

# Oracle® Identity Governance

## Configuring the Microsoft Active Directory User Management Application



12c (12.2.1.3.0)

F12370-13

August 2023

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Identity Governance Configuring the Microsoft Active Directory User Management Application, 12c (12.2.1.3.0)

F12370-13

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

Primary Author: Oracle Corporation

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

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

# Contents

## Preface

---

Audience	xiii
Documentation Accessibility	xiii
Related Documents	xiii
Conventions	xiii

## What's New In This Guide?

---

Software Updates	xv
Documentation-Specific Updates	xv

## 1 About the Microsoft Active Directory User Management Connector

---

1.1	Certified Components	1-2
1.2	Usage Recommendation	1-5
1.3	Certified Languages	1-6
1.4	Supported Connector Operations	1-7
1.5	Connector Architecture	1-7
1.6	Password Synchronization	1-11
1.7	Supported Connector Features Matrix	1-11
1.8	Connector Features	1-12
1.8.1	Full and Incremental Reconciliation	1-12
1.8.2	Limited Reconciliation	1-12
1.8.3	Batched Reconciliation	1-12
1.8.4	Reconciliation of Deleted Groups	1-13
1.8.5	Transformation and Validation of Account Data	1-13
1.8.6	Support for Connector Server	1-13
1.8.7	Connection Pooling	1-13
1.8.8	Support for Connector Operations Across Domains	1-14
1.8.9	Support for Adding the Group Name (pre-Windows 2000) Attribute	1-14
1.8.10	Support for Provisioning Groups of the Security Group - Universal Group Type	1-14
1.8.11	Support for Scripting Languages	1-14

## 2 Creating an Application By Using the Microsoft Active Directory User Management Connector

---

2.1	Process Flow for Creating an Application By Using the Connector	2-1
2.2	Prerequisites for Creating an Application By Using the Connector	2-3
2.2.1	Downloading the Connector Installation Package	2-3
2.2.2	Creating a Target System User Account for Connector Operations	2-3
2.2.2.1	Creating a User Account for Connector Operations in Microsoft Active Directory	2-4
2.2.2.2	Creating a User Account for Connector Operations in Microsoft AD LDS	2-4
2.2.3	Assigning Permissions to Perform Delete User Reconciliation Runs	2-5
2.2.4	Delegating Control for Organizational Units and Custom Object Classes	2-6
2.3	Installing the Microsoft Active Directory User Management Connector in the Connector Server	2-7
2.4	Creating an Application By Using the Connector	2-8

## 3 Configuring the Microsoft Active Directory User Management Connector

---

3.1	Basic Configuration Parameters	3-1
3.2	Advanced Settings Parameters	3-6
3.3	Attribute Mappings	3-9
3.3.1	Attribute Mappings for a Target Application	3-9
3.3.2	Attribute Mappings for an Authoritative Application	3-14
3.4	Correlation Rules for the Connector	3-16
3.4.1	Correlation Rules for a Target Application	3-16
3.4.2	Correlation Rules for an Authoritative Application	3-18
3.5	Reconciliation Jobs for the Connector	3-21
3.5.1	Reconciliation Jobs for a Target Application	3-21
3.5.2	Reconciliation Jobs for an Authoritative Application	3-28

## 4 Performing the Postconfiguration Tasks for the Microsoft Active Directory User Management Connector

---

4.1	Configuring Oracle Identity Governance	4-1
4.1.1	Creating and Activating a Sandbox	4-2
4.1.2	Creating a New UI Form	4-2
4.1.3	Publishing a Sandbox	4-2
4.1.4	Updating an Existing Application Instance with a New Form	4-2
4.2	Configuring the IT Resource for the Target System	4-3
4.3	Configuring the IT Resource for the Connector Server	4-7

4.4	Harvesting Entitlements and Sync Catalog	4-7
4.5	Enabling Logging for Microsoft Active Directory User Management Connector	4-8
4.5.1	Configuring Log File Rotation	4-9
4.6	Localizing Field Labels in UI Forms	4-10
4.7	Configuring the Connector for Provisioning Organizations	4-12
4.8	Enabling and Disabling the Passwords Must Meet Complexity Requirements Policy setting	4-12
4.9	Configuring SSL for Microsoft Active Directory and Microsoft AD LDS	4-13
4.9.1	Prerequisites	4-14
4.9.2	Configuring SSL Between Connector Server and Microsoft Active Directory	4-14
4.9.3	Configuring SSL Between Connector Server and Microsoft AD LDS	4-14
4.9.4	Configuring SSL Between Oracle Identity Governance and Connector Server	4-15
4.9.4.1	Exporting the Certificate	4-16
4.9.4.2	Configuring the Connector Server for SSL	4-16
4.9.4.3	Configuring Oracle Identity Governance for SSL	4-16
4.10	Setting Up the Lookup Definition for the Ignore Event API	4-17
4.10.1	Understanding the Ignore Event Disabled Entry	4-17
4.10.2	Adding the Ignore Event Disabled Entry	4-17

## 5 Using the Microsoft Active Directory User Management Connector

---

5.1	Guidelines on Using the Microsoft Active Directory User Management Connector	5-1
5.1.1	Guidelines on Configuring Reconciliation	5-2
5.1.2	Guidelines on Performing Provisioning Operations	5-3
5.2	Configuring Reconciliation	5-5
5.2.1	Performing Full Reconciliation and Incremental Reconciliation	5-5
5.2.2	Performing Limited Reconciliation	5-6
5.2.2.1	About Limited Reconciliation	5-6
5.2.2.2	Performing Limited Reconciliation By Using Filters	5-6
5.2.2.3	Performing Limited Reconciliation By Using the Search Base Attribute	5-8
5.2.3	Performing Batched Reconciliation	5-9
5.3	Scheduled Jobs for Lookup Field Synchronization	5-10
5.4	Configuring and Running Group Reconciliation	5-11
5.4.1	Reconciling Target System Groups into Individual Organizations	5-11
5.4.2	Reconciling Target System Groups a Single Organization	5-12
5.5	Configuring and Running Organization Reconciliation	5-12
5.6	Configuring Reconciliation Jobs	5-13
5.7	Performing Provisioning Operations	5-14
5.8	Connector Objects Used for Groups Management	5-15
5.8.1	Preconfigured Lookup Definitions for Group Operations	5-15
5.8.1.1	Lookup.ActiveDirectory.GM.Configuration	5-15
5.8.1.2	Lookup.ActiveDirectory.GM.ProvAttrMap	5-16

5.8.1.3	Lookup.ActiveDirectory.GM.ReconAttrMap	5-17
5.8.1.4	Lookup.ActiveDirectory.GM.ProvValidation	5-17
5.8.1.5	Lookup.ActiveDirectory.GM.ReconTransformation	5-18
5.8.1.6	Lookup.ActiveDirectory.GM.ReconValidation	5-18
5.8.1.7	Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults	5-18
5.8.1.8	Lookup.ActiveDirectory.GroupTypes	5-18
5.8.2	Reconciliation Scheduled Jobs for Groups Management	5-19
5.8.2.1	Active Directory Group Recon	5-19
5.8.2.2	Active Directory Group Delete Recon	5-20
5.8.3	Reconciliation Rules and Action Rules for Groups Management	5-21
5.8.3.1	Reconciliation Rule for Groups	5-22
5.8.3.2	Reconciliation Action Rules for Groups	5-22
5.8.3.3	Viewing Reconciliation Rules	5-22
5.8.3.4	Viewing Reconciliation Action Rules	5-23
5.9	Connector Objects Used for Organizational Units Management	5-24
5.9.1	Preconfigured Lookup Definitions for Organizational Unit Operations	5-24
5.9.1.1	Lookup.ActiveDirectory.OM.Configuration	5-25
5.9.1.2	Lookup.ActiveDirectory.OM.Configuration.Trusted	5-26
5.9.1.3	Lookup.ActiveDirectory.OM.ProvAttrMap	5-26
5.9.1.4	Lookup.ActiveDirectory.OM.ReconAttrMap	5-26
5.9.1.5	Lookup.ActiveDirectory.OM.ProvValidation	5-27
5.9.1.6	Lookup.ActiveDirectory.OM.ReconTransformation	5-27
5.9.1.7	Lookup.ActiveDirectory.OM.ReconValidation	5-27
5.9.1.8	Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted	5-27
5.9.1.9	Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults	5-28
5.9.2	Reconciliation Scheduled Job for Organization Unit Management	5-28
5.9.3	Reconciliation Rules and Action Rules for Organizational Units Management	5-29
5.9.3.1	Reconciliation Rule for Organizational Units	5-30
5.9.3.2	Reconciliation Action Rules for Organizational Units	5-30
5.9.3.3	Viewing Reconciliation Rules	5-30
5.9.3.4	Viewing Reconciliation Action Rules	5-31
5.10	Uninstalling the Connector	5-32

## 6 Extending the Functionality of the Microsoft Active Directory User Management Connector

---

6.1	Adding Custom Fields for Target Resource Reconciliation	6-1
6.1.1	Adding Custom Fields for Target Resource Reconciliation of Users	6-2
6.1.2	Adding Custom Fields for Target Resource Reconciliation of Groups and Organizational Units	6-3
6.2	Adding New Multivalued Fields for Target Resource Reconciliation	6-5

6.2.1	Adding New Multivalued Fields for Target Resource Reconciliation of Users	6-5
6.2.2	Adding New Multivalued Fields for Target Resource Reconciliation of Groups and Organizational Units	6-6
6.3	Adding Custom Fields for Provisioning	6-9
6.3.1	Adding Custom Fields for Provisioning Users	6-9
6.3.2	Adding Custom Fields for Provisioning Groups and Organizational Units	6-10
6.3.2.1	Adding a New Field on the Process Form	6-10
6.3.2.2	Replicating Form Designer Changes to a New UI Form	6-10
6.3.2.3	Creating an Entry in the Provisioning Lookup Definition	6-11
6.3.2.4	Enabling Update Provisioning Operations on the Custom Field	6-11
6.3.2.5	Updating the Request Dataset	6-13
6.3.2.6	Clearing Content Related to Request Datasets from the Server Cache	6-14
6.3.2.7	Importing Request Datasets	6-14
6.4	Adding New Multivalued Fields for Provisioning	6-14
6.4.1	Adding New Multivalued Fields for Provisioning Users	6-15
6.4.2	Adding New Multivalued Fields for Provisioning Groups and Organizational Units	6-15
6.4.2.1	Creating an Entry in the Provisioning Lookup Definition	6-16
6.4.2.2	Enabling Update Provisioning Operations on the Multivalued Field	6-16
6.4.2.3	Updating the Request Dataset	6-18
6.4.2.4	Clearing Content Related to Request Datasets from the Server Cache	6-19
6.4.2.5	Importing Request Datasets	6-19
6.5	Adding Terminal Services Fields for Reconciliation and Provisioning	6-19
6.6	Adding the Group Name (pre-Windows 2000) Attribute	6-20
6.6.1	About the Group Name (pre-Windows 2000) Attribute	6-21
6.6.2	Adding the Group Name Pre Windows Field for Reconciliation	6-21
6.6.3	Adding the Group Name Pre Windows Field for Provisioning	6-23
6.6.3.1	Adding the Group Name Pre Windows Field	6-23
6.6.3.2	Updating the Lookup.ActiveDirectory.GM.ProvAttrMap Lookup Definition	6-23
6.6.3.3	Enabling Update Provisioning Operations on the Group Name Pre Windows Field	6-24
6.6.3.4	Updating Adapters	6-25
6.6.3.5	Updating the Request Dataset	6-26
6.6.3.6	Running the PurgeCache Utility	6-27
6.6.3.7	Importing the Request Dataset Definitions into MDS	6-27
6.7	Configuring Transformation and Validation Of Data	6-27
6.7.1	About Configuring Transformation and Validation of Data	6-27
6.7.2	Configuring Transformation of Data During Reconciliation for Groups and Organizational Units	6-28
6.7.3	Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units	6-29
6.8	Action Scripts	6-31

6.8.1	Action Scripts for Users	6-31
6.8.1.1	About Configuring Action Scripts for Users	6-31
6.8.1.2	Running a Custom PowerShell Script for Users	6-31
6.8.1.3	Running Actions Using Visual Basic Scripts for Users	6-33
6.8.1.4	Important Notes on Running Actions Scripts for Users	6-34
6.8.1.5	Guidelines on Creating Scripts for Users	6-34
6.8.2	Action Scripts for Groups and Organizational Units	6-34
6.8.2.1	About Configuring Action Scripts for Groups and Organizational Units	6-35
6.8.2.2	Running a Custom PowerShell Script for Groups and Organizational Units	6-35
6.8.2.3	Running Actions Using Visual Basic Scripts for Groups and Organizational Units	6-37
6.8.2.4	Important Notes on Running Actions Scripts for Groups and Organizational Units	6-37
6.8.2.5	Guidelines on Creating Scripts for Groups and Organizational Units	6-38
6.9	Enabling Reconciliation and Provisioning Operations Across Multiple Domains	6-38
6.9.1	Understanding Enabling Reconciliation Across Multiple Domains	6-38
6.9.1.1	About Enabling Reconciliation Across Multiple Domains	6-39
6.9.1.2	Enabling Reconciliation Across Multiple Domains	6-39
6.9.2	Understanding Enabling Provisioning Across Multiple Domains	6-40
6.10	About Using the Connector for Multiple Trusted Source Reconciliation	6-40
6.11	Multiple Installations of the Target System	6-41
6.11.1	About Multiple Installations of the Target System	6-41
6.11.2	Configuring the Connector for Multiple Installations of the Target System	6-42
6.11.2.1	Configuring the Connector for Multiple Installations of the Target System while Upgrading from Oracle Identity Governance release 11.1.2.x to 12.2.1.3.0	6-42
6.11.2.2	Configuring the Connector for Multiple Installations of the Target System Using Application On-Boarding	6-42
6.12	Creating a Home Directory After User Create Provisioning Operation	6-43
6.13	Configuring the Connector for Provisioning Groups of the Security Group - Universal Group Type	6-43

## 7 Upgrading the Microsoft Active Directory User Management Connector

---

7.1	Preupgrade Steps	7-1
7.2	Upgrade Steps	7-2
7.3	Postupgrade Steps	7-2
7.3.1	Performing Postupgrade Steps	7-3
7.3.2	Determining Values For the FromVersion and ToVersion Attributes	7-6
7.3.3	Verifying If the Correct Process Form is Associated With the Resource Object	7-6



## 8 Troubleshooting the Microsoft Active Directory User Management Connector

---

## 9 Frequently Asked Questions

---

## A Character Lengths of Target System Fields and Process Form Fields

---

A.1	Fields with Different Lengths on the Target System and Process Form	A-1
A.2	Changing Process Form Field Lengths	A-2

## B Files and Directories in the Microsoft Active Directory User Management Connector Installation Package

---

## List of Figures

---

1-1	Connector Architecture	1-8
2-1	Overall Flow of the Process for Creating an Application By Using the Connector	2-2
3-1	Default Attribute Mappings for an AD User Account	3-13
3-2	Default Attribute Mappings for a Group Entitlement	3-13
3-3	Default Attribute Mappings for an AD User Account in an Authoritative Application	3-15
3-4	Simple Correlation Rule for a Target Application	3-17
3-5	Predefined Situations and Responses for a Target Application	3-18
3-6	Simple Correlation Rule for an Authoritative Application	3-20
3-7	Predefined Situations and Responses for an Authoritative Application	3-21
5-1	Reconciliation Rule for Groups	5-23
5-2	Reconciliation Action Rules for Groups	5-24
5-3	Reconciliation Rule for Organizational Unit	5-31
5-4	Reconciliation Action Rules for Organizational Unit	5-32
6-1	Multivalued Field Added on a New Form	6-6
6-2	New Reconciliation Field Added in the Resource Object	6-8
6-3	Preview Settings for Action Scripts	6-32
6-4	Action Scripts	6-32
7-1	RootDSE Properties Dialog Box	7-2

## List of Tables

---

1-1	Certified Components	1-2
1-2	Supported Connector Operations	1-7
1-3	Supported Connector Features Matrix	1-11
3-1	Parameters in the Basic Configuration Section for the Microsoft Active Directory User Management Connector	3-1
3-2	Advanced Setting Parameters for Oracle Database	3-7
3-3	Default Attribute Mappings for an AD User Account	3-10
3-4	Default Attribute Mappings for a Group Entitlement	3-13
3-5	AD User Account Schema Attributes for an Authoritative Application	3-14
3-6	Predefined Identity Correlation Rule for an AD Target Application	3-16
3-7	Predefined Situations and Responses for a Target Application	3-18
3-8	Predefined Identity Correlation Rule for an AD Authoritative Application	3-19
3-9	Predefined Situations and Responses for an Authoritative Application	3-20
3-10	Parameters of the Active Directory User Target Reconciliation and Active Directory User Target Concurrent Recon Jobs	3-22
3-11	Parameters of the Active Directory User Group Membership Recon Job	3-24
3-12	Parameters of the Active Directory User Target Delete Recon Job	3-25
3-13	Parameters of the Reconciliation Jobs for Entitlements	3-27
3-14	Parameters of the Active Directory User Trusted Recon Job	3-28
3-15	Parameters of the Active Directory User Trusted Delete Recon Job	3-31
4-1	Parameters of the Active Directory IT Resource for the Target System	4-3
4-2	Parameters of the Active Directory Connector Server IT Resource	4-7
5-1	Keywords and Syntax for the Filter Attribute	5-6
5-2	Attributes of the Scheduled Tasks for Lookup Field Synchronization	5-10
5-3	Entries in the Lookup.ActiveDirectory.GM.Configuration Lookup Definition	5-15
5-4	Default Entries in the Lookup.ActiveDirectory.GM.ProvAttrMap	5-16
5-5	Entries in the Lookup.ActiveDirectory.GM.ReconAttrMap	5-17
5-6	Attributes of the Active Directory Group Recon Scheduled Job	5-19
5-7	Attributes of the Active Directory Group Delete Recon Scheduled Job	5-20
5-8	Action Rules for Reconciliation	5-22
5-9	Entries in the Lookup.ActiveDirectory.OM.Configuration Lookup Definition	5-25
5-10	Entries in the Lookup.ActiveDirectory.OM.Configuration.Trusted Lookup Definition	5-26
5-11	Entries in the Lookup.ActiveDirectory.OM.ProvAttrMap	5-26
5-12	Default Entries in the Lookup.ActiveDirectory.OM.ReconAttrMap	5-27
5-13	Default Entries in the Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted Lookup Definition	5-28

5-14	Attributes of the Active Directory Organization Recon Scheduled Job	5-28
5-15	Action Rules for Reconciliation	5-30
6-1	Entries in the Updated Lookup.ActiveDirectory.GM.ReconAttrMap Lookup Definition	6-22
6-2	Entries in the Updated Lookup.ActiveDirectory.GM.ProvAttrMap Lookup Definition	6-24
8-1	Troubleshooting for the Microsoft Active Directory User Management Connector	8-1
A-1	Fields with Different Lengths on the Target System and the Process Form	A-1
B-1	Files and Directories in the Connector Installation Package	B-1

# Preface

This guide describes the connector that is used to onboard Microsoft Active Directory User Management applications to Oracle Identity Governance.

## Audience

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

## Documentation Accessibility

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

### Access to Oracle Support

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

## Related Documents

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

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

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

[http://docs.oracle.com/cd/E52734\\_01/index.html](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:

<b>Convention</b>	<b>Meaning</b>
<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.

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 Microsoft Active Directory and Microsoft Active Directory Lightweight Directory Services targets. This helps in quicker onboarding of the applications for these targets into Oracle Identity Governance by using an intuitive UI.

## Documentation-Specific Updates

These are the updates made to the connector documentation.

### Documentation-Specific Updates in Release 12.2.1.3.0

The following documentation-specific update has been made in revision "09" of this guide:

A Note about configuring the .NET Connector Server has been added to [Installing the Microsoft Active Directory User Management Connector in the Connector Server](#).

The following documentation-specific update has been made in revision "08" of this guide:

Information about configuring the system to install and run the Connector Server has been modified in [Frequently Asked Questions](#).

The following documentation-specific updates have been made in revision "07" of this guide:

- Information about Oracle Identity Manager versions prior to 11g Release 2 PS3 (11.1.2.3.0) has been removed from the guide.

- [Installing the Microsoft Active Directory User Management Connector in the Connector Server](#) has been added.
- A Note about Test Connection has been added to [Creating an Application By Using the Connector](#).

The following documentation-specific update has been made in revision "06" of this guide:

A Note about supported attribute types of the Microsoft Active Directory target system has been added to [Adding Custom Fields for Target Resource Reconciliation](#), [Adding New Multivalued Fields for Target Resource Reconciliation](#), [Adding Custom Fields for Provisioning](#), and [Adding New Multivalued Fields for Provisioning](#).

The following documentation-specific update has been made in revision "05" of this guide:

[Setting Up the Lookup Definition for the Ignore Event API](#) has been added.

The following documentation-specific update has been made in revision "04" of this guide:

[Figure 6-4](#) has been updated.

The following documentation-specific updates have been made in revision "03" of this guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row of [Table 1-1](#) has been updated to include support for Oracle Identity Governance release 12c PS4 (12.2.1.4.0).
- [Adding Custom Fields for Target Resource Reconciliation of Users](#) has been updated.

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

- The "Target systems and target system host platforms" and "Connector Server" rows of [Table 1-1](#) has been updated to include information about Microsoft Active Directory installed on Microsoft Windows Server 2019.
- Several broken links were fixed throughout the document.
- Step 4 has been modified and Step 5 has been added in [Running a Custom PowerShell Script for Users](#).
- The "Is it mandatory to use Oracle Identity Manager 11g Release 1 (1.1.1.5.2) or later with Active Directory User Management connector release 11.1.1.5.0?" question has been removed from [Frequently Asked Questions](#) as it is not applicable to this release of the connector.



# 1

## About the Microsoft Active Directory User Management Connector

Oracle Identity Governance is a centralized identity management solution that provides self service, compliance, provisioning and password management services for applications residing on-premise or on the Cloud. Oracle Identity Governance connectors are used to integrate Oracle identity Governance with the external identity-aware applications. The Microsoft Active Directory User Management (AD User Management) connector lets you onboard Microsoft Active Directory or Microsoft Active Directory Lightweight Directory Services (AD LDS), applications in Oracle Identity Governance.



### Note:

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

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

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

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

- [Certified Components](#)
- [Usage Recommendation](#)
- [Certified Languages](#)
- [Supported Connector Operations](#)
- [Connector Architecture](#)
- [Password Synchronization](#)
- [Supported Connector Features Matrix](#)
- [Connector Features](#)

**Note:**

At some places in this guide, Microsoft Active Directory and Microsoft AD LDS are referred to as **target systems**.

## 1.1 Certified Components

These are the software components and their versions required for installing and using the Active Directory connector. The target system can be Microsoft Active Directory or Microsoft AD LDS.

**Table 1-1 Certified Components**

Component	AOB Application Requirement for Microsoft Active Directory	AOB Application Requirement for Microsoft AD LDS	CI-Based Connector Requirement for Microsoft Active Directory	CI-Based Connector Requirement for Microsoft AD LDS
Oracle Identity Governance or Oracle Identity Manager	<p>You can use one of the following releases:</p> <ul style="list-style-type: none"> <li>Oracle Identity Governance 12c (12.2.1.4.0)</li> <li>Oracle Identity Governance 12c (12.2.1.3.0)</li> </ul>	<p>Oracle Identity Governance 12c(12.2.1.3.0)</p> <p>Oracle Identity Governance 12c (12.2.1.4.0)</p>	<p>You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance:</p> <ul style="list-style-type: none"> <li>Oracle Identity Governance 12c (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 (11.1.2.3.0)</li> </ul>	<p>You can use one of the following releases of Oracle Identity Manager or Oracle Identity Governance:</p> <ul style="list-style-type: none"> <li>Oracle Identity Governance 12 c 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 (11.1.2.3.0)</li> </ul>

Table 1-1 (Cont.) Certified Components

Component	AOB Application Requirement for Microsoft Active Directory	AOB Application Requirement for Microsoft AD LDS	CI-Based Connector Requirement for Microsoft Active Directory	CI-Based Connector Requirement for Microsoft AD LDS
Target systems and target system host platforms	<p>The target system can be any one of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2019, 64-bit platform</li> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2016, 64-bit platform</li> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2012, 64-bit platform</li> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2012 R2, 64-bit platform</li> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2008, both 32-bit and 64-bit platforms</li> </ul>	<p>The target system can be any one of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory Lightweight Services installed on Microsoft Windows Server 2016, 64-bit platform</li> <li>• Microsoft Active Directory Lightweight Services installed on Microsoft Windows Server 2008, both 32-bit and 64-bit platforms</li> <li>• Microsoft Active Directory Lightweight Services installed on Microsoft Windows Server 2008 R2, both 32-bit and 64-bit platforms</li> <li>• Microsoft Active Directory Lightweight Services installed on Microsoft Windows</li> </ul>	<p>The target system can be any one of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2019, 64-bit platform</li> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2016, 64-bit platform</li> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2012, 64-bit platform</li> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2012 R2, 64-bit platform</li> <li>• Microsoft Active Directory installed on Microsoft Windows Server 2008, both 32-bit and 64-bit platforms</li> </ul>	<p>The target system can be any one of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory Lightweight Services installed on Microsoft Windows Server 2016, 64-bit platform</li> <li>• Microsoft Active Directory Lightweight Services installed on Microsoft Windows Server 2012, 64-bit platform</li> <li>• Microsoft Active Directory Lightweight Services installed on Microsoft Windows Server 2012 R2, 64-bit platform</li> <li>• Microsoft Active Directory Lightweight Services installed on Microsoft Windows Server 2008, both 32-bit</li> </ul>

**Table 1-1 (Cont.) Certified Components**

Component	AOB Application Requirement for Microsoft Active Directory	AOB Application Requirement for Microsoft AD LDS	CI-Based Connector Requirement for Microsoft Active Directory	CI-Based Connector Requirement for Microsoft AD LDS
	<ul style="list-style-type: none"> <li>Microsoft Active Directory installed on Microsoft Windows Server 2008 R2, both 32-bit and 64-bit platforms</li> </ul>	<ul style="list-style-type: none"> <li>Server 2012, 64-bit platform</li> <li>Microsoft Active Directory Lightweight Directory Services installed on Microsoft Windows Server 2012 R2, 64-bit platform</li> </ul>	<ul style="list-style-type: none"> <li>Microsoft Active Directory installed on Microsoft Windows Server 2008 R2, both 32-bit and 64-bit platforms</li> </ul>	<ul style="list-style-type: none"> <li>and 64-bit platforms</li> <li>Microsoft Active Directory Lightweight Directory Services installed on Microsoft Windows Server 2008 R2, both 32-bit and 64-bit platforms</li> </ul>
Connector Server	<p>Depending on the target system version that you are using, you can use one of the following Connector Server versions:</p> <ul style="list-style-type: none"> <li>For Microsoft Active Directory installed on Microsoft Windows Server 2019, use Connector Server release 12.2.1.3.0</li> <li>For Microsoft Active Directory installed on Microsoft Windows Server 2016, 2012, or 2008, use Connector Server release 11.1.2.1.0 or 12.2.1.3.0</li> </ul>	11.1.2.1.0 or 12.2.1.3.0	<p>Depending on the target system version that you are using, you can use one of the following Connector Server versions:</p> <ul style="list-style-type: none"> <li>For Microsoft Active Directory installed on Microsoft Windows Server 2019, use Connector Server release 12.2.1.3.0</li> <li>For Microsoft Active Directory installed on Microsoft Windows Server 2016, 2012, or 2008, use Connector Server release 11.1.2.1.0 or 12.2.1.3.0</li> </ul>	11.1.2.1.0 or 12.2.1.3.0

Table 1-1 (Cont.) Certified Components

Component	AOB Application Requirement for Microsoft Active Directory	AOB Application Requirement for Microsoft AD LDS	CI-Based Connector Requirement for Microsoft Active Directory	CI-Based Connector Requirement for Microsoft AD LDS
Other software (Software used for establishing or securing communication between Oracle Identity Manager and target system.)	Certificate Services IIS Web Server	Certificate Services IIS Web Server <b>Note:</b> You must configure SSL for the connector to perform all connector operations as expected.	Certificate Services IIS Web Server	Certificate Services IIS Web Server <b>Note:</b> You must configure SSL for the connector to perform all connector operations as expected.
Microsoft .NET framework	3.5, 4, 4.5, or higher version <b>Note:</b> If you are using Microsoft .NET Framework 3.5, then apply the following patch to prevent a memory leak issue: <a href="http://support.microsoft.com/kb/981575">http://support.microsoft.com/kb/981575</a>	3.5, 4, 4.5, or higher version <b>Note:</b> If you are using Microsoft .NET Framework 3.5, then apply the following patch to prevent a memory leak issue: <a href="http://support.microsoft.com/kb/981575">http://support.microsoft.com/kb/981575</a>	3.5, 4, 4.5, or higher version <b>Note:</b> If you are using Microsoft .NET Framework 3.5, then apply the following patch to prevent a memory leak issue: <a href="http://support.microsoft.com/kb/981575">http://support.microsoft.com/kb/981575</a>	3.5, 4, 4.5, or higher version <b>Note:</b> If you are using Microsoft .NET Framework 3.5, then apply the following patch to prevent a memory leak issue: <a href="http://support.microsoft.com/kb/981575">http://support.microsoft.com/kb/981575</a>

## 1.2 Usage Recommendation

These are the recommendations for the Microsoft Active Directory User Management connector versions that you can deploy and use depending on the Oracle Identity Governance or Oracle Identity Manager version that you are using.

- If you are using Oracle Identity Governance 12c (12.2.1.3.0), 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 Oracle Identity Manager release 11g Release 2 PS3 (11.1.2.3.0), as listed in the “CI-Based Connector Requirement for Microsoft Active Directory” or “CI-Based Connector Requirement for Microsoft AD LDS or ADAM” columns of [Table 1-1](#), then use the 11.1.x version of the Microsoft Active Directory User Management connector. If you want to use the 12.2.1.x version of this connector with Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0), then you can install and use it only in the CI-based mode. If you want to use the AOB application, then you must upgrade to Oracle Identity Governance release 12.2.1.3.0.

 **Note:**

If you are using the latest 12.2.1.x version of the Microsoft Active Directory User Management 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.

- If you are using an Oracle Identity Manager release that is later than release 9.1.0.1 and earlier than Oracle Identity Manager 11g Release 1 (11.1.1.5.6), then you must use the 9.1.1 version of this connector.

## 1.3 Certified Languages

These are the languages that the connector supports.

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

- Thai
- Turkish

## 1.4 Supported Connector Operations

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

**Table 1-2 Supported Connector Operations**

Operation	Supported?
<b>User Management</b>	
Create user	Yes
Update user	Yes
Delete user	Yes
Enable user	Yes
Disable user	Yes
<b>Group Management</b>	
Create group	Yes
Delete group	Yes
<b>Organizational Unit Management</b>	
Create organizational unit	Yes
Delete organizational unit	Yes
<b>Entitlement Grant Management</b>	
Add group	Yes
Remove group	Yes

 **Note:**

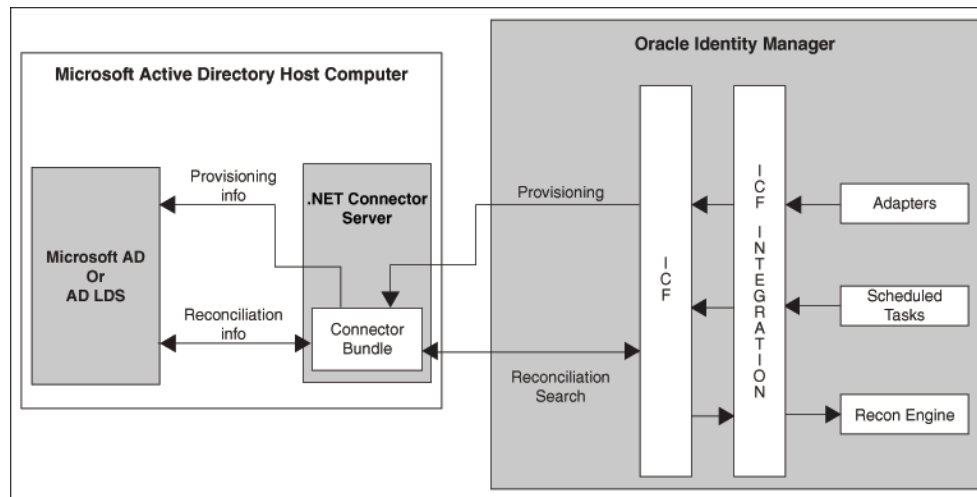
All the connector artifacts required for managing groups and organizational units (for example groups and organizational attribute mappings, reconciliation rules, jobs, and so on) are not visible in the Applications UI in Identity Self Service. However, all the required information is available in the predefined application templates of the connector installation package. For more information about the artifacts related to groups and organizational units, see [Connector Objects Used for Groups Management](#) and [Connector Objects Used for Organizational Units Management](#).

## 1.5 Connector Architecture

The Microsoft Active Directory User Management connector enables management of accounts through Oracle Identity Governance, and is implemented using the Identity Connector Framework (ICF).

[Figure 1-1](#) shows the architecture of the connector.

Figure 1-1 Connector Architecture



The Microsoft Active Directory User Management connector is built on top of System.DirectoryServices, a collection of classes managed by .NET that makes using Microsoft Active Directory easy and convenient. In the .NET Framework, classes for managing directory objects are contained within the System.DirectoryServices namespace. The classes in System.DirectoryServices wrap Active Directory Services Interfaces (ADSI) functionality.

ADSI is a built-in component of Microsoft Windows and shipped with different providers to access directories such as WinNT for local account management, NDS for accessing Novell eDirectory (formally known as Novell Directory Services), and LDAP for accessing any directory that supports Lightweight Directory Access Protocol (LDAP) v3. This connector uses the LDAP provider to access Microsoft Active Directory.

The earlier version of this connector represented a high-level connector with many configuration settings and lookup definitions that were used to customize the provisioning process. In addition, using SSL certificate for securing communication between Oracle Identity Governance and the target system was mandatory. In contrast, the current version of the connector provides low-level operations by using the Connector Framework and the consumer application is responsible for setting up the provisioning process. By using the internal mechanism of ADSI and the .NET Framework, the default communication between the .NET Connector Server and Microsoft Active Directory is "secure." However, if you are using Microsoft AD LDS as the target system, then you must configure SSL between Oracle Identity Manager and the target system.



 **Note:**

For performing password reset provisioning operations, the communication with the target system must be secure. If you are using Microsoft AD as the target system, there is no need to enable SSL between the .NET Connector Server and the target system. This is because the default communication between the .NET Connector Server and the target system is "secure."

However, in the case of Microsoft AD LDS, the default communication between the .NET Connector Server and Microsoft AD LDS is not "secure." Therefore, it is required to configure SSL between the .NET Connector Server and Microsoft AD LDS for the password reset functionality to work as expected.

As the current version of this connector provides low-level provisioning functionality, an integration code called Integrated Common Framework (ICF) Common is used.

Instead of communicating directly with the native API, ICF Common communicates with the connector framework through its API, and then calls SPI operations on a specific version of this connector. Between the Java ICF and the connector, the .NET Connector Framework resides (in the context of which the connector is running) and bridges the Java ICF and .NET connector. The connector is deployed in the .NET connector framework.

Oracle Identity Governance communicates with a .NET Connector Server over the network. The .NET Connector Server serves as a proxy to provide any authenticated application access to the current version of the connector deployed within the .NET Connector Server. Note that the Connector Server need not be on the domain controller on which the target system is running. Connector Server can be configured on any machine in the Microsoft Active Directory domain.

The Microsoft Active Directory User Management connector is a .NET connector that supports provisioning to and reconciliation from Microsoft Windows servers running, Microsoft Active Directory Domain Services (AD DS) and Microsoft Active Directory Lightweight Directory Services (AD LDS).

The Microsoft Active Directory User Management connector is implemented using the ICF. The ICF provides a container that separates the connector bundle from the application (for example, Oracle Identity Governance or Oracle Waveset). 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.

 **See Also:**

Understanding the Identity Connector Framework in *Developing and Customizing Applications for Oracle Identity Governance* for more information about the ICF

The connector can be configured to run in one of the following modes:

- Identity reconciliation

Identity reconciliation is also known as authoritative or trusted source reconciliation. In this form of reconciliation, OIM Users are created or updated corresponding to the creation of and updates to users on the target system. The identity reconciliation mode also supports reconciliation of objects like groups and organizations (OUs) created on the target system.

In the identity reconciliation mode, depending on the data that you want to reconcile, you use different scheduled tasks. For example, you use the Active Directory User Trusted Recon scheduled job to reconcile user data from the target system. See [Reconciliation Jobs for an Authoritative Application](#) for more information about scheduled tasks used in this mode.

- Account Management

Account management is also known as target resource management. This mode of the connector enables the following operations:

- Provisioning

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

Users and organizations are organized in hierarchical format on the target system. Before you can provision users to (that is, create users in) the required organizational units (OUs) on the target system, you must fetch into Oracle Identity Governance the list of OUs used on the target system. This is achieved by using a lookup synchronization scheduled job.

Similarly, before you can provision users to the required groups on the target system, you must fetch into Oracle Identity Governance the list of all groups used on the target system. This is also achieved by using a lookup synchronization scheduled job.

The connector enables group assignment provisioning operations in which you set or change the target system group membership profiles of users. The connector also supports provisioning (updating) of the Windows Terminal Services Profile attributes. Accessing these attributes involves the use of components that are native to the Microsoft Windows platform.

- Target resource reconciliation

To perform target resource reconciliation, the Active Directory User Target Recon scheduled job is used. The connector applies filters to locate users to be reconciled from the target system and then fetches the attribute values of these users.

Depending on the data that you want to reconcile, you use different scheduled jobs. For example, you use the Active Directory User Target Recon scheduled job to reconcile user data in the target resource mode. For more information about scheduled jobs used in this mode, see [Reconciliation Jobs for a Target Application](#).

## 1.6 Password Synchronization

This connector cannot propagate password changes from Microsoft Active Directory to Oracle Identity Governance.

To implement this feature, you must install the Microsoft Active Directory password synchronization connector. See *Deploying the Connector in Oracle Identity Manager Connector Guide for Microsoft Active Directory Password Synchronization* for more information about scenarios in which both the password synchronization connector and this connector are deployed.

## 1.7 Supported Connector Features Matrix

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

**Table 1-3 Supported Connector Features Matrix**

Feature	AOB Connector	CI-Based Connector
Full reconciliation	Yes	Yes
Incremental reconciliation	Yes	Yes
Limited reconciliation	Yes	Yes
Batched reconciliation	Yes	Yes
Connection pooling	Yes	Yes
Use connector server	Yes	Yes
Deleted groups reconciliation	Yes	Yes
Transformation and validation of account data	Yes	Yes
Perform reconciliation and provisioning operations across domains	Yes	Yes
Perform connector operations on user-defined object classes	No	Yes
Add dynamic auxiliary object classes	No	Yes
Add and include the Group Name (pre-Windows 2000) attribute in connector operations	Yes	Yes
Provision groups of the Security Group - Universal type	Yes	Yes
Add custom object categories in connector operations	Yes	Yes
Compatibility with high-availability target system environments	Yes	Yes
Test connection	Yes	No

## 1.8 Connector Features

The features of the connector include support for connector server, transformation and validation of account data, full, incremental, limited, and batched reconciliation, high-availability configuration and so on.

The following are features of this connector:

- [Full and Incremental Reconciliation](#)
- [Limited Reconciliation](#)
- [Batched Reconciliation](#)
- [Reconciliation of Deleted Groups](#)
- [Transformation and Validation of Account Data](#)
- [Support for Connector Server](#)
- [Connection Pooling](#)
- [Support for Connector Operations Across Domains](#)
- [Support for Adding the Group Name \(pre-Windows 2000\) Attribute](#)
- [Support for Provisioning Groups of the Security Group - Universal Group Type](#)
- [Support for Scripting Languages](#)
- [Support for High-Availability Configuration of the Target System](#)

### 1.8.1 Full and Incremental 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.

After the first full reconciliation run, incremental reconciliation is automatically enabled. In incremental reconciliation, user accounts that have been added or modified since the last reconciliation run are fetched into Oracle Identity Governance.

You can perform a full reconciliation run at any time.

See [Performing Full Reconciliation and Incremental Reconciliation](#) for more information.

### 1.8.2 Limited Reconciliation

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

See [Performing Limited Reconciliation](#) for more information.

### 1.8.3 Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See [Performing Batched Reconciliation](#) for more information.

## 1.8.4 Reconciliation of Deleted Groups

You can configure the connector for reconciling information about groups deleted in the target system.

In target resource mode, if a group is deleted on the target system, then the corresponding group is revoked from Oracle Identity Governance.

See [Active Directory Group Delete Recon](#) for more information about the scheduled job used for reconciling deleted groups.

## 1.8.5 Transformation and Validation of Account Data

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

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

## 1.8.6 Support for Connector Server

Connector Server is a component provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles. In other words, a connector server enables remote execution of an Oracle Identity Governance connector.

The Active Directory User Management connector is written using Microsoft .NET. A .NET environment is required for the execution of this connector code. Therefore, it is mandatory to deploy this connector on the .NET Connector Server shipped along with the connector package. The Active Directory User Management connector operates in the context of the .NET Connector Framework, which in turn requires an application to execute. Therefore, by default, Oracle provides the .NET Connector Server to run the Active Directory User Management connector.

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

## 1.8.7 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Governance connectors can use these connections to communicate with target systems.

At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each set basic configuration parameters that you provide while creating an application. For example, if you have three applications for three

installations of the target system, then three connection pools will be created, one for each target system installation.

For more information about the parameters that you can configure for connection pooling, see [Advanced Settings Parameters](#).

## 1.8.8 Support for Connector Operations Across Domains

The connector supports reconciliation and provisioning operations across domains.

This means that, for example, you can assign a user in one domain to a group in another domain. You can also reconcile a user record even if the user and the user's manager belong to different domains.

See [Enabling Reconciliation and Provisioning Operations Across Multiple Domains](#) for more information.

## 1.8.9 Support for Adding the Group Name (pre-Windows 2000) Attribute

You add the Group Name (pre-Windows 2000) attribute to Oracle Identity Governance and then include it for reconciliation and provisioning operations.

During group provisioning, by default, the value that you specify for the Group Name field on the OIM process form, is entered as the value of the Group Name and Group Name (pre-Windows 2000) attributes of the target system. If you want to specify different values for the Group Name and Group Name (pre-Windows 2000) attributes in the target system, then you must create the Group Name (pre-Windows 2000) field on the OIM process form.

See [Adding the Group Name \(pre-Windows 2000\) Attribute](#) for more information.

## 1.8.10 Support for Provisioning Groups of the Security Group - Universal Group Type

The connector lets you create a group of the type Security Group - Universal.

For more information, see [Configuring the Connector for Provisioning Groups of the Security Group - Universal Group Type](#).

## 1.8.11 Support for Scripting Languages

The connector supports any scripting language that has a script executor in the ICF. Currently, the connector supports two script executor implementations: a Windows shell script executor (batch scripts) and a Boo script executor.

Although Visual Basic scripts are not directly supported, a Visual Basic script can be called using a shell script.

For more information, see [Action Scripts](#).

## 1.8.12 Support for High-Availability Configuration of the Target System

You can configure the connector for compatibility with high-availability target system environments.

It can read information about backup target system hosts from the Backup Host Names parameter of the Basic Configuration section and apply this information when it is unable to connect to the primary host.

For more information about the Backup Host Names parameter, see [Basic Configuration Parameters](#).

# 2

## Creating an Application By Using the Microsoft Active Directory User Management 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](#)
- [Installing the Microsoft Active Directory User Management Connector in the Connector Server](#)
- [Creating an Application By Using the Connector](#)

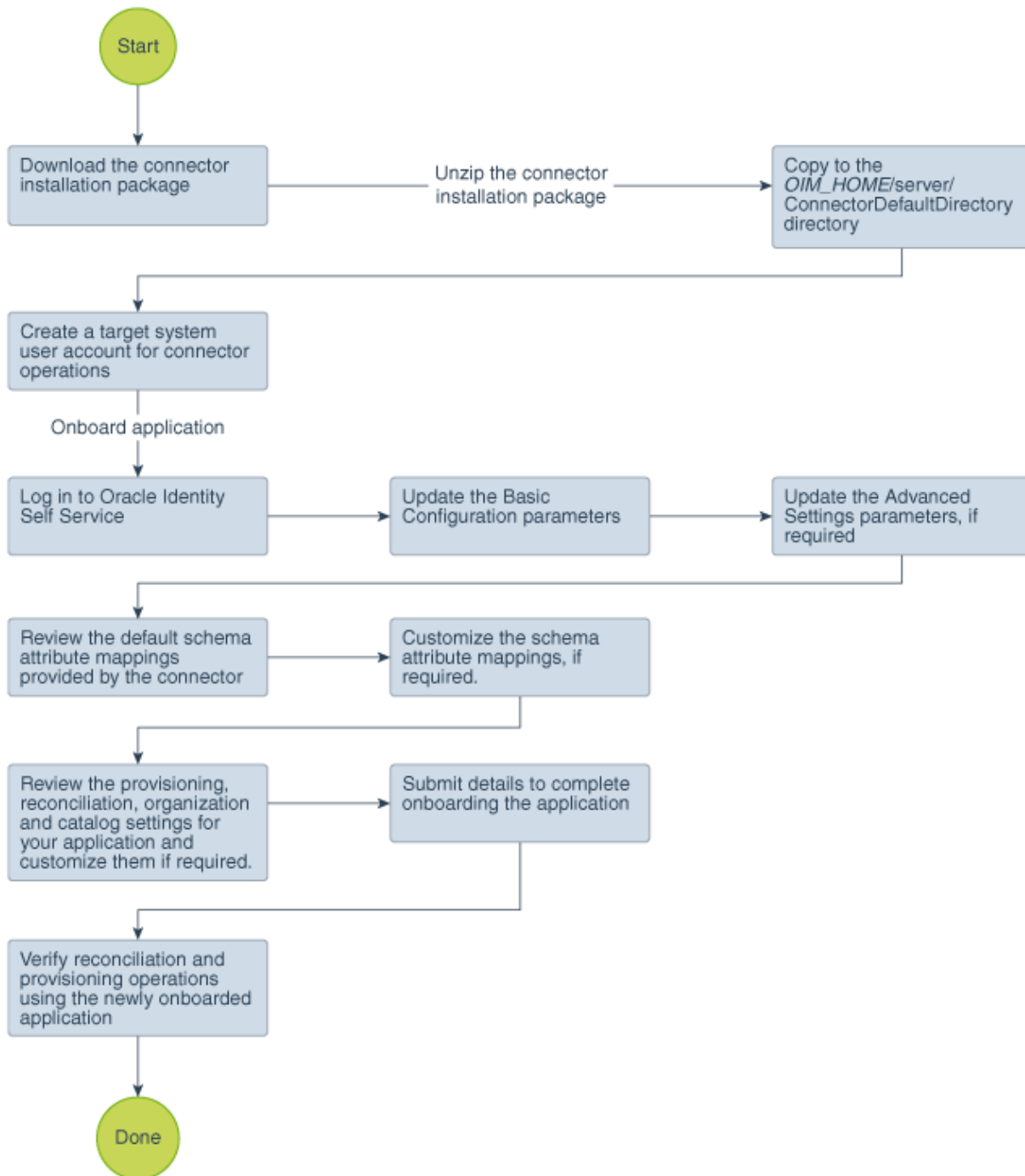
### 2.1 Process Flow for Creating an Application By Using the Connector

From Oracle Identity Governance release 12.2.1.3.0 onward, connector deployment is handled using the application onboarding capability of Identity Self Service.

[Figure 2-1](#) is a flowchart depicting high-level steps for creating an application in Oracle Identity Governance by using the connector installation package.



Figure 2-1 Overall Flow of the Process for Creating an Application By Using the Connector



## 2.2 Prerequisites for Creating an Application By Using the Connector

Learn about the tasks that you must complete before you create the application.

- [Downloading the Connector Installation Package](#)
- [Creating a Target System User Account for Connector Operations](#)
- [Assigning Permissions to Perform Delete User Reconciliation Runs](#)
- [Delegating Control for Organizational Units and Custom Object Classes](#)

### 2.2.1 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*. For example, for this connector, the director name is *activedirectory-12.2.1.3.0*.
6. Copy the *CONNECTOR\_NAME-RELEASE\_NUMBER* directory to the *OIM\_HOME/server/ConnectorDefaultDirectory* directory.

### 2.2.2 Creating a Target System User Account for Connector Operations

Oracle Identity Governance requires a target system user account to access the target system during reconciliation and provisioning operations. You provide the credentials of this user account in the Basic Configuration section while creating an application.

Depending on the target system that you are using, perform the procedure described in one of the following sections:

- [Creating a User Account for Connector Operations in Microsoft Active Directory](#)
- [Creating a User Account for Connector Operations in Microsoft AD LDS](#)

## 2.2.2.1 Creating a User Account for Connector Operations in Microsoft Active Directory

You can use a Microsoft Windows 2008 Server (Domain Controller) administrator account for connector operations. Alternatively, you can create a user account and assign the minimum required rights to the user account.

To create the Microsoft Active Directory user account for connector operations:

### See Also:

Microsoft Active Directory documentation for detailed information about performing this procedure

1. Create a group (for example, OIMGroup) on the target system. While creating the group, select **Security Group** as the group type and **Global** or **Universal** as the group scope.

### Note:

In a parent-child domain setup, create the group in the parent domain.

2. Make this group a member of the Account Operators group.
3. Assign all read permissions to this group. If there are multiple child domains in the forest, then log in to each child domain and add the above group to the Account Operators group of each child domain.

### Note:

You assign read permissions on the Security tab of the Properties dialog box for the user account. This tab is displayed only in Advanced Features view. To switch to this view, select Advanced Features from the View menu on the Microsoft Active Directory console.

4. Create a user (for example, OIMUser) on the target system. In a parent-child domain setup, create the user in the parent domain.
5. Make the user a member of the group (for example, OIMGroup) created in Step 1.

## 2.2.2.2 Creating a User Account for Connector Operations in Microsoft AD LDS

You must create and use a user account that belongs to the Administrators group for performing connector operations.

To create the Microsoft AD LDS user account for connector operations:

 **See Also:**

Microsoft AD LDS documentation for detailed information about these steps

1. Create a user account in Microsoft AD LDS.
2. Set a password for the user account.
3. Enable the user account by setting the `msDS-UserAccountDisabled` field to `false`.
4. Enter a value in the `userPrincipalName` field.

The value that you provide must be in the `user_name@domain_name` format, for example, `OIMuser@example.com`.

5. Add the distinguished name of the user to the Administrators group.

 **Note:**

To create the user account for connector operations in a standalone Microsoft AD LDS instance:

- a. Create a user account in the standalone computer.
- b. Add the newly created user to the AD LDS Administrators group[`CN=Administrators,CN=Roles,DC=X`].

## 2.2.3 Assigning Permissions to Perform Delete User Reconciliation Runs

In order to enable the user account that you created for performing connector operations to retrieve information about deleted user accounts during delete reconciliation runs, you must assign permissions to the deleted objects container (`CN=DeletedObjects`) in the target system.

 **Note:**

In a forest environment, if you are performing reconciliation by using the Global Catalog Server, then perform the procedure described in this section on all child domains.

To do so:

1. Log in to the target system as an administrator.
2. In a terminal window, run the following command:

```
dsacl DELETED_OBJ_DN /takeownership
```

In this command, replace `DELETED_OBJ_DN` with the distinguished name of the deleted directory object.

Sample value:

```
dsaclns "CN=Deleted Objects,DC=mydomain,dc=com" /takeownership
```

3. In a terminal window, run the following command to grant a user or group permissions to perform successful runs of the delete user reconciliation scheduled job:

```
dsaclns DELETED_OBJ_DN /G USER_OR_GROUP:PERMISSION
```

In this command, replace:

- *DELETED\_OBJ\_DN* with the distinguished name of the deleted directory object.
- *USER\_OR\_GROUP* with name of the user or group to which you want to assign permissions
- *PERMISSION* with the permissions to grant.

Sample value:

```
dsaclns "CN=Deleted Objects,DC=mydomain,dc=com" /G ROOT3\OIMUser:LCRP
```

## 2.2.4 Delegating Control for Organizational Units and Custom Object Classes

By default, user accounts that belong to the Account Operators group can manage only user and group objects. To manage organizational units or custom object classes, you must assign the necessary permissions to a user account. In other words, you must delegate complete control for an organizational unit or custom object class to a user or group object. In addition, you need these permissions to successfully perform provisioning of custom object classes.

This is achieved by using the Delegation of Control Wizard. An example for managing organizational units is creating organizational units.

To delegate control for an organizational unit or custom object class to a user account:

### Note:

In a parent-child deployment environment or forest topology, perform this procedure on all the child domains.

1. In the Active Directory Users and Computers window, in the navigation tree, right-click the organizational unit whose control you want to delegate, and then click **Delegate Control**.

The Delegation of Control Wizard appears.

### Note:

If you want to delegate control for all organization units under the root context, then delegate control at the root context level.

2. On the Welcome to the Delegation of Control Wizard page, click **Next**.

3. On the Users or Groups page, to select either a user or group to whom you want to delegate control:
  - a. Click **Add**.
  - b. In the Select Users, Computers, or Groups dialog box, enter a user or group name. For example, enter `OIMUser`.
  - c. Click **Check Names**.
  - d. Click **OK** to close the dialog box.
4. Click **Next**.
5. On the Tasks to Delegate page, select the **Create a custom task to delegate** option, and then click **Next**.
6. On the Active Directory Object Type page, select **Only the following objects in the folder**, and then select **Organization Unit Objects**. If you are delegating control for custom object classes, then select the custom object class for which you want to delegate control.
7. Select the **Create selected objects in the folder** and **Delete selected objects in the folder** options, and then click **Next**.
8. On the Permissions page:
  - For Organizational Units, select **Full Control**, click **Next**, and then click **Finish**.
  - For custom object classes, select the required permissions, click **Next** and then click **Finish**.

## 2.3 Installing the Microsoft Active Directory User Management Connector in the Connector Server

Installation in the Connector Server consists of copying and extracting the connector bundle to the Connector Server and configuring the IT resource.

To copy and extract the connector bundle to the Connector Server:

1. Stop the Connector Server.

 **Note:**

You can download the necessary Connector Server from the Oracle Technology Network web page.

2. From the installation media, copy and extract contents of the bundle/`ActiveDirectory.Connector-12.3.0.0.zip` file to the `CONNECTOR_SERVER_HOME` directory.
3. Rename `Shell-ScriptExecutorFactory.dll` file to `Shell.ScriptExecutorFactory.dll`.
4. Start the Connector Server for the connector bundle to be picked up by the Connector Server.

 **Note:**

- For information about configure the IT resource for the Connector Server, see [Configuring the IT Resource for the Connector Server](#).
- For information about configuring the .NET Connector Server, see [Configuring the .NET Connector Server](#).

## 2.4 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.

 **Note:**

You can verify and test connectivity using the **Test Connection** option only after the completion of following actions:

- AOB installation
- Extracted bundle/ActiveDirectory.Connector-12.3.0.0.zip is copied to the Connector Server home directory
- IT Resource for the Connector Server is configured
- IT Resource for the Target System is configured

 **See Also:**

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



# 3

## Configuring the Microsoft Active Directory User Management Connector

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

- [Basic Configuration Parameters](#)
- [Advanced Settings Parameters](#)
- [Attribute Mappings](#)
- [Correlation Rules for the Connector](#)
- [Reconciliation Jobs for the Connector](#)

### 3.1 Basic Configuration Parameters

These are the connection-related parameters that Oracle Identity Governance requires to connect to Microsoft Active Directory or Microsoft AD LDS. These parameters are common for both target applications and authoritative applications.

**Table 3-1 Parameters in the Basic Configuration Section for the Microsoft Active Directory User Management Connector**

Parameter	Mandatory?	Description
Connector Server Name	Yes	If you are using this connector with a .NET Connector Server, then enter the name of Connector Server IT resource. Default value: Active Directory Connector Server
Domain Name	Yes	Enter the domain name for the Microsoft Active Directory domain controller in which you are creating an application by using the connector. Sample value: example.com <b>Note:</b> This is a mandatory parameter if you are using Microsoft Active Directory as the target system.

**Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the Microsoft Active Directory User Management Connector**

Parameter	Mandatory?	Description
Admin User Name	Yes	<p>Enter the user name of account that you create by performing the procedure described in <a href="#">Creating a Target System User Account for Connector Operations</a>.</p> <p>Enter the value for this parameter in the following format:</p> <p><i>DOMAIN_NAME\USER_NAME</i></p> <p>Sample value: mydomain\admin</p> <p><b>Note:</b> If you are using AD LDS as the target system and this machine belongs to a workgroup, then enter a value for this parameter.</p> <p>Enter a value for this parameter in the following format:</p> <p><i>USER_NAME</i></p> <p>Sample value: admin</p>
Admin Password	Yes	<p>Enter the password of the user account that you create by performing the procedure described in <a href="#">Creating a Target System User Account for Connector Operations</a>.</p>
Container	Yes	<p>Enter the fully qualified domain name of the user container into or from which users must be provisioned or reconciled into Oracle Identity Governance, respectively.</p> <p>Sample value: DC=example, DC=com</p>

**Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the Microsoft Active Directory User Management Connector**

Parameter	Mandatory?	Description
LDAP Host Name	Yes	<p>Enter the host name, IP address, or domain name of the Microsoft Windows computer (target system host computer) on which Microsoft Active Directory is installed.</p> <p><b>Note:</b> If you do not specify a value for this parameter and the Backup Host Names parameter (discussed later in this table), then a serverless bind is used. The connector leverages ADSI for determining the domain controller in the domain and then creates the directory entry. Therefore, all interactions with the target system are not specific to a domain controller.</p> <p>To determine the host name, on the computer hosting the target system, right-click <b>My Computer</b> and select <b>Properties</b>. On the Computer Name tab of the System Properties dialog box, the host name is specified as the value of the Full computer name field.</p> <p>Sample values: w2khost 172.20.55.120 example.com</p>
Domain Controller	No	<p>Enter the name of the domain controller from which user accounts must be reconciled.</p> <p><b>Note:</b> The value specified in this parameter is used if the value of the Search Child Domains parameter of Advanced Settings is set to <code>no</code>. If you specify no value for the Domain Controller parameter and the value of the Search Child Domains parameter is set to <code>no</code>, then the connector automatically finds a domain controller for the target system and reconciles users from it.</p> <p>Sample value: <code>mynewdc</code></p>

**Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the Microsoft Active Directory User Management Connector**

Parameter	Mandatory?	Description
Port	No	Enter the number of the port at which Microsoft AD LDS is listening. Sample value: 50001 <b>Note:</b> Do not enter a value for this parameter if you are using Microsoft Active Directory as the target system.

**Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the Microsoft Active Directory User Management Connector**

Parameter	Mandatory?	Description
UseSSL	No	<p>Enter <i>yes</i> if the target system has been configured for SSL. This enables secure communication between the Connector Server and target system. Otherwise, enter <i>no</i>.</p> <p>Default value: <i>no</i></p> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• For resetting user password during provisioning operations, the communication with the target system must be secure. The default communication between the .NET Connector Server and Microsoft Active Directory is secure. Therefore, even if you set the value of this parameter to <i>no</i>, it is possible to reset user passwords during provisioning operations because the default communication is secure. For more information about configuring SSL, see <a href="#">Configuring SSL for Microsoft Active Directory and Microsoft AD LDS</a> .</li><li>• The default communication between the .NET Connector Server and Microsoft AD LDS is not secure. Therefore, for enabling password reset provisioning operations, you must set the value of this parameter to <i>yes</i> to secure communication with Microsoft AD LDS. For more information about configuring SSL, see <a href="#">Configuring SSL Between Connector Server and Microsoft AD LDS</a> .</li></ul>

**Table 3-1 (Cont.) Parameters in the Basic Configuration Section for the Microsoft Active Directory User Management Connector**

Parameter	Mandatory?	Description
Backup Host Names	No	Enter the host name of the backup domain controller to which Oracle Identity Governance must switch to if the primary domain controller becomes unavailable. Sample value: mydc1;mydc2;mydc3 <b>Note:</b> Multiple backup domain controllers must be separated by semicolon (;).
Is ADLDS?	No	Enter <i>yes</i> to specify that the target system is Microsoft AD LDS. Enter <i>no</i> to specify that the target system is Microsoft Active Directory. Default value: <i>no</i>
Global Catalog Server	No	Enter the host on which the global catalog server is located. <b>Note:</b> The value specified in this parameter is used if you set the value of the Search Child Domains parameter to <i>yes</i> . If no value is specified for the Global Catalog Server parameter and the Search Child Domains parameter is set to <i>yes</i> , then the connector automatically finds a global catalog server for the target system, and then reconciles user accounts from the domain controller on which the global catalog server is running. It is strongly recommended to provide a value for this parameter if you have set the value of the Search Child Domains parameter to <i>yes</i> . Sample value: myglobalcatalogdc

## 3.2 Advanced Settings Parameters

These are the configuration-related entries that the connector uses during reconciliation and provisioning operations. These parameters are common for both target applications and authoritative applications.

**Table 3-2 Advanced Setting Parameters for Oracle Database**

Parameter	Mandatory?	Description
Object Class	No	<p>This parameter holds the name of the object class to which the connector assigns newly created users on the target system.</p> <p>If you create a custom object class, then enter the name of that object class. For example, <code>InetOrgPerson</code>.</p> <p><b>Default value:</b> <code>User</code></p>
Lockout Threshold	No	<p>Enter the number of unsuccessful login attempts after which a user's account must be locked.</p> <p><b>Note:</b> This entry is applicable only for the Microsoft AD LDS target system.</p> <p><b>Default value:</b> <code>5</code></p>
Always Use Object GUID?	No	<p>This parameter specifies whether the connector must use the GUID of an object for searching records during reconciliation.</p> <p><b>Default value:</b> <code>yes</code></p> <p><b>Note:</b> Do <i>not</i> change the value of this entry.</p>
Native Guid Convention	No	<p>This parameter specifies whether GUID is stored in its native format. This entry is used by the connector internally.</p> <p><b>Default value:</b> <code>true</code></p> <p><b>Note:</b> Do <i>not</i> change the value of this entry.</p>
Page Size	No	<p>Enter the page size of the records fetched by the connector in each call to the target system during a reconciliation run. Paging splits the entire result set of a query into smaller subsets called, appropriately enough, pages.</p> <p>In general, it is recommended to set this value to the maximum page size for simple searches. By setting the page size to the maximum value, you can minimize the network roundtrips necessary to retrieve each page, which tends to be a more expensive operation for simple searches.</p> <p>While it is possible to specify a <code>PageSize</code> greater than the <code>MaxPageSize</code> of the target system, the Active Directory server will ignore it and use the <code>MaxPageSize</code> instead. No exception will be generated in this case.</p> <p>In some cases, you might need to specify a smaller page size to avoid timeouts or overtaxing the server. Some queries are especially expensive, so limiting the number of results in a single page can help avoid this.</p> <p><b>Default value:</b> <code>1000</code></p>

**Table 3-2 (Cont.) Advanced Setting Parameters for Oracle Database**

Parameter	Mandatory?	Description
Search Child Domains	No	<p>This parameter determines the search scope of users, groups, or organizational units within the domain name specified as the value of the DomainName attribute.</p> <p>Enter <code>no</code> if you want the connector to search for users, groups, or organizational units only from the specified domain. The domain name is specified as the value of the DomainName attribute. Note that the connector fetches records from the domain controller that is specified as the value of the Domain Controller parameter of Basic Configuration.</p> <p>Enter <code>yes</code> if you want the connector to search for users, groups, or organizational units from the specified domain and its child domains. In this case, the global catalog server is used for fetching records. Note that you specify the global catalog server as the value of the Global Catalog Server parameter of Basic Configuration.</p> <p><b>Default value:</b> <code>no</code></p>
Connector Name	Yes	<p>This parameter holds the name of the connector class.</p> <p><b>Value:</b> <code>Org.IdentityConnectors.ActiveDirectory.ActiveDirectoryConnector</code></p>
Bundle Name	Yes	<p>This parameter holds the name of the connector bundle package.</p> <p><b>Value:</b> <code>ActiveDirectory.Connector</code></p>
Bundle Version	Yes	<p>This parameter holds the version of the connector bundle class.</p> <p><b>Value:</b> <code>12.3.0.0</code></p>
Recon Date Format	No	<p>This parameter holds the format in which the last reconciliation run timing must be displayed.</p> <p><b>Default value:</b> <code>yyyyMMddHHmmss.OZ</code></p>
Maintain Hierarchy?	No	<p>Enter <code>yes</code> to specify that you want to maintain in Oracle Identity Governance the same organization hierarchy that is maintained on the target system. Otherwise, enter <code>no</code>.</p> <p><b>Default value:</b> <code>no</code></p>
Use Delete Tree For Accounts	No	<p>This parameter specifies whether the associated leaf nodes of an <code>__ACCOUNT__</code> object to be deleted are to be removed along with the object. If the value of this entry is not set to <code>true</code> and the <code>__ACCOUNT__</code> object to be deleted has leaf nodes, then the operation fails and an error message is displayed.</p> <p>If the value of this entry is set to <code>false</code>, then the <code>__ACCOUNT__</code> objects are removed from the child list of its parent only. Otherwise, regardless of the object class, the whole tree is removed recursively.</p> <p><b>Default value:</b> <code>false</code></p>
Create Home Directory	No	<p>This parameter holds the information whether a home directory must be created.</p> <p>Enter <code>yes</code> if you want the connector to create a home directory for user accounts. Otherwise, enter <code>no</code>.</p> <p><b>Default value:</b> <code>yes</code></p>
Pool Max Idle	No	<p>Maximum number of idle objects in a pool.</p> <p><b>Default value:</b> <code>10</code></p>



**Table 3-2 (Cont.) Advanced Setting Parameters for Oracle Database**

Parameter	Mandatory?	Description
Pool Max Size	No	Maximum number of connections that the pool can create. <b>Default value:</b> 10
Pool Max Wait	No	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. <b>Default value:</b> 150000
Pool Min Evict Idle Time	No	Minimum time, in milliseconds, the connector must wait before evicting an idle object. <b>Default value:</b> 120000
Pool Min Idle	No	Minimum number of idle objects in a pool. <b>Default value:</b> 1

## 3.3 Attribute Mappings

The attribute mappings on the Schema page vary depending on whether you are creating a target application or an authoritative application.

- [Attribute Mappings for a Target Application](#)
- [Attribute Mappings for an Authoritative Application](#)

### 3.3.1 Attribute Mappings for a Target Application

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

#### AD User Account Attributes

[Table 3-3](#) lists the user-specific attribute mappings between the process form fields in Oracle Identity Governance and AD target system attributes. 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*.

 **Note:**

If you are using AD LDS as the target system, then you must perform the following on the default attribute mappings list of the Schema page:

- Delete the rows containing the following Display Name attributes:
  - Redirection Mail Id
  - Terminal Allow Login
  - Terminal Home Directory
  - Terminal Profile Path
- Update the “User Id” Display Name row with the following values:
  - In the Target Attribute column, replace sAMAccountName with `__UPN_WO_DOMAIN__`.
  - Deselect the Provision Field checkbox.
  - Select the Recon Field checkbox.

**Table 3-3 Default Attribute Mappings for an AD User Account**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
User Id	sAMAccountName	String	No	Yes	Yes	No	Not applicable
User Principal Name	userPrincipalName	String	No	Yes	Yes	No	Not applicable
First Name	givenName	String	No	Yes	Yes	No	Not applicable
Middle Name	middleName	String	No	Yes	Yes	No	Not applicable
Last Name	sn	String	No	Yes	Yes	No	Not applicable
Full Name	displayName	String	No	Yes	Yes	No	Not applicable
Password Never Expires	PasswordNeverExpires	Boolean	No	Yes	Yes	No	Not applicable
User Must Change Password At Next Logon	__PASSWORD_EXPIRED__	Boolean	No	Yes	Yes	No	Not applicable

**Table 3-3 (Cont.) Default Attribute Mappings for an AD User Account**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Account is Locked out	__LOCK_OUT__	Boolean	No	Yes	Yes	No	Not applicable
Telephone Number	telephoneNumber	String	No	Yes	Yes	No	Not applicable
Account Expiration Date	__PASSWORD_EXPIRATION_DATE__	Date	No	Yes	Yes	No	Not applicable
E Mail	mail	String	No	Yes	Yes	No	Not applicable
Post Office Box	postOfficeBox	String	No	Yes	Yes	No	Not applicable
City	l	String	No	Yes	Yes	No	Not applicable
State	st	String	No	Yes	Yes	No	Not applicable
Zip	postalCode	String	No	Yes	Yes	No	Not applicable
Home Phone	homePhone	String	No	Yes	Yes	No	Not applicable
Mobile	mobile	String	No	Yes	Yes	No	Not applicable
Pager	pager	String	No	Yes	Yes	No	Not applicable
Fax	facsimileTelephoneNumber	String	No	Yes	Yes	No	Not applicable
Title	title	String	No	Yes	Yes	No	Not applicable
Department	department	String	No	Yes	Yes	No	Not applicable
Company	company	String	No	Yes	Yes	No	Not applicable
Manager Name	manager	String	No	Yes	Yes	No	Not applicable
Office	physicalDeliveryOfficeName	String	No	Yes	Yes	No	Not applicable
Country	c	String	No	Yes	Yes	No	Not applicable

**Table 3-3 (Cont.) Default Attribute Mappings for an AD User Account**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Provision Field?	Recon Field?	Key Field?	Case Insensitive?
Street	streetAddress	String	No	Yes	Yes	No	Not applicable
Terminal Home Directory	TerminalServicesHomeDirectory	String	No	Yes	Yes	No	Not applicable
Terminal Allow Login	AllowLogon	Boolean	No	Yes	Yes	No	Not applicable
Terminal Profile Path	TerminalServicesProfilePath	String	No	Yes	Yes	No	Not applicable
Status	__ENABLE__	String	No	No	Yes	No	Not applicable
AD Server		Long	Yes	No	Yes	Yes	No
Unique Id	__UID__	String	No	No	Yes	Yes	No
Common Name	cn	String	Yes	No	Yes	No	Not applicable
Organization Name	ad_container	String	Yes	No	Yes	No	Not applicable
Password	__PASSWORD__	String	No	Yes	No	No	Not applicable
Password Not Required	PasswordNotRequired	Boolean	No	Yes	No	No	Not applicable
Homedirectory	homeDirectory	String	No	Yes	No	No	Not applicable
Redirection Mail Id	__MAILREDIRECTION__	String	No	Yes	No	No	Not applicable
User Full DN	__NAME_	String	No	Yes	No	No	Not applicable

Figure 3-1 shows the default User account attribute mappings for an AD Target application.

**Figure 3-1 Default Attribute Mappings for an AD User Account**

AD User

+ Add Attribute

Application Attribute				Provisioning Property		Reconciliation Properties			
Identity Attribute	Display Name	Target Attribute	Data Type	Mandatory	Provision Field	Recon Field	Key Field	Case Insensitive	
Enter a value	AD Server		Long	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	Unique Id	__UID__	String	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	Password	__PASSWORD__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	User Id	sAMAccountName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	User Principal Nam	userPrincipalName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	First Name	givenName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	Middle Name	middleName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	Last Name	sn	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	Full Name	displayName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮
Enter a value	Common Name	cn	String	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕ ⋮

### Group Entitlement Attributes

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

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

**Table 3-4 Default Attribute Mappings for a Group Entitlement**

Display Name	Target Attribute	Data Type	Mandatory Provisioning Property?	Recon Field?	Key Field?	Case Insensitive?
Group Name	__GROUPS__	String	No	Yes	Yes	No

Figure 3-2 shows the default Group entitlement mapping.

**Figure 3-2 Default Attribute Mappings for a Group Entitlement**

groups

+ Add Attribute | Delete Form Use Bulk

Application Attribute			Provisioning Property		Reconciliation Properties		
Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Key Field	Case Insensitive	
Group Name	__GROUPS__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	✕ ⋮

### 3.3.2 Attribute Mappings for an Authoritative Application

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

[Table 3-5](#) lists the user-specific attribute mappings between the reconciliation fields in Oracle Identity Governance and AD target system attributes. The table also lists the data type for a given attribute and specified whether it is a mandatory attribute for reconciliation.

If required, you can edit these attributes mappings by adding new attributes or deleting existing attributes on the Schema page as described in *Creating an Authoritative Application in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

You may use the default schema that has been set for you or update and change it before continuing to the next step.

The Organization Name, Xellerate Type, and Role identity attributes are mandatory fields on the OIG User form that cannot be left blank during reconciliation. As there are no corresponding attributes in the target system for the Organization Name, Xellerate Type, and Role identity attributes, they have been mapped to attributes in Oracle Identity Governance. In addition, the connector provides default values (as listed in the “Default Value for Identity Display Name” column of [Table 3-5](#)) that it can use during reconciliation. For example, the default target attribute value for the Organization Name attribute is Xellerate Users. This implies that the connector reconciles all target system user accounts into the Xellerate Users organization in Oracle Identity Governance. Similarly, the default attribute value for Xellerate Type attribute is End-User, which implies that all reconciled user records are marked as end users.

#### Note:

If you are using AD LDS as the target system, then you must perform the following on the default attribute mappings list of the Schema page:

- Delete the row containing the Manager Login Display Name attribute.
- In the “User Login” Display Name row, update the Target Attribute mapping by replacing sAMAccountName with `__UPN_WO_DOMAIN__`.

**Table 3-5 AD User Account Schema Attributes for an Authoritative Application**

Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Default Value for Identity Display Name
Manager Login	Manager Id	String	No	Yes	NA
Status	__ENABLE_ _	String	No	Yes	NA
ObjectGUID	__UID__	String	No	Yes	NA

**Table 3-5 (Cont.) AD User Account Schema Attributes for an Authoritative Application**

Identity Display Name	Target Attribute	Data Type	Mandatory Reconciliation Property?	Recon Field?	Default Value for Identity Display Name
User Login	sAMAccountName	String	No	Yes	NA
First Name	givenName	String	No	Yes	NA
Last Name	sn	String	No	Yes	NA
Middle Name	middleName	String	No	Yes	NA
Xellerate Type	OIM User Type	String	No	Yes	End-User
Role	OIM Employee Type	String	No	Yes	Full-Time
Organization Name	__PARENTCN__	String	No	Yes	Xellerate Users
Email	mail	String	No	Yes	NA

Figure 3-3 shows the default AD User account attribute mappings for an AD authoritative application.

**Figure 3-3 Default Attribute Mappings for an AD User Account in an Authoritative Application**

AD User Trusted

+ Add Attribute

Application Attribute			Reconciliation Properties			
Identity Display Name	Target Attribute	Data Type	Mandatory	Recon Field	Advanced	Delete
Manager Login	Manager Id	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Status	__ENABLE__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
ObjectGUID	__UID__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
User Login	sAMAccountName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
First Name	givenName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Last Name	sn	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Middle Name	middleName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Xellerate Type	OIM User Type	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Role	OIM Employee Type	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Organization Name	__PARENTCN__	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Email	mail	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

## 3.4 Correlation Rules for the Connector

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

- [Correlation Rules for a Target Application](#)
- [Correlation Rules for an Authoritative Application](#)

### 3.4.1 Correlation Rules for a Target Application

When you create a Target application, the connector uses correlation rules to determine the identity to which Oracle Identity Governance must assign a resource.

#### Predefined Identity Correlation Rules

By default, the Active Directory User Management 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 3-6](#) lists the default simple correlation rule for an AD target system. 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 3-6** Predefined Identity Correlation Rule for an AD Target Application

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__UID__	Equals	ObjectGUID	No
sAMAccountName	Equals	User Login	No

#### Note:

If you are using Microsoft AD LDS as the target system, then you must update the identity reconciliation rule by replacing sAMAccountName in the Target Attribute column with `userPrincipalName`.

The identity correlation rule for an AD target application is as follows:

(\_\_UID\_\_ Equals ObjectGUID) OR (sAMAccountName Equals User Login)

The identity correlation rule for an AD LDS target application is as follows:

(\_\_UID\_\_ Equals ObjectGUID) OR (userPrincipalName Equals User Login)

In the first identity rule component:



- `__UID__` is an attribute on the target system that uniquely identifies the user account.
- ObjectGUID is the unique identifier of the resource assigned to the OIG User.

In the second identity rule component:

- For an AD target application, sAMAccountName is a field on Microsoft Active Directory that represents the login name of the user account.
- For an AD LDS target application, For an AD LDS target application, userPrincipalName is a field on AD LDS that represents the domain-specific name of the user.
- User Login is the field on the OIM User form.

Both the rule components are joined using the OR logical operator.

Figure 3-4 shows the simple correlation rule for this connector that is applicable to both AD and AD LDS target systems.

**Figure 3-4 Simple Correlation Rule for a Target Application**

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
<code>__UID__</code>	Equals	ObjectGUID	<input type="checkbox"/>	<input type="button" value="X"/>
sAMAccountName	Equals	User Login	<input type="checkbox"/>	<input type="button" value="X"/>

Rule Operator

OR

### Predefined Situations and Responses

The Active Directory User Management 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.

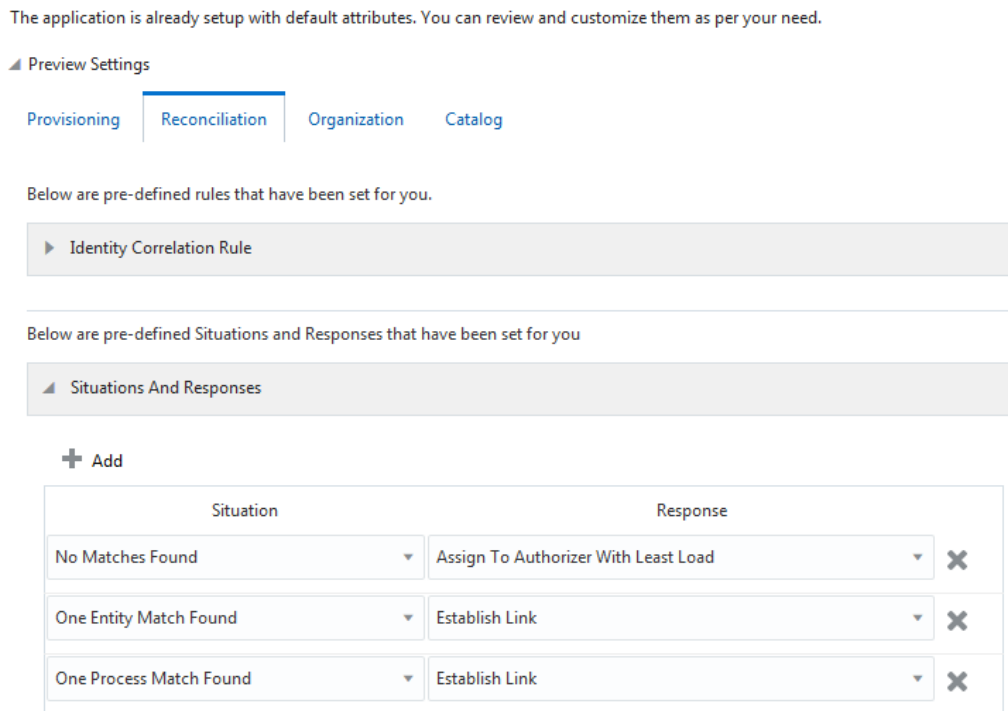
Table 3-7 lists the default situations and responses for this connector that is applicable to both AD and AD LDS target systems. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see Updating Situations and Responses in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-7 Predefined Situations and Responses for a Target Application**

Situation	Response
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Figure 3-5 shows the situations and responses that the connector provides by default for both AD and AD LDS target applications.

**Figure 3-5 Predefined Situations and Responses for a Target Application**



### 3.4.2 Correlation Rules for an Authoritative Application

When you create an Authoritative application, the connector uses correlation rules to determine the identity that must be reconciled into Oracle Identity Governance.

#### Predefined Identity Correlation Rules

By default, the Active Directory User Management connector provides a simple correlation rule when you create an Authoritative 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 an AD authoritative application. 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 an AD Authoritative Application**

Target Attribute	Element Operator	Identity Attribute	Case Sensitive?
__UID__	Equals	ObjectGUID	No
sAMAccountName	Equals	User Login	No



**Note:**

If you are using Microsoft AD LDS as the target system, then you must update the identity reconciliation rule by replacing sAMAccountName in the Target Attribute column with userPrincipalName.

The identity correlation rule for an AD target application is as follows:

(\_\_UID\_\_ Equals ObjectGUID) OR (sAMAccountName Equals User Login)

The identity correlation rule for an AD LDS target application is as follows:

(\_\_UID\_\_ Equals ObjectGUID) OR (userPrincipalName Equals User Login)

In the first identity rule component:

- \_\_UID\_\_ is an attribute on the target system that uniquely identifies the user account.
- ObjectGUID is the unique identifier of the resource assigned to the OIG User.

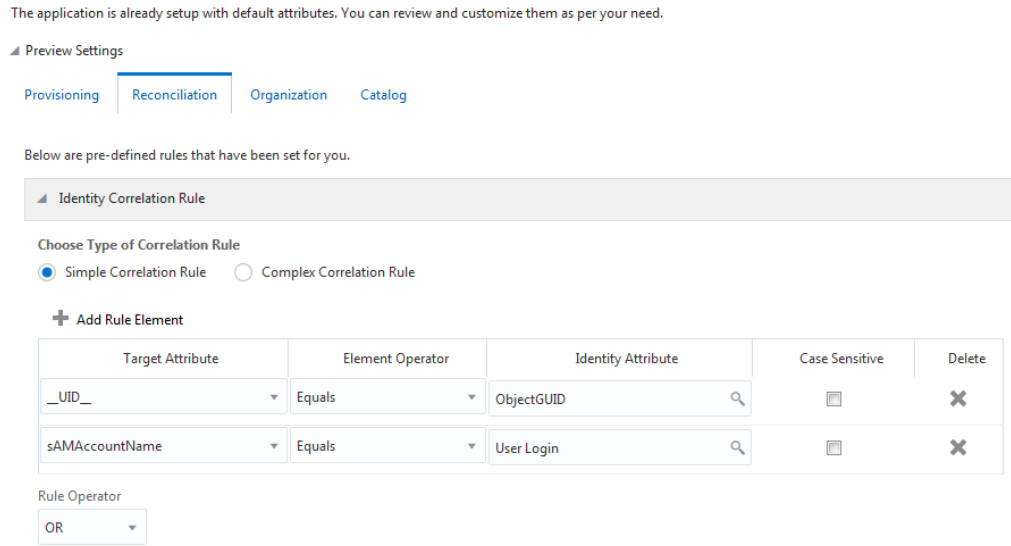
In the second identity rule component:

- For an AD target application, sAMAccountName is a field on Microsoft Active Directory that represents the login name of the user account.
- For an AD LDS target application, userPrincipalName is a field on AD LDS that represents the domain-specific name of the user.
- User Login is the field on the OIG User form.

Both the rule components are joined using the OR logical operator.

Figure 3-6 shows the simple correlation rule for an AD authoritative application.

**Figure 3-6 Simple Correlation Rule for an Authoritative Application**



### Predefined Situations and Responses

The Active Directory User Management connector provides a default set of situations and responses when you create an Authoritative 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 both AD and AD LDS authoritative application. If required, you can edit these default situations and responses or add new ones. For more information about adding or editing situations and responses, see *Updating Situations and Responses in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance*.

**Table 3-9 Predefined Situations and Responses for an Authoritative Application**

Situation	Response
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

[Figure 3-7](#) shows the situations and responses for an authoritative application that the connector provides by default for both AD and AD LDS target systems.

**Figure 3-7** Predefined Situations and Responses for an Authoritative Application

Preview Settings

Reconciliation Organization

Below are the pre-defined reconciliation settings that have been set for you

▶ Identity Correlation Rule

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

▲ Situations And Responses

+ Add

Situation	Response	
No Matches Found	Create User	✕
One Entity Match Found	Establish Link	✕
One Process Match Found	Establish Link	✕

## 3.5 Reconciliation Jobs for the Connector

These are the reconciliation jobs that the connector creates after you create a target or an authoritative application

- [Reconciliation Jobs for a Target Application](#)
- [Reconciliation Jobs for an Authoritative Application](#)

### 3.5.1 Reconciliation Jobs for a Target Application

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

#### User Reconciliation Job

Use the Active Directory User Target Reconciliation job to reconcile user data from a target application.

#### Note:

In release 12.2.1.3.0 of the connector, a new job named Active Directory User Target Concurrent Recon has been introduced, which is similar to the Active Directory User Target Reconciliation job. The Active Directory User Target Concurrent Recon job is recommended for performing bulk reconciliation, reconciles user data from a target application in the multithreaded mode. You can search for and run this scheduled job from Oracle Identity System Administration. The parameters of this job is the same as that of the Active Directory User Target Reconciliation job.

**Table 3-10 Parameters of the Active Directory User Target Reconciliation and Active Directory User Target Concurrent Recon Jobs**

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. Do <i>not</i> modify this value.
Number of Batches	Enter the number of batches in which the connector must reconcile user records. Default value: All
Search Scope	Enter <code>subtree</code> if you want the scope of the search for records to be reconciled to include the container specified by the Search Base parameter and all of its child containers. For example, if the search base is set to <code>OU=abc,DC=corp,DC=com</code> , then the search would cover the <code>abc</code> OU and all of its child OUs.  Enter <code>onelevel</code> if you want the scope of the search for records to be restricted to only the container specified by the Search Base parameter. The connector does not include the child containers of the specified container in the search. For example if the search base is set to <code>OU=abc,DC=corp,DC=com</code> , then the search would cover only the <code>abc</code> OU.  <b>Note:</b> If you want to enter <code>onelevel</code> , then ensure that you do not include a space between the words "one" and "level." Default value: <code>subtree</code>
Scheduled Task Name	This parameter holds the name of the scheduled job. <b>Note:</b> For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter. Default value: <code>Active Directory User Target Recon</code>
Sort Direction	Use this parameter to specify whether the connector must sort the records that it fetches in ascending or descending order. The value of this attribute can be either <code>asc</code> or <code>desc</code> . Default value: <code>asc</code>
Incremental Recon Attribute	Enter the name of the target system attribute that holds last update-related number, non-decreasing value. For example, numeric or strings. The value in this attribute is used during incremental reconciliation to determine the newest or most youngest record reconciled from the target system. Default value: <code>uSNChanged</code> <b>Note:</b> Do not change the value of this attribute.

**Table 3-10 (Cont.) Parameters of the Active Directory User Target Reconciliation and Active Directory User Target Concurrent Recon Jobs**

Parameter	Description
Sort By	<p>Enter the name of the target system field by which the connector must sort records in a batch.</p> <p>Default value: <code>sAMAccountName</code></p> <p><b>Note:</b> If you are using AD LDS as the target system, then change the default value of this parameter to some other attribute (for example, <code>cn</code>) because the <code>sAMAccountName</code> attribute does not exist on the AD LDS target system.</p>
Latest Token	<p>This parameter holds the value of the <code>uSNChanged</code> attribute of a domain controller that the connector uses for reconciliation.</p> <p><b>Note:</b> The reconciliation engine automatically enters a value for this attribute. It is recommended that you do not change the value of this parameter. If you manually specify a value for this attribute, then the connector only user accounts whose <code>uSNChanged</code> value is greater than the Latest Token attribute value.</p>
Filter	<p>Enter the expression for filtering records that the scheduled job must reconcile.</p> <p>Sample value: <code>startsWith('userPrincipalName', 'John')</code></p> <p>For information about the filters expressions that you can create and use, see ICF Filter Syntax in <i>Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance</i>.</p>
Batch Start	<p>Enter the number of the target system record from which a batched reconciliation run must begin.</p> <p>Default value: 1</p> <p>This parameter is used in conjunction with the Batch Size, Number of Batches, Sort By, and Sort Direction parameters. All these parameters are discussed in <a href="#">Performing Batched Reconciliation</a>.</p>
Batch Size	<p>Enter the number of records that the connector must include in each batch that it fetches from the target system.</p> <p>Default value: 100</p> <p>This attribute is used in conjunction with the Batch Start, Number of Batches, Sort By, and Sort Direction attributes. All these attributes are discussed in <a href="#">Performing Batched Reconciliation</a>.</p>
Object Type	<p>This parameter holds the type of object you want to reconcile.</p> <p>Default value: <code>User</code></p> <p><b>Note:</b> If you configure the connector to provision users to a custom class (for example, <code>InetOrgPerson</code>) then enter the value of the object class here.</p>

**Table 3-10 (Cont.) Parameters of the Active Directory User Target Reconciliation and Active Directory User Target Concurrent Recon Jobs**

Parameter	Description
Search Base	<p>Enter the container in which the connector must search for user records during reconciliation.</p> <p>Sample Value: ou=org1,dc=corp,dc=com</p> <p><b>Note:</b> If you do not specify a value for this attribute, then the connector uses value specified as the value of the Container parameter of the Basic Configuration section as the value of this parameter.</p>

### Incremental Reconciliation Job

Use the Active Directory User Group Membership Recon job to reconcile user accounts with group changes. The first time you run this job, the connector fetches only the user account that was last updated in the target system and automatically populates the Sync Token parameter value with the latest timestamp. In the subsequent runs, the connector fetches only information about user accounts that have group changes.

**Table 3-11 Parameters of the Active Directory User Group Membership Recon Job**

Parameter	Description
Application Name	<p>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.</p> <p>Do <i>not</i> modify this value.</p>
Scheduled Task Name	<p>This parameter holds the name of the scheduled job.</p> <p><b>Note:</b> For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter.</p> <p>Default value: Active Directory User Group Membership Recon</p>
Object Type	<p>This parameter holds the type of object you want to reconcile.</p> <p>Default value: User</p> <p><b>Note:</b> If you configure the connector to provision users to a custom class (for example, InetOrgPerson) then enter the value of the object class here.</p>



**Table 3-11 (Cont.) Parameters of the Active Directory User Group Membership Recon Job**

Parameter	Description
Users Page Size	Enter the number of records that the connector must fetch in each call to the target system during a reconciliation run. Default value: 100
Timeout	Enter an integer value that specifies the number of seconds within which the connector must fetch the number of records specified in the Users Page Size parameter, failing which an exception is thrown. Default value: 300
Sync Token	Ensure that this parameter is left blank when you run group membership reconciliation for the first time. The connector fetches only the last-updated user record from the target system and automatically enters a value for this attribute in an XML serialized format. From the next reconciliation run onward, only data about records that are updated since the last reconciliation run ended are fetched into Oracle Identity Manager.
User Group MemberShip Recon	Enter <i>yes</i> to specify that the connector must fetch details of a user's group membership. Otherwise enter <i>no</i> , in which case the connector fetches only user data. Default value: <i>yes</i>

**Delete User Reconciliation Job**

The Active Directory User Target Delete Recon job is used to reconcile data about deleted users from a target application. During a reconciliation run, for each deleted user account on the target system, the Active Directory resource is revoked for the corresponding OIM User.

**Table 3-12 Parameters of the Active Directory User Target Delete Recon Job**

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. Do <i>not</i> modify this value.

**Table 3-12 (Cont.) Parameters of the Active Directory User Target Delete Recon Job**

Parameter	Description
Sync Token	<p>This parameter must be left blank when you run delete reconciliation for the first time. This ensures that data about all records that are deleted from the target system are fetched into Oracle Identity Governance.</p> <p>After the first delete reconciliation run, the connector automatically enters a value for this attribute in an XML serialized format. From the next reconciliation run onward, only data about records that are deleted since the last reconciliation run ended are fetched into Oracle Identity Governance.</p> <p>This attribute stores values in the following format:  <code>&lt;String&gt;0 {uSNChanged} {True/False} {DOMAIN_CONTROLLER}&lt;/String&gt;</code></p> <p>A value of <code>True</code> in the preceding format specifies that the Global Catalog Server is used during delete reconciliation runs. In addition, <code>DOMAIN_CONTROLLER</code> is replaced with the name of the domain controller on which the Global Catalog Server is running.</p> <p>A value of <code>False</code> specifies that the Global Catalog Server is not used during delete reconciliation runs. In addition, <code>DOMAIN_CONTROLLER</code> will be replaced with the name of the domain controller from which data about deleted records is fetched.</p>
Scheduled Task Name	<p>This parameter holds the name of the scheduled job.</p> <p><b>Note:</b> For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter.</p> <p>Default value: Active Directory User Target Delete Recon</p>
Object Type	<p>This parameter holds the type of object you want to reconcile.</p> <p>Default value: User</p> <p><b>Note:</b> If you configure the connector to provision users to a custom class (for example, <code>InetOrgPerson</code>) then enter the value of the object class here.</p>
Delete Recon	<p>This parameter specifies whether the connector must perform delete reconciliation.</p> <p>Default value: yes</p> <p><b>Note:</b> Do <i>not</i> change the value of this attribute.</p>

### Reconciliation Jobs for Entitlements

The following jobs are available for reconciling entitlements:

- Active Directory Organization Lookup Recon  
This reconciliation job is used to synchronize organization lookup fields in Oracle Identity Governance with organization-related data in the target system.
- Active Directory Group Lookup Recon

This reconciliation job is used to synchronize group lookup fields in Oracle Identity Governance with group-related data in the target system.

The parameters for both the reconciliation jobs are the same.

**Table 3-13 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. Do <i>not</i> modify this value.
Decode Attribute	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). Default value: <code>distinguishedName</code>
Filter	Enter a filter to filter out records to be stored in the lookup definition. For more information about the Filter attribute, see <a href="#">Performing Limited Reconciliation</a> .
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. Depending on the reconciliation job you are using, the default values are as follows: <ul style="list-style-type: none"> <li>• For Active Directory Organization Lookup Recon - <code>Lookup.ActiveDirectory.OrganizationalUnits</code></li> <li>• For Active Directory Group Lookup Recon - <code>Lookup.ActiveDirectory.Groups</code></li> </ul>
Object Type	Enter the type of object whose values must be synchronized. Depending on the scheduled job you are using, the default values are as follows: <ul style="list-style-type: none"> <li>• For Active Directory Organization Lookup Recon - <code>OrganizationalUnit</code></li> <li>• For Active Directory Group Lookup Recon - <code>Group</code></li> </ul> <b>Note:</b> Do <i>not</i> change the value of this attribute.
Code Key Attribute	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). Default value: <code>distinguishedName</code> <b>Note:</b> Do <i>not</i> change the value of this attribute.

## 3.5.2 Reconciliation Jobs for an Authoritative Application

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

### User Reconciliation Job

The Active Directory User Trusted Recon job is used to reconcile user data from a target application.

**Table 3-14 Parameters of the Active Directory User Trusted Recon Job**

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. Do <i>not</i> modify this value.
Number of Batches	Enter the number of batches in which the connector must reconcile user records. Default value: All
Search Scope	Enter <code>subtree</code> if you want the scope of the search for records to be reconciled to include the container specified by the Search Base parameter and all of its child containers. For example, if the search base is set to <code>OU=abc,DC=corp,DC=com</code> , then the search would cover the abc OU and all of its child OUs. Enter <code>onelevel</code> if you want the scope of the search for records to be restricted to only the container specified by the Search Base parameter. The connector does not include the child containers of the specified container in the search. For example if the search base is set to <code>OU=abc,DC=corp,DC=com</code> , then the search would cover only the abc OU. <b>Note:</b> If you want to enter <code>onelevel</code> , then ensure that you do not include a space between the words "one" and "level." Default value: <code>subtree</code>
Manager Id	Enter the distinguished name of a user who is a manager. The connector fetches all user records that have their manager properties set to this distinguished name. If you are using Microsoft Active Directory as the target system, then the default value of this parameter is <code>sAMAccountName</code> . If you are using Microsoft AD LDS as the target system, then set the value of this parameter to <code>__UPN_WO_DOMAIN__</code> . Default value: <code>sAMAccountName</code>

**Table 3-14 (Cont.) Parameters of the Active Directory User Trusted Recon Job**

Parameter	Description
Scheduled Task Name	<p>This parameter holds the name of the scheduled job.</p> <p><b>Note:</b> For the scheduled job included with this connector, you must not change the value of this parameter. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this parameter.</p> <p>Default value: <code>Active Directory User Trusted Recon</code></p>
Sort Direction	<p>Use this parameter to specify whether the connector must sort the records that it fetches in ascending or descending order. The value of this attribute can be either <code>asc</code> or <code>desc</code>.</p> <p>Default value: <code>asc</code></p>
Incremental Recon Attribute	<p>Enter the name of the target system attribute that holds last update-related number, non-decreasing value. For example, numeric or strings.</p> <p>The value in this attribute is used during incremental reconciliation to determine the newest or most youngest record reconciled from the target system.</p> <p>Default value: <code>uSNChanged</code></p>
Maintain Hierarchy	<p>Enter <code>yes</code> to specify that you want to maintain in Oracle Identity Governance the same organization hierarchy that is maintained on the target system. Otherwise, enter <code>no</code>.</p> <p>Default value: <code>no</code></p> <p><b>Note:</b> If you set this parameter to <code>yes</code>, then you must schedule the job for organization reconciliation (Active Directory Organization Recon) to run before this scheduled job.</p>
Sort By	<p>Enter the name of the target system field by which the connector must sort records in a batch.</p> <p>Default value: <code>samAccountName</code></p> <p><b>Note:</b> If you are using AD LDS as the target system, then change the default value of this parameter to some other attribute (for example, <code>cn</code>) because the <code>sAMAccountName</code> attribute does not exist on the AD LDS target system.</p>
Latest Token	<p>This parameter holds the value of the <code>uSNChanged</code> attribute of a domain controller that the connector uses for reconciliation.</p> <p><b>Note:</b> The reconciliation engine automatically enters a value for this attribute. It is recommended that you do not change the value of this parameter. If you manually specify a value for this attribute, then the connector only user accounts whose <code>uSNChanged</code> value is greater than the Latest Token attribute value.</p>

**Table 3-14 (Cont.) Parameters of the Active Directory User Trusted Recon Job**

Parameter	Description
Filter	<p>Enter the expression for filtering records that the scheduled job must reconcile.</p> <p>Sample value: <code>startsWith('userPrincipalName', 'John')</code></p> <p>For information about the filters expressions that you can create and use, see ICF Filter Syntax in <i>Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance</i>.</p>
Batch Start	<p>Enter the number of the target system record from which a batched reconciliation run must begin.</p> <p>Default value: 1</p> <p>This parameter is used in conjunction with the Batch Size, Number of Batches, Sort By, and Sort Direction parameters. All these parameters are discussed in <a href="#">Performing Batched Reconciliation</a>.</p>
Batch Size	<p>Enter the number of records that the connector must include in each batch that it fetches from the target system.</p> <p>Default value: 100</p> <p>This attribute is used in conjunction with the Batch Start, Number of Batches, Sort By, and Sort Direction attributes. All these attributes are discussed in <a href="#">Performing Batched Reconciliation</a>.</p>
Object Type	<p>This parameter holds the type of object you want to reconcile.</p> <p>Default value: User</p> <p><b>Note:</b> If you configure the connector to provision users to a custom class (for example, InetOrgPerson) then enter the value of the object class here.</p>
Search Base	<p>Enter the container in which the connector must search for user records during reconciliation.</p> <p>Sample Value: <code>ou=org1,dc=corp,dc=com</code></p> <p><b>Note:</b> If you do not specify a value for this attribute, then the connector uses value specified as the value of the Container parameter of the Basic Configuration section as the value of this parameter.</p>

### Delete User Reconciliation Job

The Active Directory User Trusted Delete Recon job is used to reconcile data about deleted users from an Authoritative application. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted.

**Table 3-15 Parameters of the Active Directory User Trusted Delete Recon Job**

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. Do <i>not</i> modify this value.
Sync Token	<p>This parameter must be left blank when you run delete reconciliation for the first time. This ensures that data about all records that are deleted from the target system are fetched into Oracle Identity Governance.</p> <p>After the first delete reconciliation run, the connector automatically enters a value for this attribute in an XML serialized format. From the next reconciliation run onward, only data about records that are deleted since the last reconciliation run ended are fetched into Oracle Identity Governance.</p> <p>This attribute stores values in the following format:  <code>&lt;String&gt;0 {uSNChanged} {True/False} {DOMAIN_CONTROLLER}&lt;/String&gt;</code></p> <p>A value of <code>True</code> in the preceding format specifies that the Global Catalog Server is used during delete reconciliation runs. In addition, <code>DOMAIN_CONTROLLER</code> is replaced with the name of the domain controller on which the Global Catalog Server is running.</p> <p>A value of <code>False</code> specifies that the Global Catalog Server is not used during delete reconciliation runs. In addition, <code>DOMAIN_CONTROLLER</code> will be replaced with the name of the domain controller from which data about deleted records is fetched.</p>
Scheduled Task Name	<p>This parameter holds the name of the scheduled job.</p> <p><b>Note:</b> For the scheduled job included with this connector, you must not change the value of this attribute. However, if you create a new job or create a copy of the job, then enter the unique name for that scheduled job as the value of this attribute.</p> <p>Default value: <code>Active Directory User Trusted Delete Recon</code></p>
Object Type	<p>This parameter holds the type of object you want to reconcile.</p> <p>Default value: <code>User</code></p> <p><b>Note:</b> If you configure the connector to provision users to a custom class (for example, <code>InetOrgPerson</code>) then enter the value of the object class here.</p>
Delete Recon	<p>This parameter specifies whether the connector must perform delete reconciliation.</p> <p>Default value: <code>yes</code></p> <p><b>Note:</b> Do <i>not</i> change the value of this attribute.</p>

# 4

## Performing the Postconfiguration Tasks for the Microsoft Active Directory User Management Connector

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

- [Configuring Oracle Identity Governance](#)
- [Configuring the IT Resource for the Target System](#)
- [Configuring the IT Resource for the Connector Server](#)
- [Harvesting Entitlements and Sync Catalog](#)
- [Enabling Logging for Microsoft Active Directory User Management Connector](#)
- [Localizing Field Labels in UI Forms](#)
- [Configuring the Connector for Provisioning Organizations](#)
- [Enabling and Disabling the Passwords Must Meet Complexity Requirements Policy setting](#)
- [Configuring SSL for Microsoft Active Directory and Microsoft AD LDS](#)
- [Setting Up the Lookup Definition for the Ignore Event API](#)

### 4.1 Configuring Oracle Identity Governance

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



**Note:**

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

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

- [Creating and Activating a Sandbox](#)
- [Creating a New UI Form](#)
- [Publishing a Sandbox](#)
- [Updating an Existing Application Instance with a New Form](#)



## 4.1.1 Creating and Activating a Sandbox

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

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

## 4.1.2 Creating a New UI Form

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

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

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

## 4.1.3 Publishing a Sandbox

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

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

## 4.1.4 Updating an Existing Application Instance with a New Form

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

To update an existing application instance with a new form:

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

 **See Also:**

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

## 4.2 Configuring the IT Resource for the Target System

If you have used the target system, then you must configure values for the parameters of the Active Directory IT resource.

If you are using the connector for group management or organizational unit management, then you must configure values for the parameters of the Active Directory IT resource.

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

In Oracle Identity System Administration, search for and edit the Active Directory IT resource to specify values for the parameters of IT resource listed in [Table 4-1](#). For more information about searching for IT resources and updating its parameters, see *Managing IT Resources in Oracle Fusion Middleware Administering Oracle Identity Governance*.

**Table 4-1 Parameters of the Active Directory IT Resource for the Target System**

Parameter	Description
ADLDSPort	Enter the number of the port at which Microsoft AD LDS is listening. Sample value: 50001 <b>Note:</b> Do not enter a value for this parameter if you are using Microsoft ActiveDirectory as the target system.
BDCHostNames	Enter the host name of the backup domain controller to which Oracle Identity Governance must switch to if the primary domain controller becomes unavailable. Sample value: mydc1;mydc2;mydc3 <b>Note:</b> Multiple backup domain controllers must be separated by semicolon (;).

**Table 4-1 (Cont.) Parameters of the Active Directory IT Resource for the Target System**

Parameter	Description
Configuration Lookup	<p>This parameter holds the name of the lookup definition that stores configuration information used during reconciliation and provisioning.</p> <p>If you have configured your target system as a target resource, then enter <code>Lookup.Configuration.ActiveDirectory</code>.</p> <p>If you have configured your target system as a trusted source, then enter <code>Lookup.Configuration.ActiveDirectory.Trusted</code>.</p> <p>Default value: <code>Lookup.Configuration.ActiveDirectory</code></p>
Connector Server Name	<p>Name of the IT resource of the type "Connector Server."</p> <p><b>Note:</b> Enter a value for this parameter only if you have deployed the Active Directory User Management connector in the Connector Server.</p> <p>Default value: <code>Active Directory Connector Server</code></p>
Container	<p>Enter the fully qualified domain name of the user container into or from which users must be provisioned or reconciled into Oracle Identity Governance, respectively.</p> <p>Sample value: <code>DC=example,DC=com</code></p>
DirectoryAdminName	<p>Enter the user name of account that you create by performing the procedure described in <a href="#">Creating a Target System User Account for Connector Operations</a>.</p> <p>Enter the value for this parameter in the following format: <code>DOMAIN_NAME\USER_NAME</code></p> <p>Sample value: <code>mydomain\admin</code></p> <p><b>Note:</b> If you are using AD LDS as the target system and this machine belongs to a workgroup, enter the username of the account created in <a href="#">Creating a Target System User Account for Connector Operations</a>.</p> <p>Enter a value for this parameter in the following format: <code>USER_NAME</code></p> <p>Sample value: <code>admin</code></p>
DirectoryAdminPassword	<p>Enter the password of the user account that you create by performing the procedure described in <a href="#">Creating a Target System User Account for Connector Operations</a>.</p>

**Table 4-1 (Cont.) Parameters of the Active Directory IT Resource for the Target System**

Parameter	Description
DomainName	<p>Enter the domain name for the Microsoft Active Directory domain controller on which the connector is being installed.</p> <p>Sample value: <code>example.com</code></p> <p><b>Note:</b> This is a mandatory parameter if you are using Microsoft Active Directory as the target system.</p>
isADLDS	<p>Enter <code>yes</code> to specify that the target system is Microsoft AD LDS.</p> <p>Enter <code>no</code> to specify that the target system is Microsoft Active Directory.</p>
LDAPHostName	<p>Enter the host name, IP address, or domain name of the Microsoft Windows computer (target system host computer) on which Microsoft Active Directory is installed.</p> <p><b>Note:</b> If you do not specify a value for this parameter and the <code>BDCHostNames</code> parameter (discussed earlier in this table), then a serverless bind is used. The connector leverages ADSI for determining the domain controller in the domain and then creates the directory entry. Therefore, all interactions with the target system are not specific to a domain controller.</p> <p>To determine the host name, on the computer hosting the target system, right-click <b>My Computer</b> and select <b>Properties</b>. On the Computer Name tab of the System Properties dialog box, the host name is specified as the value of the Full computer name field.</p> <p>Sample values:</p> <p><code>w2khost</code></p> <p><code>172.20.55.120</code></p> <p><code>example.com</code></p>
SyncDomainController	<p>Enter the name of the domain controller from which user accounts must be reconciled.</p> <p><b>Note:</b> The value specified in this parameter is used if the value of the <code>SearchChildDomains</code> lookup entry is set to <code>no</code>. If no value is specified for the <code>SyncDomainController</code> parameter and the <code>SearchChildDomains</code> lookup entry is set to <code>no</code>, then the connector automatically finds a domain controller for the target system and reconciles users from it.</p> <p>Sample value: <code>mynewdc</code></p>

**Table 4-1 (Cont.) Parameters of the Active Directory IT Resource for the Target System**

Parameter	Description
SyncGlobalCatalogServer	<p>Enter the host on which the global catalog server is located.</p> <p><b>Note:</b> The value specified in this parameter is used if the value of the SearchChildDomains lookup entry is set to <code>yes</code>. If no value is specified for the SyncGlobalCatalogServer parameter and the SearchChildDomains lookup entry is set to <code>yes</code>, then the connector automatically finds a global catalog server for the target system, and then reconciles user accounts from the domain controller on which the global catalog server is running.</p> <p>It is strongly recommended to provide a value for this parameter if you have set the SearchChildDomains lookup entry to <code>yes</code>.</p> <p>Sample value: <code>myglobalcatalogdc</code></p>
UseSSL	<p>Enter <code>yes</code> if the target system has been configured for SSL. This enables secure communication between the Connector Server and target system. Otherwise, enter <code>no</code>.</p> <p>Default value: <code>no</code></p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>For resetting user password during provisioning operations, the communication with the target system must be secure. The default communication between the .NET Connector Server and Microsoft Active Directory is secure. Therefore, even if you set the value of this parameter to <code>no</code>, it is possible to reset user passwords during provisioning operations because the default communication is secure.</li> <li>The default communication between the .NET Connect <a href="#">Configuring SSL for Microsoft Active Directory and Microsoft AD LDS</a> or Server and Microsoft AD LDS is not secure. Therefore, for enabling password reset provisioning operations, you must set the value of this parameter to <code>yes</code> to secure communication with Microsoft AD LDS. See <a href="#">Configuring SSL for Microsoft Active Directory and Microsoft AD LDS</a> for more information about configuring SSL.</li> </ul>

## 4.3 Configuring the IT Resource for the Connector Server

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

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

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

**Table 4-2 Parameters of the Active Directory Connector Server IT Resource**

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: <code>myhost.com</code>
Key	Enter the key for the connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: <code>8759</code>
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. Sample value: <code>0</code> A value of <code>0</code> 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> . Default value: <code>false</code> <b>Note:</b> It is recommended that you configure SSL to secure communication with the connector server. To configure SSL between Oracle Identity Governance and Connector Server, see <a href="#">Configuring SSL Between Oracle Identity Governance and Connector Server</a> .

## 4.4 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 [Scheduled Jobs for Lookup Field Synchronization](#)
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

 **See Also:**

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

## 4.5 Enabling Logging for Microsoft Active Directory User Management Connector

The Active Directory User Management connector uses the built-in logging mechanism of the .NET framework. Logging for the Active Directory User Management connector is not integrated with Oracle Identity Governance. The log level is set in the .NET Connector Server configuration file (ConnectorServer.exe.config).

To enable logging for the Active Directory User Management connector, perform the following procedure:

1. Go to the directory where the ConnectorServer.exe.config file is installed. The default directory is C:\Program Files\Identity Connectors\Connector Server.

The ConnectorServer.exe.config file must be present in this directory.

2. In the ConnectorServer.exe.config file, add the lines shown in bold text:

```
<system.diagnostics>
  <trace autoflush="true" indentsize="4">
    <listeners>
      <remove name="Default" />
      <add name="myListener"
type="System.Diagnostics.TextWriterTraceListener"
initializeData="c:\connectorserver2.log" traceOutputOptions="DateTime">
        <filter type="System.Diagnostics.EventTypeFilter"
initializeData="Information" />
      </add>
    </listeners>
  </trace>
  <switches>
    <add name="ActiveDirectorySwitch" value="4" />
  </switches>
</system.diagnostics>
```

The `value="4"` sets the log level to Verbose. This value can be set as any one of the following log levels:

- `value="4" or value="Verbose"`  
This value sets the log level to the "Verbose" level. It is most granular
- `value="3" or value="Information"`  
This value sets the log level to the "Information" level.
- `value="2" or value="Warning"`  
This value sets the log level to the "Warning" level
- `value="1" or value="Error"`  
This value sets the log level to the "Error" level

- `value="0"`

Logging is not configured when the value is set to "0".

However, remember that the logging level has a direct effect on the performance of the .NET Connector Server.

3. After you make the configuration change, stop and then restart the .NET Connector Server service. Or, you can also restart the .NET Connector Server using the following command:

```
ConnectorServer.exe /run
```

## 4.5.1 Configuring Log File Rotation

Information about events that occur during the course of reconciliation and provisioning operations are stored in a log file. As you use the connector over a period time, the amount of information written to a log file increases. If no rotation is performed, then log files become huge.

To avoid such a scenario, perform the procedure described in this section to configure rotation of the log file.

To configure rotation of a log file on a daily basis:

1. Log in to the computer that is hosting the Connector Server.
2. Stop the Connector Server.
3. Back up the ConnectorServer.exe.config file. The default location of this file is C:\Program Files\Identity Connectors\Connector Server.
4. In a text editor, open the ConnectorServer.exe.config file for editing.
5. Search for the `<listeners>` and `</listeners>` elements and replace the text between these elements with the following:

```
<remove name="Default" />
<add name="FileLog"
type="Microsoft.VisualBasic.Logging.FileLogTraceListener,Microsoft.VisualBasic,Version=8.0.0.0,Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"
initializeData="FileLogWriter"
traceOutputOptions="DateTime"
BaseFileName="ConnectorServerDaily"
Location="Custom"
CustomLocation="C:\ConnectorServerLog\"
LogFileCreationSchedule="Daily">
<filter type="System.Diagnostics.EventTypeFilter" initializeData="Information"/>
</add>
```

6. Save the file and close it.
7. Start the Connector Server.



### See Also:

The following URL for more information about configuring log file rotation:

<http://msdn.microsoft.com/en-us/library/microsoft.visualbasic.logging.filelogtracelistener.aspx>



## 4.6 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 field label that you add to in UI forms:

1. Log in to Oracle Enterprise Governance.
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 (oracle.iam.console.identity.sysadmin.ear\_V2.0\_metadata.zip) 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.xlf`

### Note:

You will not be able to view the BizEditorBundle.xlf unless you complete creating the application for your target system or perform any customization such as creating a UDF.

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 Microsoft Active Directory application instance. The original code is:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
<Field_Name>_c_description']">
<source><Field_Label></source>
```

```

<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ad11.entity.<UI_Form_Name>EO.<Field_Name>__c_LABEL">
<source><Field_Label></source>
<target/>
</trans-unit>

```

The sample edit of the code is as follows:

```

<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_ADUSER_FULLNAME__c_description']}">
<source>Full Name</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ad11.entity.ad11EO.UD_ADUSER_FULLNAME__c_LABEL">
<source>Full Name</source>
<target/>
</trans-unit>

```

- d. Open the resource file from the connector package, for example `ActiveDirectoryIdC_ja.properties`, and get the value of the attribute from the file, for example, `global.udf.UD_ADUSER_FULLNAME=\u6C0F\u540D`.
- e. Replace the original code shown in Step 6.c with the following:

```

<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_<Field_Name>__c_description']}">
<source><Field_Label></source>
<target>global.udf.<UD_<Field_Name></target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.<UI_Form_Name>.entity.
<UI_Form_Name>EO.UD_<Field_Name>__c_LABEL">
<source><Field_Label></source>
<target><global.udf.UD_<Field_Name></target>
</trans-unit>

```

As an example, the code for Full Name is as follows:

```

<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_ADUSER_FULLNAME__c_description']}">
<source>Full Name</source>
<target>\u6C0F\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.ad11.entity.ad11EO.UD_ADUSER_FULLNAME__c_LABEL">
<source>Full Name</source>
<target>\u6C0F\u540D</target>
</trans-unit>

```

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





**Note:**

The procedure to configure SSL is discussed later in this guide.

If you configure SSL and you want to enable both the default Microsoft Windows password policy and a custom password policy, then you must enable the "Passwords must meet complexity requirements" policy setting.



**Note:**

If you install Microsoft ADAM in a domain controller then it acquires all the policies of Microsoft Active Directory installed in the same domain controller. If you install Microsoft ADAM in a workgroup, then the local system policies are applied.

To enable or disable the "Passwords must meet complexity requirements" policy setting, check the password policy setting and select **Enabled** if you want to enable password policies or **Disabled** if you do not want to disable password policies.

For detailed information on enabling and disabling the "Passwords must meet complexity requirements" policy, see the Microsoft Active Directory User Management documentation.

## 4.9 Configuring SSL for Microsoft Active Directory and Microsoft AD LDS

This section discusses the following topics to configure SSL communication between Oracle Identity Governance and the target system:



**Note:**

- In this section, Microsoft ADAM and Microsoft AD LDS have both been referred to as **Microsoft AD LDS**.
- If you are using Microsoft AD LDS, then you must configure SSL for all connector operations to work as expected.
- For detailed instructions of the procedures, see the Microsoft Active Directory User Management documentation.

- [Prerequisites](#)
- [Configuring SSL Between Connector Server and Microsoft Active Directory](#)
- [Configuring SSL Between Connector Server and Microsoft AD LDS](#)
- [Configuring SSL Between Oracle Identity Governance and Connector Server](#)

## 4.9.1 Prerequisites

Public key certificates are used for determining the identity and authenticity of clients in software security systems. Certificate Services create and manage public key certificates. This ensures that organizations have a reliable and secure way to create, manage, and distribute these certificates.

### Note:

- Before you begin installing Active Directory Certificate Services (AD CS), you must ensure that Internet Information Services (IIS) is installed on the computer hosting the target system.
- For detailed steps to install Certificate Services on the corresponding Windows Server, refer to the Microsoft documentation.

If you are installing Certificate Services on Windows Server 2008, ensure to add the following features using the Server Manager console on the computer which is running the Connector Server:

- Remote Server Administration Tools
- Role Administration Tools
- Active Directory Certificate Services Tools
- AD DS and AD LDS Tools

## 4.9.2 Configuring SSL Between Connector Server and Microsoft Active Directory

You can configure SSL between Connector Server and Microsoft Active Directory by ensuring that the computer hosting Microsoft Active Directory has LDAP enabled over SSL (LDAPS).

### Note:

To configure SSL, the computer hosting the target system and the computer on which the Connector Server is running must be in the same domain.

To enable LDAPS, request a new certificate using the Automatic Certificate Request Setup Wizard.

## 4.9.3 Configuring SSL Between Connector Server and Microsoft AD LDS

To configure SSL between Connector Server and Microsoft AD LDS, ensure that ADAM is SSL-enabled.

To configure SSL between Connector Server and Microsoft AD LDS, perform the following procedures:

1. Request a certificate when Microsoft AD LDS is deployed within the connector domain or used as a standalone deployment.

 **Note:**

- This procedure can be performed either on the computer on which the Connector Server is running or on the computer hosting the target system.
- Before you begin generating the certificate, you must ensure that Internet Information Services (IIS) is installed on the target system host computer.

2. Issue the certificate that you requested earlier when Microsoft AD LDS was deployed within the connector domain in the Microsoft Active Directory Certificate Services window.
3. In the Microsoft Management Console, add the certificate to the personal store of the Microsoft AD LDS service.
4. Assign permissions to the MachineKeys folder that contains the certificate key. To do so, add the following groups and users and then provide full Control permission:
  - Administrators
  - Everyone
  - NETWORK SERVICE
  - The user name of the account used to install Microsoft ADAM
  - SYSTEM

Note that the path to the MachineKeys folder is similar to the following:

```
C:\Documents and Settings\All Users\Application  
Data\Microsoft\Crypto\RSA\MachineKeys
```

Assign the same groups and users to the certificate.

5. Restart the Microsoft AD LDS instance for the changes to take effect.
6. Test the certificate from the AD LDS Tools Command Prompt window. If SSL is successfully configured, then status messages about the connection are displayed on the LDAPS window.

## 4.9.4 Configuring SSL Between Oracle Identity Governance and Connector Server

The following sections provide information about configuring SSL between Oracle Identity Governance and Connector Server:

- [Exporting the Certificate](#)
- [Configuring the Connector Server for SSL](#)
- [Configuring Oracle Identity Governance for SSL](#)

### 4.9.4.1 Exporting the Certificate

**Note:**

Perform this procedure on the computer hosting the connector server.

To export the certificate requested and issued from the Microsoft Management console, navigate to and open the Certificate Export Wizard. Ensure to export the certificate in the Base-64 encoded X.509(.CER) file format.

### 4.9.4.2 Configuring the Connector Server for SSL

**Note:**

- Perform this procedure on the computer hosting the connector server.
- Connector Server 12c (12.2.1.3.0) can be used with older versions of connectors.

See *Configuring the .NET Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance* for detailed instructions to configure the Connector Server for SSL.

### 4.9.4.3 Configuring Oracle Identity Governance for SSL

The following is the procedure to configure Oracle Identity Governance for SSL:

1. Copy the certificate generated in [Exporting the Certificate](#) to the computer on which Oracle Identity Governance is running.
2. Import the target system certificate into the JDK used by Oracle Identity Governance (running on Oracle WebLogic Application Server) by running the following command:

```
keytool -import -keystore MY_CACERTS -file CERT_FILE_NAME -storepass  
PASSWORD
```

In this command:

- *MY\_CACERTS* is the full path and name of the certificate store (the default is cacerts).
- *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 command:

```
keytool -import -keystore /home/testoc4j/OIM/  
jrockit_160_14_R27.6.5-32/jre/lib/security/cacerts -file /home/  
ADSSLCer.cer -storepass sample_password
```

3. Import the target system certificate into the keystore of the application server by running the following command:

```
keytool -import -keystore MY_CACERTS -file CERT_FILE_NAME -storepass
PASSWORD
```

In this command:

- *MY\_CACERTS* is the full path and name of the certificate store (the default is *WEBLOGIC\_HOME/server/lib/DemoTrust.jks*)
- *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 command:

```
keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -file /
home/ADSSLCer.cer -storepass DemoTrustKeyStorePassPhrase
```

4. Set the value of the **UseSSL** parameter in [Basic Configuration Parameters](#) to `true`.

## 4.10 Setting Up the Lookup Definition for the Ignore Event API

This section discusses the following topics:

- [Understanding the Ignore Event Disabled Entry](#)
- [Adding the Ignore Event Disabled Entry](#)

### 4.10.1 Understanding the Ignore Event Disabled Entry

You can add the 'Ignore Event Disabled' entry to the Configuration lookup definition (Lookup.Configuration.ActiveDirectory.Trusted and Lookup.Configuration.ActiveDirectory for trusted source and target resource modes, respectively) to specify whether reconciliation events must be created for target system records that already exist in Oracle Identity Manager.

If you set the value of the Ignore Event Disabled entry to `true`, then reconciliation events are created for all records being fetched from the target system, irrespective of their presence in Oracle Identity Manager. If you set the value of this entry to `false`, then reconciliation events for target system records that are already present in Oracle Identity Manager are not created.

### 4.10.2 Adding the Ignore Event Disabled Entry

You add the 'Ignore Event Disabled' entry to specify whether reconciliation events must be created for target system records that already exist in Oracle Identity Manager. To do so:

1. Log in to the Design Console.
2. Expand **Administration**, and then double-click **Lookup Definition**.
3. Search for and open one of the following lookup definitions:  
For the trusted source mode: **Lookup.Configuration.ActiveDirectory.Trusted**  
For target resource mode: **Lookup.Configuration.ActiveDirectory**
4. On the Lookup Code Information tab, click **Add**.  
A new row is added.



5. In the **Code Key** column of the new row, enter `Ignore Event Disabled`.
6. In the **Decode** column of the new row, depending on your requirement, enter `true` or `false`.
7. Click the Save icon.

 **Note:**

If you are adding the Ignore Event Disabled entry in the AOB installation setup, then open the Advanced Settings section and perform step 4 onwards only.

# 5

## Using the Microsoft Active Directory User Management Connector

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

The following topics discuss information related to using the connector for performing reconciliation and provisioning operations:

### Note:

These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- [Guidelines on Using the Microsoft Active Directory User Management Connector](#)
- [Configuring Reconciliation](#)
- [Scheduled Jobs for Lookup Field Synchronization](#)
- [Configuring and Running Group Reconciliation](#)
- [Configuring and Running Organization Reconciliation](#)
- [Configuring Reconciliation Jobs](#)
- [Performing Provisioning Operations](#)
- [Connector Objects Used for Groups Management](#)
- [Connector Objects Used for Organizational Units Management](#)
- [Uninstalling the Connector](#)

### 5.1 Guidelines on Using the Microsoft Active Directory User Management Connector

These guidelines give information on what to do when using the connector.

You must apply the following guidelines while performing reconciliation and provisioning operations:

- [Guidelines on Configuring Reconciliation](#)
- [Guidelines on Performing Provisioning Operations](#)

## 5.1.1 Guidelines on Configuring Reconciliation

The following are guidelines that you must apply while configuring reconciliation:

- Before a target resource reconciliation run is performed, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before user reconciliation runs.
- If you are using Oracle Identity Governance release 11.1.2.x or later, then before you perform a reconciliation run, create an application instance.
- The scheduled job for user reconciliation must be run before the scheduled job for reconciliation of deleted user data.
- In the identity reconciliation mode, if you want to configure group reconciliation, then note that group reconciliation does not cover reconciliation of updates to existing groups on the target system. If you modify the name of a group on the target system, then it is reconciled as a new group in Oracle Identity Governance.
- In the identity reconciliation mode, if you want to configure organization reconciliation, then note that:
  - Organization reconciliation does not cover reconciliation of updates to existing organization names on the target system. If you modify the name of an organization on the target system, then it is reconciled as a new organization in Oracle Identity Governance.
  - Organization reconciliation events created by the scheduled job for organization reconciliation (Active Directory Organization Recon) must be successfully processed before the scheduled job for trusted source reconciliation (Active Directory User Trusted Recon) is run. In other words, organization reconciliation must be run and the organization records reconciled from the target system must be successfully linked in Oracle Identity Governance.
  - On the target system, users are created in specific organizations. During trusted source reconciliation of user data, if you want OIM Users to be created in the same organizations on Oracle Identity Governance, then you must set the MaintainHierarchy attribute of the trusted source reconciliation scheduled task to `yes`. In addition, you must configure organization reconciliation to run before trusted source reconciliation.
  - In Oracle Identity Governance, the organization namespace is a flat namespace although it allows parent-child hierarchical relationships between organizations. Therefore, two Microsoft Active Directory OUs with the same name cannot be created in Oracle Identity Governance, even if they have different parent OUs on the target system.
  - The name of an organization in Oracle Identity Governance cannot contain special characters, such as the equal sign (=) and comma (,). However, these special characters can be used in the name of an organization on the target system.
  - The synchronization of organization lookup fields is independent of whether or not you configure organization reconciliation.
- If you are going to configure Microsoft AD LDS as the trusted source, then you must ensure that a value (either `true` or `false`) is set for the `msDS-`

UserAccountDisabled field of each user record on the target system. In Microsoft ADAM, the msDS-UserAccountDisabled field does not have a default value.

- The Filter attribute must contain only attributes that are present in the Decode column of the lookup definition that holds reconciliation attribute mapping.

## 5.1.2 Guidelines on Performing Provisioning Operations

The following are guidelines that you must apply while performing provisioning operations:

- Before you perform provisioning operations, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before provisioning operations.
- When both Microsoft Active Directory User Management and Microsoft Exchange connectors are deployed in your environment, do *not* specify a value for the Redirection Mail Id field.

If you specify a value for the Redirection Mail Id field during a user provisioning operation, then a corresponding mail user account is created in Microsoft Exchange. When an Exchange mail user account is created through Active Directory, then some of the fields of an Exchange mail user account such as Maximum Receive Size cannot be updated. This also means that the Microsoft Exchange Connector cannot be used for further provisioning operations of this user. This is because the user is already created in Microsoft Exchange as a Mailuser.

Note that the Microsoft Exchange connector cannot be used to convert Mailuser, mail user accounts created in the manner described in the preceding paragraph, to Mailbox as this is not allowed by the target. Therefore, it is recommended not to specify a value for the Redirection Mail Id field if both Microsoft Active Directory and Microsoft Exchange connector are deployed.

- Passwords for user accounts provisioned from Oracle Identity Governance must adhere to the password policy set in Microsoft Active Directory.

### Note:

If you install Microsoft ADAM in a domain controller then it acquires all the policies of Microsoft Active Directory installed in the same domain controller. If you install Microsoft ADAM in a workgroup, then the local system policies are applied.

In Microsoft Active Directory, password policies are controlled through password complexity rules. These complexity rules are enforced when passwords are changed or created. While changing the password of a Microsoft Active Directory account by performing a provisioning operation on Oracle Identity Governance, you must ensure that the new password adheres to the password policies on the target system.

### See Also:

For more information about password guidelines applicable on the target system, see the Microsoft Active Directory User Management documentation.

- Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

- The character length of target system fields must be taken into account when specifying values for the corresponding Oracle Identity Governance fields. For example, ensure that the value you specify for the User Login field in Oracle Identity Governance contains no more than 20 characters. This is because the sAMAccountName attribute in the target system (corresponding to the User Login field in Oracle Identity Governance) cannot contain more than 20 characters.
- On the target system, the Manager Name field accepts only DN values. Therefore, when you set or modify the Manager Name field on Oracle Identity Governance, you must enter the DN value.

For example:

```
cn=abc,ou=lmn,dc=corp,dc=com
```

- If the value that you specify for the Manager Name field contains special characters, then you must prefix each special character with a backslash (\). For example, if you want to specify CN=John Doe #2,OU=sales,DC=example,DC=com as the value of the Manager Name field, then you must specify the following as the value:

```
CN=John Doe \#2,OU=sales,DC=example,DC=com
```

The following is the list of special characters that must be prefixed with a backslash (\):

- Number sign (#)
  - Backslash (\)
  - Plus sign (+)
  - Equal sign (=)
  - Comma (,)
  - Semicolon (;)
  - Less than symbol (<)
  - Greater than symbol (>)
  - Quotation mark (")
- While specifying a value for the Home Directory field, follow these guidelines:
    - The value must always begin with two backslashes (\\).
    - The value must contain at least one backslash (\), but not at the end.

**Correct sample values:**

```
\\SOME_MACHINE\SOME_SHARE\SOME_DIRECTORY
```

```
\\SOME_MACHINE\SOME_SHARE\SOME_DIRECTORY\SOME_OTHER_DIRECTORY
```

**Incorrect sample values:**

```
\\SOME_MACHINE\SOME_SHARE\  
\\SOME_MACHINE
```

- If you want to provision users and groups under the Users container, then include the following entry in the **Lookup.ActiveDirectory.OrganizationalUnits** lookup definition:

**Code Key:**

```
IT_RESOURCE_KEY~CN=Users,DC=childtest,DC=test,DC=idm,DC=central,DC=example,DC=com
```

**Decode:**

```
IT_RESOURCE_NAME~CN=Users,DC=childtest,DC=test,DC=idm,DC=central,DC=example,DC=com
```

In the Code Key and Decode values, replace:

- *IT\_RESOURCE\_KEY* with the numeric code assigned to each IT resource in Oracle Identity Governance. You can determine the value of the IT resource key by performing lookup field synchronization of organizational units and then finding the IT resource key from the code key value of the Lookup.ActiveDirectory.OrganizationalUnits lookup definition.
- *IT\_RESOURCE\_NAME* with the name of the IT resource in Oracle Identity Governance.

## 5.2 Configuring Reconciliation

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

This section discusses the following topics related to configuring reconciliation:

- [Performing Full Reconciliation and Incremental Reconciliation](#)
- [Performing Limited Reconciliation](#)
- [Performing Batched Reconciliation](#)

### 5.2.1 Performing Full Reconciliation and Incremental 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.

In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Governance.

For performing a full reconciliation run, values for the following parameters of the jobs for reconciling user records must not be present:

- Batch Start
- Filter
- Latest Token

At the end of the reconciliation run, the Latest Token parameter of the job for user record reconciliation is automatically set to the highest value of the uSNChanged attribute of a domain controller that is used for reconciliation. From the next run onward, only records

created or modified after the value in the latest token attribute are considered for reconciliation. This is incremental reconciliation.

## 5.2.2 Performing Limited Reconciliation

These topics help you understand limited reconciliation and the ways in which it can be achieved.

- [About Limited Reconciliation](#)
- [Performing Limited Reconciliation By Using Filters](#)
- [Performing Limited Reconciliation By Using the Search Base Attribute](#)

### 5.2.2.1 About Limited Reconciliation

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 can perform limited reconciliation the first time you perform a reconciliation run. In other words, by using filters or by specifying a search base while configuring a scheduled job for full reconciliation, you can perform limited reconciliation.

### 5.2.2.2 Performing Limited Reconciliation By Using Filters

You can perform limited reconciliation by creating filters for the reconciliation module.

This connector provides a Filter attribute (a scheduled task attribute) that allows you to use any of the Microsoft Active Directory resource attributes to filter the target system records. [Table 5-1](#) lists the filter syntax that you can use and the corresponding description and sample values.



#### Note:

Filters with wildcard characters are not supported.

**Table 5-1 Keywords and Syntax for the Filter Attribute**

Filter Syntax	Description
<b>String Filters</b>	
<code>startsWith('ATTRIBUTE_NAME','PREFIX')</code>	Records whose attribute value starts with the specified prefix are reconciled. <b>Example:</b> <code>startsWith('userPrincipalName','John')</code> In this example, all records whose <code>userPrincipalName</code> begins with 'John' are reconciled.

Table 5-1 (Cont.) Keywords and Syntax for the Filter Attribute

Filter Syntax	Description
<code>endsWith('ATTRIBUTE_NAME','SUFFIX')</code>	<p>Records whose attribute value ends with the specified suffix are reconciled.</p> <p><b>Example:</b> <code>endsWith('sn','Doe')</code></p> <p>In this example, all records whose last name ends with 'Doe' are reconciled.</p>
<code>contains('ATTRIBUTE_NAME','STRING')</code>	<p>Records where the specified string is contained in the attribute's value are reconciled.</p> <p><b>Example:</b> <code>contains('displayName','Smith')</code></p> <p>In this example, all records whose display name contains 'Smith' are reconciled.</p>
<code>containsAllValues('ATTRIBUTE_NAME', ['STRING1','STRING2',...,'STRINGn'])</code>	<p>Records that contain all the specified strings for a given attribute are reconciled.</p> <p><b>Example:</b> <code>containsAllValues('objectClass', ['person','top'])</code></p> <p>In this example, all records whose objectClass contains both "top" and "person" are reconciled.</p>
<b>Equality and Inequality Filters</b>	
<code>equalTo('ATTRIBUTE_NAME','VALUE')</code>	<p>Records whose attribute value is equal to the value specified in the syntax are reconciled.</p> <p><b>Example:</b> <code>equalTo('sAMAccountName','Sales Organization')</code></p> <p>In this example, all records whose sAMAccountName is Sales Organization are reconciled.</p>
<code>greaterThan('ATTRIBUTE_NAME','VALUE')</code>	<p>Records whose attribute value (string or numeric) is greater than (in lexicographical or numerical order) the value specified in the syntax are reconciled.</p> <p><b>Example 1:</b> <code>greaterThan('cn','bob')</code></p> <p>In this example, all records whose common name is present after the common name 'bob' in the lexicographical order (or alphabetical order) are reconciled.</p> <p><b>Example 2:</b> <code>greaterThan('employeeNumber','1000')</code></p> <p>In this example, all records whose employee number is greater than 1000 are reconciled.</p>
<code>greaterThanOrEqualTo('ATTRIBUTE_NAME','VALUE')</code>	<p>Records whose attribute value (string or number) is lexicographically or numerically greater than or equal to the value specified in the syntax are reconciled.</p> <p><b>Example 1:</b> <code>greaterThanOrEqualTo('sAMAccountName','S')</code></p> <p>In this example, all records whose sAMAccountName is equal to 'S' or greater than 'S' in lexicographical order are reconciled.</p> <p><b>Example 2:</b> <code>greaterThanOrEqualTo('employeeNumber','1000')</code></p> <p>In this example, all records whose employee number is greater than or equal to 1000 are reconciled.</p>



Table 5-1 (Cont.) Keywords and Syntax for the Filter Attribute

Filter Syntax	Description
<code>lessThan('ATTRIBUTE_NAME','VALUE')</code>	<p>Records whose attribute value (string or numeric) is less than (in lexicographical or numerical order) the value specified in the syntax are reconciled.</p> <p><b>Example 1:</b> <code>lessThan('sn','Smith')</code></p> <p>In this example, all records whose last name is present after the last name 'Smith' in the lexicographical order (or alphabetical order) are reconciled.</p> <p><b>Example 2:</b> <code>lessThan('employeeNumber','1000')</code></p> <p>In this example, all records whose employee number is less than 1000 are reconciled.</p>
<code>lessThanOrEqualTo('ATTRIBUTE_NAME','VALUE')</code>	<p>Records whose attribute value (string or numeric) is lexicographically or numerically less than or equal to the value specified in the syntax are reconciled.</p> <p><b>Example 1:</b> <code>lessThanOrEqualTo('sAMAccountName','A')</code></p> <p>In this example, all records whose sAMAccountName is equal to 'A' or less than 'A' in lexicographical order are reconciled.</p> <p><b>Example 2:</b> <code>lessThanOrEqualTo('employeeNumber','1000')</code></p> <p>In this example, all records whose employee number is less than or equal to 1000 are reconciled.</p>
<b>Complex Filters</b>	
<code>&lt;FILTER1&gt; &amp; &lt;FILTER2&gt;</code>	<p>Records that satisfy conditions in both filter1 and filter2 are reconciled. In this syntax, the logical operator &amp; (ampersand symbol) is used to combine both filters.</p> <p><b>Example:</b> <code>startsWith('cn','John') &amp; endsWith('sn','Doe')</code></p> <p>In this example, all records whose common name starts with John and last name ends with Doe are reconciled.</p>
<code>&lt;FILTER1&gt;   &lt;FILTER2&gt;</code>	<p>Records that satisfy either the condition in filter1 or filter2 are reconciled. In this syntax, the logical operator   (vertical bar) is used to combine both filters.</p> <p><b>Example:</b> <code>contains('sAMAccountName','Andy')   contains('sn','Brown')</code></p> <p>In this example, all records that contain 'Andy' in the sAMAccountName attribute or records that contain 'Brown' in the last name are reconciled.</p>
<code>not(&lt;FILTER&gt;)</code>	<p>Records that do not satisfy the given filter condition are reconciled.</p> <p><b>Example:</b> <code>not(contains('cn','Mark'))</code></p> <p>In this example, all records that does not contain the common name 'Mark' are reconciled.</p>

### 5.2.2.3 Performing Limited Reconciliation By Using the Search Base Attribute

You can perform limited reconciliation by using the Search Base parameter of the reconciliation job.

By specifying a value for the Search Base parameter, you can limit the container from which the user, group, or organization records must be reconciled. This is the starting point for the search in the hierarchical structure for objects in Microsoft Active Directory.

## 5.2.3 Performing Batched Reconciliation

You can perform batched reconciliation to reconcile a specific number of records from the target system into Oracle Identity Governance.

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete. You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, specify values for the following parameter of the reconciliation jobs:

- **Batch Size:** Use this parameter to specify the number of records that must be included in each batch.
- **Batch Start:** Use this parameter to specify the record number from which batched reconciliation must begin.
- **Number of Batches:** Use this parameter to specify the total number of batches that must be reconciled. The default value of this parameter is `All`. If you do not want to implement batched reconciliation, then accept the default value. When you accept the default value, the values of the Batch Size, Batch Start, Sort By, and Sort Direction parameters are ignored.
- **Sort By:** Use this parameter to specify the name of the target system field by which the records in a batch must be sorted.
- **Sort Direction:** Use this parameter to specify the whether records being fetched must be sorted in ascending or descending order. The value of this parameter can be either `asc` or `desc`.

If batched reconciliation fails, then you only need to rerun the reconciliation job without changing the values of the job parameters.

After completing batched reconciliation, if you want to perform incremental reconciliation, then specify the value of the `highestCommittedUSN` attribute (see Step 3 of [Preupgrade Steps](#)) as the value of the Latest Token parameter. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token parameter.



### Note:

Sorting large number of records on the target system fails during batched reconciliation. Therefore, it is recommended that you use the `PageSize` parameter of [Advanced Settings Parameters](#) to fetch records from the target system.

## 5.3 Scheduled Jobs for Lookup Field Synchronization

Scheduled jobs for lookup field synchronization fetch the most recent values from specific fields in the target system to lookup definitions in Oracle Identity Governance. These lookup definitions are used as an input source for lookup fields in Oracle Identity Governance.

The following are the scheduled jobs for lookup field synchronization:



### Note:

The procedure to configure these scheduled tasks is described later in the guide.

- **Active Directory Group Lookup Recon**  
This scheduled task is used to synchronize group lookup fields in Oracle Identity Governance with group-related data in the target system.
- **Active Directory Organization Lookup Recon**  
This scheduled task is used to synchronize organization lookup fields in Oracle Identity Governance with organization-related data in the target system.

[Table 5-2](#) describes the attributes of both scheduled jobs.

**Table 5-2 Attributes of the Scheduled Tasks for Lookup Field Synchronization**

Attribute	Description
Code Key Attribute	<p>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). Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> <li>• For Active Directory Group Lookup Recon: <code>distinguishedName</code></li> <li>• For Active Directory Organization Lookup Recon: <code>distinguishedName</code></li> </ul> <p><b>Note:</b> You must not change the value of this attribute.</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). Depending on the scheduled job you are using, the default values are as follows:</p> <ul style="list-style-type: none"> <li>• For Active Directory Group Lookup Recon: <code>distinguishedName</code></li> <li>• For Active Directory Organization Lookup Recon: <code>distinguishedName</code></li> </ul>
Filter	<p>Enter a filter to filter out records to be stored in the lookup definition. For more information about the Filter attribute, see <a href="#">Performing Limited Reconciliation</a>.</p>

**Table 5-2 (Cont.) Attributes of the Scheduled Tasks for Lookup Field Synchronization**

Attribute	Description
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile records. Sample value: <code>Active Directory</code>
Lookup Name	Enter the name of the lookup definition in Oracle Identity Governance that must be populated with values fetched from the target system. <b>Note:</b> If the lookup name that you specify as the value of this attribute is not present in Oracle Identity Governance, then this lookup definition is created while the scheduled job is run. Depending on the scheduled job you are using, the default values are as follows: <ul style="list-style-type: none"> <li>For Active Directory Group Lookup Recon: <code>Lookup.ActiveDirectory.Groups</code></li> <li>For Active Directory Organization Lookup Recon: <code>Lookup.ActiveDirectory.OrganizationalUnits</code></li> </ul>
Object Type	This attribute holds the name of the type of object you want to reconcile. Depending on the scheduled job you are using, the default values are as follows: <ul style="list-style-type: none"> <li>For Active Directory Group Lookup Recon: <code>Group</code></li> <li>For Active Directory Organization Lookup Recon: <code>OrganizationalUnit</code></li> </ul>

## 5.4 Configuring and Running Group Reconciliation

There are two scenarios in which group reconciliation can be performed.

Depending on the scenario in which you want to perform group reconciliation, perform one of the following procedures:

- See [Reconciling Target System Groups into Individual Organizations](#) to reconcile each target system group into an organization of its own.
- See [Reconciling Target System Groups a Single Organization](#) to reconcile each target system group into a single organization.

### 5.4.1 Reconciling Target System Groups into Individual Organizations

Create an organizational unit in Oracle Identity Governance with the name of the group (available in the target system), and then reconcile groups to this newly created organizational unit. In other words, suppose a scenario in which you want every target system group to be reconciled into an organization of its own.

To perform group reconciliation in this scenario:

- Ensure that the value of the Configuration Lookup parameter of the IT resource is set to `Lookup.Configuration.ActiveDirectory`.
- Search for and open the **Active Directory Group Recon** scheduled job.
- Set the value of the Resource Object Name attribute of the scheduled job to `Xellerate Organization`. Note that you need not specify a value for the Organization Name

attribute. If you specify a value for the Organization Name attribute, then the value is ignored.

4. Run the Active Directory Group Recon scheduled job.
5. After completion of the reconciliation run:
  - Clear the value in the Latest Token attribute of the scheduled job.
  - Specify `AD Group` as value of the Resource Object Name attribute of the scheduled job.
6. Run the Active Directory Group Recon scheduled job again.
7. In the Administrative and User Console, verify whether an organizational unit with the name of the group is created, and then the organizational unit has the AD Group resource object in the 'Provisioned' state.

## 5.4.2 Reconciling Target System Groups a Single Organization

This procedure describes how to perform group reconciliation when all groups available on the target system must be reconciled under the same organizational unit in Oracle Identity Governance. In other words, suppose a scenario in which you want all target system groups to be reconciled into a single organization.

To perform group reconciliation in this scenario:

1. Log in to the Design Console.
2. Expand **Administration**, and then double-click **Lookup Definition**.
3. Search for and open the **Lookup.ActiveDirectory.GM.ReconAttrMap** lookup definition.
4. Change the Decode value of the **OIM Org Name** entry from `sAMAccountName` to `Organization Name`.
5. Save and close the lookup definition.
6. Log in to the Administrative and User Console.
7. Search for and open the **Active Directory Group Recon** scheduled job, and then:
  - Clear the value in the Latest Token attribute.
  - In the **Resource Object Name** attribute field, specify `AD Group` as the value.
  - In the **Organization Name** attribute field, specify the name of an organizational unit under which all groups from the target system must be reconciled.
8. Run the Active Directory Group Recon scheduled job.

## 5.5 Configuring and Running Organization Reconciliation

You can configure and run the scheduled job for organization reconciliation.

The following is the procedure to run the scheduled job for organization reconciliation:

1. Ensure that the value of the Configuration Lookup parameter of the IT resource is set to `Lookup.Configuration.ActiveDirectory.Trusted`.
2. Search for and open the **Active Directory Organization Recon** scheduled job.

3. Set the value of the Resource Object Name attribute of the scheduled job to `Xellerate Organization`. This creates organizations in Oracle Identity Governance after the scheduled job is run.
4. Run the Active Directory Organization Recon scheduled job.
5. After completion of the reconciliation run:
  - Clear the value in the Latest Token attribute of the scheduled job.
  - Specify `AD Organizational Unit` as value of the Resource Object Name attribute of the scheduled job.
6. Set the value of the Configuration Lookup parameter of the IT resource to `Lookup.Configuration.ActiveDirectory`.
7. Run the Active Directory Organization Recon scheduled job again.
8. In the Administrative and User Console, verify whether the AD Organizational Unit Resource is provisioned to the organizations created in Step 3 of this section.

 **Note:**

OIM created Organizations do not relate to the OU objects on the Directory Resources of Microsoft Active Directory. The connector does not support the creation of any OU objects in OIM which can then be provisioned to Microsoft Active Directory. Instead, OUs can be created directly on the Directory Services of Microsoft Active Directory.

In addition, as a best practice, ensure that all newly created OUs and other objects are fetched into OIM from the target system by performing a trusted resource reconciliation run.

## 5.6 Configuring Reconciliation Jobs

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

You can apply this procedure to configure the reconciliation jobs for users and entitlements.

To configure a reconciliation job:

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

- **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type. See *Creating Jobs in Oracle Fusion Middleware Administering Oracle Identity Governance*.

In addition to modifying the job details, you can enable or disable a job.

5. On the **Job Details** tab, in the Parameters region, specify values for the attributes of the scheduled task.

 **Note:**

Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

6. Click **Apply** to save the changes.

 **Note:**

You can use the Scheduler Status page in Identity System Administration to either start, stop, or reinitialize the scheduler.

## 5.7 Performing Provisioning Operations

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

To perform provisioning operations in Oracle Identity Governance:

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

 **See Also:**

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

## 5.8 Connector Objects Used for Groups Management

Learn about the objects that are used by the connector to perform group management operations such as create, update, and delete.

- [Preconfigured Lookup Definitions for Group Operations](#)
- [Reconciliation Scheduled Jobs for Groups Management](#)
- [Reconciliation Rules and Action Rules for Groups Management](#)

### 5.8.1 Preconfigured Lookup Definitions for Group Operations

The lookup definitions for Groups are automatically created in Oracle Identity Governance after you create the application by using the connector.

- [Lookup.ActiveDirectory.GM.Configuration](#)
- [Lookup.ActiveDirectory.GM.ProvAttrMap](#)
- [Lookup.ActiveDirectory.GM.ReconAttrMap](#)
- [Lookup.ActiveDirectory.GM.ProvValidation](#)
- [Lookup.ActiveDirectory.GM.ReconTransformation](#)
- [Lookup.ActiveDirectory.GM.ReconValidation](#)
- [Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults](#)
- [Lookup.ActiveDirectory.GroupTypes](#)

#### 5.8.1.1 Lookup.ActiveDirectory.GM.Configuration

The `Lookup.ActiveDirectory.GM.Configuration` lookup definition holds configuration entries that are specific to the group object type. This lookup definition is used during group management operations when your target system is configured as a target resource.

[Table 5-3](#) lists the default entries in this lookup definition.

**Table 5-3** Entries in the `Lookup.ActiveDirectory.GM.Configuration` Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	<code>Lookup.ActiveDirectory.GM.ProvAttrMap</code>	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See <a href="#">Lookup.ActiveDirectory.GM.ProvAttrMap</a> for more information about this lookup definition.



**Table 5-3 (Cont.) Entries in the Lookup.ActiveDirectory.GM.Configuration Lookup Definition**

Code Key	Decode	Description
Provisioning Validation Lookup	Lookup.ActiveDirectory.GM.ProvValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See <a href="#">Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units</a> for more information about adding entries in this lookup definition.
Recon Attribute Defaults	Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults	This entry holds the name of the lookup definition that maps fields on the group form and their default values. See <a href="#">Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults</a> for more information about this lookup definition.
Recon Attribute Map	Lookup.ActiveDirectory.GM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See <a href="#">Lookup.ActiveDirectory.GM.ReconAttrMap</a> for more information about this lookup definition.
Recon Transformation Lookup	Lookup.ActiveDirectory.GM.ReconTransformation	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See <a href="#">Configuring Transformation of Data During Reconciliation for Groups and Organizational Units</a> for more information about adding entries in this lookup definition.
Recon Validation Lookup	Lookup.ActiveDirectory.GM.ReconValidation	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation. See <a href="#">Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults</a> for more information about adding entries in this lookup definition.

### 5.8.1.2 Lookup.ActiveDirectory.GM.ProvAttrMap

The Lookup.ActiveDirectory.GM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is preconfigured and is used during group provisioning operations.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning.

**Table 5-4 Default Entries in the Lookup.ActiveDirectory.GM.ProvAttrMap**

Group Field on Oracle Identity Governance (Code Key)	Target System Field (Decode)	Description
__NAME__	__NAME__="CN=\${Group_Name},\${Organization_Name}"	Group name with full DN
Display Name	displayName	Display name for a group
Group Name	sAMAccountName	Group name
Group Type	groupType	Group type
Organization Name[LOOKUP,IGNORE]	IGNORED	Name of the organization to which the group belongs

**Table 5-4 (Cont.) Default Entries in the Lookup.ActiveDirectory.GM.ProvAttrMap**

Group Field on Oracle Identity Governance (Code Key)	Target System Field (Decode)	Description
Unique Id	__UID__	Object GUID of the group

### 5.8.1.3 Lookup.ActiveDirectory.GM.ReconAttrMap

The Lookup.ActiveDirectory.GM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is preconfigured and used for performing target resource group reconciliation runs.

[Table 5-5](#) lists the group fields of the target system from which values are fetched during reconciliation. The Active Directory Group Recon scheduled job is used to reconcile group data.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation.

**Table 5-5 Entries in the Lookup.ActiveDirectory.GM.ReconAttrMap**

Group Field on Oracle Identity Governance (Code Key)	Microsoft Active Directory Field (Decode)	Description
Display Name	displayName	Display name for a group
Group name	sAMAccountName	Group name
Group Type	groupType	Group type
OIM Org Name	sAMAccountName	OIM organization name Note that this value does not contain the DN.
Organization Name[LOOKUP]	ad_container	Organization name with DN format For example, OU=Org1,DC=example,dc=com
Org Name	sAMAccountName	Organization name without DN format
Org Type	OIM Organization Type	Organization type
Unique Id	__UID__	Object GUID of the group

### 5.8.1.4 Lookup.ActiveDirectory.GM.ProvValidation

The Lookup.ActiveDirectory.GM.ProvValidation lookup definition is used to configure validation of attribute values entered on the process form during group provisioning operations. See [Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units](#) or more information about adding entries in this lookup definition.

### 5.8.1.5 Lookup.ActiveDirectory.GM.ReconTransformation

The Lookup.ActiveDirectory.GM.ReconTransformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See [Configuring Transformation of Data During Reconciliation for Groups and Organizational Units](#) for more information about adding entries in this lookup definition.

### 5.8.1.6 Lookup.ActiveDirectory.GM.ReconValidation

The Lookup.ActiveDirectory.GM.ReconValidation lookup definition is used to configure validation of attribute values that are fetched from the target system during group reconciliation. See [Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units](#) for more information about adding entries in this lookup definition.

### 5.8.1.7 Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults

The Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults lookup definition holds mappings between reconciliation fields (for group) and their default values. This lookup definition is used when there is a mandatory field on the group form, but no corresponding field in the target system from which values can be fetched during group reconciliation.

This lookup definition is empty by default. If you add entries to this lookup definition, then the Code Key and Decode values must be in the following format:

**Code Key:** Name of the reconciliation field of the AD Group resource object

**Decode:** Corresponding default value to be displayed

For example, assume a field named Group ID is a mandatory field on the group form. Suppose the target system contains no field that stores information about the group ID for an account. During reconciliation, no value for the Group ID field is fetched from the target system. However, as the Group ID field cannot be left empty, you must specify a value for this field. Therefore, create an entry in this lookup definition with the Code Key value set to `Group ID` and Decode value set to `GRP1223`. This implies that the value of the Group ID field on the group form displays GRP1223 for all accounts reconciled from the target system.

### 5.8.1.8 Lookup.ActiveDirectory.GroupTypes

The Lookup.ActiveDirectory.GroupTypes lookup definition holds information about group types that you can select for the group that you create through Oracle Identity Governance. The following is the format of the Code Key and Decode values in this lookup definition:

**Code Key:** Group type code on the target system

**Decode:** Corresponding group type to be displayed in the Group Type lookup field of the OIM User form

## 5.8.2 Reconciliation Scheduled Jobs for Groups Management

After you create an application, reconciliation scheduled jobs are automatically created in Oracle Identity Governance. You must configure these scheduled jobs to suit your requirements by specifying values for its attributes.

You must specify values for the attributes of the following scheduled jobs:

- [Active Directory Group Recon](#)
- [Active Directory Group Delete Recon](#)

### 5.8.2.1 Active Directory Group Recon

Use the Active Directory Group Recon scheduled job to reconcile group data from the target system.

**Table 5-6 Attributes of the Active Directory Group Recon Scheduled Job**

Attribute	Description
Filter	Expression for filtering records. See <a href="#">Performing Limited Reconciliation By Using Filters</a> for more information. Default value: None <b>Note:</b> While creating filters, ensure to use attributes specific to Groups.
Incremental Recon Attribute	Enter the name of the target system attribute that holds last update-related number, non-decreasing value. For example, <code>numeric</code> or <code>strings</code> . The value in this attribute is used during incremental reconciliation to determine the newest or most youngest record reconciled from the target system. Default value: <code>uSNChanged</code> <b>Note:</b> Do <i>not</i> change the value of this attribute.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile group or organization data. Default value: <code>Active Directory</code>
Latest Token	This attribute holds the value of the <code>uSNChanged</code> attribute of a domain controller that is used for reconciliation. Sample value: 0 <b>Note:</b> The reconciliation engine automatically enters a value for this attribute. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only groups or organizational units whose <code>uSNChanged</code> value is greater than the Latest Token attribute value are reconciled.
Object Type	Type of object to be reconciled. Default value: <code>Group</code>
Organization Name	Enter the name of the organization to which all groups fetched from the target system is linked. See <a href="#">Configuring and Running Group Reconciliation</a> for more information on the usage of this attribute.
Organization Type	Type of organization to be created in Oracle Identity Governance. Default value: <code>Company</code>
Resource Object Name	Name of the resource object that is used for reconciliation. Default value: <code>AD Group</code>

**Table 5-6 (Cont.) Attributes of the Active Directory Group Recon Scheduled Job**

Attribute	Description
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: Active Directory Group Recon
Search Base	Enter the container in which the search for group records must be performed during reconciliation. Sample Value: ou=org1,dc=corp,dc=com <b>Note:</b> If you do not specify a value for this attribute, then the value specified as the value of the Container parameter of the IT resource is used as the value of this attribute.
Search Scope	Enter <code>subtree</code> if you want the scope of the search for records to be reconciled to include the container specified by the Search Base attribute and all of its child containers. For example, if the search base is set to <code>OU=abc,DC=corp,DC=com</code> , then the search would cover the abc OU and all of its child OUs. Enter <code>onelevel</code> if you want the scope of the search for records to be restricted to only the container specified by the Search Base attribute. Child containers of the specified container are not included in the search. For example if the search base is set to <code>OU=abc,DC=corp,DC=com</code> , then the search would cover only the abc OU. <b>Note:</b> If you want to enter <code>onelevel</code> , then ensure that you do not include a space between "one" and "level." Default value: <code>subtree</code>

### 5.8.2.2 Active Directory Group Delete Recon

Use the Active Directory Group Delete Recon scheduled job to reconcile data about deleted groups.

**Table 5-7 Attributes of the Active Directory Group Delete Recon Scheduled Job**

Attribute	Description
Delete Recon	Specifies whether delete reconciliation must be performed. Default value: <code>yes</code> <b>Note:</b> Do <i>not</i> change the value of this attribute.
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile group data. Default value: <code>Active Directory</code>
Object Type	This attribute holds the type of object you want to reconcile. Default value: <code>Group</code>
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Default value: <code>AD Group</code>
Scheduled Task Name	This attribute holds the name of the scheduled task. Default value: <code>Active Directory Group Delete Recon</code>

**Table 5-7 (Cont.) Attributes of the Active Directory Group Delete Recon Scheduled Job**

Attribute	Description
Sync Token	<p>This attribute must be left blank when you run delete reconciliation for the first time. This ensures that data about all records that are deleted from the target system are fetched into Oracle Identity Governance.</p> <p>After the first delete reconciliation run, the connector automatically enters a value for this attribute in an XML serialized format. From the next reconciliation run onward, only data about records that are deleted since the last reconciliation run ended are fetched into Oracle Identity Governance.</p> <p>This attribute stores values in the following format:</p> <pre>&lt;String&gt;0 {uSNChanged} {True/False} {DOMAIN_CONTROLLER}&lt;/String&gt;</pre> <p>A value of <code>True</code> in the preceding format specifies that the Global Catalog Server is used during delete reconciliation runs. In addition, <code>DOMAIN_CONTROLLER</code> is replaced with the name of the domain controller on which the Global Catalog Server is running.</p> <p>A value of <code>False</code> specifies that the Global Catalog Server is not used during delete reconciliation runs. In addition, <code>DOMAIN_CONTROLLER</code> is replaced with the name of the domain controller from which data about deleted records is fetched.</p>
Organization Name	<p>Enter the name of the organization to which data about all deleted groups fetched from the target system is linked.</p> <p>There are two scenarios in which group reconciliation is performed. These scenarios are described in <a href="#">Configuring and Running Group Reconciliation</a>.</p> <p>If you have configured the connector to perform group reconciliation in scenario 1, then you need not specify a value for this attribute. In case you specify a value, it is ignored by the connector.</p> <p>If you have configured the connector to perform group reconciliation in scenario 2, then enter the same organization name specified for the Organization Name attribute of the Active Directory Group Recon scheduled job.</p>

### 5.8.3 Reconciliation Rules and Action Rules for Groups Management

Reconciliation rules are used by the reconciliation engine to determine the identity to which Oracle Identity Governance must assign a newly discovered account on the target system. Reconciliation action rules define that actions the connector must perform based on the reconciliation rules.

- [Reconciliation Rule for Groups](#)
- [Reconciliation Action Rules for Groups](#)
- [Viewing Reconciliation Rules](#)
- [Viewing Reconciliation Action Rules](#)

### 5.8.3.1 Reconciliation Rule for Groups

The following is the process-matching rule for groups:

**Rule name:** AD Group

**Rule element:** Organization Name Equals OIM Org Name

In this rule element:

- Organization Name is the Organization Name field of the OIM User form.
- OIM Org Name is the name of the group in Oracle Identity Governance. OIM Org Name is the value specified in the Organization Name attribute of the ActiveDirectory Group Recon scheduled job.

### 5.8.3.2 Reconciliation Action Rules for Groups

[Table 5-8](#) lists the action rules for groups reconciliation.

**Table 5-8 Action Rules for Reconciliation**

Rule Condition	Action
No Matches Found	Assign to Authorizer With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

### 5.8.3.3 Viewing Reconciliation Rules

After you create the application by using the connector, you can view the reconciliation rule by performing the following steps:

1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for the **AD Group** rule. [Figure 5-1](#) shows the reconciliation rule for groups.

**Figure 5-1 Reconciliation Rule for Groups**

**Reconciliation Rule Builder**

Name:  Operator:  AND  OR  Valid

Object:   Active

For User  For Organization

Description:

**Rule Elements**

**Rule Definition**

Rule: AD Group

- Organization Name Equals OIM Org Name

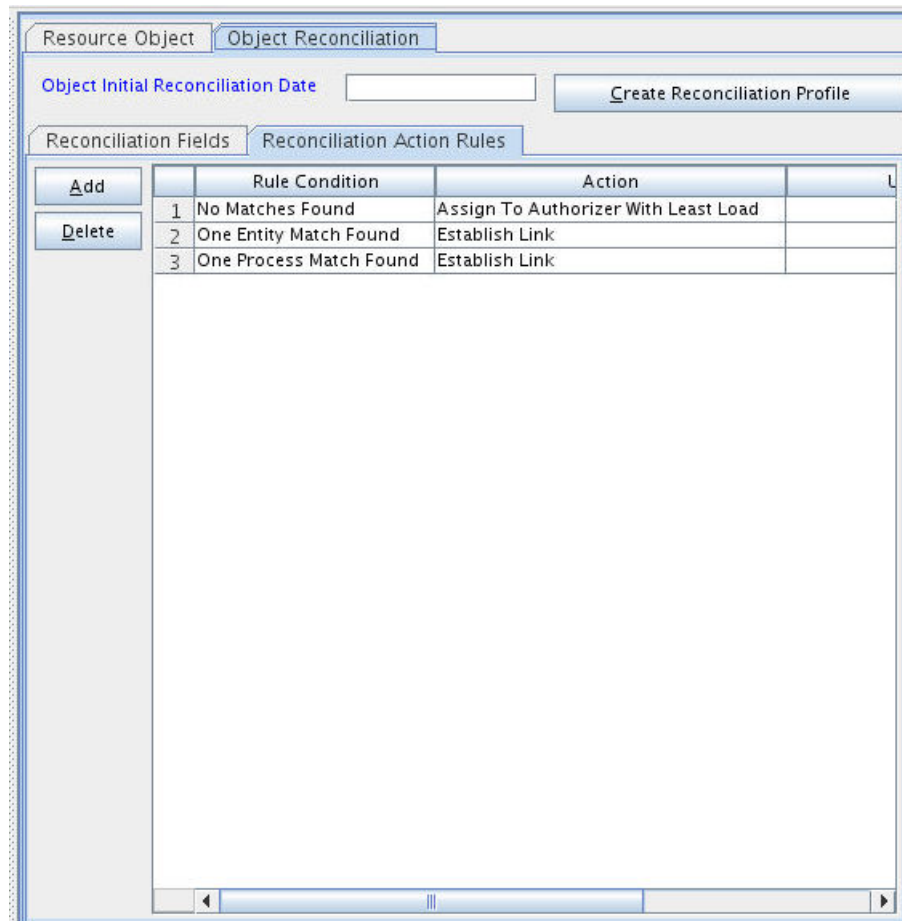
### 5.8.3.4 Viewing Reconciliation Action Rules

After you create the application by using connector, you can view the reconciliation action rules for groups by performing the following steps:

1. Log in to the Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. Search for and open the **AD Group** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. [Figure 5-2](#) shows the reconciliation action rules for groups.



**Figure 5-2 Reconciliation Action Rules for Groups**



## 5.9 Connector Objects Used for Organizational Units Management

Learn about the objects that are used by the connector to perform organizational units management operations such as create, update, and delete.

- [Preconfigured Lookup Definitions for Organizational Unit Operations](#)
- [Reconciliation Scheduled Job for Organization Unit Management](#)
- [Reconciliation Rules and Action Rules for Organizational Units Management](#)

### 5.9.1 Preconfigured Lookup Definitions for Organizational Unit Operations

The lookup definitions for Organizational Units are automatically created in Oracle Identity Governance after you create the application by using the connector.

- [Lookup.ActiveDirectory.OM.Configuration](#)
- [Lookup.ActiveDirectory.OM.Configuration.Trusted](#)
- [Lookup.ActiveDirectory.OM.ProvAttrMap](#)

- [Lookup.ActiveDirectory.OM.ReconAttrMap](#)
- [Lookup.ActiveDirectory.OM.ProvValidation](#)
- [Lookup.ActiveDirectory.OM.ReconTransformation](#)
- [Lookup.ActiveDirectory.OM.ReconValidation](#)
- [Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted](#)
- [Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults](#)

### 5.9.1.1 Lookup.ActiveDirectory.OM.Configuration

The `Lookup.ActiveDirectory.OM.Configuration` lookup definition holds configuration entries that are specific to the organizational unit object type. This lookup definition is used during organizational unit management operations when your target system is configured as a target resource.

[Table 5-9](#) lists the default entries in this lookup definition.

**Table 5-9 Entries in the Lookup.ActiveDirectory.OM.Configuration Lookup Definition**

Code Key	Decode	Description
Provisioning Attribute Map	<code>Lookup.ActiveDirectory.OM.ProvAttrMap</code>	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See <a href="#">Lookup.ActiveDirectory.OM.ProvAttrMap</a> for more information about this lookup definition.
Provisioning Validation Lookup	<code>Lookup.ActiveDirectory.OM.ProvValidation</code>	This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See <a href="#">Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults</a> for more information about adding entries in this lookup definition.
Recon Attribute Defaults	<code>Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults</code>	This entry holds the name of the lookup definition that maps fields on the organizational unit form and their default values. See <a href="#">Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults</a> for more information about this lookup definition.
Recon Attribute Map	<code>Lookup.ActiveDirectory.OM.ReconAttrMap</code>	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See <a href="#">Lookup.ActiveDirectory.OM.ReconAttrMap</a> for more information about this lookup definition.
Recon Transformation Lookup	<code>Lookup.ActiveDirectory.OM.ReconTransformation</code>	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See <a href="#">Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults</a> for more information about adding entries in this lookup definition.
Recon Validation Lookup	<code>Lookup.ActiveDirectory.OM.ReconValidation</code>	This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation. See <a href="#">Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults</a> for more information about adding entries in this lookup definition.

### 5.9.1.2 Lookup.ActiveDirectory.OM.Configuration.Trusted

The Lookup.ActiveDirectory.OM.Configuration.Trusted lookup definition holds configuration entries that are specific to the organizational unit object type. This lookup definition is used during trusted source reconciliation runs for organizational units.

Table 5-10 lists the default entries in this lookup definition.

**Table 5-10 Entries in the Lookup.ActiveDirectory.OM.Configuration.Trusted Lookup Definition**

Code Key	Decode	Description
Recon Attribute Defaults	Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults	This entry holds the name of the lookup definition that maps fields on the organizational unit form and their default values. See <a href="#">Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults</a> for more information about this lookup definition.
Recon Attribute Map	Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See <a href="#">Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted</a> for more information about this lookup definition.

### 5.9.1.3 Lookup.ActiveDirectory.OM.ProvAttrMap

The Lookup.ActiveDirectory.OM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definition is preconfigured and used during provisioning.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning.

**Table 5-11 Entries in the Lookup.ActiveDirectory.OM.ProvAttrMap**

Organizational Unit Field on Oracle Identity Governance (Code Key)	Target System Field (Decode)	Description
__NAME__	__NAME__="OU=\$(Display_Name),\$ (Container)	Organizational unit name with full DN
Container[LOOKUP,IGNORE]	IGNORED	Organization name with DN format For example, OU=org1,dc=example,dc=com
Display Name[IGNORE]	IGNORED	Display name for an organizational unit
Unique Id	__UID__	Object GUID of the organizational unit

### 5.9.1.4 Lookup.ActiveDirectory.OM.ReconAttrMap

The Lookup.ActiveDirectory.OM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is

preconfigured and used for performing target resource reconciliation runs for organizational units.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation.

**Table 5-12 Default Entries in the Lookup.ActiveDirectory.OM.ReconAttrMap**

Organization Field on Oracle Identity Governance (Code Key)	Microsoft Active Directory Field (Decode)	Description
Container[LOOKUP]	ad_container	Organization name with DN format. For example, OU=org1, dc=example, dc=com
Display Name	ou	Display name for an organizational unit
Unique Id	__UID__	Object GUID of the organizational unit

### 5.9.1.5 Lookup.ActiveDirectory.OM.ProvValidation

The Lookup.ActiveDirectory.OM.ProvValidation lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations for organizational units. See [Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units](#) for more information about adding entries in this lookup definition.

### 5.9.1.6 Lookup.ActiveDirectory.OM.ReconTransformation

The Lookup.ActiveDirectory.OM.ReconTransformation lookup definition is used to configure transformation of attribute values that are fetched from the target system during reconciliation of organizational units. See [Configuring Transformation of Data During Reconciliation for Groups and Organizational Units](#) for more information about adding entries in this lookup definition.

### 5.9.1.7 Lookup.ActiveDirectory.OM.ReconValidation

The Lookup.ActiveDirectory.OM.ReconValidation lookup definition is used to configure validation of attribute values that are fetched from the target system during reconciliation. See [Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units](#) for more information about adding entries in this lookup definition.

### 5.9.1.8 Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted

The Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes. This lookup definitions is preconfigured and used during trusted source reconciliation runs for organizational units. [Table 5-13](#) lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation.

**Table 5-13 Default Entries in the Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted Lookup Definition**

OIM User Form Field (Code Key)	Target System Field (Decode)
Org Name	ou

### 5.9.1.9 Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults

The Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults lookup definition holds mappings between fields on the organizational unit form and their default values. This lookup definition is used when there is a mandatory field on the organizational unit form, but no corresponding field in the target system from which values can be fetched during organizational unit reconciliation.

This lookup definition is empty by default. If you add entries to this lookup definition, then the Code Key and Decode values must be in the following format:

**Code Key:** Name of the reconciliation field of the AD Organizational Unit resource object

**Decode:** Corresponding default value to be displayed

For example, assume a field named Organization ID is a mandatory field on the organizational unit form. Suppose the target system contains no field that stores information about the organization ID for an account. During reconciliation, no value for the Organization ID field is fetched from the target system. However, as the Organization ID field cannot be left empty, you must specify a value for this field. Therefore, create an entry in this lookup definition with the Code Key value set to `Organization ID` and Decode value set to `ORG1332`. This implies that the value of the Organization ID field on the organizational unit form displays `ORG1332` for all accounts reconciled from the target system.

## 5.9.2 Reconciliation Scheduled Job for Organization Unit Management

You use the Active Directory Organization Recon scheduled job to reconcile organization unit data from the target system. This scheduled job is automatically created in Oracle Identity Governance after you create an application. You must configure this scheduled job to suit your requirements by specifying values for its attributes.

**Table 5-14 Attributes of the Active Directory Organization Recon Scheduled Job**

Attribute	Description
Filter	<p>Expression for filtering records. See <a href="#">Performing Limited Reconciliation By Using Filters</a> for more information.</p> <p>Default value: <code>None</code></p> <p><b>Note:</b> While creating filters, ensure to use attributes specific to Organizational Units.</p>

**Table 5-14 (Cont.) Attributes of the Active Directory Organization Recon Scheduled Job**

Attribute	Description
Incremental Recon Attribute	<p>Enter the name of the target system attribute that holds last update-related number, non-decreasing value. For example, <code>numeric</code> or <code>strings</code>.</p> <p>The value in this attribute is used during incremental reconciliation to determine the newest or most youngest record reconciled from the target system.</p> <p>Default value: <code>uSNChanged</code></p> <p><b>Note:</b> Do <i>not</i> change the value of this attribute.</p>
IT Resource Name	<p>Enter the name of the IT resource for the target system installation from which you want to reconcile organization data.</p> <p>Default value: <code>Active Directory</code></p>
Latest Token	<p>This attribute holds the value of the <code>uSNChanged</code> attribute of a domain controller that is used for reconciliation.</p> <p>Sample value: <code>0</code></p> <p><b>Note:</b> The reconciliation engine automatically enters a value for this attribute. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only groups or organizational units whose <code>uSNChanged</code> value is greater than the Latest Token attribute value are reconciled.</p>
Object Type	<p>Type of object to be reconciled.</p> <p>Default value: <code>organizationalUnit</code></p>
Resource Object Name	<p>Name of the resource object that is used for reconciliation.</p> <p>Default value: <code>Xellerate Organization</code></p>
Scheduled Task Name	<p>Name of the scheduled task used for reconciliation.</p> <p>Default value: <code>Active Directory Organization Recon</code></p>
Search Base	<p>Enter the container in which the search for organization records must be performed during reconciliation.</p> <p>Sample Value: <code>ou=org1,dc=corp,dc=com</code></p> <p><b>Note:</b> If you do not specify a value for this attribute, then the value specified as the value of the Container parameter of the IT resource is used as the value of this attribute.</p>
Search Scope	<p>Enter <code>subtree</code> if you want the scope of the search for records to be reconciled to include the container specified by the Search Base attribute and all of its child containers. For example, if the search base is set to <code>OU=abc,DC=corp,DC=com</code>, then the search would cover the <code>abc</code> OU and all of its child OUs.</p> <p>Enter <code>onelevel</code> if you want the scope of the search for records to be restricted to only the container specified by the Search Base attribute. Child containers of the specified container are not included in the search. For example if the search base is set to <code>OU=abc,DC=corp,DC=com</code>, then the search would cover only the <code>abc</code> OU.</p> <p><b>Note:</b> If you want to enter <code>onelevel</code>, then ensure that you do not include a space between "one" and "level."</p> <p>Default value: <code>subtree</code></p>

### 5.9.3 Reconciliation Rules and Action Rules for Organizational Units Management

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

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

- [Reconciliation Rule for Organizational Units](#)
- [Reconciliation Action Rules for Organizational Units](#)
- [Viewing Reconciliation Rules](#)
- [Viewing Reconciliation Action Rules](#)

### 5.9.3.1 Reconciliation Rule for Organizational Units

The following is the process-matching rule for organizational units:

**Rule name:** AD Organizational Unit

**Rule element:** Organization Name Equals Display Name

In this rule element:

- Organization Name is the Organization Name field of the OIM User form.
- Display Name is the name of an organizational unit in Oracle Identity Governance.

### 5.9.3.2 Reconciliation Action Rules for Organizational Units

[Table 5-15](#) lists the action rules for groups reconciliation.

**Table 5-15 Action Rules for Reconciliation**

Rule Condition	Action
No Matches Found	Assign to Authorizer With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

### 5.9.3.3 Viewing Reconciliation Rules

After you create the application by using the connector, you can view the reconciliation rule by performing the following steps:

1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for the **AD Organizational Unit Recon Rule** rule. [Figure 5-4](#) shows the reconciliation rule for organizational units.

**Figure 5-3 Reconciliation Rule for Organizational Unit**

The screenshot shows the 'Reconciliation Rule Builder' window. The 'Name' field is 'AD Organizational Unit'. The 'Object' field is also 'AD Organizational Unit'. The 'Operator' is set to 'AND'. There are checkboxes for 'Valid' and 'Active', both of which are checked. Below the operator are radio buttons for 'For User' (unselected) and 'For Organization' (selected). The 'Description' field contains 'AD Organizational Unit matching rule'. Below this is a 'Rule Elements' section with a 'Rule Definition' area. On the left of this area are buttons for 'Add Rule', 'Add Rule Element', 'Delete', and 'Legend'. On the right, a tree view shows a rule named 'Rule: AD Organizational Unit' with a sub-element 'Organization Name Equals Display Name'.

### 5.9.3.4 Viewing Reconciliation Action Rules

After you create the application by using connector, you can view the reconciliation action rules for groups by performing the following steps:

1. Log in to the Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. Search for and open the **AD Organizational Unit** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. shows the reconciliation action rules for organizational units. [Figure 5-4](#) shows the reconciliation action rules for organizational units.



**Figure 5-4 Reconciliation Action Rules for Organizational Unit**

The screenshot shows a software interface for configuring reconciliation rules. At the top, there are tabs for 'Resource Object' and 'Object Reconciliation'. Below the tabs, there is a field for 'Object Initial Reconciliation Date' and a 'Create Reconciliation Profile' button. The main area is divided into two sections: 'Reconciliation Fields' and 'Reconciliation Action Rules'. The 'Reconciliation Action Rules' section contains a table with three rows of rules. To the left of the table are 'Add' and 'Delete' buttons.

	Rule Condition	Action	
1	No Matches Found	Assign To Authorizer With Least Load	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

## 5.10 Uninstalling the Connector

Uninstalling the connector deletes all the account-related data associated with its resource objects.

If you want to uninstall the connector for any reason, then run the Uninstall Connector utility. Before you run this utility, ensure that you set values for `ObjectType` and `ObjectValues` properties in the `ConnectorUninstall.properties` file. For example, if you want to delete resource objects, scheduled tasks, and scheduled jobs associated with the connector, then enter "ResourceObject", "ScheduleTask", "ScheduleJob" as the value of the `ObjectType` property and a semicolon-separated list of object values corresponding to your connector (for example, `ActiveDirectory User; ActiveDirectory Group`) as the value of the `ObjectValues` property.



**Note:**

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

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

# 6

## Extending the Functionality of the Microsoft Active Directory User Management Connector

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

By default the connector is configured to perform a certain set of tasks. For addressing your specific business requirements, you can extend the functionality of the connector by performing the procedures described in the following sections:

- [Adding Custom Fields for Target Resource Reconciliation](#)
- [Adding New Multivalued Fields for Target Resource Reconciliation](#)
- [Adding Custom Fields for Provisioning](#)
- [Adding New Multivalued Fields for Provisioning](#)
- [Adding Terminal Services Fields for Reconciliation and Provisioning](#)
- [Adding the Group Name \(pre-Windows 2000\) Attribute](#)
- [Configuring Transformation and Validation Of Data](#)
- [Action Scripts](#)
- [Enabling Reconciliation and Provisioning Operations Across Multiple Domains](#)
- [About Using the Connector for Multiple Trusted Source Reconciliation](#)
- [Multiple Installations of the Target System](#)
- [Creating a Home Directory After User Create Provisioning Operation](#)
- [Configuring the Connector for Provisioning Groups of the Security Group - Universal Group Type](#)

### 6.1 Adding Custom Fields for Target Resource Reconciliation

You can add additional fields for user, group, or organizational unit reconciliation.

- [Adding Custom Fields for Target Resource Reconciliation of Users](#)
- [Adding Custom Fields for Target Resource Reconciliation of Groups and Organizational Units](#)



#### Note:

Binary attributes are not supported. Connector supports `string`, `long`, `char`, `double`, `float`, `int`, and `bool` attribute types of the Microsoft Active Directory target system.

## 6.1.1 Adding Custom Fields for Target Resource Reconciliation of Users

You can add additional fields for user reconciliation.

 **Note:**

This section describes an optional procedure. You need not perform this procedure if you do not want to add custom fields for reconciliation.

To add a custom field for target resource reconciliation for users:

To add a custom field for target resource reconciliation for users:

1. Log in to Identity Self Service as an administrator.
2. Click the **Manage** tab, and then click the **Applications** box to open the Applications page.
3. Search for and open the Active Directory Target application to which you want to add custom fields.
4. Select **Schema** and then click **Add Attribute**.
5. In the newly added row, add the new attribute name, the OIM Profile and target system attribute that it will map to, and so on. For example, enter values for the **Display Name**, **Identity Attribute**, **Target Attribute**, and **Data Type** fields. Then, select the **Recon Field** checkbox and any other reconciliation properties as required.
6. Click **Apply** to save the changes.
7. Log in to Oracle Identity System Administration as an administrator.
8. Create and activate a sandbox.
9. Select **Form Designer**.
10. Create a new form with the following values and then click **Create**:
  - a. In the **Resource Type** field, enter the Active Directory Target application to which you added custom fields.
  - b. In the **Form Name** field, enter a form name. If you add attributes incrementally to the application, then you must create new forms every time you add new attributes. Therefore, it is recommended that you include a version number in the form name.
11. Ensure that the newly created attribute is present in the list of attributes on the form and save the changes. Then, publish the sandbox.
12. Navigate to Application Instances and search for and open the application instance associated with the application to which you added the new attributes.
13. From the **Form** dropdown, select the new version of the form you just created and then click **Apply**.

The newly added fields are now available to be added to the View and Modify forms of the application by creating a new Sandbox and using the normal customize forms process.

## 6.1.2 Adding Custom Fields for Target Resource Reconciliation of Groups and Organizational Units

You can add additional fields for group or organizational unit reconciliation.

### Note:

This section describes an optional procedure. You need not perform this procedure if you do not want to add custom fields for reconciliation.

To add a custom field for target resource reconciliation:

1. Log in to the Oracle Identity Governance Design Console.
2. Add the custom field to the list of reconciliation fields in the resource object as follows:
  - a. Expand **Resource Management** and then double-click **Resource Objects**.
  - b. Search for and open one of the following resource objects:
    - For groups: **AD Group**
    - For organizational units: **AD Organizational Unit**
  - c. On the Object Reconciliation tab, click **Add Field**.
  - d. In the Add Reconciliation Field dialog box, enter the details of the field.
    - For example, enter `Description` in the Field Name field and select **String** from the Field Type list.
    - Note that if you are adding a boolean field, then select **String** as the field type.
  - e. Click **Save** and close the dialog box.
  - f. Click **Create Reconciliation Profile**. This copies changes made to the resource object into MDS.
  - g. Click **Save**.
3. Create an entry for the field in the lookup definition for reconciliation as follows:
  - a. Expand **Administration** and then double-click **Lookup Definition**.
  - b. Search for and open one of the following lookup definitions:
    - For groups: **Lookup.ActiveDirectory.GM.ReconAttrMap**
    - For organizational units: **Lookup.ActiveDirectory.OM.ReconAttrMap**
  - c. Click **Add** and enter the Code Key and Decode values for the field. The Code Key value is the name of the field that you provide for the reconciliation field in Step 2.d. The Decode value is the name of the target system field.
    - For example, enter `Description` in the Code Key field and then enter `description` in the Decode field.
  - d. Click **Save**.

4. Add the custom field on the process form as follows:
  - a. Expand **Development Tools** and then double-click **Form Designer**.
  - b. Search for and open one of the following process forms:  
For groups: **UD\_ADGRP**  
For organizational units: **UD\_ADOU**
  - c. Click **Create New Version**, and then click **Add**.
  - d. Enter the details of the field.  
For example, if you are adding the Description field, enter `UD_ADGRP_DESCRIPTION` in the Name field, and then enter the rest of the details of this field.
  - e. Click **Save** and then click **Make Version Active**.
5. If you are using Oracle Identity Governance release 11.1.2.x or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
  - a. Log in to Oracle Identity System Administration.
  - b. Create and active a sandbox. See [Creating and Activating a Sandbox](#) for more information.
  - c. Create a new UI form to view the newly added field along with the rest of the fields. See [Creating a New UI Form](#) for more information about creating a UI form.
  - 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 5.c), and then save the application instance.
  - e. Publish the sandbox. See [Publishing a Sandbox](#) for more information.
6. Create a reconciliation field mapping for the custom field in the provisioning process as follows:
  - a. Log in to the Design Console.
  - b. Expand **Process Management** and then double-click **Process Definition**.
  - c. Search for and open one of the following provisioning process:  
For groups: **AD Group**  
For organizational units: **AD Organizational Unit**
  - d. On the Reconciliation Field Mappings tab of the provisioning process, click **Add Field Map**.
  - e. In the Add Reconciliation Field Mapping dialog box, from the Field Name field, select the value for the field that you want to add.  
For example, from the Field Name field, select **Description**.
  - f. Double-click the Process Data field, and then select **UD\_ADGRP\_DESCRIPTION**.
  - g. Click **Save** and close the dialog box.
  - h. Click **Save**.

## 6.2 Adding New Multivalued Fields for Target Resource Reconciliation

You can add new multivalued fields for user, group, or organizational unit during target resource reconciliation.

- [Adding New Multivalued Fields for Target Resource Reconciliation of Users](#)
- [Adding New Multivalued Fields for Target Resource Reconciliation of Groups and Organizational Units](#)



### Note:

Binary attributes are not supported. Connector supports `string`, `long`, `char`, `double`, `float`, `int`, and `bool` attribute types of the Microsoft Active Directory target system.

### 6.2.1 Adding New Multivalued Fields for Target Resource Reconciliation of Users

You can add multivalued fields for user reconciliation between Oracle Identity Governance and the target system.



### Note:

This procedure can be applied to add user fields only.

You must ensure that new fields you add for reconciliation contain only string-format data. Binary fields must not be brought into Oracle Identity Governance natively.

To add a new multivalued field for target resource reconciliation:

1. On the Application On-Boarding UI, select the Active Directory Target application.
2. Select **Schema** and then click **Add Attribute**.
3. In the newly added row, enter values for the **Display Name** and **Target Attribute** fields.
4. To select a value for the **Data Type** field, click the drop-down and select **String**.
5. Select the **Recon Field** checkbox.
6. Click **Advanced Settings** denoted by three horizontal lines at the end of the row and select the **Lookup** checkbox.
7. In the **List of values** field, enter the name of the lookup definition and click **OK**.
8. Click **Apply**.

## 6.2.2 Adding New Multivalued Fields for Target Resource Reconciliation of Groups and Organizational Units

You can add multivalued fields for reconciliation of groups and organizational units between Oracle Identity Governance and the target system.

 **Note:**

This procedure can be applied to add either group or organizational unit fields.

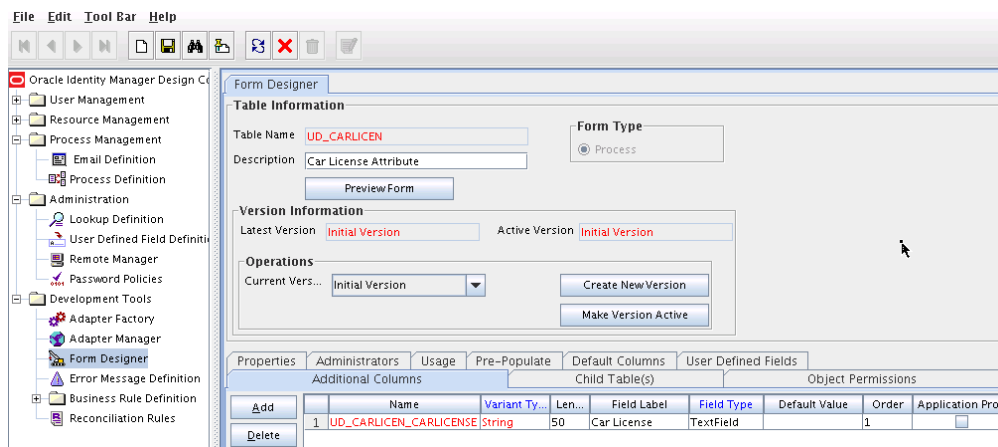
You must ensure that new fields you add for reconciliation contain only string-format data. Binary fields must not be brought into Oracle Identity Governance natively.

To add a new multivalued field for target resource reconciliation:

1. Log in to the Oracle Identity Governance Design Console.
2. Create a form for the multivalued field as follows:
  - a. Expand **Development Tools** and double-click **Form Designer**.
  - b. Create a form by specifying a table name and description, and then click **Save**.
  - c. Click **Add** and enter the details of the field.
  - d. Click **Save** and then click **Make Version Active**. shows the multivalued field added on a new form.

Figure 6-1

**Figure 6-1 Multivalued Field Added on a New Form**

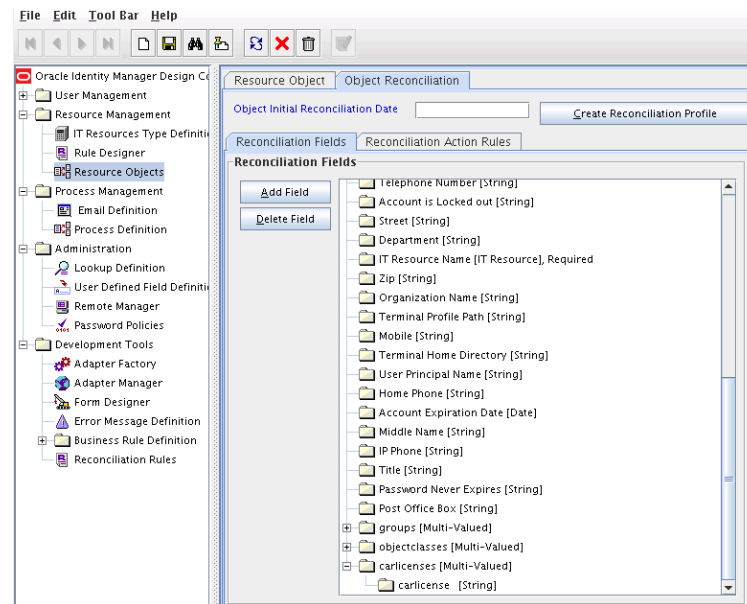


3. Add the form created for the multivalued field as a child form of the process form as follows:



- a. Search for and open one of the following process forms:  
For groups: **UD\_ADGRP**  
For organizational units: **UD\_ADOU**
  - b. Click **Create New Version**.
  - c. Click the **Child Table(s)** tab.
  - d. Click **Assign**.
  - e. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.
  - f. Click **Save** and then click **Make Version Active**.
4. If you are using Oracle Identity Governance release 11.1.2.x or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
- a. Log in to Oracle Identity System Administration.
  - b. Create and activate a sandbox. See [Creating and Activating a Sandbox](#) for more information.
  - c. Create a new UI form to view the newly added field along with the rest of the fields. See [Creating a New UI Form](#) for more information about creating a UI form.
  - 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 4.c), and then save the application instance.
  - e. Publish the sandbox. See [Publishing a Sandbox](#) for more information.
5. Add the new multivalued field to the list of reconciliation fields in the resource object as follows:
- a. Log in to the Design Console.
  - b. Expand **Resource Management** and then double-click **Resource Objects**.
  - c. Search for and open one of the following resource objects:  
For groups: **AD Group**  
For organizational units: **AD Organizational Unit**
  - d. On the Object Reconciliation tab, click **Add Field**.
  - e. In the Add Reconciliation Fields dialog box, enter the details of the field.  
For example, enter `carlicenses` in the **Field Name** field and select **Multi-Valued Attribute** from the Field Type list.
  - f. Click **Save** and then close the dialog box.
  - g. Right-click the newly created field and select **Define Property Fields**.
  - h. In the Add Reconciliation Fields dialog box, enter the details of the newly created field.  
For example, enter `carlicense` in the Field Name field and select **String** from the Field Type list.
  - i. Click **Save**, and then close the dialog box. [Figure 6-2](#) shows the new reconciliation field added in the resource object.

Figure 6-2 New Reconciliation Field Added in the Resource Object



- j. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.
6. Create an entry for the field in the lookup definition for reconciliation as follows:
    - a. Expand **Administration** and then double-click **Lookup Definition**.
    - b. Search for and open one of the following lookup definitions:  
 For groups: **Lookup.ActiveDirectory.GM.ReconAttrMap**  
 For organizational units: **Lookup.ActiveDirectory.OM.ReconAttrMap**

 **Note:**

For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

- c. Click **Add** and enter the Code Key and Decode values for the field, and then Click **Save**. The Code Key and Decode values must be in the following format:  
**Code Key:**  
`MULTIVALUED_FIELD_NAME~CHILD_RESOURCE_OBJECT_FIELD_NAME`  
**Decode:** Corresponding target system attribute.  
 For example, enter `carlicenses~carlicense` in the Code Key field and then enter `carlicense` in the Decode field.
7. Create a reconciliation field mapping for the new field as follows:
    - a. Expand **Process Management** and double-click **Process Definition**.
    - b. Search for and open one of the following process definitions:

For groups: **AD Group**

For organizational units: **AD Organizational Unit**

- c. On the Reconciliation Field Mappings tab of the AD Group or AD Organizational Unit process definition, click **Add Table Map**.
- d. In the Add Reconciliation Table Mapping dialog box, select the field name and table name from the list, click **Save**, and then close the dialog box.
- e. Right-click the newly created field, and select **Define Property Field Map**.
- f. In the Field Name field, select the value for the field that you want to add.
- g. Double-click the **Process Data Field** field, and then select **UD\_CARLICEN**.
- h. Select **Key Field for Reconciliation Field Matching** and click **Save**.

## 6.3 Adding Custom Fields for Provisioning

You can add additional fields while provisioning users, groups, or organizational units.

- [Adding Custom Fields for Provisioning Users](#)
- [Adding Custom Fields for Provisioning Groups and Organizational Units](#)



### Note:

Binary attributes are not supported. Connector supports `string`, `long`, `char`, `double`, `float`, `int`, and `bool` attribute types of the Microsoft Active Directory target system.

### 6.3.1 Adding Custom Fields for Provisioning Users

You can add additional fields while provisioning users.



### Note:

This section describes an optional procedure. You need not perform this procedure if you do not want to add custom fields for provisioning.

To add a custom field for provisioning users:

1. On the Application On-Boarding UI, select the Active Directory Target application.
2. Select **Schema** and then click **Add Attribute**.
3. In the newly added row, enter values for the **Display Name** and **Target Attribute** fields.
4. To select a value for the **Data Type** field, click the drop-down and select **String**.
5. Select the **Provision Field** checkbox.
6. Click **Apply**.

## 6.3.2 Adding Custom Fields for Provisioning Groups and Organizational Units

You can map additional attributes for provisioning apart from the default attributes.

To add a custom field for provisioning for groups and organizational units, perform the procedures listed in the following sections:

- [Adding a New Field on the Process Form](#)
- [Replicating Form Designer Changes to a New UI Form](#)
- [Creating an Entry in the Provisioning Lookup Definition](#)
- [Enabling Update Provisioning Operations on the Custom Field](#)
- [Updating the Request Dataset](#)
- [Clearing Content Related to Request Datasets from the Server Cache](#)
- [Importing Request Datasets](#)

### 6.3.2.1 Adding a New Field on the Process Form

If you have added the field on the process form by performing Step 4 of [Adding Custom Fields for Target Resource Reconciliation of Groups and Organizational Units](#), then you need not add the field again. If you have not added the field, then add it as follows:

1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Development Tools** and then double-click **Form Designer**.
3. Search for and open one of the following process forms:  
For groups: **UD\_ADGRP**  
For organizational units: **UD\_ADOU**
4. Click **Create New Version**, and then click **Add**.
5. Enter the details of the field.  
For example, if you are adding the Description field, enter `UD_ADGRP_DESCRIPTION` in the Name field, and then enter the rest of the details of this field.
6. Click **Save** and then click **Make Version Active**.

### 6.3.2.2 Replicating Form Designer Changes to a New UI Form

If you are using Oracle Identity Governance release 11.1.2.x or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:

1. Log in to Oracle Identity System Administration.
2. Create and active a sandbox. See [Creating and Activating a Sandbox](#) for more information.
3. Create a new UI form to view the newly added field along with the rest of the fields. See [Creating a New UI Form](#) for more information about creating a UI form.

4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 3.c), and then save the application instance.
5. Publish the sandbox. See [Publishing a Sandbox](#) for more information.

### 6.3.2.3 Creating an Entry in the Provisioning Lookup Definition

Create an entry for the field in the lookup definition for provisioning as follows:

1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Administration** and then double-click **Lookup Definition**.
3. Search for and open one of the following lookup definitions:

For groups: **Lookup.ActiveDirectory.GM.ProvAttrMap**

For organizational units: **Lookup.ActiveDirectory.OM.ProvAttrMap**

4. Click **Add** and then enter the Code Key and Decode values for the field. The Decode value must be the name of the field on the target system.

For example, enter `Description` (name of the field added to the process form in Step 2 of this procedure) in the Code Key field and then enter `description` in the Decode field.

#### Note:

If the field added is Boolean, then enter the Decode value in the following format:

```
TARGET_ATTR_NAME=(OIM_PROCESS_FORM_FIELD_NAME=='1')?"TRUE":"FALSE"
```

For example, consider the target system attribute `OCSUserEnabled` and a field named `OCSUserEnabled` in the process form. In this case, the decode value of the `OCSUserEnabled` code key is as follows:

```
OCSUserEnabled=(OCSUserEnabled == '1') ? "TRUE":"FALSE"
```

5. Click **Save**.

### 6.3.2.4 Enabling Update Provisioning Operations on the Custom Field

After adding the custom field, you must enable update provisioning operations on that field as follows:

1. In the provisioning process, add a new task for updating the field as follows:
  - a. Expand **Process Management** and then double-click **Process Definition**.
  - b. Search for and open one of the following provisioning process:

For groups: **AD Group**

For organizational units: **AD Organizational Unit**

- c. Click **Add** and enter the task name and task description. The following are sample values:

**Task Name:** `Description Updated`

**Task Description:** Process Task for handling update of the description field.

- d. In the Task Properties section, select the following fields:
  - Conditional
  - Allow Cancellation while Pending
  - Allow Multiple Instances
- e. Click **Save**.
2. In the provisioning process, select the adapter name in the Handler Type section as follows:
  - a. Go to the Integration tab, click **Add**.
  - b. In the Handler Selection dialog box, select **Adapter**.
  - c. From the Handler Name column, select **adpADIDCUPDATEATTRIBUTEVALUE**.
  - d. Click **Save** and close the dialog box.
3. In the Adapter Variables region, click the **procInstanceKey** variable.
4. In the dialog box that is displayed, create the following mapping:
 

**Variable Name:** `procInstanceKey`

**Map To:** `Process Data`

**Qualifier:** `Process Instance`
5. Click **Save** and close the dialog box.
6. If you are enabling update provisioning operations for a Group custom field, then repeat Steps 3 through 5 for all the variables listed in the following table. This table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
<code>procInstanceKey</code>	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
<code>itResourceFieldName</code>	Literal	String	UD_ADGRP_SERVER
<code>attrFieldName</code>	Literal	String	CUSTOM_FIELD_NAME
<code>objectType</code>	Literal	String	Group

7. If you are enabling update provisioning operations for an Organizational Unit custom field, then repeat Steps 3 through 5 for all the variables listed in the following table. This table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
<code>procInstanceKey</code>	Process Data	Process Instance	NA

Variable	Map To	Qualifier	Literal Value
Adapter Return Variable	Response Code	NA	NA
itResourceFieldName	Literal	String	UD_ADOU_SERVER
attrFieldName	Literal	String	CUSTOM_FIELD_NAME
objectType	Literal	String	organizationalUnit

8. On the Responses tab, click **Add** to add at least the SUCCESS response code, with Status C. This ensures that if the custom task is successfully run, then the status of the task is displayed as Completed.
9. Click the Save icon and close the dialog box, and then save the process definition.

### 6.3.2.5 Updating the Request Dataset

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the XML file located in the *OIM\_HOME/dataset/file* directory for editing.
2. Add the AttributeReference element and specify values for the mandatory attributes of this element.

For example, while performing the procedure described in [Adding a New Field on the Process Form](#), if you added Employee ID as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Employee ID"
attr-ref = "Employee ID"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

In this AttributeReference element:

- For the name attribute, enter the value in the Name column of the process form without the tablename prefix.  
For example, if UD\_ADUSER\_EMPLOYEE\_ID is the value in the Name column of the process form, then you must specify `Employee ID` as the value of the name attribute in the AttributeReference element.
- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing the procedure described in [Adding a New Field on the Process Form](#).
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing the procedure described in [Adding a New Field on the Process Form](#).
- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing the procedure described in [Adding a New Field on the Process Form](#).

- For the length attribute, enter the value that you entered in the Length column of the process form while performing the procedure described in [Adding a New Field on the Process Form](#).
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing the procedure described in [Adding a New Field on the Process Form](#), if you added more than one attribute on the process form, then repeat this step for each attribute added.

3. Save and close the XML file.

### 6.3.2.6 Clearing Content Related to Request Datasets from the Server Cache

Run the PurgeCache utility to clear content related to request datasets from the server cache.

See Running the PurgeCache Utility in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about the PurgeCache utility.

### 6.3.2.7 Importing Request Datasets



**Note:**

Perform the procedure described in this section only if you have enabled request-based provisioning.

Import into MDS, the request dataset definitions in XML format.

## 6.4 Adding New Multivalued Fields for Provisioning

You can add new multivalued fields for user, group, or organizational unit during a provisioning operation.

- [Adding New Multivalued Fields for Provisioning Users](#)
- [Adding New Multivalued Fields for Provisioning Groups and Organizational Units](#)



**Note:**

Binary attributes are not supported. Connector supports `string`, `long`, `char`, `double`, `float`, `int`, and `bool` attribute types of the Microsoft Active Directory target system.



## 6.4.1 Adding New Multivalued Fields for Provisioning Users

You can add multivalued fields for provisioning users between Oracle Identity Governance and the target system.

### Note:

This procedure can be applied to add user fields only.

You must ensure that new fields you add for reconciliation contain only string-format data. Binary fields must not be brought into Oracle Identity Governance natively.

To add a new multivalued field for provisioning:

1. On the Application On-Boarding UI, select the Active Directory Target application.
2. Select **Schema** and then click **Add Attribute**.
3. In the newly added row, enter values for the **Display Name** and **Target Attribute** fields.
4. To select a value for the **Data Type** field, click the drop-down and select **String**.
5. Select the **Provision Field** checkbox.
6. Click **Advanced Settings** denoted by three horizontal lines at the end of the row and select the **Lookup** checkbox.
7. In the **List of values** field, enter the name of the lookup definition and click **OK**.
8. Click **Apply**.

## 6.4.2 Adding New Multivalued Fields for Provisioning Groups and Organizational Units

You can add new multivalued fields for provisioning.

### Note:

Before starting the following procedure, perform Steps 1 through 4 as described in [Adding New Multivalued Fields for Target Resource Reconciliation of Groups and Organizational Units](#). If these steps have been performed while adding new multivalued fields for target resource reconciliation, then you need not repeat the steps.

To add new multivalued fields for provisioning:

- [Creating an Entry in the Provisioning Lookup Definition](#)
- [Enabling Update Provisioning Operations on the Multivalued Field](#)
- [Updating the Request Dataset](#)
- [Clearing Content Related to Request Datasets from the Server Cache](#)

- [Importing Request Datasets](#)

### 6.4.2.1 Creating an Entry in the Provisioning Lookup Definition

Create an entry for the field in the lookup definition for provisioning as follows:

1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Administration** and double-click **Lookup Definition**.
3. Search for and open one of the lookup definitions:
  - For a group field on Microsoft Active Directory, open **Lookup.ActiveDirectory.GM.ProvAttrMap**.
  - For a organizational unit field on Microsoft Active Directory, open **Lookup.ActiveDirectory.OM.ProvAttrMap**.
4. Click **Add** and then enter the Code Key and Decode values for the field. The Code Key and Decode values must be in the following format:

**Code Key:** *CHILD\_FORM\_NAME-CHILD\_FIELD\_LABEL*

In this format, *CHILD\_FORM\_NAME* specifies the name of the child form. *CHILD\_FIELD\_NAME* specifies the name of the field on the OIM User child form in the Administrative and User Console.

**Decode:** Corresponding target system attribute

 **Note:**

For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

### 6.4.2.2 Enabling Update Provisioning Operations on the Multivalued Field

Enable update provisioning operations on the multivalued field as follows:

1. Expand **Process Management**, and then double-click **Process Definition**.
2. Search for and open one of the following process definitions:

For groups: **AD Group**

For organizational units: **AD Organizational Unit**
3. Click **Add** and enter the task name and description. For example, enter `Car License Insert` as the task name and task description.
4. In the Task Properties section, select the following:
  - Conditional
  - Allow cancellation while Pending
  - Allow Multiple Instances
  - **UD\_CARLICEN**, to add the child table from the Child Table list
  - **Insert**, to add the data from the Trigger Type list

5. Click **Save**.
6. On the Integration tab in the AD User provisioning Process, click **Add** and then select **Adapter**. From the list of adapters, select **adpADIDCUPDATECHILDTABLEVALUES**.
7. Click **Save** and then close the dialog box.
8. In the Adapter Variables region, click the **procInstanceKey** variable.
9. In the dialog box that is displayed, create the following mapping:
  - **Variable Name:** `procInstanceKey`
  - **Map To:** `Process Data`
  - **Qualifier:** `Process Instance`
10. Click **Save** and close the dialog box.
11. If you are enabling update provisioning operations on a Group multivalued field, then repeat Steps 8 through 10 for all the variables listed in the following table. This table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
<code>procInstanceKey</code>	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
<code>itResourceFieldName</code>	Literal	String	UD_ADGRP_SERVER
<code>childTableName</code>	Literal	String	UD_CHILD_PROCESS_FORM_NAME
<code>objectType</code>	Literal	String	Group

12. If you are enabling update provisioning operations on an Organizational Unit multivalued field, then repeat Steps 8 through 10 for all the variables listed in the following table. This table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
<code>procInstanceKey</code>	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
<code>itResourceFieldName</code>	Literal	String	UD_ADOU_SERVER
<code>childTableName</code>	Literal	String	UD_CHILD_PROCESS_FORM_NAME
<code>objectType</code>	Literal	String	organizationalUnit

13. On the Responses tab, click **Add** to add at least the SUCCESS response code, with Status `C`. This ensures that if the custom task is successfully run, then the status of the task is displayed as `Completed`.
14. Click the Save icon, close the dialog box, and then save the process definition.
15. Add the Car License Update process task by performing Steps 1 through 15 with the following difference:

While performing Step 4, instead of selecting **UD\_CARLICEN** from the Child Table list, select **UD\_CARLICN**. Similarly, instead of selecting **Insert** from the Trigger Type list, select **Update**.

16. Add the Car License Delete process task by performing Steps 1 through 15 with the following difference:

While performing Step 4, instead of selecting **UD\_CARLICEN** from the Child Table list, select **UD\_CARLICN**. Similarly, instead of selecting **Insert** from the Trigger Type list, select **Delete**.

17. Click **Save** on Process Task.

### 6.4.2.3 Updating the Request Dataset



#### Note:

Perform the procedure described in this section only if you have enabled request-based provisioning.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the XML file located in the *OIM\_HOME/dataset/file* directory for editing.
2. Add the `AttributeReference` element and specify values for the mandatory attributes of this element.

For example, if you added Car License as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Car License"
attr-ref = "Car License"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

In this `AttributeReference` element:

- For the `name` attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if `UD_CAR_LICENSE` is the value in the Name column of the process form, then you must specify `Car License` as the value of the `name` attribute in the `AttributeReference` element.

- For the `attr-ref` attribute, enter the value that you entered in the Field Label column of the process form.
- For the `type` attribute, enter the value that you entered in the Variant Type column of the process form.
- For the `widget` attribute, enter the value that you entered in the Field Type column of the process form.

- For the length attribute, enter the value that you entered in the Length column of the process form.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you add more than one attribute on the process form, then repeat this step for each attribute added.

3. Save and close the XML file.

#### 6.4.2.4 Clearing Content Related to Request Datasets from the Server Cache

 **Note:**

Perform the procedure described in this section only if you have enabled request-based provisioning.

Run the PurgeCache utility to clear content related to request datasets from the server cache. See *Purging Cache* in *Oracle Fusion Middleware Administering Oracle Identity Governance* for more information about the PurgeCache utility.

#### 6.4.2.5 Importing Request Datasets

 **Note:**

Perform the procedure described in this section only if you have enabled request-based provisioning.

Import into MDS, the request dataset definitions in XML format.

## 6.5 Adding Terminal Services Fields for Reconciliation and Provisioning

You can add additional terminal services fields for reconciliation and provisioning operations.

 **Note:**

The information in this section is applicable only to the Microsoft Active Directory target system and only if you are going to use the target system as a target resource.

Terminal Services fields are only supported for Microsoft Active Directory and not Microsoft AD LDS. Skip this section you are using Microsoft AD LDS as the target system.

By default, the following terminal services fields are readily available for reconciliation and provisioning:

- AllowLogon
- TerminalServicesProfilePath
- TerminalServicesHomeDirectory

If required, you can add the following terminal services fields for reconciliation and provisioning operations:

- TerminalServicesInitialProgram
- TerminalServicesWorkDirectory
- AllowLogon
- MaxConnectionTime
- MaxDisconnectionTime
- MaxIdleTime
- ConnectClientDrivesAtLogon
- ConnectClientPrintersAtLogon
- DefaultToMainPrinter
- BrokenConnectionAction
- ReconnectionAction
- EnableRemoteControl
- TerminalServicesProfilePath
- TerminalServicesHomeDirectory
- TerminalServicesHomeDrive

The procedure described in the following sections can be applied to add terminal services fields for reconciliation and provisioning. Note that the terminal field names in the preceding list must be used as the decode value in the Lookup.ActiveDirectory.UM.ProvAttrMap and Lookup.ActiveDirectory.UM.ReconAttrMap lookup definitions for provisioning and reconciliation, respectively.

- [Adding Custom Fields for Target Resource Reconciliation of Groups and Organizational Units](#)
- [Adding Custom Fields for Provisioning Groups and Organizational Units](#)

## 6.6 Adding the Group Name (pre-Windows 2000) Attribute

You can add a group name (pre-Windows 2000) attribute for reconciliation and provisioning.

This section discusses the following topics related to adding the Group Name (pre-Windows 2000 ) attribute for reconciliation and provisioning:

- [About the Group Name \(pre-Windows 2000\) Attribute](#)
- [Adding the Group Name Pre Windows Field for Reconciliation](#)

- [Adding the Group Name Pre Windows Field for Provisioning](#)

## 6.6.1 About the Group Name (pre-Windows 2000) Attribute

Group Name and Group Name (pre-Windows 2000) are two of the attributes specific to groups in the target system.

Oracle Identity Governance contains only the Group Name field in its process form. By default, during group provisioning, the value that you specify for the Group Name field in the OIM process form, is entered as the value of the Group Name and Group Name (pre-Windows 2000) attributes. If you want to specify different values for the Group Name and Group Name (pre-Windows 2000) attributes in the target system, then you must create the Group Name (pre-Windows 2000) field on the OIM process form. To do so, you must add a new field (Group Name Pre Windows) in Oracle Identity Governance for reconciliation and provisioning operations.

## 6.6.2 Adding the Group Name Pre Windows Field for Reconciliation

You can add the Group Name Pre Windows field for reconciliation.

To do so, perform the following procedure:

1. Log in to the Oracle Identity Governance Design Console.
2. Add the Group Name Pre Windows field to the list of reconciliation fields in the resource object as follows:
  - a. Expand **Resource Management** and then double-click **Resource Objects**.
  - b. Search for and open the **AD Group** resource object.
  - c. On the Object Reconciliation tab, click **Add Field**.
  - d. In the Add Reconciliation Field dialog box, enter `Group Name Pre Windows` in the Field Name field and select **String** from the Field Type list.
  - e. Click **Save** and close the dialog box.
  - f. Click **Create Reconciliation Profile**. This copies changes made to the resource object into MDS.
  - g. Click **Save**.
3. Update the **Lookup.ActiveDirectory.GM.ReconAttrMap** lookup definition for reconciliation as follows:
  - a. Expand **Administration** and then double-click **Lookup Definition**.
  - b. Search for and open the **Lookup.ActiveDirectory.GM.ReconAttrMap** lookup definition.
  - c. Click **Add** to create an entry for the Group Name Pre Windows field.
  - d. In the Code Key column, enter `Group Name Pre Windows`. In the Decode column, enter `sAMAccountName`.
  - e. In the Code Key column, locate **Group Name** and change its Decode value to `cn`. [Table 6-1](#) lists the updated list of entries in the **Lookup.ActiveDirectory.GM.ReconAttrMap** lookup definition.

**Table 6-1 Entries in the Updated Lookup.ActiveDirectory.GM.ReconAttrMap Lookup Definition**

Group Field on Oracle Identity Governance	Microsoft Active Directory Field
Display Name	displayName
Group name	cn
Group Name Pre Windows	sAMAccountName
Group Type	groupType
OIM Org Name	sAMAccountName
Organization Name[LOOKUP]	ad_container
Org Name	sAMAccountName
Org Type	OIM Organization Type
Unique Id	__UID__

- f. Click **Save**.
4. Add the Group Name Pre Windows field on the process form as follows:
  - a. Expand **Development Tools** and then double-click **Form Designer**.
  - b. Search for and open the **UD\_ADGRP** process form.
  - c. Click **Create New Version**, and then click **Add**.
  - d. Enter the details of the new field. In the Name field, enter `UD_ADUSER_GROUPNAME_PREWINDOWS`. In the Field Label column, enter `Group Name Pre Windows`. Enter the rest of the details of this field.
  - e. On the Properties tab, select the **Group Name Pre Windows** field, and then click **Add Property**. The Add Property dialog box displays.
  - f. From the Property Name list, select **Required**.
  - g. In the Property Value field, enter `True`.
  - h. Click the Save icon and close the dialog box.
  - i. Click **Save** and then click **Make Version Active**.
5. Create a reconciliation field mapping for the new field in the provisioning process as follows:
  - a. Expand **Process Management** and then double-click **Process Definition**.
  - b. Search for and open the **AD Group** provisioning process.
  - c. On the Reconciliation Field Mappings tab of the provisioning process, click **Add Field Map**.
  - d. In the Add Reconciliation Field Mapping dialog box, from the Field Name field, select **Group Name Pre Windows**.
  - e. Double-click the Process Data field, and then select **UD\_ADGRP\_GROUPNAME\_PREWINDOWS**.
  - f. Click **Save** and close the dialog box.
  - g. Click **Save**.
6. Expand **Resource Management** and then double-click **Resource Objects**.
7. Click **Create Reconciliation Profile**.



## 6.6.3 Adding the Group Name Pre Windows Field for Provisioning

You can add the Group Name Pre Windows field for provisioning.

To do so, perform the following procedures:

- [Adding the Group Name Pre Windows Field](#)
- [Updating the Lookup.ActiveDirectory.GM.ProvAttrMap Lookup Definition](#)
- [Enabling Update Provisioning Operations on the Group Name Pre Windows Field](#)
- [Updating Adapters](#)
- [Updating the Request Dataset](#)
- [Running the PurgeCache Utility](#)
- [Importing the Request Dataset Definitions into MDS](#)

### 6.6.3.1 Adding the Group Name Pre Windows Field

If you have added the field on the process form by performing Step 4 of [Adding the Group Name Pre Windows Field for Reconciliation](#), then you need not add the field again. If you have not added the field, then:

1. Log in to the Oracle Identity Governance Design Console.
2. Expand **Development Tools** and then double-click **Form Designer**.
3. Search for and open the **UD\_ADGRP** process form.
4. Click **Create New Version**, and then click **Add**.
5. In the **Name** field, enter `UD_ADUSER_GROUPNAME_PREWINDOWS`.
6. In the Field Label column, enter `Group Name Pre Windows`. Then, enter values for the rest of the columns as listed for the Group Name field.
7. On the Properties tab, select the **Group Name Pre Windows** field, and then click **Add Property**. The Add Property dialog box displays.
8. From the Property Name list, select **Required**.
9. In the Property Value field, enter `True`.
10. Click the Save icon and close the dialog box.
11. Click **Save** and then click **Make Version Active**.

### 6.6.3.2 Updating the Lookup.ActiveDirectory.GM.ProvAttrMap Lookup Definition

Update the Lookup.ActiveDirectory.GM.ProvAttrMap lookup definition for provisioning as follows:

1. Expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.ActiveDirectory.GM.ProvAttrMap** lookup definition.
3. Click **Add** to create an entry for the Group Name Pre Windows field.
4. In the Code Key column, enter `Group Name Pre Windows`. In the Decode column, enter `sMAccountName`.

5. In the Code Key column, locate and replace **Group Name** with `Group Name [IGNORE]`, and change its Decode value to `IGNORED`. Table 6-1 lists the updated list of entries in the `Lookup.ActiveDirectory.GM.ProvAttrMap` lookup definition.

**Table 6-2** Entries in the Updated `Lookup.ActiveDirectory.GM.ProvAttrMap` Lookup Definition

Group Field on Oracle Identity Governance	Microsoft Active Directory Field
<code>__NAME__</code>	<code>__NAME__="CN=\${Group_Name},\${Organization_Name}"</code>
Display Name	<code>displayName</code>
Group Name[IGNORE]	<code>IGNORED</code>
Group Name Pre Windows	<code>sAMAccountName</code>
Group Type	<code>groupType</code>
Organization Name[LOOKUP,IGNORE]	<code>IGNORED</code>
Unique Id	<code>__UID__</code>

6. Click **Save**.

### 6.6.3.3 Enabling Update Provisioning Operations on the Group Name Pre Windows Field

Enable update provisioning operations on the Group Name Pre Windows field as follows:

1. In the provisioning process, add a new task for updating the field as follows:
  - a. Expand **Process Management** and then double-click **Process Definition**.
  - b. Search for and open the **AD Group** provisioning process.
  - c. Click **Add** and enter the task name and task description as follows:
 

**Task Name:** `Group Name Pre Windows Updated`

**Task Description:** `Process Task for handling update of the Group Name Pre Windows field.`
  - d. In the Task Properties section, select the **Conditional**, **Allow Cancellation while Pending**, and **Allow Multiple Instances** fields.
  - e. Click **Save**.
2. In the provisioning process, select the adapter name in the Handler Type section as follows:
  - a. Go to the Integration tab, click **Add**.
  - b. In the Handler Selection dialog box, select **Adapter**.
  - c. From the Handler Name column, select **adpADIDCUPDATEATTRIBUTEVALUE**.
  - d. Click **Save** and close the dialog box.
3. In the Adapter Variables region, click the **procInstanceKey** variable.
4. In the dialog box that is displayed, create the following mapping:
 

**Variable Name:** `procInstanceKey`

**Map To:** Process Data

**Qualifier:** Process Instance

5. Click **Save** and close the dialog box.
6. Repeat Steps 3 through 5 for all the variables listed in the following table. This table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
procInstanceKey	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
itResourceFieldName	Literal	String	UD_ADGRP_SERVER
attrFieldName	Literal	String	Group Name Pre Windows
objectType	Literal	String	Group

7. On the Responses tab, click **Add** to add at least the SUCCESS response code, with Status C. This ensures that if the custom task is successfully run, then the status of the task is displayed as Completed.
8. Click the Save icon and close the dialog box, and then save the process definition.

### 6.6.3.4 Updating Adapters

If the Group Name Updated process task calls the adpADIDCUPDATEATTRIBUTEVALUES adapter, then:

1. Remove the **adpADIDCUPDATEATTRIBUTEVALUES** adapter and add the **adpADIDCUPDATEATTRIBUTEVALUE** adapter.
2. On the Integration tab, in the Adapter Variables region, click the **procInstanceKey** variable.
3. In the dialog box that is displayed, create the following mapping:

**Variable Name:** procInstanceKey

**Map To:** Process Data

**Qualifier:** Process Instance

4. Click **Save** and close the dialog box.
5. Repeat Steps 2 through 4 for all the variables listed in the following table. This table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

Variable	Map To	Qualifier	Literal Value
procInstanceKey	Process Data	Process Instance	NA
Adapter Return Variable	Response Code	NA	NA
itResourceFieldName	Literal	String	UD_ADGRP_SERVER
attrFieldName	Literal	String	Group Name
objectType	Literal	String	Group

### 6.6.3.5 Updating the Request Dataset

**Note:**

Perform the procedures described in this section only if you want to perform request-based provisioning.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

1. In a text editor, open the XML file located in the *OIM\_HOME/dataset/file* directory for editing.
2. Add the `AttributeReference` element and specify values for the mandatory attributes of this element.

For example, while performing the procedure described in [Adding the Group Name Pre Windows Field](#), if you added Employee ID as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "GroupName PreWindows"
attr-ref = "Group Name Pre Windows"
type = "String"
widget = "text"
length = "70"
available-in-bulk = "false"/>
```

In this `AttributeReference` element:

- For the `name` attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if `UD_ADUSER_GROUPNAME_PREWINDOWS` is the value in the Name column of the process form, then you must specify `GroupName PreWindows` as the value of the `name` attribute in the `AttributeReference` element.

- For the `attr-ref` attribute, enter the value that you entered in the Field Label column of the process form while performing the procedure described in [Adding the Group Name Pre Windows Field](#).
- For the `type` attribute, enter the value that you entered in the Variant Type column of the process form while performing the procedure described in [Adding the Group Name Pre Windows Field](#).
- For the `widget` attribute, enter the value that you entered in the Field Type column of the process form, while performing the procedure described in [Adding the Group Name Pre Windows Field](#).
- For the `length` attribute, enter the value that you entered in the Length column of the process form while performing the procedure described in [Adding the Group Name Pre Windows Field](#).
- For the `available-in-bulk` attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing the procedure described in [Adding the Group Name Pre Windows Field](#) if you added more than one attribute on the process form, then repeat this step for each attribute added.

3. Save and close the XML file.

### 6.6.3.6 Running the PurgeCache Utility



#### Note:

Perform the procedures described in this section only if you want to perform request-based provisioning.

Run the PurgeCache utility to clear content related to request datasets from the server cache. See [Purging Cache in Oracle Fusion Middleware Administering Oracle Identity Governance](#) for more information about the PurgeCache utility.

### 6.6.3.7 Importing the Request Dataset Definitions into MDS



#### Note:

Perform the procedures described in this section only if you want to perform request-based provisioning.

Import into MDS, the request dataset definitions in XML format.

## 6.7 Configuring Transformation and Validation Of Data

You can configure transformation and validation of data for users, groups, and organizations.

- [About Configuring Transformation and Validation of Data](#)
- [Configuring Transformation of Data During Reconciliation for Groups and Organizational Units](#)
- [Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units](#)

### 6.7.1 About Configuring Transformation and Validation of Data

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

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

Similarly, you can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can

validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

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

## 6.7.2 Configuring Transformation of Data During Reconciliation for Groups and Organizational Units

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

### Note:

This section describes an optional procedure. Perform this procedure only if you want to configure transformation of data during reconciliation.

You can configure transformation of reconciled data according to your requirements. For example, you can automate the look up of the field name from an external system and set the value based on the field name.

To configure transformation of data:

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

The only criteria for the class is that it should have a method with the following name and signature:

```
public Object transform(HashMap hmUserDetails, HashMap hmEntitlementDetails,
String sField) {}
```

2. Create a JAR file to hold the Java class.
3. Run the Oracle Identity Governance Upload JARs utility to post the JAR file to the Oracle Identity Governance database. This utility is copied into the following location when you install Oracle Identity Governance:

### Note:

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

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

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Governance administrator, URL of the Oracle Identity Governance host computer, context factory value, type of JAR file being uploaded, and the

location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. Add an entry in the lookup definition for transformation as follows:
  - a. Log in to the Design Console.
  - b. Search for and open one of the following lookup definitions:
    - For groups: **Lookup.ActiveDirectory.GM.ReconTransformation**
    - For organizational units: **Lookup.ActiveDirectory.OM.ReconTransformation**
  - c. In the **Code Key** column, enter the reconciliation field name for the attribute on which you want to apply the transformation. For example: `First Name`.
  - d. In the **Decode** column, enter the name of the class file. For example: `com.transformationexample.MyTransformer`.
  - e. Save the changes to the lookup definition.

 **Note:**

To configure the transformation of data during trusted source reconciliation, then add the following entries in the `Lookup.ActiveDirectory.OM.Configuration.Trusted` lookup definition:

- **Code Key value:** `Recon Transformation Lookup`
- **Decode value:** `Lookup.ActiveDirectory.OM.ReconTransformation`

### 6.7.3 Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units

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 validation of data:

1. Write code that implements the required validation logic in a Java class.  
This validation class must implement the `validate` method.
2. Create a JAR file to hold the Java class.
3. Run the Oracle Identity Governance Upload JARs utility to post the JAR file to the Oracle Identity Governance database. This utility is copied into the following location when you install Oracle Identity Governance:

 **Note:**

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

- For Microsoft Windows: *OIM\_HOME*/server/bin/UploadJars.bat
- For UNIX: *OIM\_HOME*/server/bin/UploadJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Governance administrator, URL of the Oracle Identity Governance host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. If you created the Java class for validating a process form field for reconciliation, then:
  - a. Log in to the Design Console.
  - b. Search for and open one of the following lookup definitions:
    - For groups: **Lookup.ActiveDirectory.GM.ReconValidation**
    - For organizational units: **Lookup.ActiveDirectory.OM.ReconValidation**
  - c. In the **Code Key** column, enter the resource object field name. In the **Decode** column, enter the class name (for example: `com.validate.MyValidation`).
  - d. Save the changes to the lookup definition.
  - e. Search for and open one of the following lookup definitions:
    - For groups: **Lookup.ActiveDirectory.GM.Configuration**
    - For organizational units: **Lookup.ActiveDirectory.OM.Configuration**
  - f. Ensure that the value of the **Recon Validation Lookup** entry is set to one of the following:
    - For groups: `Lookup.ActiveDirectory.GM.ReconValidation`.
    - For organizational units: `Lookup.ActiveDirectory.OM.ReconValidation`.
  - g. Save the changes to the lookup definition.
5. If you created the Java class for validating a process form field for provisioning, then:
  - a. Log in to the Design Console.
  - b. Search for and open one of the following lookup definitions:
    - For groups: **Lookup.ActiveDirectory.GM.ProvValidation**
    - For organizational units: **Lookup.ActiveDirectory.OM.ProvValidation**
  - c. In the **Code Key** column, enter the process form field name. In the **Decode** column, enter the class name (for example: `com.validate.MyValidation`).
  - d. Save the changes to the lookup definition.
  - e. Search for and open one of the following lookup definitions:
    - For groups: **Lookup.ActiveDirectory.GM.Configuration**
    - For organizational units: **Lookup.ActiveDirectory.OM.Configuration**
  - f. Ensure that the value of the **Provisioning Validation Lookup** entry is set to one of the following:
    - For groups: `Lookup.ActiveDirectory.GM.ProvValidation`.
    - For organizational units: `Lookup.ActiveDirectory.OM.ProvValidation`.



- g. Save the changes to the lookup definition.

## 6.8 Action Scripts

**Actions** are scripts that you can configure 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. Similarly, you can run custom PowerShell scripts before or after creating, updating, or deleting a mailbox.

The following are topics pertaining to action scripts:

- [Action Scripts for Users](#)
- [Action Scripts for Groups and Organizational Units](#)

### 6.8.1 Action Scripts for Users

The following are topics pertaining to action scripts for users:

- [About Configuring Action Scripts for Users](#)
- [Running a Custom PowerShell Script for Users](#)
- [Running Actions Using Visual Basic Scripts for Users](#)
- [Important Notes on Running Actions Scripts for Users](#)
- [Guidelines on Creating Scripts for Users](#)

#### 6.8.1.1 About Configuring Action Scripts for Users

You can configure **Action Scripts** by writing your own PowerShell 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*.



#### Note:

The scripting language used is PowerShell.

#### 6.8.1.2 Running a Custom PowerShell Script for Users

As an example, the following procedure describes the steps to run a custom PowerShell script before a create operation:

1. Select an application of your choice after creating it or while updating it.
2. Select **Settings, User**, and then **Provisioning**. All available action scripts are displayed.

**Figure 6-3 Preview Settings for Action Scripts**

Preview Settings

Provisioning Reconciliation Organization Catalog

Below are the pre-defined provisioning configurations that have been set for you.

Global Configuration

Validation Script

Transformation Script

Account Name

User ID

Capabilities

Below capabilities are available for this application. You can associate pre / post action scripts against them.

Action	Action Script
<input checked="" type="checkbox"/> change user password	Action Script
<input checked="" type="checkbox"/> delete	Action Script
<input checked="" type="checkbox"/> create	Action Script

- To view its contents, click any of the enabled action scripts.

**Figure 6-4 Action Scripts**

Action Script:create

<p>Trigger Time</p> <p>Before</p> <p>Language</p> <p>Shell</p> <p>Target</p> <p>Resource</p> <p>Script</p> <p><i>Enter the target to execute the script.</i></p> <p>Compile</p>	<p>Trigger Time</p> <p>After</p> <p>Language</p> <p>Shell</p> <p>Target</p> <p>Resource</p> <p>Script</p> <p>PowerShell.exe -File C:\ActionScripts\postcreate.ps1 Exit</p> <p>Compile</p>
---	---

Save Cancel

4. Set the value of the **Target** field to **Resource** only. The script is executed on the computer where the target system is running.
5. Click **Edit**, and then enter the following content in the **Script** field:

```
Powershell.exe -File NAME_AND_FULL_LOCATION_OF_THE_CUSTOM_SCRIPT
Exit
```

Sample value:

```
Powershell.exe -File C:\myscripts\CustomScript.ps1
Exit
```

6. Click **Save** and then click **Apply** to commit the action scripts to the database.
7. Log in to the computer running the connector server and create the custom script (in this example the customScript.ps1 script, located in the C:\myscripts directory) file with the following content:

```
$Class = "organizationalUnit"
$OU = "OU=ScriptOU81"
$objADSI = [ADSI]"LDAP://Dc=extest,DC=com"
$objOU = $objADSI.create($Class, $OU)
$objOU.setInfo()
```

This script runs before every create provisioning operation. This script creates an Organization named 'ScriptOU81'. Similarly, you can write custom scripts as per your requirement.

#### Note:

- If you are using a PowerShell script, then before running the script by using the connector or Oracle Identity Governance, verify the following on the computer running the connector server:
  - You must be able to connect manually to the AD server with the values specified in the script using the PowerShell window without any issues.
  - From the command prompt, navigate to the directory containing the batch file. Then, run the batch file with appropriate parameters and ensure that the PowerShell script runs on AD server without any issues.
- Process form fields marked as IGNORE are not sent to the connector.

### 6.8.1.3 Running Actions Using Visual Basic Scripts for Users

The following is an example procedure for running actions using Visual Basic scripts that consumes data dynamically from the process form. This is an example procedure for an After Create action, which requires creating a user in an organizational unit in addition to the one in which the user is provisioned to.

1. Create a file (a script) on the computer running Oracle Identity Governance with the following data:

```
C:\arg.vbs %givenName%
```

Note that there is a space between C:\arg.vbs and %givenName%.

2. On the machine hosting the target system, create a file in the C:\ directory. For example, create an arg.vbs file.
3. Include the following lines in the arg.vbs file:

```
Set args = WScript.Arguments
GivenNameFromArg = args.Item(0)
lengthGivenName = Len(GivenNameFromArg) - 2
GivenNameTrim = Mid(GivenNameFromArg, 2, lengthGivenName)
Set objOU = GetObject("LDAP://ausovm3194win.matrix.com:389/
OU=TestOrg4,dc=matrix,dc=com")
Set objUser = objOU.Create("User", "cn=scriptCreate" & GivenNameTrim )
objUser.Put "givenName", "scriptCreate" & GivenNameTrim
objUser.Put "sAMAccountName", "scriptCreate " & GivenNameTrim
objUser.Put "userPrincipalName", "scriptCreate" & GivenNameTrim
objUser.Put "displayName", "scriptCreate" & GivenNameTrim
objUser.Put "sn", "scriptCreate" & GivenNameTrim
objUser.SetInfo
```

4. Save and close the file.
5. Provision a user account on Oracle Identity Governance.

### 6.8.1.4 Important Notes on Running Actions Scripts for Users

The following are important notes on running actions scripts:

- Any errors encountered while running action scripts are ignored and are not propagated to Oracle Identity Governance.
- During create operations, all attributes part of process form are available to the script.
- During update operations, only the attribute that is being updated is available to the script.
- During delete operations, only the `__UID__` (GUID) attribute is available to the script.

### 6.8.1.5 Guidelines on Creating Scripts for Users

The following are the guidelines that you must apply or be aware of while configuring action scripts:

- All field names used in the scripts must be enclosed within `%%`.
- You can call any VB script from a shell and pass the process form fields.
- You cannot include the Password field in the script. This is because password is stored as a guarded string. Therefore, we do not get the exact password when we fetch values for the Password field.
- Addition of child table attributes belongs to the 'Update' category and not 'Create.'

## 6.8.2 Action Scripts for Groups and Organizational Units

The following are topics pertaining to action scripts for groups and organizational units:

- [About Configuring Action Scripts for Groups and Organizational Units](#)
- [Running a Custom PowerShell Script for Groups and Organizational Units](#)

- [Running Actions Using Visual Basic Scripts for Groups and Organizational Units](#)
- [Important Notes on Running Actions Scripts for Groups and Organizational Units](#)
- [Guidelines on Creating Scripts for Groups and Organizational Units](#)

## 6.8.2.1 About Configuring Action Scripts for Groups and Organizational Units

You can configure **Action Scripts** by writing your own PowerShell 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.



### Note:

The scripting language used is PowerShell.

## 6.8.2.2 Running a Custom PowerShell Script for Groups and Organizational Units

As an example, the following procedure describes the steps to run a custom PowerShell script before a create operation:

1. Log in to the Design Console.
2. Search for and open one of the following lookup definitions:
  - For groups: **Lookup.ActiveDirectory.GM.Configuration**
  - For organizational units: **Lookup.ActiveDirectory.OU.Configuration**
3. Add the following new values:
  - **Code Key:** *TIMING* Action Language  
Sample value: Before Create Action Language
  - **Decode:** Enter the scripting language of the script you want to execute  
Sample value: Shell
4. Add these new values:
  - **Code Key:** *TIMING* Action File  
Sample value: Before Create Action File
  - **Decode:** Enter the full path of the batch file that invokes the script. (Oracle Identity Governance must be able to access this file.)  
Sample value: /scratch/Scripts/InvokeCustomScript.bat
5. Add these new values:
  - **Code Key:** *TIMING* Action Target  
Sample value: Before Create Action Target
  - **Decode:** Resource (do *not* modify this value)
6. Save the lookup definition.

7. On the computer running Oracle Identity Governance, create the /scratch/Scripts/InvokeCustomScript.bat file with the following content:

```
Powershell.exe -File NAME_AND_FULL_LOCATION_OF_THE_CUSTOM_SCRIPT  
Exit
```

Sample value:

```
Powershell.exe -File C:\myscripts\CustomScript.ps1  
Exit
```

8. Log in to the computer running the connector server and create the custom script (in this example the customScript.ps1 script, located in the C:\myscripts directory) file with the following content:

```
$Class = "organizationalUnit"  
$OU = "OU=ScriptOU81"  
$objADSI = [ADSI]"LDAP://Dc=extest,DC=com"  
$objOU = $objADSI.create($Class, $OU)  
$objOU.setInfo()
```

This script runs before every create provisioning operation. This script creates an Organization named 'ScriptOU81'. Similarly, you can write custom scripts as per your requirement.

 **Note:**

If you are using a PowerShell script, then before running the script by using the connector or Oracle Identity Governance, verify the following on the computer running the connector server:

- You must be able to connect manually to the AD server with the values specified in the script using the PowerShell window without any issues.
- From the command prompt, navigate to the directory containing the batch file. Then, run the batch file with appropriate parameters and ensure that the PowerShell script runs on AD server without any issues.

Note that you can pass process form fields to scripts that call the before or after action scripts. These process form fields must be present in Lookup.ActiveDirectory.GM.ProvAttrMap or Lookup.ActiveDirectory.OU.ProvAttrMap lookup definitions and be mapped to a corresponding target system attribute. For example, you can pass the First Name process form field (present in Lookup.ActiveDirectory.GM.ProvAttrMap or Lookup.ActiveDirectory.OU.ProvAttrMap lookup definitions) to an action script by specifying "givenName," which is the name of the corresponding attribute in the target system.

 **Note:**

Process form fields marked as IGNORE are not sent to the connector.

### 6.8.2.3 Running Actions Using Visual Basic Scripts for Groups and Organizational Units

The following is an example procedure for running actions using Visual Basic scripts that consumes data dynamically from the process form. This is an example procedure for an After Create action, which requires creating a user in an organizational unit in addition to the one in which the user is provisioned to.

1. Create a file (a script) on the computer running Oracle Identity Governance with the following data:

```
C:\arg.vbs %givenName%
```

Note that there is a space between C:\arg.vbs and %givenName%.

2. On the machine hosting the target system, create a file in the C:\ directory. For example, create an arg.vbs file.
3. Include the following lines in the arg.vbs file:

```
Set args = WScript.Arguments
GivenNameFromArg = args.Item(0)
lengthGivenName = Len(GivenNameFromArg) - 2
GivenNameTrim = Mid(GivenNameFromArg, 2, lengthGivenName)
Set objOU = GetObject("LDAP://ausovm3194win.matrix.com:389/
OU=TestOrg4,dc=matrix,dc=com")
Set objUser = objOU.Create("User", "cn=scriptCreate" & GivenNameTrim )
objUser.Put "givenName", "scriptCreate" & GivenNameTrim
objUser.Put "sAMAccountName", "scriptCreate " & GivenNameTrim
objUser.Put "userPrincipalName", "scriptCreate" & GivenNameTrim
objUser.Put "displayName", "scriptCreate" & GivenNameTrim
objUser.Put "sn", "scriptCreate" & GivenNameTrim
objUser.SetInfo
```

4. Save and close the file.
5. Provision a user account on Oracle Identity Governance.

### 6.8.2.4 Important Notes on Running Actions Scripts for Groups and Organizational Units

The following are important notes on running actions scripts:

- Any errors encountered while running action scripts are ignored and are not propagated to Oracle Identity Governance.
- During create operations, all attributes part of process form are available to the script.
- During update operations, only the attribute that is being updated is available to the script.

If other attributes are also required, then a new adapter calling `ICProvisioningManager#updateAttributeValues(String objectType, String[] labels)` must be created and used. During adapter mapping in process task, add the form field labels of the dependent attributes.

- During delete operations, only the `__UID__` (GUID) attribute is available to the script.

## 6.8.2.5 Guidelines on Creating Scripts for Groups and Organizational Units

The following are the guidelines that you must apply or be aware of while configuring action scripts:

- Your script file can contain scripts that include attributes present in the decode column of any of the following lookup definitions:
  - Lookup.ActiveDirectory.GM.ProvAttrMap
  - Lookup.ActiveDirectory.OM.ProvAttrMap
- All field names used in the scripts must be enclosed within %%.
- You can call any VB script from a shell and pass the process form fields.
- You cannot include the Password field in the script. This is because password is stored as a guarded string. Therefore, we do not get the exact password when we fetch values for the Password field.
- Addition of child table attributes belongs to the 'Update' category and not 'Create.'

## 6.9 Enabling Reconciliation and Provisioning Operations Across Multiple Domains

The Microsoft Active Directory User Management connector supports reconciliation and provisioning operations across multiple domains in a single forest.



### Note:

The information in this section is applicable *only* if you are using Microsoft Active Directory as the target system. Enabling reconciliation and provisioning operations across multiple domains is not supported if you are using Microsoft AD LDS as the target system.

Reconciliation runs are performed by using the Global Catalog Server and provisioning operations are performed by using LDAP referrals.

If you want to enable reconciliation and provisioning across multiple domains, then perform the procedure described in the following sections:

- [Understanding Enabling Reconciliation Across Multiple Domains](#)
- [Understanding Enabling Provisioning Across Multiple Domains](#)

### 6.9.1 Understanding Enabling Reconciliation Across Multiple Domains

This following sections help you understand enabling reconciliation across multiple domains:

- [About Enabling Reconciliation Across Multiple Domains](#)
- [Enabling Reconciliation Across Multiple Domains](#)



### 6.9.1.1 About Enabling Reconciliation Across Multiple Domains

To perform reconciliation across multiple domains, this connector uses both the domain controller and the Global Catalog Server for fetching records from the target system.

During reconciliation, records from the Global Catalog Server are fetched to the connector. After a record is fetched into the connector, the distinguishedName and uSNChanged attribute values are read. By using the distinguishedName, the connector performs an LDAP query on the domain controller that contains the actual data (referrals are used here). This approach is used for reconciliation because the Global Catalog Server has only partial set of records. Complete data can only be fetched from the domain controller.

After all records are fetched into Oracle Identity Governance, the reconciliation engine updates the Latest Token attribute of the scheduled job with the maximum value of the uSNChanged attribute of a domain controller on which the Global Catalog Server is running. From the next reconciliation run onward, only records whose uSNChanged attribute values are greater than current value in the Latest Token attribute are fetched from the Global Catalog Server. Therefore, any updates made to a record on the target system must update the uSNChanged attribute of that record in the Global Catalog Server so that the connector can detect records that have been updated since the last reconciliation run and then fetch them into Oracle Identity Governance.

### 6.9.1.2 Enabling Reconciliation Across Multiple Domains

To enable reconciliation across multiple domains:

1. Set the value of the Search Child Domains parameter of [Advanced Settings Parameters](#) to `yes`.
2. Specify the name of the domain controller that is hosting the Global Catalog Server as the value of the Global Catalog Server parameter of the [Basic Configuration Parameters](#) section.

#### Note:

- If the value of the Search Child Domains parameter is set to `yes` and no value is specified for the Global Catalog Server parameter, then the connector determines the Global Catalog Server on its own. It is strongly recommended that you specify a value for the Search Child Domains parameter in the [Advanced Settings Parameters](#) and the Global Catalog Server parameter in the [Basic Configuration Parameters](#).
- While performing group reconciliation in a cross-domain environment, the connector fetches only those groups of the account that are visible to the domain controller on which the account is present.
- It is recommended to not enter any value for LDAP Host Name parameter of the [Basic Configuration Parameters](#) section. The connector will automatically find the right domain controller to fetch complete user information after obtaining the distinguished name from the global catalog server. If you specify a value for the LDAP Host Name parameter, then the connector ignores it and determines the appropriate domain controller (for fetching user information) by using the ADSI referrals feature.

## 6.9.2 Understanding Enabling Provisioning Across Multiple Domains

In a parent-child deployment environment of the target system, before performing provisioning operations across multiple domains, it is expected that the target system IT resource is configured with the parent domain. In a replication environment of the target system, before performing provisioning operations across multiple domains, it is expected that the target system IT resource is configured with any of the domain controllers.

This scenario is illustrated by the following example:

Suppose a parent-child domain environment in which the parent domain is dc1 and child domain is dc2. The target system IT resource is configured to include dc1 as the value of the LDAP Host Name parameter and the name of the parent domain as the value of the DomainName parameter.

During provisioning, if we select an organization that belongs to the child domain, multiple groups that span across domains, and the manager from the parent domain, then LDAP referrals are internally used by ADSI (Active Directory Service Interfaces). This is because all connectors operations are leveraged to ADSI, which enables creation of an account in the child domain even without providing any details of the child domain in the IT resource.

All this information is internally calculated depending upon the organization that is selected during the provisioning operation. In the connector, the referral chasing option is set to `All`, which means that all referrals are chased when any referral is provided by the domain controller. Therefore, no explicit configuration procedure is required to enable provisioning across multiple domains.



### See Also:

The ADSI documentation for more information about LDAP referrals

## 6.10 About Using the Connector for Multiple Trusted Source Reconciliation

You can use the connector for more than one trusted source reconciliation.

The following are examples of scenarios in which there is more than one trusted source for user data in an organization:

- One of the target systems is a trusted source for data about employees. The second target system is a trusted source for data about contractors. The third target system is a trusted source for data about interns.
- One target system holds the data of some of the identity fields that constitute an OIM User. Two other systems hold data for the remaining identity fields. In other words, to create an OIM User, data from all three systems would need to be reconciled.

If the operating environment of your organization is similar to that described in either one of these scenarios, then this connector enables you to use the target system as one of the trusted sources of user data in your organization.

## 6.11 Multiple Installations of the Target System

You can use the Active Directory User Management connector in an environment containing multiple target systems.

The following are topics related to multiple target system installations:

- [About Multiple Installations of the Target System](#)
- [Configuring the Connector for Multiple Installations of the Target System](#)

### 6.11.1 About 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.

#### Note:

The information in this section also applies to Microsoft AD LDS.

- If you are upgrading from 11.1.2.x to 12.2.1.3.0, then:

Perform the procedure described in this section if your environment has multiple installations of the target system, which share the same schema managed by this connector. In such a scenario, if you are using Oracle Identity Governance release 12.2.1.3.0, then only the IT resource information must be changed. If you are using Oracle Identity Governance release 12.2.1.3.0, then the IT resource information must be changed and application instances must be created.

In addition, irrespective of the Oracle Identity Governance release that you are using, scheduled tasks must be replicated, but the underlying workflow and process form is shared across all installations of the target system.

If your environment has multiple installations of the target system and the schema differs (that is, different sets of attributes must be managed by using the connector. In other words, you need different process forms, workflows, and so on), then you must use the connector cloning feature.

- If you are using Application On-Boarding, then:

Perform the procedure described in this section if your environment has multiple installations of the target system, which share the same schema managed by this connector. In such a scenario, if you are using Oracle Identity Governance release 12.2.1.3.0, then the basic configuration information must be changed and a new application must be created.

If your environment has multiple installations of the target system and the schema differs (that is, different sets of attributes must be managed by using the connector. In other words, you need different process forms, workflows, and so on), then you must create a new application.

You may want to configure the connector for multiple installations of Microsoft Active Directory. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Example Multinational Inc. have their own installations of Microsoft Active Directory. The company has recently installed Oracle Identity Governance, and they want to configure Oracle Identity Governance to link all the installations of Microsoft Active Directory.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of Microsoft Active Directory.

## 6.11.2 Configuring the Connector for Multiple Installations of the Target System

You can configure the connector for multiple installations of the target system by upgrading the connector from Oracle Identity Governance release 11.1.2.x to 12.2.1.3.0 or through application on-boarding.

To configure the connector for multiple installations of the target system, perform one of the procedures listed in the following sections:

- [Configuring the Connector for Multiple Installations of the Target System while Upgrading from Oracle Identity Governance release 11.1.2.x to 12.2.1.3.0](#)
- [Configuring the Connector for Multiple Installations of the Target System Using Application On-Boarding](#)

### 6.11.2.1 Configuring the Connector for Multiple Installations of the Target System while Upgrading from Oracle Identity Governance release 11.1.2.x to 12.2.1.3.0

To configure the connector for multiple installations of the target system:

1. Create IT resources of the Active Directory IT resource type so that there is one IT resource for each installation of the target system. If you are using Oracle Identity Governance release 12.2.1.3.0 or later, then in addition to creating the IT resource, you must create the application instance.
2. Create copies of the reconciliation scheduled tasks for each installation of the target system. While creating a scheduled task, specify attribute values corresponding to the target system installation for which you are creating the scheduled task.
3. Manually synchronize the lookup definitions in Oracle Identity Governance with the lookup field values on the target system.

### 6.11.2.2 Configuring the Connector for Multiple Installations of the Target System Using Application On-Boarding

To configure the connector for multiple installations of the target system:

1. Create a new application using application on-boarding for multiple installation of the target system.

2. Manually synchronize the lookup definitions in Oracle Identity Governance with the lookup field values on the target system.

## 6.12 Creating a Home Directory After User Create Provisioning Operation

You can initiate the process to update the home directory after the Create User provisioning operation.

To accomplish this task in Application On-Boarding, you must write a post-create Action Script and make the home directory creation changes in that script itself.

## 6.13 Configuring the Connector for Provisioning Groups of the Security Group - Universal Group Type

You can create a group of type Security Group - Universal by adding this group type to the Lookup.ActiveDirectory.GroupTypes lookup definition.

There are six types of groups that you can create in the target system. By default, this connector is shipped with only five group types that you can select for the group that you create through Oracle Identity Governance. If you want to create a group of type Security Group - Universal, then you must add this group type to the Lookup.ActiveDirectory.GroupTypes lookup definition as follows:

1. Log in to the Design Console.
2. Expand **Administration**, and then double-click **Lookup Definition**.
3. Search for and open **Lookup.ActiveDirectory.GroupTypes** lookup definition.
4. Click **Add**.
5. In the new row that is added, enter the following values:

**Code Key:** - 2147483640

**Decode:** Security Group - Universal

6. Click the Save icon.

You can now search for **-2147483640** and select the **Security Group - Universal** group type while creating a group through Oracle Identity Governance.

# 7

## Upgrading the Microsoft Active Directory User Management Connector

If you have already deployed 11.1.1.6.0 version of this connector, then you can upgrade the connector to version 12.2.1.3.0.

### Note:

- The connector upgrade from version 11.1.1.6.0 to 12.2.1.3.0 is only supported in the CI-based mode.
- Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Governance database. Refer to the database documentation for information about creating a backup.
- As a best practice, first perform the upgrade procedure in a test environment.

- [Preupgrade Steps](#)
- [Upgrade Steps](#)
- [Postupgrade Steps](#)

### 7.1 Preupgrade Steps

You must perform the following preupgrade steps to prepare your environment for upgrading the connector:

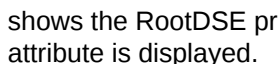
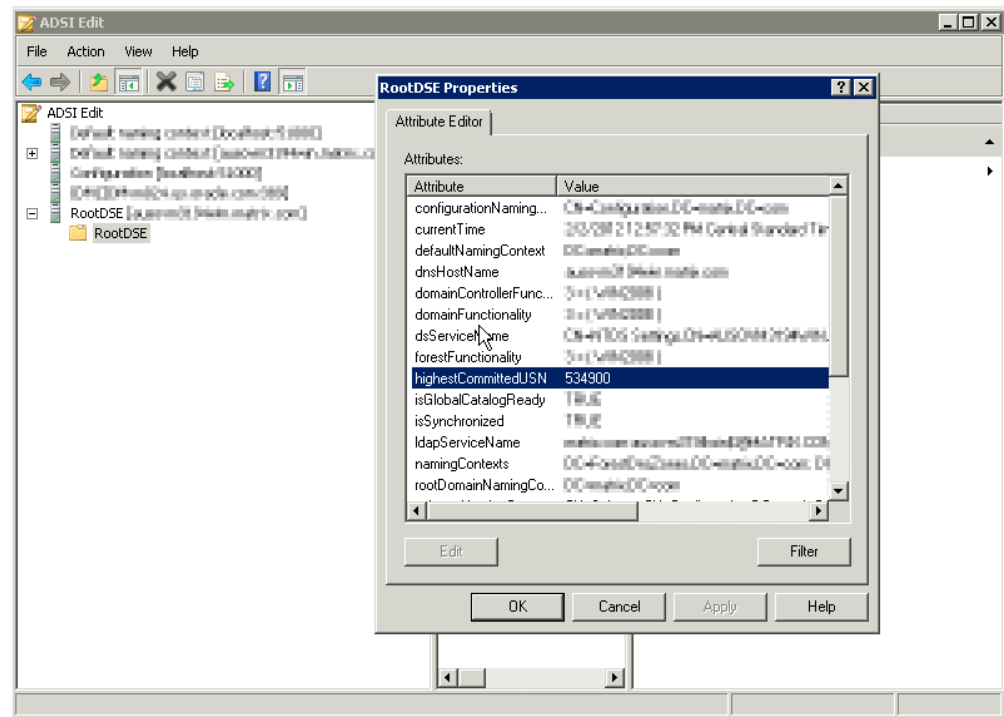
1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Governance.
2. Perform the preupgrade procedure documented in *Managing Connector Lifecycle of Oracle Fusion Middleware Administering Oracle Identity Governance*.
3. On the target system, obtain the maximum value of the uSNChanged attribute as follows:
  - a. If you are using the connector across multiple domains, then on the domain controller on which the Global Catalog Server is running, navigate to RootDSE, and then look for the RootDSE properties.
  - b. If you are using the connector in a single domain, then on the domain controller used for reconciliation, navigate to RootDSE, and then look for the RootDSE properties.
  - c. In the RootDSE properties dialog box, search for the highestCommittedUSN attribute, and note down its value. The use of this value is described later in this chapter.  shows the RootDSE properties dialog box in which the highestCommittedUSN attribute is displayed.

Figure 7-1 RootDSE Properties Dialog Box



4. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Governance. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector. See *Managing Connector Lifecycle of Oracle Fusion Middleware Administering Oracle Identity Governance* for more information.

## 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:

- Development Environment  
Perform the upgrade procedure by using the wizard mode.
- Staging or Production Environment  
Perform the upgrade procedure by using the silent mode. In the silent mode, use the silent.xml file that is exported from the development environment.

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

## 7.3 Postupgrade Steps

Postupgrade steps involve uploading new connector jars, configuring the upgraded IT resource of the source connector, deploying the Connector Server, and configuring the latest token value of the scheduled job.

The following sections describe the procedures that you must perform after the upgrade operation:

- [Performing Postupgrade Steps](#)
- [Determining Values For the FromVersion and ToVersion Attributes](#)
- [Verifying If the Correct Process Form is Associated With the Resource Object](#)

## 7.3.1 Performing Postupgrade Steps

Postupgrade steps involves performing the following procedure to conclude the upgrade operation:

1. Perform the postupgrade procedure documented in *Managing Connector Lifecycle of Oracle Fusion Middleware Administering Oracle Identity Governance*.
2. If you are using Oracle Identity Governance release 11.1.2.x or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
  - a. Log in to Oracle Identity System Administration.
  - b. Create and activate a sandbox. See [Creating and Activating a Sandbox](#) for more information.
  - c. Create a new UI form to view the upgraded fields. See [Creating a New UI Form](#) for more information about creating a UI form.
  - 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. See [Publishing a Sandbox](#) for more information.
3. If you are using Oracle Identity Governance release 11.1.2.x or later and you are upgrading from release 11.1.1.5.0 to 11.1.1.6.0, then perform the following procedure to remove the auxiliary class child form (from the AD User form) that is retained after upgrade:
  - a. Create a new version of the upgraded **AD User** form.
  - b. Delete the **UD\_ADUSRCLS** child form, and make the version active.
  - c. Run the FVC utility using this newly created form. See Step 4 for detailed information on running FVC utility.
4. Run the Form Version Control (FVC) utility to manage user data changes on a form after an upgrade operation. To do so:
  - a. In a text editor, open the fvc.properties file located in the *OIM\_DC\_HOME* directory and include the following entries:

```
ResourceObject;AD User
FormName;UD_ADUSER
FromVersion;SPECIFY_THE_VERSION_OF_THE_FORM_USED_BY_USER_ACCOUNTS_CREATED_BY_US
ING_THE_SOURCE_CONNECTOR
ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UP
GRADE
ParentParent;UD_ADUSER_AD;UD_ADUSER_SERVER
```



 **Note:**

To determine values for the FromVersion and ToVersion attributes, see [Determining Values For the FromVersion and ToVersion Attributes](#).

To verify whether you are specifying the correct process form associated with the resource object, perform the procedure described in [Verifying If the Correct Process Form is Associated With the Resource Object](#).

- b. Run the FVC utility. This utility is copied into the following directory when you install the design console:

**For Microsoft Windows:**

*OIM\_DC\_HOME*/fvcutil.bat

**For UNIX:**

*OIM\_DC\_HOME*/fvcutil.sh

When you run this utility, you are prompted to enter the login credentials of the Oracle Identity Governance administrator, and the logger level and log file location.

5. To manage AD Group form changes after an upgrade operation, run the FVC utility by performing the instructions in step [4.a](#) and [4.b](#) with the following difference:

While perform Step [4.a](#), replace the entry added in Step [4.a](#) with the following:

```
ResourceObject;AD Group
FormName;UD_ADGRP
FromVersion;SPECIFY_THE_VERSION_OF_THE_FORM_USED_BY_USER_ACCOUNTS_CREATED_BY_USING_THE_SOURCE_CONNECTOR
ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UPGRADE
ParentParent;UD_ADGRP_ADSERVER;UD_ADGRP_SERVER
```

6. To manage AD Organization Unit form changes after an upgrade operation, run the FVC utility by performing the instructions in step [4.a](#) and [4.b](#) with the following difference:

While perform Step [4.a](#), replace the entry added in Step [4.a](#) with the following:

```
ResourceObject;AD Organizational Unit
FormName;UD_OU
FromVersion;SPECIFY_THE_VERSION_OF_THE_FORM_USED_BY_USER_ACCOUNTS_CREATED_BY_USING_THE_SOURCE_CONNECTOR
ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UPGRADE
ParentParent;UD_OU_AD;UD_OU_SERVER
```

7. If you are upgrading the connector from release 11.1.1.5.0 to 11.1.1.6.0, then run the PostUpgradeScript.sql script as follows:

 **Note:**

- Skip performing this step if you upgrading the connector directly from release 9.1.x to 11.1.1.6.0.
- If you first performed an upgrade from release 9.1.x to 11.1.1.5.0, and then are upgrading from release 11.1.1.5.0 to 11.1.1.6.0, then in the PostUpgradeScript.sql file, replace "ADOU" with "OU", and then run the script.

- a. Connect to the Oracle Identity Governance database by using the OIM User credentials.
  - b. Run the PostUpgradeScript.sql located in the ConnectorDefaultDir/AD\_PACKAGE/upgrade directory.
8. Deploy the Connector Server.
  9. Re-configure the IT resource of the source connector (an earlier release of the connector that must be upgraded).

10. Configure the latest token value of the scheduled job as follows:

The following scheduled jobs contain the Latest Token attribute:

Active Directory User Target Recon

Active Directory User Trusted Recon

Active Directory Group Recon

Active Directory Organization Recon

After upgrading the connector, you can perform either full reconciliation or incremental reconciliation. To perform incremental reconciliation, specify the value of the highestCommittedUSN attribute (noted in [Preupgrade Steps](#)) as the value of the Latest Token attribute. This ensures that records created or modified since the last reconciliation run (the one that you performed in [Preupgrade Steps](#)) are fetched into Oracle Identity Governance. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token attribute.

See [Performing Full Reconciliation and Incremental Reconciliation](#) for more information about performing full or incremental reconciliation.

11. Configure the sync token value of the scheduled job as follows:

The following scheduled jobs contain the Sync Token attribute:

Active Directory User Target Delete Recon

Active Directory User Trusted Delete Recon

Active Directory Group Delete Recon

After upgrading the connector, you can perform either full delete reconciliation or incremental delete reconciliation. To perform full delete reconciliation, you must not specify any value for the Sync Token attribute of the scheduled job. To perform incremental delete reconciliation, you must specify the value of the Sync Token attribute in the following format:

```
<String>0|{uSNChanged}|{True/False}|{DOMAIN_CONTROLLER}</String>
```

In this format, replace:

- {uSNChanged} with the value of the highestCommittedUSN attribute noted in [Preupgrade Steps](#).
- {True/False} with one of the following values:
  - True if the Global Catalog Server is used during delete reconciliation runs
  - False if the Global Catalog Server is not used during delete reconciliation runs
- {DOMAIN\_CONTROLLER} with the name of the domain controller on which you located RootDSE while performing the procedure described in [Preupgrade Steps](#).

## 7.3.2 Determining Values For the FromVersion and ToVersion Attributes

To determine values for the FromVersion and ToVersion attributes:

1. Log in to the Design Console.
2. Expand **Development Tools** and then double-click **Form Designer**.
3. Search for and open the form whose version you are trying to determine. For example, **UD\_ADUSER**.
4. In the Version Information region, search for and note down the value of the Active Version field, for example, *initial version*. This is the value of the ToVersion attribute.
5. In the Operations region, click the Current Version list, and note down the second highest value in the list, for example **Immediate Version**. This is the value of the FromVersion attribute.

## 7.3.3 Verifying If the Correct Process Form is Associated With the Resource Object

In the fvc.properties file, you might want to specify the process form name too. To verify whether you are specifying the correct process form associated with the resource object:

1. Log in to the Design Console.
2. Expand **Process Management** and then double-click **Process Definition**.
3. Search for and open the process form associated with the resource object.
4. In the Form Assignment region, note down the value of the Table Name field. This value is name of the process form that is linked to the process definition and resource object.

# 8

## Troubleshooting the Microsoft Active Directory User Management Connector

These are the solutions to problems you might encounter while using the Microsoft Active Directory User Management connector.

 **Note:**

From release 12.2.1.3.0 onward, the IT Resource of CI-based mode is mapped to Basic Configuration of AOB. Similarly, the main configuration lookup definition of CI-based mode is mapped to Advanced Settings of AOB. All solutions described in this chapter are applicable to Users, Groups, and Organizational Units and been documented using the AOB terminology. Therefore, if you are referring to this table for solutions to any User operations, then consider the AOB terminology. If you are referring to this table for solutions to any Groups or Organizational Units operations, then replace the AOB terminology with the terminology for CI-based mode.

**Table 8-1 Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
The following error is encountered: <code>java.net.UnknownHostException:</code>	Ensure that the host name in the IT resource for the Connector Server is specified correctly.
The following error is encountered: <code>InvalidCredentialException:</code> <code>Remote framework key is</code> <code>invalid</code>	Ensure that the value of the Key parameter of the IT resource for the Connector Server is specified correctly.
The following error is encountered: <code>ConnectorException:</code> <code>java.net.ConnectException:</code> <code>Connection refused</code>	Ensure that the port number in the IT resource for the Connector Server is specified correctly.

**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
<p>The following error is encountered in the reconciliation job:</p> <pre>org.identityconnectors.framework.common.exceptions.ConnectorException: The server does not support the requested critical extension.</pre>	<p>The following are the possible reasons for the occurrence of this error:</p> <ul style="list-style-type: none"> <li>If the connector is configured for Microsoft AD LDS, then none of the reconciliation job parameters mention the parameter that is not present in the Microsoft AD LDS User Schema. For example, the sAMAccountName attribute is not a valid attribute on Microsoft AD LDS. Therefore, ensure that attributes that are not present on Microsoft AD LDS are not specified as values of reconciliation job parameters such as Sort By.</li> <li>The number of records that the connector must fetch are large in number. To fix this issue, remove the values specified for the Batch Size, Number of Batches, Batch Start, Sort Direction, and Sort By parameters of the reconciliation jobs. You can always use the Page Size parameter of the Advanced Settings section for granular-level setting. The connector uses the ICF Handler for sending data to Oracle Identity Governance, and the ICF and ICFINTG layers take care of processing the data and generating the reconciliation event.</li> <li>A multivalued field on the target system is mapped to a single-valued field on the AD User form in Oracle Identity Governance. To avoid encountering this issue, ensure that multivalued fields on the target system are mapped to the corresponding multivalued field on the AD User form.</li> </ul>
<p>While starting the Connector Server, the following exception is encountered:</p> <pre>Unhandled Exception: System.Net.Sockets.SocketException: Only one usage of each socket address (protocol/network address/port) is normally permitted</pre>	<p>This exception is encountered because the Connector Server uses a port that has already been used (mostly by another instance of the Connector Server). You can fix this issue by performing one of the following steps:</p> <ul style="list-style-type: none"> <li>If the Connector Server service is running, then stop it.</li> <li>Search for and open the ConnectorServer.exe.Config file, change the port value to 8758 or 8755, and then start the Connector Server. The default location of the ConnectorServer.exe.Config file is C:\Program Files\Identity Connectors\Connector Server.</li> </ul>
<p>The following error is encountered while running the Active Directory Target Reconciliation scheduled job:</p> <pre>ADP ClassLoader failed to load: Script1 java.lang.ClassNotFoundException: ADP ClassLoader failed to load: Script1</pre>	<p>Ensure that the value for the Filter syntax attribute of the scheduled job is specified correctly. See <a href="#">Performing Limited Reconciliation By Using Filters</a> for more information.</p>

**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
<p>All reconciliation runs are successful, but the following error is encountered while running provisioning operations:</p> <pre>Neither able to connect to Primary Domain Controller nor to any of Back up Domain Controllers.</pre>	<p>Ensure that the value of the LDAPHostName parameter of the IT resource is specified correctly.</p> <p>To determine the host name, on the computer hosting the target system, right-click <b>My Computer</b> and select <b>Properties</b>. On the Computer Name tab of the System Properties dialog box, the host name is specified as the value of the Full computer name field.</p>
<p>The Connector Server throws an Out of Memory exception.</p>	<p>A memory leak issue occurs in Microsoft .NET Framework 3.5. To fix this issue, you must apply the hotfix (listed in the following Web site) on the computer hosting the Connector Server:</p> <p><a href="http://support.microsoft.com/kb/981575">http://support.microsoft.com/kb/981575</a></p>
<p>Unable to start the Connector Server after extracting the contents of the connector bundle into the <code>CONNECTOR_SERVER_HOME</code> directory. The following exception is encountered:</p> <pre>ConnectorServer.exe Information: 0 : Starting connector server: C:\Program Files\Identity Connectors\Connector Server ConnectorServer.exe Error: 0 : Exception occurred starting connector server System.IO.FileNotFoundException: Could not load file or assembly 'System.Core, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e 089' or one of its dependencies. The system cannot find the file specified. File name: 'System.Core, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e 089' at Org.IdentityConnectors.Commo n.CollectionUtil.NewSet[T,U] (IEnumerable`1 collection)</pre> <p><b>Note:</b> This error is encountered only if you use the command prompt to start the Connector Server. If you use <code>services.msc</code> to start the Connector Server, then the Connector Server stops soon after it started.</p>	<p>This exception is encountered if the Microsoft .NET Framework is not present. You must install .NET Framework 3.5 or later on the computer that is hosting the Connector Server.</p> <p><b>Note:</b> If you are installing .NET Framework 3.5, then ensure you install the following patch to avoid the memory leak issue:</p> <p><a href="http://support.microsoft.com/kb/981575">http://support.microsoft.com/kb/981575</a></p>

**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
<p>All connector operations such as reconciliation and provisioning operations fail and the following error is encountered:</p> <pre>oracle.iam.connectors.icfcommon.exceptions.IntegrationException: ConnectorKey( bundleName=ActiveDirectory.Connector bundleVersion=1.1.0.6380 connectorName=Org.IdentityConnectors.ActiveDirectory.ActiveDirectoryConnector) not found</pre> <p>In addition, the same error message is written to the Connector Server log file.</p>	<p>The following are the possible reasons for the occurrence of this error:</p> <ul style="list-style-type: none"> <li>The connector bundle is not extracted in the <i>CONNECTOR_SERVER_HOME</i> directory.</li> <li>The Connector Server is started before you extract the contents of the connector bundle.</li> <li>Cache-related issue in Oracle Identity Governance.</li> </ul> <p>Perform the following steps to fix this issue:</p> <ol style="list-style-type: none"> <li>Stop the Connector Server.</li> <li>Extract the contents of the connector bundle into the <i>CONNECTOR_SERVER_HOME</i> directory.</li> <li>Start the Connector Server.</li> <li>Run the PurgeCache utility on the computer hosting Oracle Identity Governance.</li> <li>Restart Oracle Identity Governance.</li> </ol>
<p>The following error is encountered while performing any connector operation:</p> <pre>A local error has occurred</pre>	<p>This error is encountered if you specify a value for the DirectoryAdminName IT resource parameter in an incorrect format. You must use only the following format to specify a value for this parameter:</p> <pre>DOMAIN_NAME\USER_NAME</pre> <p>See the "Admin User Name" row of <a href="#">Table 3-1</a> for more information.</p>
<p>The computer hosting the Connector Server and target system is unavailable. Nothing works despite specifying a value for the Backup Host Names parameter of the Basic Configuration section.</p>	<p>The computer hosting the Connector Server must be up and running always. Instead of deploying the Connector Server on PDC and BDC hosts, follow the following guidelines to avoid this error:</p> <ul style="list-style-type: none"> <li>Have a dedicated computer for the Connector Server. Note that you can specify a value for the Backup Host Names parameter of the Basic Configuration section even if the Connector Server is running on a dedicated computer.</li> <li>The computer hosting the Connector Server must be in the same domain as the target system.</li> <li>Deploy the Connector Server and configure the Active Directory Connector Server IT resource. For more information about the IT resource, see <a href="#">Configuring the IT Resource for the Connector Server</a>.</li> </ul>
<p>A target resource reconciliation run fails with the following error:</p> <pre>Row index out of bounds</pre> <p>However, users are brought into Oracle Identity Governance and are linked successfully.</p>	<p>This issue is encountered when a scheduled job updates the usNChanged attribute of the target system. As a work around, create a new scheduled job and perform a reconciliation run.</p>

**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
<p>The following error is encountered in the Connector Server log file:</p> <pre>org.identityconnectors.framework.common.exceptions.ConnectorException: java.net.ConnectException: Connection timed out</pre>	<p>The following are two of the possible reasons for the occurrence of this error:</p> <ul style="list-style-type: none"> <li>• The connection between the Connector Server and Oracle Identity Governance times out. To fix this issue, either set the value of the Timeout parameter of the Connector Server IT resource to 0, or increase its existing value.</li> <li>• The Connector Server port is blocked by the firewall. To fix this issue, by using the Telnet protocol, check whether the Connector Server is listening at the default port (8795). If the port is not open, then you can either open the port or choose another port for Connector Server. To change the port name, edit the ConnectorServer.exe.Config file by specifying a new port as mentioned in the following line and the restart the Connector Server: <pre>&lt;add key ="connectorserver.port" value="8759"/&gt;</pre></li> </ul>
<p>Lookup field synchronization for groups and organizations, and reconciliation of groups run successfully. However, the following error is encountered when you perform reconciliation of organizations (in other words, run the Active Directory Organization Recon scheduled job):</p> <pre>oracle.iam.reconciliation.exception.InvalidDataFormatException: Required column name RECON_ORGNAME4EAE4287 and value does not exist</pre> <p>In addition, the following error is written to the log file of Oracle Identity Governance:</p> <pre>Required column name RECON_ORGNAME&lt;.....&gt; and value does not exist</pre>	<p>This error is encountered if value of the Configuration Lookup parameter of the Active Directory IT resource is set to <code>Lookup.Configuration.ActiveDirectory</code>.</p> <p>To avoid this error, if you are performing organization reconciliation with the Xellerate User resource object, then ensure to set the value of the Configuration Lookup parameter of the Active Directory IT resource to <code>Lookup.Configuration.ActiveDirectory.Trusted</code>.</p>



**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
<p>While running the scheduled jobs for lookup field synchronization (groups and organizations), the following exception is encountered:</p> <pre>Unable to get the Directory Entry</pre> <p>In addition, the following error is written to the Connector Server log file:</p> <pre>Org.IdentityConnectors.Framework.Common.Exceptions.ConnectorException: Unable to get the Directory Entry</pre>	<p>You can perform one of the following steps to determine the cause for this error:</p> <ul style="list-style-type: none"> <li>• Check for the error message in the log files of the Connector Server to find out the root cause.</li> <li>• Check the Event Viewer. To open the Event Viewer, from the Start menu, select <b>Control Panel</b>, double-click <b>Administrative Tools</b>, and then double-click <b>Event Viewer</b>.</li> </ul> <p>The following are few of the possible reasons for the occurrence of this error:</p> <ul style="list-style-type: none"> <li>• An incorrect value is specified for the DomainName IT resource parameter. To fix this issue, specify a correct value for the DomainName IT resource parameter. Note that you must use only the following format to specify a value for this parameter: <i>DOMAIN_NAME\USER_NAME</i></li> <li>• The computer hosting the Connector Server is not present in the AD domain. To fix this issue, ensure that the Connector Server is installed on a computer that is a part of the same AD domain.</li> </ul>
<p>The following error is encountered in the log file of Oracle Identity Governance while running reconciliation jobs:</p> <pre>java.net.SocketException: Connection reset</pre>	<p>The following are two of the possible reasons for the occurrence of this error:</p> <ul style="list-style-type: none"> <li>• LDAPS is not enabled on the domain controllers. To fix this issue, enable LDAPS as described in <a href="#">Configuring SSL Between Connector Server and Microsoft Active Directory</a>.</li> <li>• Oracle Identity Governance is not set for SSL. In other words, the UseSSL parameter of the Basic Configuration section and Connector Server IT resource is set to <code>no</code> and <code>false</code>, respectively). However, the Connector Server is SSL enabled. To fix this issue, ensure to set the value of the UseSSL parameter of the Basic Configuration section and Connector Server IT resource to <code>yes</code> and <code>true</code>, respectively.</li> </ul>

**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
<p>Any connector operation (reconciliation or provisioning) fails and the following exception is encountered:</p> <p>Domain Controller not found in the domain 'SAMPLEDOMAIN.com'</p> <p>In addition, the following error is written to the Connector Server log file:</p> <pre>org.identityconnectors.framework.common.exceptions.ConnectorException: Domain controller not found in the domain</pre>	<p>The following are two of the possible reasons for the occurrence of this error:</p> <ul style="list-style-type: none"> <li>An incorrect value is specified for the DomainName IT resource parameter. To fix this issue, specify a correct value for the DomainName IT resource parameter. Note that you must use only the following format to specify a value for this parameter: <i>DOMAIN_NAME\USER_NAME</i></li> <li>The computer hosting the Connector Server is not present in the AD domain. To fix this issue, ensure that the Connector Server is installed on a computer that is a part of the same AD domain.</li> </ul>
<p>The following error is encountered in the Connector Server log file:</p> <pre>org.identityconnectors.framework.common.exceptions.ConnectorException: Neither able to connect to Primary Domain Controller nor to any of Back up Domain Controllers.</pre>	<p>This error is encountered if an incorrect value is specified for the LDAP Host Name parameter of the Basic Configuration section.</p> <p>To fix this issue, you must specify a correct value for the LDAP Host Name basic configuration parameter. To determine the correct value for this parameter, on the computer hosting the target system, right-click <b>My Computer</b> and select <b>Properties</b>. On the Computer Name tab of the System Properties dialog box, the host name is specified as the value of the Full computer name field.</p>
<p>The following error is encountered in the Connector Server log file:</p> <pre>System.IO.IOException: The handshake failed due to an unexpected packet format</pre>	<p>This error is encountered if Oracle Identity Governance is not set for SSL. In other words, the UseSSL parameter in the IT resources of the target system and Connector is set to <i>no</i> and <i>false</i>, respectively). However, the Connector Server is SSL enabled.</p> <p>To fix this issue, ensure to set the value of the UseSSL parameter in the IT resources of the target system and Connector Server to <i>yes</i> and <i>true</i>, respectively.</p>
<p>The following error is encountered in the Connector Server log file:</p> <pre>System.DirectoryServices.ActiveDirectory.DomainController.FindOneWithCredentialValidation(DirectoryContext context, String siteName, LocatorOptions flag) (in connector server logs)</pre>	<p>This error is encountered if no value has been specified for the Domain Controller parameter of the Basic Configuration section.</p> <p>To fix this issue, specify a value for the Domain Controller basic configuration parameter. For more information about this parameter, see <a href="#">Basic Configuration Parameters</a>.</p>

**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
The Active Directory User Target Reconciliation scheduled job for bulk users does not fetch all users from the target system.	<p>This issue is encountered if the reconciliation matching rule has changed.</p> <p>To fix this issue, create a reconciliation profile with the updated matching rule as follows:</p> <ol style="list-style-type: none"> <li>1. Log in to the Design Console.</li> <li>2. Expand <b>Resource Management</b> and then double-click <b>Resource Objects</b>.</li> <li>3. Search for and open the <b>AD User</b> resource object.</li> <li>4. On the Object Reconciliation tab, click <b>Create Reconciliation Profile</b> to generate the reconciliation profile will all the latest updates.</li> </ol>
No records are reconciled when the following filter is applied: <code>contains('memberOf', 'PGMGroup')</code>	This issue is encountered because "memberOf" is a multivalued attribute in the target system. For applying filters on multivalued attributes, use the "containsAllValues" filter.
The Group Display in the AD User child form is takes a long time to display all Groups. Therefore, adding the AD Group to AD User takes a significant amount of time.	To reduce the delay is displaying the groups page, enable caching in Oracle Identity Governance.
The following error is encountered in the Connector Server log file: <code>System.NotSupportedException : The server mode SSL must use a certificate with the associated private key.</code>	This issue is encountered if you have exported the certificate with a private key (for example, .pfx file, while performing the instructions in <a href="#">Exporting the Certificate</a> , but do not import it into the certificate store named 'sslstore' by using the MMC console. To avoid this issue, ensure to import the certificate into 'sslstore' by using the MMC console, if you have exported it with a private key (.pfx file).
A provisioning operation (either create or update) fails and the following error is written to the Connector Server log file: <code>The specified directory service attribute or value does not exist.</code>	<p>This issue is encountered if the schema definition for your application contains an incorrect value in the Target Attribute column. Note that the Target Attribute column values in the schema definition are target system attribute names.</p> <p>To fix this issue, scrutinize the values on the schema definition and then update the value in the Target Attribute column with the correct target system attribute name.</p>
During a bulk provisioning operation, the following error might be encountered in the Connector Server log file: <code>Max objects exceeded</code>	To fix this issue, increase the values of the Pool Max Size and Pool Max Wait parameters of the Advanced Settings section. For more information about these parameters, see <a href="#">Advanced Settings Parameters</a> .

**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
<p>OIG Users are not created after running the Active Directory User Trusted Recon scheduled job. The following message is displayed In the reconciliation event generated for the user:</p> <pre>'Data Validation Failed' as the current status and 'Invalid ManagerLogin : &lt;Manager ID&gt;' as Note.</pre>	<p>This issue is encountered due to the dependency of manager information of users. OIG User creation fails if the manager of the user is not already present in Oracle Identity Governance. To fix this issue, you must remove the manager field mapping, run the Active Directory User Trusted Recon scheduled job, and then add back the manager field mapping as follows:</p> <p>In Identity Self Service, remove the Manager field mapping as follows:</p> <ol style="list-style-type: none"> <li>1. Log in to Identity Self Service.</li> <li>2. Search for and open the Authoritative application corresponding to your target system for editing.</li> <li>3. From the Schema page, delete the row corresponding to the <b>Manager Login</b> display name.</li> <li>4. Apply the changes.</li> </ol> <p>Run the Active Directory User Trusted Recon scheduled job.</p> <p>In Identity Self Service, add the manager field mapping as follows:</p> <ol style="list-style-type: none"> <li>1. Log in to Identity Self Service.</li> <li>2. Search for and open the Authoritative application corresponding to your target system for editing.</li> <li>3. From the Schema page, add a new row by specifying <code>Manager Login</code> as the Display Name and <code>Manager ID</code> as the Target Attribute. For more information about schema attribute mappings, see <a href="#">Attribute Mappings for an Authoritative Application</a>.</li> <li>4. Apply the changes.</li> </ol> <p>Clear the value in the latest token parameter of the Active Directory User Trusted Recon scheduled job and run it.</p>

**Table 8-1 (Cont.) Troubleshooting for the Microsoft Active Directory User Management Connector**

Problem	Solution
<p>The following error is encountered in the log file of the Connector Server during a provisioning operation:</p> <pre>The remote procedure call failed and did not execute. (Exception from HRESULT: 0x800706BF)</pre>	<p>This issue is encountered when there are too many requests at the same time during a Create User or Password Update provisioning operation.</p> <p>For example, this issue can be encountered during an access policy-based provisioning operation where too many account creations are triggered.</p> <p>This error can occur on Microsoft Windows 2008, 2008 R2 or Windows 2012 domain controllers, which includes service packs as well.</p> <p>To fix this issue, you must contact Microsoft Support to apply the hotfix listed in the 2781049 article (DsAddSidHistory function fails when it is called by multiple threads in Windows Server 2008 R2 SP1) on the following Web site:</p> <p><a href="http://support.microsoft.com/">http://support.microsoft.com/</a></p> <p>You can do so by accessing the preceding URL and then searching for the 2781049 article.</p> <p><b>Note:</b> Do <i>not</i> apply the hotfix without contacting Microsoft Support.</p>
<p>The following error is encountered in the Active Directory API which is not meaningful:</p> <pre>Encountered DirectoryServicesCOMException: A device attached to the system is not functioning.</pre>	<p>This error is encountered when the sAMAccount attribute in the target system (corresponding to the User Login field in Oracle Identity Governance) contains more than 20 characters.</p> <p>If you encounter this error for User objects, then the workaround is to write a Groovy-based code (see <a href="#">About Configuring Transformation and Validation of Data</a>) on the User ID field during provisioning to check if it contains more than 20 characters or not and log an appropriate error log message.</p> <p>If you encounter this error for Groups or Organizational Unit Objects, then the workaround is to write a validation Java code (see <a href="#">Configuring Validation of Data During Reconciliation and Provisioning for Groups and Organizational Units</a>) on the corresponding field during provisioning to check if it contains more than 20 characters or not and log an appropriate error log message.</p>

# 9

## Frequently Asked Questions

Find answers to frequently asked questions related to the functionality of the Microsoft Active Directory User Management connector.

**1. What is the recommended system configuration for the computer installing and running the Connector Server?**

The computer on which you want to install and run the Connector Server must meet the following requirements:

- Intel Pentium Dual Core 2 GHz with 8 GB RAM.
- Microsoft Windows Server 2008 (both 32-bit or 64-bit), or Microsoft Windows Server 2012, 2016 or 2019 (64-bit).

**2. Where should I install the Connector Server for the Active Directory User Management connector?**

Install the Connector Server on a computer that belongs to target system domain.

**3. If the target system contains more than one domain, then should the Connector Server be installed on each domain?**

In a parent-child domain environment, a single Connector Server installed on the parent domain computer is sufficient. In addition, in a forest with disconnected domains, a single Connector Server is required for all the domains.

**4. Can Active Directory User Management connector release 9.1.x coexist with Active Directory User Management connector release 12.2.x?**

Yes. Two versions of the same connector can coexist. This can be achieved by cloning the Active Directory User Management 12.2.x connector XML and using it for installing the connector with the new name.

**5. How to establish a connection between Active Directory User Management connector release 12.2.1.3.0 and an AD LDS instance?**

The following is the procedure to establish a connection between Active Directory User Management connector release 12.2.1.3.0 and an AD LDS instance:

- a. Set the value of the `IsADLDS?` parameter of the Basic Configuration section to `yes`.
- b. Specify a value for the `Port` parameter of the Basic Configuration section.
- c. In the `Lookup.ActiveDirectory.GM.Configuration` lookup definition, search for and replace the `Lookup.ActiveDirectory.GM.ProvAttrMap` and `Lookup.ActiveDirectory.GM.ReconAttrMap` decode values with `Lookup.ActiveDirectoryLDS.GM.ProvAttrMap` and `Lookup.ActiveDirectoryLDS.GM.ReconAttrMap`, respectively.

**6. What are the steps to ensure that the service account credentials are valid?**

To ensure that the service account credentials are valid, test the connection to the target system by using an LDAP browser. After the connection is tested, provide the details in the Basic Configuration section. While providing values for parameters in the Basic Configuration section, ensure that you use the following format to specify a value for the `Domain Name` parameter:

`DOMAIN_NAME\USER_NAME`

**7. Can the Active Directory User Management connector be used to move a user from one OU to another?**

Yes. You can use the Active Directory User Management connector to move a user from one OU to another if both the OUs are in the same forest. In other words, you can use the connector to move a user from one OU to another if the OU to which the user is to be moved to is present in the organization lookup that is populated after organization lookup field synchronization.

**8. If I customize the connector, should I modify the values in the Target Attribute column (for example, OIM Employee Type, OIM User Type, and \_\_UID\_\_, and \_PARENTCN\_\_) of the Schema page for an Authoritative application?**

No. The Target Attribute column on the Schema page for an Authoritative application lists the attributes of the target system. Some of the target system attributes like OIM Employee Type, Manager Id, \_\_UID\_\_, \_\_PARENTCN\_\_, \_\_ENABLE\_\_, and OIM User Type are handled specially. Therefore, do not modify the Target Attribute column values. The following is a description of some of the attributes in the Target Attribute column:

- OIM Employee Type: The value of this attribute is the same as the value of the OIM Employee Type attribute of the Active Directory User Trusted Recon scheduled job.
- OIM User Type: The value of this attribute is the same as the value of the OIM User Type attribute of the Active Directory User Trusted Recon scheduled job.
- Manager Id: Oracle Identity Governance handles the Manager Id attribute differently. It is not the same as the manager attribute on the target system. The Manager Id attribute contains the sAMAccountName of the user's manager and *not* the manager DN.
- \_\_UID\_\_: This attribute retrieves the UID of the user.
- \_\_PARENTCN\_\_: This attribute retrieves the container of the user. This attribute is used if you want to maintain in Oracle Identity Governance the same organization hierarchy that is maintained on the target system.
- \_\_ENABLE\_\_: This attribute specifies whether the user in the target system is enabled.

**9. Why cannot I see the log files corresponding to the connector operations in the computer hosting Oracle Identity Governance?**

The Active Directory User Management connector uses the built-in logging mechanism of the .NET framework. Therefore, all connector logs are generated on the computer hosting the Connector Server. See [Enabling Logging for Microsoft Active Directory User Management Connector](#) for more information.

**10. All connector operations are performed by using the ICFINTG layer. What is the logger name used for enabling logging for ICFINTG?**

The logger name used for enabling logging for ICFINTG is ORACLE.IAM.CONNECTORS.ICFCOMMON. Note that the logger name is case sensitive.

**11. I performed trusted source and target resource reconciliation runs by specifying a value for the Filter attribute of the scheduled job. The logs of the Connector Server display information that the connector is returning the objects. However, I neither see any user records reconciled into Oracle**

**Identity Governance nor any logs on Oracle Identity Governance. What is wrong here?**

When you perform a reconciliation run by specifying a value for the Filter attribute (in other words, when you perform limited reconciliation), the connector converts the filter syntax to the LDAP filter syntax, and then searches for records that match the filter criteria. Note that the search at this point is a case-insensitive search.

The connector returns the records retrieved by the search to ICF. Before passing on these records to the reconciliation engine in Oracle Identity Governance, ICF applies the same filter criteria on the records returned by the connector. However, at this point, ICF performs a case-sensitive search. Therefore, it is possible that records are dropped by ICF and are never returned to the reconciliation engine.

The following example explains this use case:

Suppose there exist records on the target with last names (sn) "Doe" and "Doel". During reconciliation, if you specify `startsWith('sn', 'do')` as the value of the Filter attribute, then the connector searches for and returns to ICF all records whose Last Name starts with "do" (in this example, the connector returns records with last names Doe and Doel). Before passing on the records returned by the connector to the reconciliation engine in Oracle Identity Governance, ICF applies the same filter on the search records. However, no reconciliation event is generated as ICF performs a case-sensitive search and drops the two records.

**12. Is Remote Manager required for provisioning and reconciling Terminal Service attributes by using this release of the Active Directory User Management Connector?**

No. From the 11.1.1.x version of this connector, you must deploy the .NET Connector Server on any computer in the Active Directory domain. It is not mandatory to deploy the Connector Server on the domain controller or computer hosting the target system. Apart from this, there are no prerequisites for provisioning and reconciling Terminal Services attributes. In other words, you do not need Remote Manager or another Connector Server on the domain controller. Provisioning and reconciliation of Terminal Service attributes is the same as provisioning or reconciling any other attribute.

**13. Is SSL mandatory for setting passwords for users in the target system? Can I set password for a user if I set the value of the UseSSL parameter of the Basic Configuration section to no?**

SSL is not mandatory for setting user passwords. You can set password for a user even if you set the value of the UseSSL basic configuration parameter to `no`.

If you set the value of the UseSSL parameter to `yes`, then the channel between the Connector Server and target system is encrypted. In addition, secure communication is set up by using certificates.

If you set the value of the UseSSL parameter to `no`, then the channel between the Connector Server and target system is encrypted by using the ADSI "Secure" mode for communication.

For performing a password reset provisioning operation, the communication channel must be encrypted. If you are using Microsoft AD as the target system, then as discussed in the preceding paragraphs, the channel between the Connector Server and target system is encrypted. Therefore, you can perform password reset provisioning operations without configuring SSL.

If you are using Microsoft AD LDS as the target system, then the default communication channel between the Connector Server and target system is not "secure". Therefore, it is



mandatory to configure SSL between the Connector Server and Microsoft AD LDS for the password reset functionality to work as expected.

**14. Can the Active Directory User Management connector version 12.2.1.3.0 manage windows local account?**

No.

**15. Where can I find the latest version of the Active Directory User Management Connector guide?**

You can find the latest version of the Active Directory User Management Connector guide and all other ICF connector guides at the following location:

<https://docs.oracle.com/middleware/oig-connectors-12213/docs.htm>

**16. After extracting the contents of the connector bundle into the `CONNECTOR_SERVER_HOME` directory, I observed some DLLs. Does it matter whether the computer hosting the Connector Server is 32-bit or 64-bit?**

No. You can use the same DLLs on both 32-bit and 64-bit computers.

**17. I want to add users to and remove from a certain Active Directory group for provisioning and de-provisioning events, but I do not want to assign any permissions for modifying the user objects. Can I install this connector and use only user to group management part with limited permission on only group objects to change members attribute? What are the minimum permissions required for this connector?**

Managing only user-group membership is possible by providing the credentials of the user who has been delegated the control (by using the Delegation of Control Wizard in the target system) for the following tasks, in the Basic Configuration section:

- Read all user information
- Create, delete and manage groups
- Modify the membership of a group

With these credentials, you can perform reconciliation, lookup and manage groups, but not create or update user attributes.

**18. Can the Active Directory User Management connector manage a forest containing a single parent domain with many child domains using only a single AOB application?**

Yes, it is possible with a single application instance by performing the following steps:

- Set the value of the Search Child Domains parameter to `Yes` in the of Advanced Settings section. See the "Search Child Domains" row in [Advanced Settings Parameters](#) for more information.
- Ensure to specify the user name of an account that has the 'Account Operators' role on all these sub domains as the value of the Admin User Name parameter of Basic Configuration.

**19. Should the Admin User Name parameter of the Basic Configuration section contain the distinguished name of the user?**

No. You must use only the following format to specify a value for this parameter:

`DOMAIN_NAME\USER_NAME`

See [Basic Configuration Parameters](#) for more information about the Admin User Name parameter of Basic Configuration.

**20. Any user deleted on the target system will be stored in the DeletedObjects container. Can I expect the same behavior if I use the Active Directory User Management connector?**

Yes.

**21. Can a single Connector Server be used to deploy the Active Directory User Management connector bundle and Exchange connector bundle?**

Yes. A single Connector Server can both the Active Directory User Management and Exchange connector bundles. While deploying the Exchange connector, ensure not to replace the existing `ActiveDirectory.Connector.dll` file on the Connector Server, if any patch was applied on the Active Directory User Management connector.

**22. What happens when the computer (specified as the value of the LDAP Host Name basic configuration parameter) becomes unavailable during automatic provisioning? How to configure the connector to be compatible with high availability (HA) target system environments?**

When the computer (specified as the value of the LDAP Host Name parameter of the Basic Configuration section) becomes unavailable, the connector performs in one of the following manners:

- If a value has been specified for the Backup Host Names parameter of the Basic Configuration section, then the connector tries to connect to any of the backup domain controllers mentioned in the Backup Host Names parameter. You can configure the connector to be compatible with HA target systems environments by specifying a value for the Backup Host Names parameter.
- If no value has been specified for the LDAP Host Name and Backup Host Names parameters, then the connector connects to any of the domain controllers available in the same domain. This is called serverless bind.

**23. What happens when the Connector Server specified in the Basic Configuration section becomes unavailable?**

If the Connector Server is not configured for HA and it becomes unavailable, then the "connection refused" error is encountered.

To configure the Connector Server for HA, see the "Configuring Connector Load Balancer" section in the *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Governance*.

**24. Will there be an issue if I specify a value for the Port parameter of the Basic Configuration section while using Microsoft Active Directory as a target system?**

No. This is because the connector first checks for the value of the `Is ADLDS?` parameter. If the value of the `Is ADLDS?` parameter is `yes`, then the connector uses the value of the Port parameter. However, Oracle recommends not to specify a value for Port parameter if you are using Microsoft Active Directory as the target system.

**25. Can I perform user provisioning operations without configuring SSL between Oracle Identity Governance and Microsoft Active Directory? In addition, is the presence of the SSL certificate of Microsoft Active Directory required in both Oracle Identity Governance and the connector to perform all provisioning operations including password changes?**

If you are using Microsoft Active Directory as the target system, then SSL is not mandatory. The Active Directory User Management connector uses ADSI secure mode

for all provisioning operations, including password change provisioning operations. Therefore, password change provisioning operations can be handled without configuring SSL between Oracle Identity Governance and Microsoft Active Directory. However, if you are using AD LDS as the target system, then SSL is mandatory to perform password change provisioning operations.

**26. Will changes in AD groups for a user be reconciled during incremental reconciliation?**

Yes. The Active Directory Group Membership Recon can reconcile group membership changes during incremental reconciliation.

**27. Explain the appropriate use of the Domain Controller and Global Catalog Server parameters of the Basic Configuration section.**

The Domain Controller and Global Catalog Server parameters of the Basic Configuration section are used only during reconciliation. If the connector must perform reconciliation against a domain controller, then the Domain Controller parameter is used.

If the connector must perform reconciliation against the global catalog server, then the Global Catalog Server parameter is used. The following are the steps to be performed for using these parameters:

- a. Set the value of the Search Child Domains parameter of the Advanced Settings section to *yes*.
- b. Enter the global catalog server host name as the value of the Global Catalog Server parameter of the Basic Configuration section.

See [Enabling Reconciliation and Provisioning Operations Across Multiple Domains](#) for more information.

**28. What are the minimum permissions to be assigned to a user to fetch deleted user records from the target system?**

By default the service account with the Account Operators role, does not have permission to read information from the Delete Objects container. See [Assigning Permissions to Perform Delete User Reconciliation Runs](#) for more information.

**29. Where do I find the log files for connector installation?**

You find the log files for connector installation, Oracle Identity Governance server log and diagnostic log, in the following location:

*DOMAIN\_HOME/servers/oim\_server1/logs*

**30. How to create users in a specific OU in the target system?**

You can create users in a specific OU in the target system, during provisioning, by selecting a value from the Organization Name lookup field on the AD User Form page.

**31. When a group or an OU is created in the target system, will their parent organization be displayed in Oracle Identity Governance?**

When a group or an OU is created in the target system, its parent organization is not displayed in Oracle Identity Governance. Parent organizations must be reconciled separately. However, the organization hierarchy will not be maintained. Parent organizations can be reconciled by running the Active Directory Organization Recon scheduled job.

**32. Will a new group or OU be created in Oracle Identity Governance if I rename a group or an OU in the target system?**

Yes.

**33. What certificate must be exported while configuring SSL between Oracle Identity Governance and the Connector Server?**

While configuring SSL between Oracle Identity Governance and the Connector Server, export the SSL certificate (.cer file) from the computer hosting the Connector Server machine and add it to a new certificate store on the same computer. Note that the new certificate store must contain only one certificate. After configuring the details of the new certificate store in the ConnectorServer.exe.Config file, copy the exported certificate to the machine on which Oracle Identity Governance is running. Add the certificate to Oracle Identity Governance JDK store and Oracle WebLogic keystore. See [Configuring SSL for Microsoft Active Directory and Microsoft AD LDS](#) for more information.

**34. Is it correct that all traffic from Oracle Identity Governance to the target system passes through the Connector Server and there is no need to open firewall ports for direct access anymore?**

Yes, this is correct.

**35. What protocol is used for communication between Oracle Identity Governance and the target system?**

TCP protocol is used for communication between Oracle Identity Governance and the target system.

**36. Connector Architecture states the default communication between the .NET Connector Server and target system is "secure." How is this achieved?**

This connector uses the ADSI API that provides an option for specifying the type of authentication to use. See the following Microsoft Developer Network page for more information:

<http://msdn.microsoft.com/en-us/library/system.directoryservices.directoryentry.authenticationtype%28v=vs.90%29.aspx>

If you set the value of the UseSSL parameter of the Basic Configuration section to `no`, then secure authentication as discussed in the following page:

<http://msdn.microsoft.com/en-us/library/system.directoryservices.authenticationtypes%28v=vs.90%29.aspx>

# A

## Character Lengths of Target System Fields and Process Form Fields

This appendix provides information about the list of fields with different lengths on the target system and process form. In addition, it describes the procedure to change the process form field length.

This appendix includes the following topics:

- [Fields with Different Lengths on the Target System and Process Form](#)
- [Changing Process Form Field Lengths](#)

### A.1 Fields with Different Lengths on the Target System and Process Form

These are the fields whose lengths are different on the target system and on the process form.

**Table A-1 Fields with Different Lengths on the Target System and the Process Form**

Process Form Field and Field Length	Microsoft Active Directory Field and Field Length	Microsoft ADAM Field and Field Length
Department, 40	department, 64	department, 64
Fax, 40	facsimileTelephoneNumber, 64	facsimileTelephoneNumber, 64
Home Phone, 40	homePhone, 64	homePhone, 64
IP Phone, 40	ipPhone, 64	ipPhone, 64
Manager Name, 255	manager, <i>Not Specified</i>	manager, <i>Not Specified</i>
Mobile, 50	mobile, 64	mobile, 64
Office, 80	physicalDeliveryOfficeName, 128	physicalDeliveryOfficeName, 128
Organization Name, 400	Distinguished name of the organization, <i>Not Specified</i>	Distinguished name of the organization, <i>Not Specified</i>
Pager, 40	pager, 64	pager, 64
Street, 200	StreetAddress, 1024	StreetAddress, 1024
Terminal Home Directory, 60	Part of the data stored in the userParameters field, 100	NA
Terminal Profile Path, 60	Part of the data stored in the userParameters field, 100	NA

## A.2 Changing Process Form Field Lengths

You can change the length of a process form field by manually editing the `ad-target-template.xml` file.

1. In a text editor, open the `ad-target-template.xml` file located in the `xml` directory of the connector installation package.
2. Search for the `<schemaAttributes>` element and look for an entry corresponding to the process form field you want to change, and then update the value of its `length` attribute. The following is a code snippet for an entry corresponding to the First Name process form field:

```
<schemaAttributes>
  <schemaAttributes name="givenName" dataType="String"
    displayName="First Name" length="64" fieldType="TextField"
    reconcileable="true" provisionable="true" />
```

3. Save and close the file.
4. Ensure that the connector bundle contains the updated `ad-target-template.xml` file
5. Log in to Identity Self Service and create the application for your target system.

 **Note:**

Each time you manually edit the `ad-target-template.xml` file, you need to re-create the application for your target system for the changes to reflect.

# B

## Files and Directories in the Microsoft Active Directory User Management Connector Installation Package

These are the components of the connector installation package that comprise the Microsoft Active Directory User Management connector.

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

File in the Installation Package Directory	Description
bundle/ActiveDirectory.Connector-12.3.0.0	This ZIP file contains the connector bundle.
configuration/ActiveDirectory-CI.xml	This XML file contains configuration information that is used during the connector installation process.
Files in the dataset directory ModifyResourceADUser.xml ProvisionResourceADUser.xml ModifyResourceADLDSUser.xml ProvisionResourceADLDSUser.xml	These XML files specify the information to be submitted by the requester during a request-based provisioning operation. You import these XML files into Oracle Identity Manager MDS by using the Oracle Identity Manager MDS Import utility.
<b>Note:</b> The dataset XML files are applicable only if you are using Oracle Identity Manager release 11.1.1.x.	
owglue/ActiveDirectoryConnector-idmglue-1.0.12.zip	This ZIP file contains the Oracle Waveset metadata for the Microsoft Active Directory User Management connector. <b>Note:</b> This ZIP file is <i>not</i> required for the Microsoft Active Directory User Management connector that is used with Oracle Identity Manager.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. After creation of an application by using the connector, these resource bundles are copied to the Oracle Identity Governance database. <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.
upgrade/PostUpgradeScript.sql	This file is used during the connector upgrade procedure. This SQL script updates the object GUID in the older version of the connector to match the format of object GUID in the current version of the connector.

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

File in the Installation Package Directory	Description
xml/ActiveDirectory-ConnectorConfig.xml	<p>This XML file contains definitions for the following connector components:</p> <ul style="list-style-type: none"> <li>• Resource objects</li> <li>• IT resource types</li> <li>• IT resource instance</li> <li>• Process forms</li> <li>• Process tasks and adapters</li> <li>• Process definition</li> <li>• Prepopulate rules</li> <li>• Lookup definitions</li> <li>• Reconciliation rules</li> <li>• Scheduled tasks</li> </ul>
<p>xml/ActiveDirectory-Datasets.xml xml/ActiveDirectoryLDS-Datasets.xml</p> <p><b>Note:</b> The dataset XML files are applicable only if you are using Oracle Identity Manager release 11.1.1.x.</p>	<p>These XML files contain the dataset related definitions for the create and modify user provisioning operations. These files are used if you want to enable request-based provisioning. You import these XML files into Oracle Identity Manager by using the Deployment Manager.</p> <p><b>Note:</b> These files are applicable only for a CI-based connector.</p>
xml/ad-auth-template.xml	<p>This file contains definitions for the connector objects required for creating an Authoritative 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>
xml/ad-pre-config.xml	<p>This XML file contains definitions for the connector objects associated with any non-User objects such as Groups, Organizations, and so on.</p>
xml/ad-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>