 for the remaining variables listed in the Adapter Variables region.

    The following table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
Adapter Return Value	Response Code	NA	NA
Object Type	Literal	String	User
itResourceFieldName	Literal	String	UD_WEBEX_IT_RESOURCE
attributeFieldName	Literal	String	City

11. On the Responses tab, click Add to add at least the SUCCESS response code, with Status C. This ensures that if the task is successfully run, then the status of the task is displayed as `Completed`.

12. Click the Save icon and close the dialog box, and then save the process definition.

4.2.4 Replicating Form Designer Changes to a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

4.3 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the User Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the User Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations. For data that fails the validation check, the following message is displayed or recorded in the log file: Validation failed for attribute ATTRIBUTE_NAME.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

   The validation class must implement validate method with the following method signature:

   ```
   boolean validate(HashMap hmUserDetails, HashMap hmEntitlementDetails,
   String field)
   ```

   The following sample validation class checks if the value in the User Name attribute contains the number sign (#):

   ```
   public boolean validate(HashMap hmUserDetails,
   HashMap hmEntitlementDetails, String field) { /*
   *    You must write code to validate attributes. Parent
   * data values can be fetched by using hmUserDetails.get(field)
   *    For child data values, loop through the
   * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
   * Depending on the outcome of the validation operation,
   ```

```
* the code must return true or false.
*/
/*
*    In this sample code, the value "false" is returned if the field
*    contains the number sign (#). Otherwise, the value "true" is
*    returned.
*/
String sUserName=(String) hmUserDetails.get(field);
if( sUserName.contains("#")){
return false;
}
return true;
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to Oracle Identity Manager database.

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

   - For Microsoft Windows: *OIM_HOME*/server/bin/UploadJars.bat
   - For UNIX: *OIM_HOME*/server/bin/UploadJars.sh

   When you run the 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 1 as the value of the JAR type.
4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.Webex.UM.ReconValidation**.
   c. In the Code Key column, enter the resource object field name that you want to validate. For example, `Firstname`. In the Decode column, enter the class name For example, `org.identityconnectors.Webex.extension.WebexAMValidator`.
   d. Save the changes to the lookup definition.
   e. Search for and open the Lookup.Webex.UM.Configuration lookup definition.
   f. In the Code Key column, enter `Recon Validation Lookup`. In the Decode column, enter `Lookup.Webex.UM.ReconValidation`.
   g. Save the changes to the lookup definition.

5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.Webex.UM.ProvValidation**.
   c. In the Code Key column, enter.the process form field label. For example, `Firstname`. In the Decode column, enter the class name. For example, `org.identityconnectors.Webex.extension.WebexValidator`.
   d. Save the changes to the lookup definition.
   e. Search for and open the `Lookup.Webex.UM.Configuration` lookup definition.
   f. In the Code Key column, enter `Provisioning Validation Lookup`. In the Decode column, enter `Lookup.Webex.UM.ProvValidation`.
   g. Save the changes to the lookup definition.
6. Purge the cache to get the changes reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

4.4 Configuring Transformation of Data During User Reconciliation

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

To configure transformation of single-valued account data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class.

   The transformation class must implement the transform method with the following method signature:

   ```
   Object transform(HashMap hmUserDetails, HashMap hmEntitlementDetails,
   String sField)
   ```

   The following sample transformation class creates a value for the Full Name attribute by using values fetched from the User Name and Last Name attributes of the target system:

   ```
   package oracle.iam.connectors.common.transform;
   import java.util.HashMap;
   public class TransformAttribute {
   /*
   Description:Abstract method for transforming the attributes
   param hmUserDetails< String,Object>
   HashMap containing parent data details
   param hmEntitlementDetails < String,Object>
   HashMap containing child data details
   */
   public Object transform(HashMap hmUserDetails, HashMap
   hmEntitlementDetails,String sField) {
   ```

```
/*
*    You must write code to transform the attributes. Parent data
attribute values can be fetched by using hmUserDetails.get("Field
Name").
*To fetch child data values, loop through the
*    ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
*    Return the transformed attribute.
*/
String sUserName= (String)hmUserDetails.get("User Name"); String
sLastName= (String)hmUserDetails.get("Last Name"); String
sFullName=sUserName+"."+sLastName;
return sFullName;
}
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to Oracle Identity Manager database.

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

   - For Microsoft Windows: *OIM_HOME*/server/bin/UploadJars.bat
   - For UNIX: *OIM_HOME*/server/bin/UploadJars.sh

   When you run the 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 1 as the value of the JAR type.
4. Create a new lookup definition for transformation as follows:
   a. Log in to the Design Console.
   b. Expand Administration, and then double-click Lookup Definition.
   c. In the Code field, enter `Lookup.Webex.UM.ReconTransformations` as the name of the lookup definition.
   d. Select the **Lookup Type** option.
   e. On the **Lookup Code Information** tab, click **Add**.
   f. In the Code Key column, enter the resource object field name on which you want to apply transformation. For example, User Name. In the Decode column, enter the name of the class that implements the transformation logic. For example, oracle.iam.connectors.common.transform.TransformAttribute.
   g. Save the changes to the lookup definition.

5. Add an entry in the **Lookup.Webex.UM.Configuration** lookup definition to enable transformation as follows:
    a. Expand Administration, and then double-click **Lookup Definition**.
    b. Search for and open the **Lookup.Webex.UM.Configuration** lookup definition.
    c. In the Code Key column, enter Recon Transformation Lookup. In the Decode column, enter Lookup.Webex.UM.ReconTransformation.
    d. Save the changes to the lookup definition.
6. Purge the cache to get the changes reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

4.5 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector 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. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must create copies of the connector. See Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information.

4.6 Defining the Connector

You can define a customized or reconfigured connector by using Oracle Identity System Administration. Defining a connector is equivalent to registering the connector with Oracle Identity Manager.

A connector is automatically defined when you install it using the Install Connectors feature or when you upgrade it using the Upgrade Connectors feature. You must manually define a connector if:

- You import the connector by using the Deployment Manager.
- You customize or reconfigure the connector.
- You upgrade Oracle Identity Manager.

The following events take place when you define a connector:

- A record representing the connector is created in the Oracle Identity Manager database. If this record already exists, then it is updated.
- The status of the newly defined connector is set to Active. In addition, the status of a previously installed release of the same connector automatically is set to Inactive.

See Defining Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the procedure to define connectors.

5

Known Issues and Workarounds for the WebEx Connector

These are the known issues and workarounds associated with this release of the connector.

The following is an issue associated with the target system:

Time Zone Lookup Definition Gets Updated with Null Value in Oracle Identity Manager but Not in the Target System

When the Time Zone lookup definition is updated with a null value in Oracle Identity Manager, the same value is not updated in the target system. Instead, the WebEx API assigns a default value. When a user is created in Oracle Identity Manager for the first time and the Time Zone lookup definition for the user is not updated, the WebEx API assigns a default time zone value to the user. During an update operation, when the Time zone value is deleted from the lookup definition, a process task is triggered with a null value. By default, this value is automatically updated in the target system.

There is no workaround available for this issue.

A

Files and Directories on the WebEx Connector Installation Media

These are the components of the connector installation media that comprise the connector.

Table A-1 Files and Directories on the WebEx Connector Installation Media

File in the Installation Media Directory	Description
/bundle/ org.identityconnectors.webex-1.0.11150.jar	This JAR is the ICF connector bundle.
configuration/Webex-CI.xml	This XML file contains configuration information that is used 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/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

Index