

# Oracle® Identity Governance

## Configuring the GoToMeeting Application



12c (12.2.1.3.0)

F12368-03

October 2020

The Oracle logo, consisting of the word "ORACLE" in white, uppercase letters, centered within a solid red square.

ORACLE®

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

F12368-03

Copyright © 2018, 2020, Oracle and/or its affiliates.

Primary Author: Alankrita Prakash

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

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

# Contents

## Preface

---

|                             |      |
|-----------------------------|------|
| Audience                    | viii |
| Documentation Accessibility | viii |
| Related Documents           | viii |
| Conventions                 | ix   |

## What's New in This Guide

---

|                                |   |
|--------------------------------|---|
| Software Updates               | x |
| Documentation-Specific Updates | x |

## 1 Overview of the GoToMeeting Connector

---

|  |     |
|--|-----|
| 1.1 Introduction to the GoToMeeting Connector          | 1-2 |
| 1.2 Use Cases Supported by the GoToMeeting Connector   | 1-3 |
| 1.3 Roadmap for Implementing the GoToMeeting Connector | 1-3 |

## 2 Integrating GoToMeeting with OIG AD Connector

---

|   |     |
|---|-----|
| 2.1 Certified Components for the OIG AD Connector Integration             | 2-1 |
| 2.2 Usage Recommendation for the OIG AD Connector Integration             | 2-2 |
| 2.3 Operations Supported by the OIG AD Connector Integration              | 2-3 |
| 2.4 Architecture of the OIG AD Connector Integration                      | 2-3 |
| 2.5 Deploying and Using the OIG AD Connector and GoToMeeting AD Connector | 2-5 |

## 3 Implementing the GoToMeeting Connector

---

|  |     |
|--|-----|
| 3.1 About the GoToMeeting Connector                      | 3-1 |
| 3.1.1 Certified Components for the GoToMeeting Connector | 3-2 |
| 3.1.2 Usage Recommendation for the GoToMeeting Connector | 3-2 |
| 3.1.3 Certified Languages for the GoToMeeting Connector  | 3-3 |
| 3.1.4 Operations Supported by the GoToMeeting Connector  | 3-4 |
| 3.1.5 Architecture of the GoToMeeting Connector          | 3-4 |

|         |  |      |
|---------|--|------|
| 3.1.6   | Supported Features Matrix for the GoToMeeting Connector              | 3-5  |
| 3.1.7   | Features of the GoToMeeting Connector                                | 3-6  |
| 3.1.7.1 | Support for User Account Provisioning                                | 3-6  |
| 3.1.7.2 | Support for Full Reconciliation                                      | 3-6  |
| 3.1.7.3 | Support for Limited Reconciliation                                   | 3-7  |
| 3.1.7.4 | Support for the Connector Server                                     | 3-7  |
| 3.1.7.5 | Support for Cloning Applications and Creating Instance Applications  | 3-7  |
| 3.1.7.6 | Secure Communication to the Target System                            | 3-7  |
| 3.1.7.7 | Transformation and Validation of Account Data                        | 3-7  |
| 3.2     | Creating an Application By Using the GoToMeeting Connector           | 3-8  |
| 3.2.1   | Process Flow for Creating an Application By Using the Connector      | 3-8  |
| 3.2.2   | Prerequisites for Creating an Application By Using the Connector     | 3-9  |
| 3.2.2.1 | Configuring the Target System  | 3-10 |
| 3.2.2.2 | Downloading the Connector Installation Package                       | 3-10 |
| 3.2.3   | Creating an Application By Using the Connector                       | 3-11 |
| 3.3     | Configuring the GoToMeeting Connector                                | 3-12 |
| 3.3.1   | Basic Configuration Parameters                                       | 3-12 |
| 3.3.2   | Advanced Settings Parameters   | 3-14 |
| 3.3.3   | Attribute Mappings   | 3-17 |
| 3.3.4   | Rules, Situations, and Responses                                     | 3-19 |
| 3.3.5   | Reconciliation Jobs  | 3-21 |
| 3.4     | Performing the Postconfiguration Tasks for the GoToMeeting Connector | 3-23 |
| 3.4.1   | Configuring Oracle Identity Governance                               | 3-23 |
| 3.4.1.1 | Creating and Activating a Sandbox                                    | 3-24 |
| 3.4.1.2 | Creating a New UI Form   | 3-24 |
| 3.4.1.3 | Publishing a Sandbox   | 3-24 |
| 3.4.1.4 | Updating an Existing Application Instance with a New Form            | 3-25 |
| 3.4.2   | Harvesting Entitlements and Sync Catalog                             | 3-25 |
| 3.4.3   | Managing Logging   | 3-26 |
| 3.4.3.1 | Understanding Log Levels   | 3-26 |
| 3.4.3.2 | Enabling Logging   | 3-27 |
| 3.4.4   | Configuring the IT Resource for the Connector Server                 | 3-29 |
| 3.4.5   | Localizing Field Labels in UI Forms                                  | 3-29 |
| 3.4.6   | Configuring SSL for the Connector                                    | 3-31 |
| 3.5     | Using the GoToMeeting Connector                                      | 3-32 |
| 3.5.1   | Configuring Reconciliation   | 3-32 |
| 3.5.1.1 | Performing Full Reconciliation                                       | 3-32 |
| 3.5.1.2 | Performing Limited Reconciliation                                    | 3-33 |
| 3.5.1.3 | Reconciling Large Number of Records                                  | 3-33 |
| 3.5.2   | Configuring Reconciliation Jobs                                      | 3-34 |

|       |   |      |
|-------|---|------|
| 3.5.3 | Performing Provisioning Operations  | 3-35 |
| 3.5.4 | Uninstalling the GoToMeeting Connector                                    | 3-35 |
| 3.6   | Extending the Functionality of the GoToMeeting Connector                  | 3-36 |
| 3.6.1 | Configuring the Connector for Multiple Installations of the Target System | 3-36 |
| 3.6.2 | Configuring Transformation and Validation of Data                         | 3-36 |
| 3.6.3 | Configuring Action Scripts  | 3-37 |
| 3.7   | Upgrading the GoToMeeting Connector                                       | 3-37 |
| 3.7.1 | Preupgrade Steps  | 3-38 |
| 3.7.2 | Upgrade Steps   | 3-38 |
| 3.7.3 | Postupgrade Steps   | 3-38 |
| 3.8   | Known Issues and Workarounds for the GoToMeeting Connector                | 3-41 |

## A Files and Directories in the GoToMeeting Connector Package

## List of Figures

---

|     |  |      |
|-----|--|------|
| 2-1 | Architecture of the OIG AD Connector Integration                               | 2-4  |
| 3-1 | Architecture of the GoToMeeting Connector                                      | 3-5  |
| 3-2 | Overall Flow of the Process for Creating an Application By Using the Connector | 3-9  |
| 3-3 | Default Attribute Mappings for GoToMeeting User Account                        | 3-18 |
| 3-4 | Default Attribute Mappings for Licenses Entitlement                            | 3-19 |
| 3-5 | Simple Correlation Rule for GoToMeeting  | 3-20 |
| 3-6 | Predefined Situations and Responses for GoToMeeting                            | 3-21 |

## List of Tables

---

|      |   |      |
|------|---|------|
| 2-1  | Certified Components for the OIG AD Connector Integration               | 2-2  |
| 2-2  | Supported Connector Operations for the OIG AD Connector Integration     | 2-3  |
| 3-1  | Certified Components for the GoToMeeting Connector                      | 3-2  |
| 3-2  | Supported Connector Operations for the GoToMeeting Connector            | 3-4  |
| 3-3  | Supported Features Matrix for the GoToMeeting Connector                 | 3-5  |
| 3-4  | Basic Configuration Parameters for GoToMeeting                          | 3-12 |
| 3-5  | Advanced Settings Parameters for GoToMeeting                            | 3-14 |
| 3-6  | Default Attribute Mappings for GoToMeeting User Account                 | 3-18 |
| 3-7  | Default Attribute Mappings for Licenses Entitlement                     | 3-19 |
| 3-8  | Predefined Identity Correlation Rule for GoToMeeting                    | 3-20 |
| 3-9  | Predefined Situations and Responses for GoToMeeting                     | 3-20 |
| 3-10 | Parameters of the GoToMeeting Full User Reconciliation Job              | 3-21 |
| 3-11 | Parameters of the Reconciliation Jobs for Entitlements                  | 3-22 |
| 3-12 | Log Levels and ODL Message Type:Level Combinations                      | 3-26 |
| 3-13 | Parameters of the IT Resource for the Connector Server                  | 3-29 |
| A-1  | Files and Directories in the GoToMeeting Connector Installation Package | A-1  |

# Preface

This guide describes the connector that is used to onboard GoToMeeting applications to Oracle Identity Governance. You can implement the GoToMeeting connector either by using GoToMeeting with Oracle Identity Governance Connector for Microsoft Active Directory User Management or by using the predefined integration.

## 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](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](http://docs.oracle.com/cd/E22999_01/index.htm)



---

## Conventions

The following text conventions are used in this document:

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

---

# 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 GoToMeeting Application.

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

- [Software Updates](#)  
These include updates made to the connector software.
- [Documentation-Specific Updates](#)  
These include major changes made to the connector documentation. These changes are not related to software updates.

## Software Updates

These are the updates made to the connector software.

### Software Updates in Release 12.2.1.3.0

The following is the software update in release 12.2.1.3.0:

#### Support for Onboarding Applications Using the Connector

From this release onward, the connector bundle includes application onboarding templates required for performing connector operations on the GoToMeeting 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 update has been made in revision "03" of this guide:

Logger names present in [Enabling Logging](#) have been updated.

The following documentation-specific updates have been made in revision "02" of this guide:

- The "Oracle Identity Governance or Oracle Identity Manager" rows in [Table 2-1](#) and [Table 3-1](#) have been updated to include support for Oracle Identity Governance release 12c PS4 (12.2.1.4.0).

- The "Oracle Identity Governance or Oracle Identity Manager" row in [Table 3-1](#) has been updated to include information about mandatory patches that you must apply to Oracle Identity Governance release 12c PS3 (12.2.1.3.0).
- The "Connector Server JDK" row of [Table 3-1](#) has been updated.
- Some editorial corrections have been made.

# 1

## Overview of the GoToMeeting 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 GoToMeeting connector enables you to onboard applications in Oracle Identity Governance for GoToMeeting.

### Note:

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

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

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

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

- [Introduction to the GoToMeeting Connector](#)
- [Use Cases Supported by the GoToMeeting Connector](#)
- [Roadmap for Implementing the GoToMeeting Connector](#)

### Note:

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

## 1.1 Introduction to the GoToMeeting Connector

The GoToMeeting connector enables Oracle Identity Governance to manage the identity data for GoToMeeting by integrating Oracle Identity Governance with the GoToMeeting Admin Center (Admin Center) either by using Oracle Identity Governance Connector for Microsoft Active Directory User Management (OIG AD connector) or by using the predefined GoToMeeting connector.

Both the implementations can be configured to run in the Target (account management) mode.

The following sections provide details on the GoToMeeting connector implementations:

- [OIG AD Connector Integration](#)
- [Predefined Integration](#)

### **OIG AD Connector Integration**

This implementation of the connector integrates Oracle Identity Governance with the Admin Center by using Microsoft Active Directory (AD) as a middleware. In this implementation, AD is used as a user source for performing user management operations in the Admin Center.

The OIG AD connector allows synchronization of the GoToMeeting user information between Oracle Identity Governance and AD. The GoToMeeting Active Directory Connector (GoToMeeting AD connector) helps in fetching the attributes from AD and then synchronizing the data with the Admin Center.

This is an optional integration, and you can choose this integration for managing GoToMeeting users if you have already configured Microsoft Active Directory with the Admin Center.

See [Integrating GoToMeeting with OIG AD Connector](#).

### **Predefined Integration**

You can implement the GoToMeeting connector using the predefined integration. This implementation of the connector integrates Oracle Identity Governance with the Admin Center by using GoToMeeting Administration APIs. The Admin Center is used as a target (managed) resource of the identity data for Oracle Identity Governance.

The information about users that are created or modified directly on the Admin Center can be reconciled into Oracle Identity Governance. This data is used to add or modify resources (that is, accounts) that are allocated to Oracle Identity Governance Users. In addition, you can use Oracle Identity Governance to provision or update GoToMeeting accounts that are assigned to Oracle Identity Governance Users.

See [Implementing the GoToMeeting Connector](#).

 **Note:**

In this guide,

- Oracle Identity Governance Connector for Microsoft Active Directory User Management is referred to as the **OIG AD connector**.
- GoToMeeting Active Directory Connector is referred to as the **GoToMeeting AD connector**.
- GoToMeeting Admin Center is referred to as the **target system**.

## 1.2 Use Cases Supported by the GoToMeeting Connector

GoToMeeting is a cloud-based application that offers online meeting, screen sharing, and video conferencing features. The GoToMeeting connector helps in managing GoToMeeting users and their accounts through Oracle Identity Governance.

The following is a common scenario in which the GoToMeeting connector can be used:

Organizations use GoToMeeting for a real-time collaboration of users across various locations. The administrator needs to assign an account with a valid GoToMeeting license to each GoToMeeting user, and also ensure that the user is unable to access the application using the account after leaving the organization.

The GoToMeeting connector provides a user management functionality that enables automation of provisioning and deprovisioning of GoToMeeting User accounts. The connector enables organizations to manage identities and licenses for GoToMeeting users through Oracle Identity Governance. For example, after a user joins an organization, an account is automatically provisioned to the user based on the predefined access policies in Oracle Identity Governance. In addition, the user is assigned a GoToMeeting license. Similarly, this account is deactivated after the user leaves the organization. This saves time and provides robust security because of less manual intervention.

## 1.3 Roadmap for Implementing the GoToMeeting Connector

This is the organization of information available in this guide for understanding, deploying, and using the GoToMeeting connector.

The rest of this guide is divided into the following chapters:

- [Integrating GoToMeeting with OIG AD Connector](#) provides information on understanding the OIG AD connector integration with GoToMeeting. It also provides guidelines on deploying and using the required connectors (OIG AD connector and GoToMeeting AD connector) for implementing this integration approach.
- [Implementing the GoToMeeting Connector](#) provides information on understanding, deploying, and using the predefined GoToMeeting connector. It also provides details on upgrading the connector and extending its functionality to address your specific requirements.
- [Files and Directories in the GoToMeeting Connector Package](#) lists the files and directories that comprise the connector installation package.

# 2

## Integrating GoToMeeting with OIG AD Connector

In this integration, the user management operations are implemented in the Admin Center by using Microsoft Active Directory as a middleware. The OIG AD connector and GoToMeeting AD connector help in synchronizing GoToMeeting user attributes between Oracle Identity Governance, Microsoft Active Directory, and GoToMeeting directory services.

This chapter contains the following sections:

- [Certified Components for the OIG AD Connector Integration](#)
- [Usage Recommendation for the OIG AD Connector Integration](#)
- [Operations Supported by the OIG AD Connector Integration](#)
- [Architecture of the OIG AD Connector Integration](#)
- [Deploying and Using the OIG AD Connector and GoToMeeting AD Connector](#)

### Note:

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

## 2.1 Certified Components for the OIG AD Connector Integration

These are the software components and their versions required for integrating Oracle Identity Governance with GoToMeeting using the OIG AD 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 2-1 Certified Components for the OIG AD Connector Integration**

| 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: <ul style="list-style-type: none"> <li>Oracle Identity Governance release 12c PS4 (12.2.1.4.0)</li> <li>Oracle Identity Governance 12c (12.2.1.3.0)</li> </ul> | You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: <ul style="list-style-type: none"> <li>Oracle Identity Governance release 12c PS4 (12.2.1.4.0)</li> <li>Oracle Identity Governance 12c (12.2.1.3.0)</li> <li>Oracle Identity Manager 11g Release 2 PS3 BP06 (11.1.2.3.6)</li> </ul> |
| Target system   | GoToMeeting Admin Center  | GoToMeeting Admin Center  |
| Oracle Identity Governance Connector for Microsoft Active Directory User Management | 12.2.1.3.0  | 12.2.1.3.0  |
| GoToMeeting Active Directory Connector  | 1.5.1.68  | 1.5.1.68  |

## 2.2 Usage Recommendation for the OIG AD Connector Integration

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

- If you are using Oracle Identity Governance release 12c (12.2.1.3.0) or later, then use the latest 12.2.1.x version of the OIG AD connector. Deploy the connector using the **Applications** option on the **Manage** tab of Identity Self Service.
- If you are using the Oracle Identity Manager release listed in the “Requirement for CI-Based Connector” column in [Certified Components for the OIG AD Connector Integration](#), then use the 11.1.x version of the 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 12c (12.2.1.3.0) or later.

### Note:

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



## 2.3 Operations Supported by the OIG AD Connector Integration

These are the user management operations supported by integrating GoToMeeting with Oracle Identity Governance using the OIG AD connector.

**Table 2-2 Supported Connector Operations for the OIG AD Connector Integration**

| Operation              | Supported? |
|------------------------|------------|
| <b>User Management</b> |            |
| Create user            | Yes        |
| Update user            | Yes        |
| Delete user            | Yes        |
| Enable user            | Yes        |
| Disable user           | Yes        |

## 2.4 Architecture of the OIG AD Connector Integration

In this implementation, Microsoft Active Directory is used as a target (managed) resource of the identity data for Oracle Identity Governance.

The following connectors are used to synchronize data between Oracle Identity Governance and the Admin Center:

- **Oracle Identity Governance Connector for Microsoft Active Directory User Management**

The OIG AD connector allows synchronization of user information between Oracle Identity Governance and AD, and is configured to run in the account management mode. This mode enables the following operations:

- **Provisioning**

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

- **Target resource reconciliation**

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

See Connector Architecture in *Oracle Identity Governance Configuring the Microsoft Active Directory User Management Application*.

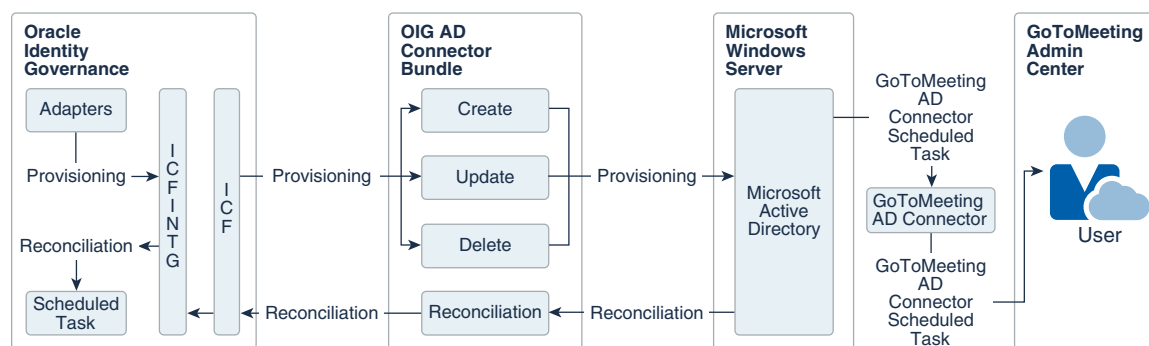
- **GoToMeeting Active Directory Connector**

GoToMeeting uses a lightweight AD connector behind the firewall to synchronize user information between AD and GoToMeeting directory services. These user accounts are included as members of a Microsoft Active Directory group (specified as values of the AD Sync Group attribute of AD), which is used for synchronizing the accounts from AD to the Admin Center through the GoToMeeting AD connector scheduled task.

For details on the GoToMeeting AD connector, visit the GoToMeeting website at <https://www.gotomeeting.com/>, navigate to Support, and search for Active Directory Connector.

Figure 2-1 depicts the components used for integrating Oracle Identity Governance with GoToMeeting using the OIG AD connector.

**Figure 2-1 Architecture of the OIG AD Connector Integration**



As shown in Figure 2-1, AD is configured as a target resource of Oracle Identity Governance. The OIG AD connector is a .NET framework-based connector that is implemented using the Identity Connector Framework (ICF) component. The ICF component provides basic reconciliation and provisioning operations that are common to all Oracle Identity Governance connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. ICF is distributed together with Oracle Identity Governance. Therefore, you do not need to configure or modify ICF.

This implementation enables provisioning of User accounts on the target system through the following two-step process:

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

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

## 2.5 Deploying and Using the OIG AD Connector and GoToMeeting AD Connector

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

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

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

The procedure for deploying and using the GoToMeeting AD connector is available in the GoToMeeting product documentation. For the detailed instructions on deploying and using the GoToMeeting AD connector, visit the GoToMeeting website at <https://www.gotomeeting.com/>, navigate to Support, and search for Active Directory Connector.

# 3

## Implementing the GoToMeeting Connector

You can implement the GoToMeeting connector using the out-of-the-box integration, which enables Oracle Identity Governance to integrate with GoToMeeting using GoToMeeting Administration APIs.

The following sections provide an overview of the predefined connector and instructions on onboarding applications, configuring and using the connector, and extending its functionality to address your specific requirements:

- [About the GoToMeeting Connector](#)
- [Creating an Application By Using the GoToMeeting Connector](#)
- [Configuring the GoToMeeting Connector](#)
- [Performing the Postconfiguration Tasks for the GoToMeeting Connector](#)
- [Using the GoToMeeting Connector](#)
- [Extending the Functionality of the GoToMeeting Connector](#)
- [Upgrading the GoToMeeting Connector](#)
- [Known Issues and Workarounds for the GoToMeeting Connector](#)

### 3.1 About the GoToMeeting Connector

The GoToMeeting connector can be configured to run in the Target (account management) mode. In this mode, the Admin Center is used as a target (managed) resource of the identity data for Oracle Identity Governance.

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

- [Certified Components for the GoToMeeting Connector](#)
- [Usage Recommendation for the GoToMeeting Connector](#)
- [Certified Languages for the GoToMeeting Connector](#)
- [Operations Supported by the GoToMeeting Connector](#)
- [Architecture of the GoToMeeting Connector](#)
- [Supported Features Matrix for the GoToMeeting Connector](#)
- [Features of the GoToMeeting Connector](#)

### 3.1.1 Certified Components for the GoToMeeting Connector

These are the software components and their versions required for installing and using the GoToMeeting 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 3-1 Certified Components for the GoToMeeting Connector**

| Component   | Requirement for AOB Application  | Requirement for CI-Based Connector   |
|---|--|--|
| Oracle Identity Governance or Oracle Identity Manager | <p>You can use any one of the following releases:</p> <ul style="list-style-type: none"> <li>Oracle Identity Governance release 12c PS4 (12.2.1.4.0)</li> <li>Oracle Identity Governance 12c (12.2.1.3.0)</li> </ul> <p><b>Note:</b> If you are using Oracle Identity Governance 12c (12.2.1.3.0), then ensure to download and apply patches 26616250 and 25323654 from <a href="#">My Oracle Support</a>.</p> | <p>You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:</p> <ul style="list-style-type: none"> <li>Oracle Identity Governance release 12c PS4 (12.2.1.4.0)</li> <li>Oracle Identity Governance 12c (12.2.1.3.0)</li> <li>Oracle Identity Manager 11g Release 2 PS3 BP06 (11.1.2.3.6)</li> </ul> |
| Target system   | GoToMeeting Admin Center   | GoToMeeting Admin Center   |
| 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   |

### 3.1.2 Usage Recommendation for the GoToMeeting Connector

These are the recommendations for the GoToMeeting 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 the Oracle Identity Manager release listed in the “Requirement for CI-Based Connector” column in [Certified Components for the GoToMeeting Connector](#), then use the 11.1.x version of the 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 12c (12.2.1.3.0) or later.

 **Note:**

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

### 3.1.3 Certified Languages for the GoToMeeting 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

### 3.1.4 Operations Supported by the GoToMeeting Connector

These are the list of operations that the connector supports.

**Table 3-2 Supported Connector Operations for the GoToMeeting Connector**

| Operation                           | Supported? |
|-------------------------------------|------------|
| <b>User Management</b>              |            |
| Create user                         | Yes        |
| Update user                         | Yes        |
| Delete user                         | Yes        |
| <b>Entitlement Grant Management</b> |            |
| Add child table values              | Yes        |
| Update child table values           | Yes        |
| Remove child table values           | Yes        |

### 3.1.5 Architecture of the GoToMeeting Connector

You can configure the GoToMeeting connector to run in the Target (or account management) mode, and is implemented using the Identity Connector Framework (ICF) component.

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.

The connector enables the following operations:

- Provisioning
 

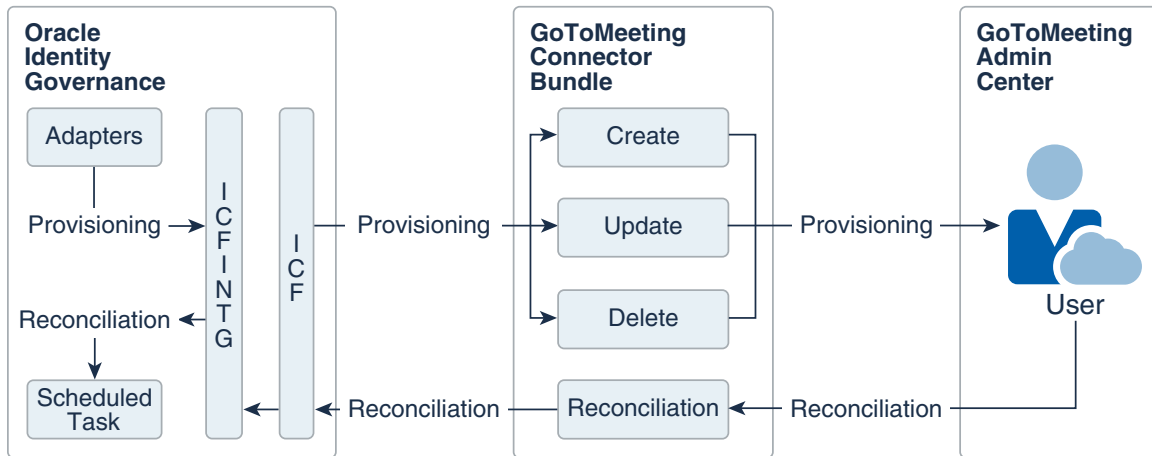
Provisioning involves creating and updating users on the Admin Center through Oracle Identity Governance. When you allocate (or provision) a GoToMeeting resource to an Oracle Identity Governance User, the operation results in the creation of an account in the Admin Center for that user. In the Oracle Identity Governance context, the term **provisioning** is also used to mean updates made to the account through Oracle Identity Governance.
- Target resource reconciliation
 

To perform target resource reconciliation, the GoToMeeting Reconciliation job is used. The connector then fetches the user attribute values from the Admin Center.

The connector supports OAuth 2.0 security protocol for authenticating to the target system, and uses access token and refresh token values as inputs from the user.

Figure 3-1 depicts the architecture of the GoToMeeting connector.

**Figure 3-1 Architecture of the GoToMeeting Connector**



As shown in [Figure 3-1](#), the Admin Center is configured as a target resource of Oracle Identity Governance. Through the provisioning operations that are performed on Oracle Identity Governance, accounts are created and updated on the Admin Center for Oracle Identity Governance Users.

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

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

During provisioning, the adapters invoke ICF operation, ICF invokes the Create operation on GoToMeeting Connector Bundle, and then the bundle calls the OAuth API for connecting to the Admin Center and performing user authentication. The Admin Center accepts provisioning data from the bundle using GoToMeeting Administration APIs, carries out the operation, and returns the response back to the bundle. The bundle then passes it to the adapters.

### 3.1.6 Supported Features Matrix for the GoToMeeting Connector

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

**Table 3-3 Supported Features Matrix for the GoToMeeting Connector**

| Feature  | AOB Application | CI-Based Connector |
|--|-----------------|--------------------|
| Clone applications or create new application instances | Yes             | Yes                |
| Perform user provisioning                              | Yes             | Yes                |
| Perform full reconciliation                            | Yes             | Yes                |



**Table 3-3 (Cont.) Supported Features Matrix for the GoToMeeting Connector**

| Feature   | AOB Application | CI-Based Connector |
|---|-----------------|--------------------|
| Perform limited reconciliation                                | Yes             | Yes                |
| Configure validation and transformation of account data       | Yes             | Yes                |
| Use connector server  | Yes             | Yes                |
| Provide secure communication to the target system through SSL | Yes             | Yes                |

## 3.1.7 Features of the GoToMeeting Connector

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.

The following are the features of this connector:

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

### 3.1.7.1 Support for User Account Provisioning

You can use the connector for provisioning user accounts.

You perform provisioning operations in Oracle Identity Governance by using the Create User page. See *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.

### 3.1.7.2 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](#).

### 3.1.7.3 Support for Limited Reconciliation

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

To limit or filter the records that are fetched into Oracle Identity Governance during a reconciliation run, see [Performing Limited Reconciliation](#).

### 3.1.7.4 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*.

### 3.1.7.5 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*.

### 3.1.7.6 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](#).

### 3.1.7.7 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*.

## 3.2 Creating an Application By Using the GoToMeeting Connector

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

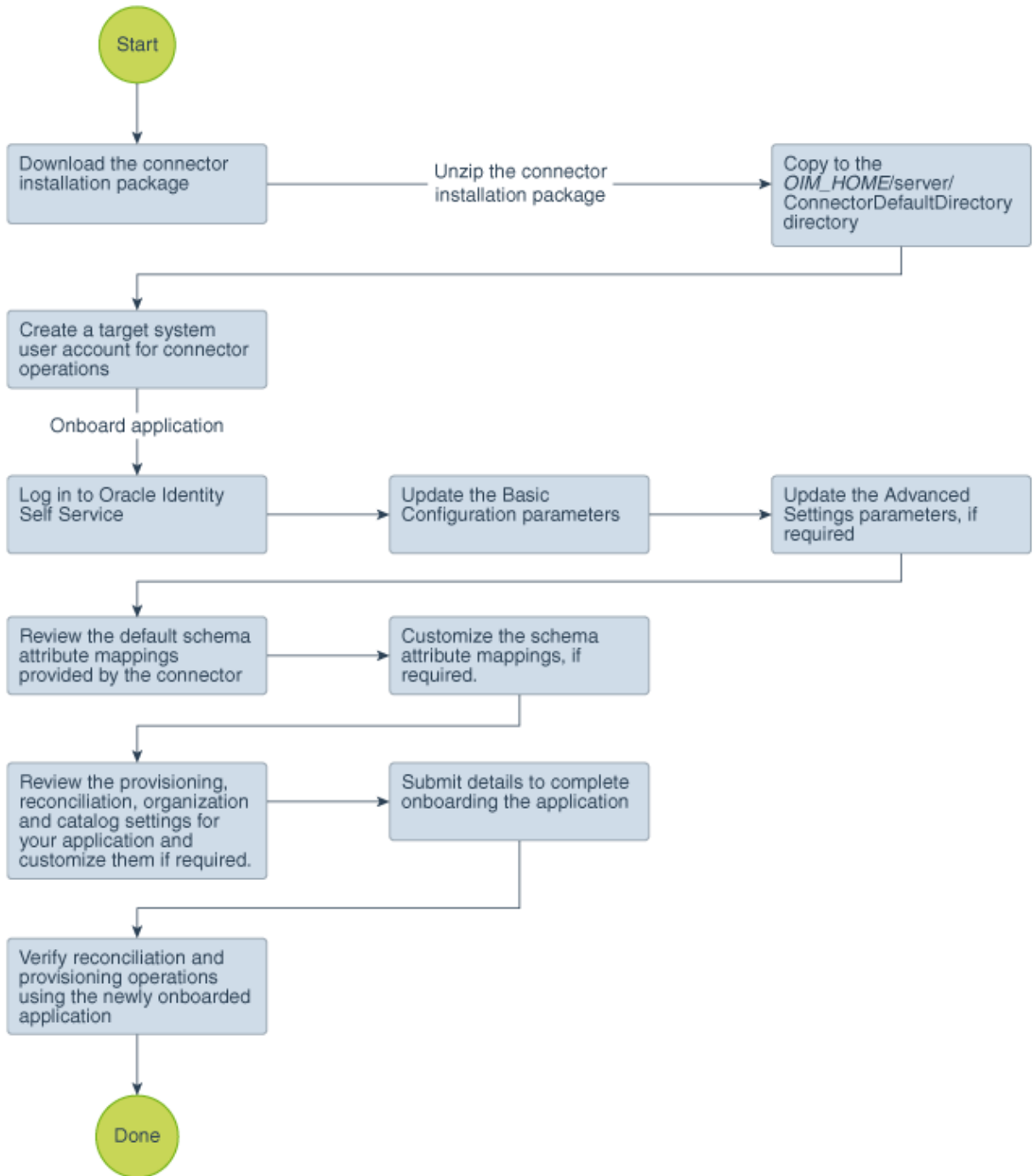
- [Process Flow for Creating an Application By Using the Connector](#)
- [Prerequisites for Creating an Application By Using the Connector](#)
- [Creating an Application By Using the Connector](#)

### 3.2.1 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 3-2](#) is a flowchart depicting high-level steps for creating an application in Oracle Identity Governance by using the connector installation package.

Figure 3-2 Overall Flow of the Process for Creating an Application By Using the Connector



### 3.2.2 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](#)

### 3.2.2.1 Configuring the Target System

Configuring the target system involves creating a developer application and obtaining the consumer key and consumer secret values. It also involves generating the access token and refresh token values and obtaining the account key for your developer account.

To obtain these values, perform the following tasks on the target system:

1. Set up the Developer Sandbox, create a developer application (GoToMeeting App), and obtain the consumer key and consumer secret values that are generated after the application is created.

You provide the consumer key and consumer secret values for the `clientId` and `clientSecret` basic configuration parameters.

2. Generate the access token and refresh token values using the consumer key value that you obtained in Step 1.

You provide the access token and refresh token values for the `customAuthHeaders` basic configuration parameter. You manually generate these tokens for the first time. Subsequently, the GoToMeeting Update Access Token scheduled job is run to renew these values in a periodic manner.

In addition to the access token and refresh token values, the account key value is displayed for your Developer Sandbox account. You provide the account key value for the `uriPlaceholder` basic configuration parameter.

The detailed instructions for performing these preinstallation tasks are available in the GoToMeeting Developer Center documentation at <https://goto-developer.logmeininc.com/>.

### 3.2.2.2 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.

### 3.2.3 Creating an Application By Using the Connector

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

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

 **Note:**

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

1. Create an application in Identity Self Service. The high-level steps are as follows:
  - a. Log in to Identity Self Service either by using the **System Administration** account or an account with the **ApplicationInstanceAdministrator** admin role.
  - b. Ensure that the **Connector Package** option is selected when creating an application.
  - c. Update the basic configuration parameters to include connectivity-related information.
  - d. If required, update the advanced setting parameters to update configuration entries related to connector operations.
  - e. Review the default user account attribute mappings. If required, add new attributes or you can edit or delete existing attributes.
  - f. Review the provisioning, reconciliation, organization, and catalog settings for your application and customize them if required. For example, you can customize the default correlation rules for your application if required.
  - g. Review the details of the application and click **Finish** to submit the application details.

The application is created in Oracle Identity Governance.
  - h. When you are prompted whether you want to create a default request form, click **Yes** or **No**.

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

 **See Also:**

- [Configuring the GoToMeeting 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

## 3.3 Configuring the GoToMeeting Connector

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

- [Basic Configuration Parameters](#)
- [Advanced Settings Parameters](#)
- [Attribute Mappings](#)
- [Rules, Situations, and Responses](#)
- [Reconciliation Jobs](#)

### 3.3.1 Basic Configuration Parameters

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

**Table 3-4 Basic Configuration Parameters for GoToMeeting**

| Parameter          | Mandatory? | Description  |
|--------------------|------------|--|
| authenticationType | Yes        | Type of authentication that is used by your target system. This connector supports authenticating to the target system by using OAuth 2.0 custom authentication type.<br><b>Default value:</b> Other<br>Do <i>not</i> modify the value of the parameter. |
| clientId           | No         | Enter the consumer key value that is generated after creating the developer application.<br><b>Sample value:</b> ABCDEbkTacBC7emdnbABCDEFa96DsEYN<br>See <a href="#">Configuring the Target System</a> for details on obtaining the consumer key value.  |

Table 3-4 (Cont.) Basic Configuration Parameters for GoToMeeting

| Parameter             | Mandatory? | Description  |
|-----------------------|------------|--|
| clientSecret          | No         | Enter the consumer secret value that is generated after creating the developer application.<br><b>Sample value:</b> AB9CDo00abCo2l03<br>See <a href="#">Configuring the Target System</a> for details on obtaining the consumer secret value.  |
| customAuthHeaders     | No         | Enter the access token and refresh token values in the following format:<br>"access_token=ACCESSTOKEN","refresh_token=REFRESHTOKEN"<br>In this format, replace <i>ACCESSTOKEN</i> with the access token value and <i>REFRESHTOKEN</i> with the refresh token value. These values are generated after setting up the Developer Sandbox.<br><b>Sample value:</b><br>access_token=ABabEXAMPLe0Q0ZjABCabc0AbAbC","refresh_token=hABCfd9oABc6abcDeFGabcdXhwRMIHav"<br>See <a href="#">Configuring the Target System</a> for details on obtaining the access token and refresh token values. |
| host                  | Yes        | Enter the host name of your target system.<br><b>Sample value:</b> api.getgo.com   |
| uriPlaceholder        | No         | Enter the account key value that is displayed while generating the access token and refresh token values for your Developer Sandbox account.<br><b>Sample value:</b> "account_key;5253092000266355206"<br>See <a href="#">Configuring the Target System</a> for details on obtaining the account key value.  |
| Connector Server Name | No         | If you have deployed the GoToMeeting connector in the Connector Server, then enter the name of the IT resource of type "Connector Server".<br>By default, this field is blank. If you have deployed the connector in a Java Connector Server, then enter the name of the IT resource for the Connector Server.   |
| port                  | No         | Enter the port number at which the target system is listening.<br><b>Sample value:</b> 443   |
| proxyHost             | No         | Enter the name of the proxy host that is used to connect to an external target system.<br><b>Sample value:</b> proxy.gotomeeting.com   |
| 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.  |
| proxyPort             | No         | Enter the proxy port number.<br><b>Sample value:</b> 80  |
| proxyUser             | No         | Enter the proxy user name of the target system user account that Oracle Identity Governance uses to connect to the target system.<br><b>Sample value:</b> johnsmith  |
| sslEnabled            | No         | If the target system requires SSL connectivity, then set the value of this parameter to <code>true</code> . Otherwise set the value to <code>false</code> .<br><b>Default value:</b> true  |



## 3.3.2 Advanced Settings Parameters

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

**Table 3-5 Advanced Settings Parameters for GoToMeeting**

| Parameter      | Mandatory? | Description   |
|----------------|------------|---|
| nameAttributes | Yes        | <p>This entry holds the name attribute for all the object classes that are handled by the connector.</p> <p><b>Default value:</b><br/>"__ACCOUNT__.firstName", "__GROUP__.name", "__LICENSE__.description"</p> <p>In this default value, the __ACCOUNT__.firstName value implies that the name attribute of the connector for __ACCOUNT__ object class is mapped to firstName, which is the corresponding name attribute for User account in the target system.</p> |

**Table 3-5 (Cont.) Advanced Settings Parameters for GoToMeeting**

| Parameter     | Mandatory? | Description   |
|---------------|------------|---|
| relURIs       | Yes        | <p>This entry holds the relative URL for all operations supported by the connector for each object class.</p> <p><b>Default value:</b></p> <pre>"__ACCOUNT__.licenseKeys.UPDATEOP=/admin/rest/v1/accounts/\${account_key}\$/licenses/\${licenseKeys}\$/users/\${__UID__\$}" , "__ACCOUNT__.CREATEOP=/admin/rest/v1/accounts/\${account_key}\$/users" , "__ACCOUNT__.UPDATEOP=/admin/rest/v1/accounts/\${account_key}\$/users/\${__UID__\$}" , "__ACCOUNT__.SEARCHOP=/admin/rest/v1/accounts/\${account_key}\$/users?\$(Filter Suffix)&amp;pageSize=\$(PAGE_SIZE)&amp;offset=\$(PAGE_OFFSET)\$" , "__ACCOUNT__.DELETEOP=/admin/rest/v1/accounts/\${account_key}\$/users/\${__UID__\$}" , "__ACCOUNT__.__ROLE__.UPDATEOP=/admin/rest/v1/accounts/\${account_key}\$/users/\${__UID__\$}" , "__LICENSE__.SEARCHOP=/admin/rest/v1/accounts/\${account_key}\$/licenses?pageSize=\$(PAGE_SIZE)&amp;offset=\$(PAGE_OFFSET)\$" , "__ACCOUNT__.__LICENSE__.SEARCHOP=/admin/rest/v1/accounts/\${account_key}\$/licenses?pageSize=\$(PAGE_SIZE)&amp;offset=\$(PAGE_OFFSET)\$" , "__GROUP__.SEARCHOP=/admin/rest/v1/accounts/\${account_key}\$/groups? pageSize=\$(PAGE_SIZE)&amp;offset=\$(PAGE_OFFSET)\$" , "__ACCOUNT__.__LICENSE__.ADDATTRIBUTE=/admin/rest/v1/accounts/\${account_key}\$/licenses/\${__LICENSE__.key}\$/users/\${__UID__\$}" , "__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE=/admin/rest/v1/accounts/\${account_key}\$/licenses/\${__LICENSE__.key}\$/users/\${__UID__\$}" , "__ACCOUNT__.groupKey.UPDATEOP=/admin/rest/v1/accounts/\${account_key}\$/groups/\${groupKey}\$/users/\${__UID__\$}"</pre> <p>In this default value, the <code>__ACCOUNT__.CREATEOP=/admin/rest/v1/accounts/\${account_key}\$/users</code> value implies that <code>/admin/rest/v1/accounts/\${account_key}\$/users</code> is the relative URL for all create provisioning operations that are performed on the <code>__ACCOUNT__</code> object class.</p> |
| uidAttributes | Yes        | <p>This entry holds the UID attribute for all the object classes that are handled by the connector.</p> <p><b>Default value:</b></p> <pre>"__ACCOUNT__.key" , "__GROUP__.key" , "__LICENSE__.key"</pre> <p>In this default value, the <code>__ACCOUNT__.key</code> value implies that the <code>__UID__</code> attribute (that is, GUID) of the connector for <code>__ACCOUNT__</code> object class is mapped to key, which is the corresponding UID attribute for User account in the target system.</p>   |

Table 3-5 (Cont.) Advanced Settings Parameters for GoToMeeting

| Parameter                  | Mandatory? | Description  |
|----------------------------|------------|--|
| Bundle Version             | No         | This entry holds the version of the connector bundle class.<br>Do not modify this entry.<br><b>Default value:</b> 12.3.0   |
| Bundle Name                | No         | This entry holds the name of the connector bundle package.<br><b>Default value:</b> org.identityconnectors.genericrest<br>Do not modify this entry.  |
| simpleMultivaluedAttribute | No         | This entry holds the name of the attributes that can hold multiple values.<br><b>Default value:</b> "__ACCOUNT__=primaryLicense"<br>In this default value, the primaryLicense attribute holds the value as License because multiple licenses can be assigned to a user account.  |
| Connector Name             | No         | This entry holds the name of the connector class.<br><b>Default value:</b><br>org.identityconnectors.genericrest.GenericRESTConnector  |
| customPayload              | No         | This entry lists the request payload formats for all the connector operations that are not in standard JSON format.<br><b>Default value:</b><br><pre>"__ACCOUNT__".CREATEOP={\"users\": [{\"email\": \"\$(email)\$\", \"firstName\": \"\$(__NAME__)\$\", \"lastName\": \"\$(lastName)\$\", \"locale\": \"\$(locale)\$\"}], \"groupKey\": \"\$(groupKey)\$\", \"licenseKeys\": [\$(licenseKeys)\$]}</pre> |
| jsonResourcesTag           | No         | This entry holds the JSON tag value that is used during reconciliation for parsing multiple entries in a single payload.<br><b>Default value:</b><br>"__ACCOUNT__=results", "__GROUP__=results", "__LICENSE__=results"   |
| httpHeaderContentType      | No         | This entry holds the content type expected by the target system in the request header.<br><b>Default value:</b> application/json   |
| httpHeaderAccept           | No         | This entry holds the accept type expected from the target system in the request header.<br><b>Default value:</b> application/json  |

**Table 3-5 (Cont.) Advanced Settings Parameters for GoToMeeting**

| Parameter                    | Mandatory? | Description  |
|------------------------------|------------|--|
| opTypes                      | No         | <p>This entry specifies the HTTP operation type for each object class supported by this connector.</p> <p><b>Default value:</b></p> <pre>"__ACCOUNT__.licenseKeys.UPDATEOP=PUT", "__ACCOUNT__.groupKey.UPDATEOP=PUT", "__ACCOUNT__.CREATEOP=POST", "__ACCOUNT__.UPDATEOP=PUT", "__ACCOUNT__.SEARCHOP=GET", "__ACCOUNT__.DELETEOP=DELETE", "__ACCOUNT__.__LICENSE__.UPDATEOP=POST", "__ACCOUNT__.__LICENSE__.DELETEOP=DELETE"</pre> <p>Values are comma separated, and are in the following format:<br/><i>OBJ_CLASS.OP=HTTP_OP</i></p> <p>In this format, <i>OBJ_CLASS</i> is the connector object class, <i>OP</i> is the connector operation (for example, CreateOp, UpdateOp, SearchOp), and <i>HTTP_OP</i> is the HTTP operation (GET, PUT, or POST).</p>  |
| specialAttributeHandling     | No         | <p>This entry lists the <b>special attribute</b>, which is an attribute in an object class that can be managed only through a separate REST API endpoint rather than the same endpoint of the base object class.</p> <p><b>Default value:</b></p> <pre>"__ACCOUNT__.__LICENSE__.ADDATTRIBUTE=SINGLE", "__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE=SINGLE", "__ACCOUNT__.__LICENSE__.CREATEOP=SINGLE", "__ACCOUNT__.__LICENSE__.UPDATEOP=SINGLE", "__ACCOUNT__.licenseKeys.UPDATEOP=SINGLE", "__ACCOUNT__.groupKey.UPDATEOP=SINGLE"</pre> <p>Values are sent to the target system in separate calls, one at a time. In addition, values are comma separated, and are in the following format:<br/><i>OBJ_CLASS.ATTR_NAME.PROV_OP=SINGLE</i></p> <p>For example, the <i>__ACCOUNT__.groupKey.UPDATEOP=SINGLE</i> value in decode implies that during an update provisioning operation, values for the <i>groupKey</i> attribute of the <i>__ACCOUNT__</i> object class is sent to the target system in separate calls, one at a time.</p> |
| specialAttributeTargetFormat | No         | <p>This entry lists the format in which a special attribute is present in the target system response.</p> <p><b>Default value:</b></p> <pre>"__ACCOUNT__.__GROUP__=managedGroupKeys", "__ACCOUNT__.__LICENSE__=licenseKeys"</pre> <p>For example, the <i>__ACCOUNT__.__LICENSE__</i> attribute is present as <i>licenseKeys</i> in the target system response. Values are comma separated, and are presented in the following format:<br/><i>OBJ_CLASS.ATTR_NAME= TARGET_FORMAT</i></p>  |

### 3.3.3 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.

### GoToMeeting User Account Attributes

This table lists the mapping of attribute between the process form fields and GoToMeeting columns. The table also lists whether a specific attribute is used during provisioning or reconciliation and whether it is a matching key field for fetching records during reconciliation.

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

**Table 3-6 Default Attribute Mappings for GoToMeeting User Account**

| Display Name   | Target Attribute | Data Type | Mandatory Provisioning Property? | Provisioning Field? | Recon Field | Key Field? | Case Insensitive? |
|----------------|------------------|-----------|----------------------------------|---------------------|-------------|------------|-------------------|
| User key       | __UID__          | String    | No                               | Yes                 | Yes         | Yes        | NA                |
| First Name     | __NAME__         | String    | Yes                              | Yes                 | Yes         | No         | NA                |
| Last Name      | lastName         | String    | Yes                              | Yes                 | Yes         | No         | NA                |
| Group          | groupKey         | String    | No                               | Yes                 | Yes         | No         | NA                |
| Locale         | locale           | String    | Yes                              | Yes                 | Yes         | No         | NA                |
| Email          | email            | String    | Yes                              | Yes                 | Yes         | Yes        | Yes               |
| PrimaryLicense | licenseKeys      | String    | Yes                              | Yes                 | Yes         | No         | NA                |
| IT Resource    | NA               | Long      | Yes                              | No                  | Yes         | Yes        | NA                |

Figure 3-3 shows the default GoToMeeting User account attribute mapping.

**Figure 3-3 Default Attribute Mappings for GoToMeeting User Account**

GoToMeeting User

+ Add Attribute

| Application Attribute |                |                  |           | Provisioning Property               |                                     | Reconciliation Properties           |                                     |                                     |                          |
|-----------------------|----------------|------------------|-----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| Identity Attribute    | Display Name   | Target Attribute | Data Type | Mandatory                           | Provisioning Field                  | Recon Field                         | Key Field                           | Case Insensitive                    |                          |
| Enter a value         | User key       | __UID__          | String    | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Enter a value         | First Name     | __NAME__         | String    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |
| Enter a value         | Last Name      | lastName         | String    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |
| Enter a value         | Group          | groupKey         | String    | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |
| Enter a value         | IT Resource    |                  | Long      | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| Enter a value         | Locale         | locale           | String    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |
| Enter a value         | Email          | email            | String    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Enter a value         | PrimaryLicense | licenseKeys      | String    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |

### Licenses Entitlement Attributes

This is the default mapping of attributes between process form fields and licenses-related columns in the target system. The table lists whether a given attribute is mandatory during provisioning. It also lists whether a given attribute is used during reconciliation and whether it is a matching key field for fetching records during reconciliation.

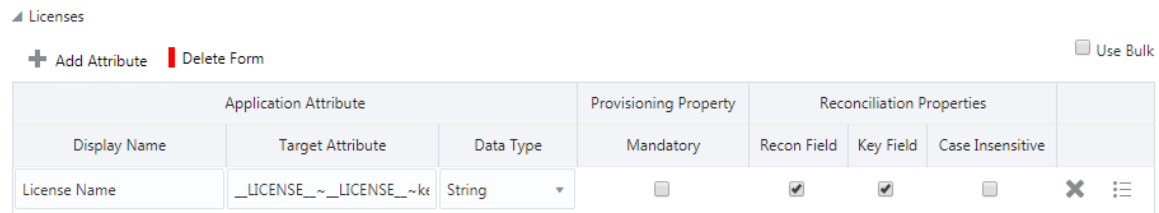
If required, you can edit the default attribute mappings by adding new attributes or deleting existing attributes as described in *Creating a Target Application of Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-7 Default Attribute Mappings for Licenses Entitlement**

| Display Name | Application Attribute               | Data Type | Mandatory Provisioning Property? | Recon Field | Key Field? | Case Insensitive? |
|--------------|-------------------------------------|-----------|----------------------------------|-------------|------------|-------------------|
| License Name | __LICENSE__<br>~__LICENSE_<br>_~key | String    | No                               | Yes         | Yes        | No                |

Figure 3-4 shows the default Licenses entitlement mapping.

**Figure 3-4 Default Attribute Mappings for Licenses Entitlement**



## 3.3.4 Rules, Situations, and Responses

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

### Predefined Identity Correlation Rules

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

Table 3-8 lists the default simple correlation rule for the GoToMeeting connector. If required, you can edit the default correlation rule or add new rules. You can create complex correlation rules also. For more information about adding or editing simple or complex correlation rules, see *Updating Identity Correlation Rule in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-8 Predefined Identity Correlation Rule for GoToMeeting**

| Target Attribute | Element Operator | Identity Attribute | Case Sensitive? |
|------------------|------------------|--------------------|-----------------|
| email            | Equals           | Email              | No              |

In this identity rule:

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

Figure 3-5 shows the simple correlation rule for the GoToMeeting connector.

**Figure 3-5 Simple Correlation Rule for GoToMeeting**

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

Preview Settings

Provisioning | Reconciliation | Organization | Catalog

Below are pre-defined rules that have been set for you.

Identity Correlation Rule

Choose Type of Correlation Rule

Simple Correlation Rule  Complex Correlation Rule

+ Add Rule Element

| Target Attribute | Element Operator | Identity Attribute | Case Sensitive           | Delete                           |
|------------------|------------------|--------------------|--------------------------|----------------------------------|
| email            | Equals           | Email              | <input type="checkbox"/> | <input type="button" value="X"/> |

Rule Operator

AND

### Predefined Situations and Responses

The GoToMeeting 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 3-9 lists the default situations and responses for the GoToMeeting 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 3-9 Predefined Situations and Responses for GoToMeeting**

| Situation              | Response       |
|------------------------|----------------|
| No Matches Found       | None           |
| One Entity Match Found | Establish Link |

**Table 3-9 (Cont.) Predefined Situations and Responses for GoToMeeting**

| Situation               | Response       |
|-------------------------|----------------|
| One Process Match Found | Establish Link |

Figure 3-6 shows the situations and responses that the connector provides by default.

**Figure 3-6 Predefined Situations and Responses for GoToMeeting**

Below are pre-defined Situations and Responses that have been set for you

▲ Situations And Responses

+ Add

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

### 3.3.5 Reconciliation Jobs

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

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*.

#### GoToMeeting Full User Reconciliation Job

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

**Table 3-10 Parameters of the GoToMeeting Full User Reconciliation Job**

| Parameter        | Value   |
|------------------|---|
| 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.<br>Do not modify this value. |



**Table 3-10 (Cont.) Parameters of the GoToMeeting Full User Reconciliation Job**

| Parameter           | Value  |
|---------------------|--|
| Filter Suffix       | Enter the search filter for fetching user records from the target system during a reconciliation run.<br><b>Sample value:</b> <code>filter=firstName%20%3D%20%22.*UserA.*%22</code><br>See <a href="#">Performing Limited Reconciliation</a> . |
| Object Type         | Type of object you want to reconcile.<br><b>Default value:</b> <code>User</code>   |
| Scheduled Task Name | This attribute holds the name of the scheduled task.<br><b>Default value:</b> <code>GoToMeeting Full User Reconciliation</code><br>Do not modify this value.   |

### Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- **GoToMeeting Licenses Lookup Reconciliation:** Use this job to reconcile all licenses-related data in the target system into lookup fields in Oracle Identity Governance.
- **GoToMeeting Group Lookup Reconciliation:** Use this job to reconcile all group data in the target system into lookup fields in Oracle Identity Governance.

The parameters for all the reconciliation jobs are the same.

**Table 3-11 Parameters of the Reconciliation Jobs for Entitlements**

| Parameter        | Description   |
|------------------|---|
| Application Name | Name of the application you created for your target system. This value is the same as the value that you provided for the Application Name field while creating your target application.<br>Do not modify this value.   |
| Lookup Name      | This parameter holds the name of the lookup definition that maps each lookup definition with the data source from which values must be fetched.<br>Depending on the reconciliation job that you are using, the default values are as follows: <ul style="list-style-type: none"> <li>• <b>GoToMeeting Licenses Lookup Reconciliation:</b> <code>Lookup.GTM.License</code></li> <li>• <b>GoToMeeting Group Lookup Reconciliation:</b> <code>Lookup.GTM.Group</code></li> </ul> |

**Table 3-11 (Cont.) Parameters of the Reconciliation Jobs for Entitlements**

| Parameter          | Description  |
|--------------------|--|
| Object Type        | <p>Enter the type of object whose values must be synchronized.</p> <p>Depending on the scheduled job that you are using, the default values are as follows:</p> <ul style="list-style-type: none"> <li>GoToMeeting Licenses Lookup Reconciliation: <code>__LICENSE__</code></li> <li>GoToMeeting Group Lookup Reconciliation: <code>__GROUP__</code></li> </ul> <p>Do not modify this value.</p> |
| Code Key Attribute | <p>Enter the name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute).</p> <p><b>Default value:</b> <code>__UID__</code></p> <p>Do not modify this value.</p>  |
| Decode Attribute   | <p>Enter the name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute).</p> <p><b>Default value:</b> <code>__NAME__</code></p>  |

## 3.4 Performing the Postconfiguration Tasks for the GoToMeeting Connector

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

Postconfiguration tasks for the connector involves configuring Oracle Identity Governance, populating Entitlement schema from child process form table and harvest roles, application instances, and entitlements into the catalog, 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 Governance](#)
- [Harvesting Entitlements and Sync Catalog](#)
- [Managing Logging](#)
- [Configuring the IT Resource for the Connector Server](#)
- [Localizing Field Labels in UI Forms](#)
- [Configuring SSL for the Connector](#)

### 3.4.1 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](#)

### 3.4.1.1 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*.

### 3.4.1.2 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.

### 3.4.1.3 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*.

### 3.4.1.4 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*

### 3.4.2 Harvesting Entitlements and Sync Catalog

You can populate Entitlement schema from child process form table, and harvest roles, application instances, and entitlements into catalog. You can also load catalog metadata.

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in [Reconciliation Jobs](#).
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

#### See Also:

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

## 3.4.3 Managing Logging

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](#)

### 3.4.3.1 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 3-12](#).

**Table 3-12 Log Levels and ODL Message Type:Level Combinations**

| Java Level                         | ODL Message Type:Level        |
|------------------------------------|-------------------------------|
| <code>SEVERE.intValue()+100</code> | <code>INCIDENT_ERROR:1</code> |
| <code>SEVERE</code>                | <code>ERROR:1</code>          |
| <code>WARNING</code>               | <code>WARNING:1</code>        |
| <code>INFO</code>                  | <code>NOTIFICATION:1</code>   |

**Table 3-12 (Cont.) Log Levels and ODL Message Type:Level Combinations**

| Java Level | ODL Message Type:Level |
|------------|------------------------|
| 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.

### 3.4.3.2 Enabling Logging

You perform this procedure to enable logging in Oracle WebLogic Server.

To enable logging:

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

```
<log_handler name='GoToMeeting-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.GENERICREST"
level=" [LOG_LEVEL]" useParentHandlers="false">
  <handler name="GoToMeeting-handler" />
  <handler name="console-handler" />
</logger>
```

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

- b. Replace both occurrences of [LOG\_LEVEL] with the ODL message type and level combination that you require. [Understanding Log Levels](#) lists

the supported message type and level combinations. Similarly, replace [FILE\_NAME] with the full path and name of the log file in which you want log messages to be recorded. The following blocks show sample values for [LOG\_LEVEL] and [FILE\_NAME]:

```
<log_handler name='GoToMeeting-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\oim_server1\logs\oim_server1-diagnostic-1.log' />  
<property name='format' value='ODL-Text' />  
<property name='useThreadName' value='true' />  
<property name='locale' value='en' />  
<property name='maxFileSize' value='5242880' />  
<property name='maxLogSize' value='52428800' />  
<property name='encoding' value='UTF-8' />  
</log_handler>
```

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

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

### 3.4.4 Configuring the IT Resource for the Connector Server

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

After you create the application for your target system, you must create an IT resource for the Connector Server as described in *Creating IT Resource of Oracle Fusion Middleware Administering Oracle Identity Governance*. While creating the IT resource, ensure to use to select **Connector Server** from the **IT Resource Type** list.

In addition, specify values for the parameters of the IT resource for the Connector Server listed in [Table 3-13](#).

**Table 3-13 Parameters of the IT Resource for the Connector Server**

| Parameter | Description   |
|-----------|---|
| Host      | Enter the host name or IP address of the computer hosting the Connector Server.<br>Sample value: myhost.com   |
| Key       | Enter the key for the Connector Server.   |
| Port      | Enter the number of the port at which the Connector Server is listening.<br>By default, this value is blank. You must enter the port number that is displayed on the terminal when you start the Connector Server.<br>Sample value: 8759  |
| 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.<br>Recommended value: 0<br>A value of 0 means that the connection never times out.  |
| UseSSL    | Enter <code>true</code> to specify that you will configure SSL between Oracle Identity Governance and the Connector Server. Otherwise, enter <code>false</code> .<br>Default value: <code>false</code><br><b>Note:</b> It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, see <i>Setting SSL for Connector Server and OIM in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance</i> . |

### 3.4.5 Localizing Field Labels in UI Forms

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

To localize a field label that is added to 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 GoToMeeting Application Instance. The original code is:

```
<trans-unit
id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_GTM_USER_FIRSTNAME__c_description']}>">
<source>First Name</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.GoToMeetingForm.e
ntity.GoToMeetingFormEO.UD_GTM_USER_ FIRSTNAME__c_LABEL">
<source>First Name</source>
<target/>
</trans-unit>
```

In this text, *GoToMeetingForm* is the current form instance name associated with the GoToMeeting application instance.

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

```
global.udf.UD_GTM_USER_FIRSTNAME=\u540D
```

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

```
<trans-unit
id="$
{adfBundle[ 'oracle.adf.businesseditor.model.util.BaseRuntimeResou
rceBundle' ]
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity
.userEO.UD_GTM_USER_FIRSTNAME__c_description' ]}>">
<source>First Name</source>
<target>\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.GoToMeetingForm.e
ntity.GoToMeetingFormEO.UD_GTM_USER_ FIRSTNAME__c_LABEL">
<source>First Name</source>
<target>\u540D</target>
</trans-unit>
```

- f. Repeat Step 6 a through Step 6 d for all attributes of the process form.
  - g. Save the file as `BizEditorBundle_LANG_CODE.xlf`. In this file name, replace `LANG_CODE` with the code of the language to which you are localizing. Sample file name: `BizEditorBundle_ja.xlf`.
7. Repackage the ZIP file and import it into MDS.

#### See Also:

Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for more information about exporting and importing metadata files

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

## 3.4.6 Configuring SSL for the Connector

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

To configure SSL:

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

```
keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -file  
CERT_FILE_NAME -storepass PASSWORD
```

In this command:

- *CERT\_FILE\_NAME* is the full path and name of the certificate file
- *PASSWORD* is the password of the keystore.

The following is a sample value for this command:

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

## 3.5 Using the GoToMeeting Connector

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

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

### 3.5.1 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](#)
- [Reconciling Large Number of Records](#)

#### 3.5.1.1 Performing Full Reconciliation

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

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

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

If the target system contains more number of records than what it can return in a single response, then use the Flat File connector to perform full reconciliation. See [Reconciling Large Number of Records](#).

### 3.5.1.2 Performing Limited Reconciliation

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

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

While creating the application, follow the instructions in [Configuring Reconciliation Jobs](#) to specify attribute values.

This connector provides a Filter Suffix attribute (a scheduled task attribute) that allows you to use any of the attributes of the target system to filter target system records. You specify a value for the Filter Suffix attribute while configuring the user reconciliation scheduled job.

#### Note:

If the target system contains more number of records than what it can return in a single response, then use the Flat File connector to perform limited reconciliation. See [Reconciling Large Number of Records](#).

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

For more information on GoToMeeting filters, see the filtering information related to GoToMeeting Administration REST API Implementation on the GoToMeeting Developer Center page at <https://goto-developer.logmeininc.com/>.

### 3.5.1.3 Reconciling Large Number of Records

During a reconciliation run, if the target system contains more number of records than what it can return in a single response, you can fetch all the records into Oracle Identity Governance using the Flat File connector.

The Flat File connector consumes information in a flat file, and generates connector metadata using the metadata generation utility.

To reconcile a large number of records from the target system into Oracle Identity Governance:

1. Export all users in the target system to a flat file.
2. Copy the flat file to a location that is accessible from Oracle Identity Governance.
3. Create a schema file representing the structure of the flat file. See *Creating a Schema File in Oracle Identity Manager Connector Guide for Flat File*.
4. Install the Flat File connector. See *Running the Connector Installer in Oracle Identity Manager Connector Guide for Flat File*.

5. Configure the Flat File IT resource. See *Configuring the IT Resource in Oracle Identity Manager Connector Guide for Flat File*.
6. Configure and run the Flat File Accounts Loader scheduled job.

While configuring this scheduled job, ensure that you set the value of the **Target IT Resource Name** attribute to `GoToMeeting` and **Target Resource Object Name** to `GoToMeeting User`.

See *Flat File Accounts Loader and IT\_RES\_NAME Flat File Accounts Loader in Oracle Identity Manager Connector Guide for Flat File* for information about the attributes of the Flat File Accounts Loader scheduled job.

## 3.5.2 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.

### 3.5.3 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

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

 **See Also:**

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

### 3.5.4 Uninstalling the GoToMeeting 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, `GoToMeeting User; GoToMeeting 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*.

## 3.6 Extending the Functionality of the GoToMeeting Connector

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

- [Configuring the Connector for Multiple Installations of the Target System](#)
- [Configuring Transformation and Validation of Data](#)
- [Configuring Action Scripts](#)

### 3.6.1 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*.

### 3.6.2 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*.

### 3.6.3 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*.

## 3.7 Upgrading the GoToMeeting Connector

If you have already deployed the 11.1.1.5.0 version of the GoToMeeting 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



## 3.7.1 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.

## 3.7.2 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.

## 3.7.3 Postupgrade Steps

Postupgrade steps involve uploading new connector JARs, configuring the upgraded IT resource of the source connector, updating the Connector Server JARs, and deleting duplicate entries for lookup definitions.

Perform the following procedure:

1. Upload new connector JARs as follows:

- a. Run the Upload JARs utility (`$ORACLE_HOME/bin/UploadJars.sh`) for uploading connector JARs.
  - b. Upload `bundle/org.identityconnectors.genericrest-12.3.0.jar` as ICFBundle.
  - c. Upload `lib/gtm-update-accesstoken.jar` as ScheduleTask.
2. Replicate all changes made to the Form Designer of the Design Console in a new UI form as follows:
  - a. Log in to Oracle Identity System Administration.
  - b. Create and activate a sandbox.
  - c. Create a new UI form to view the upgraded fields.
  - d. 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 (created in step 2.c) and then save the application instance.
  - e. Publish the sandbox.
3. Configure the upgraded IT resource of the source connector.
4. If you are using the Connector Server, update the Connector Server JARs as follows:
  - a. Navigate to the bundles directory in your Connector Server directory, and replace the existing connector server bundle JAR with the new JAR.
  - b. Restart the Connector Server.
5. If any of the previous connector artifacts are retained after a successful upgrade operation, then log in to Oracle Identity Manager Design Console and delete the following duplicate entries:
  - For the `Lookup.GoToMeeting.Configuration` lookup definition:

| Code Key | Decode   |
|----------|--|
| relURIs  | <pre> "__ACCOUNT__.licenseKeys.UPDATEOP=/admin/rest/v1/ accounts/\${account_key}\$/licenses/\${licenseKeys}\$/users/\$ (__UID__\$", "__ACCOUNT__.CREATEOP=/admin/rest/v1/accounts/\$ (account_key)\$/users", "__ACCOUNT__.UPDATEOP=/admin/ rest/v1/accounts/\${account_key}\$/users/\${__UID__\$", "__ACCOUNT__.SEARCHOP=/admin/rest/v1/accounts/\$ (account_key)\$/users/\${Filter Suffix}\$", "__ACCOUNT__.DELETEOP=/admin/ rest/v1/accounts/\${account_key}\$/users/\${__UID__\$", "__LICENSE__.SEARCHOP=/admin/rest/v1/accounts/\$ (account_key)\$/licenses", "__GROUP__.SEARCHOP=/admin/rest/v1/accounts/\$ (account_key)\$/groups", "__ACCOUNT__.__LICENSE__.ADDATTRIBUTE=/ admin/rest/v1/accounts/\${account_key}\$/licenses/\$ (__LICENSE__.key)\$/users/\${__UID__\$", "__ACCOUNT__.__LICENSE__.REMOVEATTRIBUTE=/ admin/rest/v1/accounts/\${account_key}\$/licenses/\$ (__LICENSE__.key)\$/users/\${__UID__\$", "__ACCOUNT__.groupKey.UPDATEOP=/admin/rest/v1/ accounts/\${account_key}\$/groups/\${groupKey}\$/users/\$ (__UID__\$" </pre> |

- For the Lookup.GTM.UM.ReconAttrMap lookup definition:

| Code Key                         | Decode             |
|----------------------------------|--------------------|
| PrimaryLicense[LO<br>OKUP]       | PARENT.licenseKeys |
| Licenses~License<br>Name[LOOKUP] | CHILD.licenseKeys  |

6. If any attribute mappings are missing for custom attributes, log in to Oracle Identity Manager Design Console and update the mappings.

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:**

- [Configuring Oracle Identity Governance](#) for information about creating, activating, or publishing a sandbox and creating a new UI form
- 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

## 3.8 Known Issues and Workarounds for the GoToMeeting Connector

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

The following is an issue associated with the target system:

### **An Error Occurs While Disabling a GoToMeeting Account**

If you try to disable a GoToMeeting account from Oracle Identity Governance for the first time, the disable task is rejected and the following message appears in the resource history of the account:

```
Disable operation not supported by target.
```

If you try to disable the same account more than once, then an error occurs with a message stating that duplicate schedule item for this task does not allow multiple entries. This is because the **Allow Multiple Instances** check box is not selected for the **Disable User** process task.

#### **Workaround:**

You can resolve this error from the Process Definition form of Oracle Identity Manager Design Console. To do so, perform the following steps:

1. Expand **Process Management** and double-click **Process Definition**.
2. Search for and open the **GoToMeeting User** process definition.
3. On the Tasks tab, double-click the row heading of the **Disable User** process task.
4. On the General tab of the Editing Task: Disable User dialog box, select the **Allow Multiple Instances** check box.
5. Click the Save icon.

# A

## Files and Directories in the GoToMeeting Connector Package

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

 **Note:**

If you have integrated Oracle Identity Governance with GoToMeeting using the OIG AD connector, see Files and Directories in the Microsoft Active Directory User Management Connector Installation Package in *Oracle Identity Governance Configuring the Microsoft Active Directory User Management Application* for a list of the files and directories in the OIG AD connector installation package.

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

| File in the Installation Media Directory                 | Description  |
|--|--|
| bundle/<br>org.identityconnectors.genericrest-12.3.0.jar | This JAR is the ICF connector bundle.  |
| lib/gtm-update-accesstoken.jar                           | This JAR is used for running the GoToMeeting Update Access Token scheduled task.   |
| configuration/GoToMeeting-CI-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.<br><b>Note:</b> A <b>resource bundle</b> is a file containing localized versions of the text strings that include GUI element labels and messages. |

**Table A-1 (Cont.) Files and Directories in the GoToMeeting Connector Installation Package**

| File in the Installation Media Directory | Description   |
|--|---|
| xml/GoToMeeting-ConnectorConfig.xml      | <p>This XML file contains definitions for the following connector objects:</p> <ul style="list-style-type: none"> <li>• IT resource definition</li> <li>• Process forms</li> <li>• Process tasks and adapters</li> <li>• Lookup definitions</li> <li>• Resource objects</li> <li>• Process definition</li> <li>• Scheduled tasks</li> <li>• Reconciliation rules</li> </ul> |
| xml/GoToMeeting-pre-config.xml           | <p>This XML file contains lookup definitions for the GoToMeeting Update Access Token scheduled task.</p>  |
| xml/GoToMeeting-target-template.xml      | <p>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.</p>                       |