# Contents

## Preface
- Audience xiv
- Documentation Accessibility xiv
- Related Documents xiv
- Documentation Updates xiv
- Conventions xv

## What's New in Oracle Identity Manager Connector for Microsoft Active Directory User Management?
- Software Updates xvi
- Documentation-Specific Updates xix

## 1 About the Microsoft Active Directory User Management Connector
- 1.1 Introduction to the Microsoft Active Directory User Management Connector 1-1
- 1.2 Certified Components for Microsoft Active Directory User Management Connector 1-2
- 1.3 Usage Recommendation for the Microsoft Active Directory User Management Connector 1-4
- 1.4 Certified Languages for the Microsoft Active Directory User Management Connector 1-4
- 1.5 Architecture of Microsoft Active Directory User Management Connector 1-5
- 1.6 Features of the Microsoft Active Directory User Management Connector 1-8
  - 1.6.1 Dependent Lookup Fields 1-9
  - 1.6.2 Full and Incremental Reconciliation 1-9
  - 1.6.3 Limited Reconciliation 1-9
  - 1.6.4 Batched Reconciliation 1-9
  - 1.6.5 Reconciliation of Deleted User Records 1-9
  - 1.6.6 Reconciliation of Deleted Groups 1-10
  - 1.6.7 Transformation and Validation of Account Data 1-10
  - 1.6.8 Support for Connector Server 1-10
  - 1.6.9 Connection Pooling 1-10
  - 1.6.10 Support for Connector Operations Across Domains 1-11
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6.11</td>
<td>Support for Connector Operations on User-Defined Object Classes</td>
<td>1-11</td>
</tr>
<tr>
<td>1.6.12</td>
<td>Support for Adding Dynamic Auxiliary Object Classes</td>
<td>1-11</td>
</tr>
<tr>
<td>1.6.13</td>
<td>Support for Adding the Group Name (pre-Windows 2000) Attribute</td>
<td>1-11</td>
</tr>
<tr>
<td>1.6.14</td>
<td>Support for Provisioning Groups of the Security Group - Universal Group Type</td>
<td>1-11</td>
</tr>
<tr>
<td>1.6.15</td>
<td>Support for Provisioning and Reconciling Custom Object Categories</td>
<td>1-11</td>
</tr>
<tr>
<td>1.6.16</td>
<td>Support for Scripting Languages</td>
<td>1-12</td>
</tr>
<tr>
<td>1.6.17</td>
<td>Support for High-Availability Configuration of the Target System</td>
<td>1-12</td>
</tr>
<tr>
<td>1.7</td>
<td>Lookup Definitions Used During Reconciliation and Provisioning</td>
<td>1-12</td>
</tr>
<tr>
<td>1.7.1</td>
<td>Lookup Definitions Synchronized with the AD and AD LDS Target Systems</td>
<td>1-13</td>
</tr>
<tr>
<td>1.7.2</td>
<td>Preconfigured Lookup Definitions for the Microsoft Active Directory User Management Connector</td>
<td>1-14</td>
</tr>
<tr>
<td>1.7.2.1</td>
<td>Lookup.Configuration.ActiveDirectory</td>
<td>1-14</td>
</tr>
<tr>
<td>1.7.2.2</td>
<td>Lookup.Configuration.ActiveDirectory.Trusted</td>
<td>1-17</td>
</tr>
<tr>
<td>1.7.2.3</td>
<td>Preconfigured Lookup Definitions for User Operations</td>
<td>1-19</td>
</tr>
<tr>
<td>1.7.2.4</td>
<td>Preconfigured Lookup Definitions for Group Operations</td>
<td>1-28</td>
</tr>
<tr>
<td>1.7.2.5</td>
<td>Preconfigured Lookup Definitions for Organizational Unit Operations</td>
<td>1-31</td>
</tr>
<tr>
<td>1.7.2.6</td>
<td>Preconfigured Lookup Definitions for AD LDS</td>
<td>1-34</td>
</tr>
<tr>
<td>1.8</td>
<td>Connector Objects Used During Target Resource Reconciliation</td>
<td>1-36</td>
</tr>
<tr>
<td>1.8.1</td>
<td>User Fields for Target Resource Reconciliation</td>
<td>1-36</td>
</tr>
<tr>
<td>1.8.2</td>
<td>Group Fields for Reconciliation</td>
<td>1-38</td>
</tr>
<tr>
<td>1.8.3</td>
<td>Organizational Unit Fields for Reconciliation</td>
<td>1-39</td>
</tr>
<tr>
<td>1.8.4</td>
<td>Reconciliation Rules for Target Resource Reconciliation</td>
<td>1-39</td>
</tr>
<tr>
<td>1.8.5</td>
<td>Viewing Reconciliation Rules for Target Resource Reconciliation</td>
<td>1-40</td>
</tr>
<tr>
<td>1.8.6</td>
<td>Reconciliation Action Rules for Target Resource Reconciliation</td>
<td>1-41</td>
</tr>
<tr>
<td>1.8.7</td>
<td>Viewing Reconciliation Action Rules for Target Resource Reconciliation</td>
<td>1-41</td>
</tr>
<tr>
<td>1.9</td>
<td>Connector Objects Used During Provisioning</td>
<td>1-42</td>
</tr>
<tr>
<td>1.9.1</td>
<td>Provisioning Functions</td>
<td>1-42</td>
</tr>
<tr>
<td>1.9.2</td>
<td>User Fields for Provisioning</td>
<td>1-44</td>
</tr>
<tr>
<td>1.9.3</td>
<td>Group Fields for Provisioning</td>
<td>1-48</td>
</tr>
<tr>
<td>1.9.4</td>
<td>Organizational Unit Fields for Provisioning</td>
<td>1-49</td>
</tr>
<tr>
<td>1.10</td>
<td>Connector Objects Used During Trusted Source Reconciliation</td>
<td>1-49</td>
</tr>
<tr>
<td>1.10.1</td>
<td>User Fields for Trusted Source Reconciliation</td>
<td>1-50</td>
</tr>
<tr>
<td>1.10.2</td>
<td>Organizational Unit Fields for Trusted Source Reconciliation</td>
<td>1-51</td>
</tr>
<tr>
<td>1.10.3</td>
<td>Reconciliation Rule for Trusted Source Reconciliation</td>
<td>1-51</td>
</tr>
<tr>
<td>1.10.4</td>
<td>Viewing Reconciliation Rules for Trusted Source Reconciliation</td>
<td>1-52</td>
</tr>
<tr>
<td>1.10.5</td>
<td>Reconciliation Action Rules for Trusted Source Reconciliation</td>
<td>1-52</td>
</tr>
<tr>
<td>1.10.6</td>
<td>Viewing Reconciliation Action Rules for Trusted Source Reconciliation</td>
<td>1-53</td>
</tr>
</tbody>
</table>
## Deploying the Microsoft Active Directory User Management Connector

### 2.1 Preinstallation

- **2.1.1** Creating a Target System User Account for Connector Operations 2-2
  - **2.1.1.1** Creating a User Account for Connector Operations in Microsoft Active Directory 2-2
  - **2.1.1.2** Creating a User Account for Connector Operations in Microsoft AD LDS 2-3
- **2.1.2** Assigning Permissions to Perform Delete User Reconciliation Runs 2-3
- **2.1.3** Delegating Control for Organizational Units and Custom Object Classes 2-4
- **2.1.4** About the Connector Server 2-5
- **2.1.5** Managing Logging for Microsoft Active Directory User Management Connector 2-5
  - **2.1.5.1** Enabling Logging for Microsoft Active Directory User Management Connector 2-5
  - **2.1.5.2** Configuring Log File Rotation 2-6

### 2.2 Installation

- **2.2.1** Installing Microsoft Active Directory User Management Connector in Oracle Identity Manager 2-7
  - **2.2.1.1** Running the Connector Installer 2-8
  - **2.2.1.2** Configuring the IT Resource for Microsoft AD and AD LDS 2-9
- **2.2.2** Installing the Microsoft Active Directory User Management Connector in the Connector Server 2-15
  - **2.2.2.1** Copying and Extracting the Connector Bundle to the Connector Server 2-15
  - **2.2.2.2** Configuring the IT Resource for the Connector Server 2-16

### 2.3 Postinstallation

- **2.3.1** Configuring Oracle Identity Manager 11.1.2 or Later 2-17
  - **2.3.1.1** Creating and Activating a Sandbox 2-18
  - **2.3.1.2** Creating a New UI Form 2-18
  - **2.3.1.3** Creating an Application Instance 2-18
  - **2.3.1.4** Publishing a Sandbox 2-19
  - **2.3.1.5** Harvesting Entitlements and Sync Catalog 2-19
- **2.3.2** Localizing Field Labels in UI Forms 2-20
- **2.3.3** Clearing Content Related to Connector Resource Bundles from the Server Cache 2-22
- **2.3.4** Setting Up the Lookup Definition for Connection Pooling 2-23
  - **2.3.4.1** Connection Pooling Properties 2-23
  - **2.3.4.2** Adding Connection Pooling Properties 2-23
- **2.3.5** Setting Up the Lookup Definition for the Ignore Event API 2-24
  - **2.3.5.1** Understanding the Ignore Event Disabled Entry 2-24
  - **2.3.5.2** Adding the Ignore Event Disabled Entry 2-24
Using the Microsoft Active Directory User Management Connector

3.1 Guidelines on Using the Microsoft Active Directory User Management Connector
   3.1.1 Guidelines on Configuring Reconciliation
   3.1.2 Guidelines on Performing Provisioning Operations

3.2 Scheduled Jobs for Lookup Field Synchronization

3.3 Configuring Reconciliation
   3.3.1 Full Reconciliation and Incremental Reconciliation
   3.3.2 Limited Reconciliation
      3.3.2.1 About Limited Reconciliation
      3.3.2.2 Performing Limited Reconciliation By Using Filters
      3.3.2.3 Performing Limited Reconciliation By Using the Search Base Attribute
4.14 Multiple Installations of the Target System 4-40
   4.14.1 About Multiple Installations of the Target System 4-41
   4.14.2 Configuring the Connector for Multiple Installations of the Target System 4-41
   4.14.3 Prerequisites for Performing Provisioning With Multiple Installations of the Target System 4-42
   4.14.4 Performing Provisioning Operations On Oracle Identity Manager 4-42

4.15 Creating a Home Directory After User Create Provisioning Operation 4-43
   4.15.1 About Creating a Home Directory After User Create Provisioning Operation 4-43
   4.15.2 Creating the UpdateHomeDirectoryField Adapter 4-43
   4.15.3 Updating the AD User Process Definition 4-45
   4.15.4 Updating the Create User Process Task 4-46

4.16 Configuring the Connector for Provisioning Groups of the Security Group - Universal Group Type 4-46

4.17 Configuring the Connector for Provisioning and Reconciling Custom Object Categories 4-46
   4.17.1 Adding Custom Object Category for Trusted Source Reconciliation 4-47
   4.17.2 Adding Custom Object Category for Target Resource Reconciliation 4-47
   4.17.3 Adding Custom Object Category for Provisioning 4-49

5 Troubleshooting the Microsoft Active Directory User Management Connector

6 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 On the Installation Media

C Special Characters Supported in Process Form Fields
Scheduled Jobs for Lookup Field Synchronization and Reconciliation
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Connector Architecture</td>
<td>1-5</td>
</tr>
<tr>
<td>1-2</td>
<td>Reconciliation Rule for Target Resource Reconciliation</td>
<td>1-41</td>
</tr>
<tr>
<td>1-3</td>
<td>Reconciliation Action Rules for Target Resource Reconciliation</td>
<td>1-42</td>
</tr>
<tr>
<td>1-4</td>
<td>Reconciliation Rule for Trusted Source Reconciliation</td>
<td>1-52</td>
</tr>
<tr>
<td>1-5</td>
<td>Reconciliation Action Rules for Trusted Source Reconciliation</td>
<td>1-54</td>
</tr>
<tr>
<td>2-1</td>
<td>Manage IT Resource Page</td>
<td>2-10</td>
</tr>
<tr>
<td>2-2</td>
<td>Edit IT Resource Details and Parameters Page for the Active Directory IT Resource</td>
<td>2-11</td>
</tr>
<tr>
<td>2-3</td>
<td>RootDSE Properties Dialog Box</td>
<td>2-37</td>
</tr>
<tr>
<td>3-1</td>
<td>Lookup Entries for Action Scripts</td>
<td>3-28</td>
</tr>
<tr>
<td>3-2</td>
<td>User Details Page</td>
<td>3-31</td>
</tr>
<tr>
<td>3-3</td>
<td>Step 1: Select a Resource Page</td>
<td>3-31</td>
</tr>
<tr>
<td>3-4</td>
<td>Step 2: Verify Resource Selection Page</td>
<td>3-32</td>
</tr>
<tr>
<td>3-5</td>
<td>Step 5: Provide Process Data for AD User Form Page</td>
<td>3-32</td>
</tr>
<tr>
<td>3-6</td>
<td>Step 5: Provide Process Data for Assigned Groups Form Page</td>
<td>3-33</td>
</tr>
<tr>
<td>3-7</td>
<td>Step 6: Verify Process Data Page</td>
<td>3-33</td>
</tr>
<tr>
<td>4-1</td>
<td>Multivalued Field Added on a New Form</td>
<td>4-5</td>
</tr>
<tr>
<td>4-2</td>
<td>Child Form Added to the Process Form</td>
<td>4-5</td>
</tr>
<tr>
<td>4-3</td>
<td>New Reconciliation Field Added in the Resource Object</td>
<td>4-7</td>
</tr>
<tr>
<td>4-4</td>
<td>Entry Added in the Lookup Definition</td>
<td>4-8</td>
</tr>
<tr>
<td>4-5</td>
<td>New Reconciliation Field Mapped to a Process Data Field</td>
<td>4-9</td>
</tr>
<tr>
<td>4-6</td>
<td>Entry Added to the Lookup Definition</td>
<td>4-16</td>
</tr>
<tr>
<td>4-7</td>
<td>Multivalued Field Added to the AD User Provisioning Process</td>
<td>4-17</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>1-1</td>
<td>Certified Components</td>
<td>1-2</td>
</tr>
<tr>
<td>1-2</td>
<td>Lookup Definitions Synchronized with the Target System</td>
<td>1-13</td>
</tr>
<tr>
<td>1-3</td>
<td>Entries in the Lookup.Configuration.ActiveDirectory Lookup Definition</td>
<td>1-15</td>
</tr>
<tr>
<td>1-4</td>
<td>Entries in the Lookup.Configuration.ActiveDirectory.Trusted Lookup Definition</td>
<td>1-17</td>
</tr>
<tr>
<td>1-5</td>
<td>Entries in the Lookup.ActiveDirectory.UM.Configuration Lookup Definition</td>
<td>1-19</td>
</tr>
<tr>
<td>1-6</td>
<td>Entries in the Lookup.ActiveDirectory.UM.Configuration.Trusted Lookup Definition</td>
<td>1-20</td>
</tr>
<tr>
<td>1-7</td>
<td>Default Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition</td>
<td>1-20</td>
</tr>
<tr>
<td>1-8</td>
<td>Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap Lookup Definition</td>
<td>1-24</td>
</tr>
<tr>
<td>1-9</td>
<td>Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted Lookup Definition</td>
<td>1-27</td>
</tr>
<tr>
<td>1-10</td>
<td>Entries in the Lookup.ActiveDirectory.GM.Configuration Lookup Definition</td>
<td>1-29</td>
</tr>
<tr>
<td>1-11</td>
<td>Default Entries in the Lookup.ActiveDirectory.GM.ProvAttrMap</td>
<td>1-30</td>
</tr>
<tr>
<td>1-12</td>
<td>Entries in the Lookup.ActiveDirectory.OM.Configuration Lookup Definition</td>
<td>1-32</td>
</tr>
<tr>
<td>1-13</td>
<td>Entries in the Lookup.ActiveDirectory.OM.Configuration.Trusted Lookup Definition</td>
<td>1-33</td>
</tr>
<tr>
<td>1-14</td>
<td>Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap Lookup Definition</td>
<td>1-36</td>
</tr>
<tr>
<td>1-15</td>
<td>Entries in the Lookup.ActiveDirectory.GM.ReconAttrMap</td>
<td>1-38</td>
</tr>
<tr>
<td>1-16</td>
<td>Entries in the Lookup.ActiveDirectory.OM.ReconAttrMap</td>
<td>1-39</td>
</tr>
<tr>
<td>1-17</td>
<td>Action Rules for Target Resource Reconciliation</td>
<td>1-41</td>
</tr>
<tr>
<td>1-18</td>
<td>Provisioning Functions</td>
<td>1-43</td>
</tr>
<tr>
<td>1-19</td>
<td>Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition</td>
<td>1-44</td>
</tr>
<tr>
<td>1-20</td>
<td>Entries in the Lookup.ActiveDirectory.GM.ProvAttrMap</td>
<td>1-48</td>
</tr>
<tr>
<td>1-21</td>
<td>Entries in the Lookup.ActiveDirectory.OM.ProvAttrMap</td>
<td>1-49</td>
</tr>
<tr>
<td>1-22</td>
<td>Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted Lookup Definition</td>
<td>1-50</td>
</tr>
<tr>
<td>1-23</td>
<td>Entries in the Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted Lookup Definition</td>
<td>1-51</td>
</tr>
<tr>
<td>1-24</td>
<td>Action Rules for Trusted Source Reconciliation</td>
<td>1-53</td>
</tr>
<tr>
<td>2-1</td>
<td>Parameters of the Active Directory Connector Server IT Resource</td>
<td>2-16</td>
</tr>
<tr>
<td>2-2</td>
<td>Connection Pooling Properties</td>
<td>2-23</td>
</tr>
<tr>
<td>3-1</td>
<td>Attributes of the Scheduled Tasks for Lookup Field Synchronization</td>
<td>3-6</td>
</tr>
<tr>
<td>3-2</td>
<td>Keywords and Syntax for the Filter Attribute</td>
<td>3-8</td>
</tr>
<tr>
<td>3-3</td>
<td>Attributes of the Scheduled Job for Reconciliation of User Data from a Target Resource</td>
<td>3-12</td>
</tr>
<tr>
<td>3-4</td>
<td>Attributes of the Scheduled Job for Reconciliation of User Data from a Trusted Source</td>
<td>3-13</td>
</tr>
<tr>
<td>3-5</td>
<td>Attributes of the Scheduled Jobs for Delete User Reconciliation</td>
<td>3-16</td>
</tr>
<tr>
<td>3-6</td>
<td>Attributes of the Scheduled Task for Reconciliation of Group and Organization Data</td>
<td>3-18</td>
</tr>
<tr>
<td>3-7</td>
<td>Attributes of the Active Directory Group Delete Recon Scheduled Job</td>
<td>3-19</td>
</tr>
<tr>
<td>3-8</td>
<td>Lookup Entries for Running Action Scripts</td>
<td>3-25</td>
</tr>
<tr>
<td>4-1</td>
<td>Entries in the Updated Lookup.ActiveDirectory.GM.ReconAttrMap Lookup Definition</td>
<td>4-24</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>4-2</td>
<td>Entries in the Updated Lookup.ActiveDirectory.GM.ProvAttrMap Lookup Definition</td>
<td>4-27</td>
</tr>
<tr>
<td>5-1</td>
<td>Troubleshooting the Microsoft Active Directory User Management Connector</td>
<td>5-1</td>
</tr>
<tr>
<td>A-1</td>
<td>Fields with Different Lengths on the Target System and the Process Form</td>
<td>A-1</td>
</tr>
<tr>
<td>B-1</td>
<td>Files and Directories On the Installation Media</td>
<td>B-1</td>
</tr>
<tr>
<td>C-1</td>
<td>Special Characters Supported in Process Form Fields</td>
<td>C-1</td>
</tr>
<tr>
<td>D-1</td>
<td>Scheduled Jobs for Lookup Field Synchronization and Reconciliation</td>
<td>D-1</td>
</tr>
</tbody>
</table>
Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Microsoft Active Directory and Microsoft Active Directory Lightweight Directory Services (AD LDS).

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 Manager, visit the following Oracle Help Center page:

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

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

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

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

http://download.oracle.com/docs/cd/E22999_01/index.htm
## Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
What's New in Oracle Identity Manager Connector for Microsoft Active Directory User Management?

This chapter provides an overview of the updates made to the software and documentation for release 11.1.1.6.0 of the Microsoft Active Directory User Management connector.

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

- **Software Updates**
  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- **Documentation-Specific Updates**
  This section describes major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

### Software Updates

The following section discusses software updates:

- **Software Updates in Release 11.1.1.6.0**
- **Software Updates in Release 11.1.1.5.0**

### Software Updates in Release 11.1.1.6.0

The following are the software updates in release 11.1.1.6.0:

- **Support for Adding Dynamic Auxiliary Object Classes**
- **Support for Adding the Group Name (pre-Windows 2000) Attribute**
- **Support for Provisioning Groups of the Security Group - Universal Group Type**
- **Support for Provisioning and Reconciling Custom Object Categories**

### Support for Adding Dynamic Auxiliary Object Classes

The connector provides support for adding dynamic auxiliary object classes. In addition, you can add the attributes of these dynamic auxiliary object classes for reconciliation and provisioning.
Support for Adding the Group Name (pre-Windows 2000) Attribute

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.

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

The connector provides support for provisioning groups of the type Security Group - Universal. See Configuring the Connector for Provisioning Groups of the Security Group - Universal Group Type for more information.

Support for Provisioning and Reconciling Custom Object Categories

If you are using AD LDS as the target system, then add custom object categories for provisioning and reconciliation. See Configuring the Connector for Provisioning and Reconciling Custom Object Categories for more information.

Software Updates in Release 11.1.1.5.0

The following are the software updates in release 11.1.1.5.0:

- Support for Connector Server
- Deployment Using Connector Server
- Connection Pooling
- Support for Connector Operations Across Domains
- Support for Connector Operations on User-Defined Object Classes
- Support for Addition of New Terminal Profile Fields
- Support for Scripting Languages
- Support for High-Availability Configuration of the Target System

Support for New Target Systems

From this release onward, the connector adds support for the following as target systems:

- Microsoft Active Directory installed on Microsoft Windows Server 2012
- Microsoft Active Directory Lightweight Directory Services installed on Microsoft Windows Server 2012

These target systems are mentioned in Certified Components for Microsoft Active Directory User Management Connector.
Support for Connector Server

The Microsoft 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 for this connector to be deployed on the .NET Connector Server shipped along with the connector package. The Microsoft Active Directory User Management connector operates in the context of a .NET Connector Framework, which in turn requires an application to execute. Therefore, by default, Oracle provides the .NET Connector Server to run the Microsoft Active Directory User Management connector.

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 Manager connector.

See the following sections for more information:

- About the Connector Server
- Installing the Microsoft Active Directory User Management Connector in the Connector Server

Deployment Using Connector Server

This release of the connector can be deployed using the Connector Server, which is included with the ICF. See Installing Microsoft Active Directory User Management Connector in Oracle Identity Manager for more information.

Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager 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 IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

See Setting Up the Lookup Definition for Connection Pooling for more information.

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.
Support for Connector Operations on User-Defined Object Classes

The connector can be configured to reconcile from and provision to user-defined object classes and their attributes. By default, the target system uses the user object class. The connector can be configured to accommodate user-defined object classes that you define on the target system.

See Configuring the Connector for User-Defined Object Classes for more information.

Support for Addition of New Terminal Profile Fields

Depending upon your requirement, you can add new terminal profile fields for reconciliation and provisioning. See Adding Terminal Services Fields for Reconciliation and Provisioning for more information.

Support for Scripting Languages

The connector supports any scripting language that has a script executor in the ICF. Currently, there are 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.

See Action Scripts for more information.

Support for High-Availability Configuration of the Target System

The connector can be configured for compatibility with high-availability target system environments. It can read information about backup target system hosts from the BDCHostNames parameter of the Active Directory IT resource and apply this information when it is unable to connect to the primary host.

See Table 2–1 of Configuring the IT Resource for Microsoft AD and AD LDS for more information.

Documentation-Specific Updates

The following section discusses documentation-specific updates:

• Documentation-Specific Updates in Release 11.1.1.6.0
• Documentation-Specific Updates in Release 11.1.1.5.0

Documentation-Specific Updates in Release 11.1.1.6.0

The following documentation-specific updates have been made in revision "23" of release 11.1.1.6.0:

• “Integrated Common Framework” has been corrected to “Identity Connector Framework” in Architecture of Microsoft Active Directory User Management Connector.

• Step 6 has been added to Replicating Form Designer Changes to a New UI Form.

The following documentation-specific updates have been made in revision “22” of release 11.1.1.6.0:
• The “Target systems and target system host platforms” row of the table in Certified Components for Microsoft Active Directory User Management Connector has been updated to include support for Microsoft Windows Server 2016, 64-bit platform in the Requirement for Microsoft AD LDS or ADAM column.

• Information pertaining to procedures performed on the target system has been replaced with a high-level summary in the following sections:
  – Delegating Control for Organizational Units and Custom Object Classes
  – Enabling or Disabling Password Policies in Microsoft Active Directory
  – Prerequisites
  – Configuring SSL Between Connector Server and Microsoft Active Directory
  – Configuring SSL Between Connector Server and Microsoft AD LDS
  – Exporting the Certificate
  – Configuring the Connector Server for SSL
  – Configuring Oracle Identity Manager for SSL

• A new section Configuring SSL Between Connector Server and Microsoft Active Directory has been created combining the following sections:
  – Ensuring Microsoft Active Directory on Microsoft Windows Server 2003 is SSL Enabled
  – Ensuring Microsoft Active Directory on Microsoft Windows Server 2008 is SSL Enabled
  – Configuring the SSL IT Resource Parameter

• Installing and Configuring the Connector server has been renamed as About the Connector Server.

• Configuring SSL Between Connector Server and Microsoft Active Directory has been modified.

The following documentation-specific updates have been made in revision "21" of release 11.1.1.6.0:

The "Oracle Identity Manager" row of the table in Certified Components for Microsoft Active Directory User Management Connector has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12c (12.2.1.3.0) certification.

The following documentation-specific updates have been made in revision "20" of release 11.1.1.6.0:

• The “Target systems and target system host platforms” row of the table in Certified Components for Microsoft Active Directory User Management Connector has been updated to include support for Microsoft Windows Server 2016, 64–bit platform in the Requirement for Microsoft Active directory column.

• An issue related to sAMAccount name attribute containing more than 20 characters has been added to Table 5-1, “Troubleshooting for the Microsoft Active Directory User Management Connector”.

The following documentation-specific update has been made in revision "19" of release 11.1.1.6.0:
All contents of Section 2.1.1.1, "Files and Directories On the Installation Media" have been moved to Appendix B, "Files and Directories on the Installation Media".

The following documentation-specific update has been made in revision "18" of release 11.1.1.6.0:

The "Connector Server" row of the table in Certified Components for Microsoft Active Directory User Management Connector has been updated.

The following documentation-specific update has been made in revision "17" of release 11.1.1.6.0:

A "Note" regarding the user account to be used while running the .NET Connector Server has been added to Installing and Configuring the Connector Server.

The following documentation-specific update has been made in revision "16" of release 11.1.1.6.0:

The "Microsoft .NET framework" row has been added to the table in Certified Components for Microsoft Active Directory User Management Connector.

The following documentation-specific updates have been made in revision "15" of release 11.1.1.6.0:

- The following guideline has been removed from Guidelines on Configuring Reconciliation as the connector no longer uses the said format to delete users in Oracle Identity Manager:
- Chapter 7, "Known Issues and Workarounds" has been removed.

The following documentation-specific updates have been made in revision "14" of release 11.1.1.6.0:

- A note recommending not to configure the target system as both an authoritative (trusted) source and a managed (target) resource has been removed from About the Microsoft Active Directory User Management Connector.
- A note regarding creating an IT resource when you have configured your target system as a trusted source has been added to Configuring the IT Resource for Microsoft AD and AD LDS.
- The "IT Resource Name" of Table 3-4 has been updated.
- Information regarding coexistence of Microsoft Active Directory User Management 9.x and 11.x connectors has been modified in Frequently Asked Questions.

The following documentation-specific updates have been made in revision "13" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of the table in Certified Components for Microsoft Active Directory User Management Connector has been updated.
- Information specific to Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) has been added to Usage Recommendation for the Microsoft Active Directory User Management Connector.

The following documentation-specific update has been made in revision "12" of release 11.1.1.6.0:

A "Note" has been added at the beginning of Extending the Functionality of the Microsoft Active Directory User Management Connector.
The following documentation-specific update has been made in revision "11" of release 11.1.1.6.0:

Troubleshooting the Microsoft Active Directory User Management Connector has been updated.

The following documentation-specific updates have been made in revision "10" of release 11.1.1.6.0:

- The following tables have been updated by adding a "Description" column:
  - Table 1-14
  - Table 1-15
  - Table 1-16
  - Table 1-19
  - Table 1-20
  - Table 1-21
  - Table 1-22
- Appendix B, "Special Characters Supported for Passwords" has been removed as all special characters supported by the target system can be used in password fields.

The following documentation-specific updates have been made in the revision "9" of release 11.1.1.6.0:

- The "Target systems and target system host platforms" row of the table in Certified Components for Microsoft Active Directory User Management Connector has been modified to include Windows Server 2012 R2.
- Configuring Validation of Data During Reconciliation and Provisioning has been updated to remove the statement that the validation class must implement the oracle.iam.connectors.common.validate.Validator interface.
- In Frequently Asked Questions, the recommended system configuration for the computer installing and running the Connector Server has been updated to include Windows Server 2012.
- Setting Up the Lookup Definition for the Ignore Event API has been created.

The following documentation-specific updates have been made in the revision "8" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of the table in Certified Components for Microsoft Active Directory User Management Connector has been modified to include Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0).
- Information specific to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0) has been added to Step 5 of Localizing Field Labels in UI Forms.
- Action Scripts has been updated.
- Frequently Asked Questions has been updated.

The following documentation-specific updates have been made in earlier revisions of release 11.1.1.6.0:

- The "Oracle Identity Manager" and "Target systems and target system host platforms" rows of the table in Certified Components for Microsoft Active Directory User Management Connector have been modified.
• The “NativeGuidConvention” entry has been added to Table 1-4 and Table 1-5.

• A note has been added in the "Files in the dataset directory" and "xml/ActiveDirectory-Datasets.xml" rows of Table 2–1.

• A note has been added in the instructions specific to Microsoft AD LDS in Creating a Target System User Account for Connector Operations.

• A guideline has been added to Guidelines on Performing Provisioning Operations.

• The following sections have been modified:
  – Action Scripts
  – Configuring the Connector for User-Defined Object Classes
  – Troubleshooting the Microsoft Active Directory User Management Connector

• Information about adding a boolean field has been added in Step 2.d of Adding Custom Fields for Target Resource Reconciliation.

• A note about boolean field has been added in Step 4.d of Adding Custom Fields for Provisioning.

• The following sections have been added:
  – Usage Recommendation for the Microsoft Active Directory User Management Connector
  – Assigning Permissions to Perform Delete User Reconciliation Runs
  – Delegating Control for Organizational Units and Custom Object Classes
  – Configuring Oracle Identity Manager 11.1.2 or Later
  – Localizing Field Labels in UI Forms
  – Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later
  – Creating a Home Directory After User Create Provisioning Operation
  – Frequently Asked Questions

• Instructions specific to Oracle Identity Manager release 11.1.2.x have been added in the following sections:
  – Installing Microsoft Active Directory User Management Connector in Oracle Identity Manager
  – Configuring the IT Resource for the Connector Server
  – Adding Custom Fields for Target Resource Reconciliation
  – Adding New Multivalued Fields for Target Resource Reconciliation
  – Adding Custom Fields for Provisioning

• A note has been added in the "DirectoryAdminName" row of Table 2–1, "Parameters of the Active Directory IT Resource for the Target System".

Documentation-Specific Updates in Release 11.1.1.5.0

The following are the documentation-specific updates in release 11.1.1.5.0:
• A note about details specific to the password reset provisioning operation has been added to Architecture of Microsoft Active Directory User Management Connector.

• A note about installing a patch for .NET Framework 3.5 has been added to About the Connector Server.

• Updated Installation to indicate that the connector must be installed both in Oracle Identity Manager and in the Connector Server. Removed Section 2.3.3, "Creating the IT Resource for the Connector Server" as part of this update.

• Updated sample class and examples in Configuring Transformation of Data During Reconciliation, and removed appendixes C and D.

• In Certified Components for Microsoft Active Directory User Management Connector, added the patch 14190610 as a requirement for Oracle Identity Manager.

• In Adding New Multivalued Fields for Provisioning, removed the note indicating that the child table update operations are not supported by the connector.

• A note about serverless binding has been added in the "LDAPHostName" row of Table 2–1, "Parameters of the Active Directory IT Resource for the Target System".

• Configuring Log File Rotation has been added.

• Limited Reconciliation has been modified.
1

About the Microsoft Active Directory User Management Connector

This chapter introduces the Microsoft Active Directory User Management (AD User Management) connector. This chapter contains the following sections:

- Introduction to the Microsoft Active Directory User Management Connector
- Certified Components for Microsoft Active Directory User Management Connector
- Usage Recommendation for the Microsoft Active Directory User Management Connector
- Certified Languages for the Microsoft Active Directory User Management Connector
- Architecture of Microsoft Active Directory User Management Connector
- Features of the Microsoft Active Directory User Management Connector
- Connector Objects Used During Target Resource Reconciliation
- Connector Objects Used During Provisioning
- Connector Objects Used During Trusted Source Reconciliation

1.1 Introduction to the Microsoft Active Directory User Management Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This connector enables you to use Microsoft Active Directory or Active Directory Lightweight Directory Services (AD LDS), formerly known as Microsoft Active Directory Application Mode (ADAM), either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

Note:

At some places in this guide, Microsoft Active Directory, Microsoft ADAM, and Microsoft AD LDS is referred to as the target systems.

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.
In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

1.2 Certified Components for Microsoft Active Directory User Management Connector

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 lists the certified components for both target systems.

Table 1-1 Certified Components

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement for Microsoft Active Directory</th>
<th>Requirement for Microsoft AD LDS or ADAM</th>
</tr>
</thead>
</table>
| Oracle Identity Governance or Oracle Identity Manager | You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:  
  - Oracle Identity Governance 12c (12.2.1.3.0)  
  - Oracle Identity Manager 11g Release 1 (11.1.1.5.6) and any later BP in this release track  
  - Oracle Identity Manager 11g Release 2 (11.1.2.0.6) and any later BP in this release track  
  - Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0)  
  - Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) | You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:  
  - Oracle Identity Governance 12c (12.2.1.3.0)  
  - Oracle Identity Manager 11g Release 1 (11.1.1.5.6) and any later BP in this release track  
  - Oracle Identity Manager 11g Release 2 (11.1.2.0.6) and any later BP in this release track  
  - Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0)  
  - Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) |
<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement for Microsoft Active Directory</th>
<th>Requirement for Microsoft AD LDS or ADAM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The target system can be any one of the following:</td>
<td>The target system can be any one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory installed on Microsoft Windows Server 2003, both 32-bit and 64-bit platforms</td>
<td>• Microsoft Active Directory Application Mode installed on Microsoft Windows Server 2003, both 32-bit and 64-bit platforms</td>
</tr>
<tr>
<td></td>
<td>Note: On a Microsoft Windows 2003 server on which SP1 has not been installed, you might come across the “WILL_NOT_PERFORM” error message during the password change operation. You can access information about one of the causes of and a solution for this error on the Microsoft Knowledge Base Web site at <a href="http://support.microsoft.com">http://support.microsoft.com</a></td>
<td>Note: On a Microsoft Windows 2003 server on which SP1 has not been installed, you might come across the “WILL_NOT_PERFORM” error message during the password change operation. You can access information about one of the causes of and a solution for this error on the Microsoft Knowledge Base Web site at <a href="http://support.microsoft.com">http://support.microsoft.com</a></td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory installed on Microsoft Windows Server 2003 R2, both 32-bit and 64-bit platforms</td>
<td>• Microsoft Active Directory Application Mode installed on Microsoft Windows Server 2003 R2, both 32-bit and 64-bit platforms</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory installed on Microsoft Windows Server 2008, both 32-bit and 64-bit platforms</td>
<td>• Microsoft Active Directory Lightweight Directory Services installed on Microsoft Windows Server 2008, both 32-bit and 64-bit platforms</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory installed on Microsoft Windows Server 2008 R2, both 32-bit and 64-bit platforms</td>
<td>• Microsoft Active Directory Lightweight Directory Services installed on Microsoft Windows Server 2008 R2, both 32-bit and 64-bit platforms</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory installed on Microsoft Windows Server 2012, 64-bit platform</td>
<td>• Microsoft Active Directory Lightweight Directory Services installed on Microsoft Windows Server 2012, 64-bit platform</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory installed on Microsoft Windows Server 2012 R2, 64-bit platform</td>
<td>• Microsoft Active Directory Lightweight Directory Services installed on Microsoft Windows Server 2012 R2, 64-bit platform</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory installed on Microsoft Windows Server 2016, 64-bit platform</td>
<td>• Microsoft Active Directory Lightweight Directory Services installed on Microsoft Windows Server 2016, 64-bit platform</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connector Server</th>
<th>11.1.2.1.0 or later</th>
<th>11.1.2.1.0 or later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other software (Software used for establishing or securing communication between Oracle Identity Manager and target system.)</td>
<td>Certificate Services</td>
<td>Certificate Services</td>
</tr>
<tr>
<td></td>
<td>IIS Web Server</td>
<td>IIS Web Server</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must configure SSL for the connector to perform all connector operations as expected.</td>
<td></td>
</tr>
<tr>
<td>Microsoft .NET framework</td>
<td>3.5, 4, or 4.5</td>
<td>3.5, 4, or 4.5</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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></td>
<td><strong>Note:</strong> 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></td>
</tr>
</tbody>
</table>
1.3 Usage Recommendation for the Microsoft Active Directory User Management Connector

Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of the following connectors:

**Note:**

At some places in this section, Microsoft Active Directory User Management connector releases 9.1.0.x and 9.0.4.x have been referred to as release 9.x.

- If you are using Oracle Identity Manager release 9.1.0.1 and Microsoft Windows Server 2003 Active Directory, then you must use the 9.0.4.x version of this connector.
- 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.
- If you are using Oracle Identity Manager 11g Release 1 (11.1.1.5.6) or later, Oracle Identity Manager 11g Release 2 (11.1.2.0.6) or later, Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0) or later, or Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.x version of this connector. However, if you are using Microsoft Exchange 2003, then you must use the 9.x versions for both Microsoft Active Directory User Management and Microsoft Exchange connectors.

1.4 Certified Languages for the Microsoft Active Directory User Management Connector

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Greek
- Hebrew
1.5 Architecture of Microsoft Active Directory User Management Connector

Figure 1-1 shows the architecture of the connector.

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 Manager 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 Identity Connector Framework (ICF) 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 Manager 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 Manager or Oracle Waveset). The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped along with Oracle Identity Manager. Therefore, you need not configure or modify the ICF.

See Also:
Understanding the Identity Connector Framework in Developing and Customizing Applications for Oracle Identity Manager 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 Scheduled Jobs 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 Manager. 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 Manager context, the term “provisioning” is also used to mean updates (for example enabling or disabling) made to the target system account through Oracle Identity Manager.

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 Manager 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 Manager 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 Scheduled Jobs.

This connector cannot propagate password changes from Microsoft Active Directory to Oracle Identity Manager. To implement this feature, you must install the Microsoft Active Directory password synchronization connector. For more information, see Oracle Identity Manager Connector Guide for Microsoft Active Directory Password Synchronization. That guide describes scenarios in which both the password synchronization connector and this connector are deployed.

1.6 Features of the Microsoft Active Directory User Management Connector

The following are features of the connector:

- Dependent Lookup Fields
- Full and Incremental Reconciliation
- Limited Reconciliation
- Batched Reconciliation
- Reconciliation of Deleted User Records
- Reconciliation of Deleted Groups
- Transformation and Validation of Account Data
- Support for Connector Server
- Connection Pooling
- Support for Connector Operations Across Domains
- Support for Connector Operations on User-Defined Object Classes
- Support for Adding Dynamic Auxiliary Object Classes
- Support for Adding the Group Name (pre-Windows 2000) Attribute
- Support for Provisioning Groups of the Security Group - Universal Group Type
• Support for Provisioning and Reconciling Custom Object Categories
• Support for Scripting Languages
• Support for High-Availability Configuration of the Target System

1.6.1 Dependent Lookup Fields

If you have multiple installations of the target system, the entries in lookup definitions (used as an input source for lookup fields during provisioning) can be linked to the target system installation from which they are copied. Therefore, during a provisioning operation, you can select lookup field values that are specific to the target system installation on which the provisioning operation is being performed.

See Lookup Definitions Synchronized with the AD and AD LDS Target Systems for more information about the format in which data is stored in dependent lookup definitions.

1.6.2 Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. 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 Manager.

You can perform a full reconciliation run at any time.

See Full Reconciliation and Incremental Reconciliation for more information.

1.6.3 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 Limited Reconciliation for more information.

1.6.4 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 Batched Reconciliation for more information.

1.6.5 Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records. In target resource mode, if a user record is deleted on the target system, then the corresponding AD User resource is revoked from the OIM User. In trusted source mode, if a user record is deleted on the target system, then the corresponding OIM User is deleted.

See Scheduled Jobs for Reconciliation of Deleted User Records for more information about scheduled jobs used for reconciling deleted user records.
1.6.6 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 Manager.

See Scheduled Job for Reconciliation of Deleted Groups for more information about the scheduled job used for reconciling deleted groups.

1.6.7 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

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

1.6.8 Support for Connector Server

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 for this connector to be deployed 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.

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 Manager connector.

See the following sections for more information:

- About the Connector Server
- Installing the Microsoft Active Directory User Management Connector in the Connector Server

1.6.9 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager 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 IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

See Setting Up the Lookup Definition for Connection Pooling for more information.

1.6.10 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.

1.6.11 Support for Connector Operations on User-Defined Object Classes

The connector can be configured to reconcile from and provision to user-defined object classes and their attributes. By default, the target system uses the `user` object class. The connector can be configured to accommodate user-defined object classes that you define on the target system.

See Configuring the Connector for User-Defined Object Classes for more information.

1.6.12 Support for Adding Dynamic Auxiliary Object Classes

The connector provides support for adding dynamic auxiliary object classes. In addition, you can add the attributes of these dynamic auxiliary object classes for reconciliation and provisioning.

See Adding Dynamic Auxiliary Object Classes and Their Attributes to Users for more information.

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

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.
1.6.14 Support for Provisioning Groups of the Security Group - Universal Group Type

The connector provides support for provisioning groups of the type Security Group - Universal. See Configuring the Connector for Provisioning Groups of the Security Group - Universal Group Type for more information.

1.6.15 Support for Provisioning and Reconciling Custom Object Categories

If you are using AD LDS as the target system, then add custom object categories for provisioning and reconciliation. See Configuring the Connector for Provisioning and Reconciling Custom Object Categories for more information.

1.6.16 Support for Scripting Languages

The connector supports any scripting language that has a script executor in the ICF. Currently, there are 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.

See Action Scripts for more information.

1.6.17 Support for High-Availability Configuration of the Target System

The connector can be configured for compatibility with high-availability target system environments. It can read information about backup target system hosts from the BDCHostNames parameter of the Active Directory IT resource and apply this information when it is unable to connect to the primary host.

See Step 7 of Configuring the IT Resource for Microsoft AD and AD LDS for more information about the BDCHostNames parameter of the IT resource.

1.7 Lookup Definitions Used During Reconciliation and Provisioning

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

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

- Lookup Definitions Synchronized with the AD and AD LDS Target Systems
- Preconfigured Lookup Definitions for the Microsoft Active Directory User Management Connector
1.7.1 Lookup Definitions Synchronized with the AD and AD LDS Target Systems

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Organizational Unit lookup field to select an organizational unit from the list of organizational units in the lookup field. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

The following is the format in which data is stored after lookup definition synchronization:

Code Key: `<IT_RESOURCE_KEY>~<LOOKUP_FIELD_VALUE>`

In this format:
- `ITRESOURCE_KEY` is the numeric code assigned to each IT resource in Oracle Identity Manager.
- `LOOKUP_FIELD_VALUE` is the connector attribute value defined for code.

Sample value: `1-OU=TestOrg8,DC=matrix,DC=com`

Decode: `<IT_RESOURCE_NAME>~<LOOKUP_FIELD_VALUE>`

In this format:
- `IT_RESOURCE_NAME` is the name of the IT resource in Oracle Identity Manager.
- `LOOKUP_FIELD_VALUE` is the connector attribute value defined for decode.

Sample value: `Active Directory~OU=TestOrg8,DC=matrix,DC=com`

For example, in the Lookup.ActiveDirectory.Groups lookup definition, values will be stored in the following format:

Code Key: `<ITRESOURCE_KEY>~<DISTINGUISHED_NAME>`

Decode: `<ITRESOURCE_NAME>~<DISTINGUISHED_NAME>`

During a provisioning operation, lookup fields are populated with values corresponding to the target system that you select for the operation.

The "Lookup Definition" column of Table 1-2 lists the Oracle Identity Manager lookup definitions that correspond to target system lookup fields listed in the "Target System Field" column of the table.

Table 1-2 Lookup Definitions Synchronized with the Target System

<table>
<thead>
<tr>
<th>Lookup Definition</th>
<th>Target System Field</th>
<th>Scheduled Task for Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup.ActiveDirectory.Groups</td>
<td>The distinguishedName field of groups</td>
<td>You use the Active Directory Group Lookup Recon scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.</td>
</tr>
</tbody>
</table>
Table 1-2 (Cont.) Lookup Definitions Synchronized with the Target System

<table>
<thead>
<tr>
<th>Lookup Definition</th>
<th>Target System Field</th>
<th>Scheduled Task for Synchronization</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup.ActiveDirectory.OrganizationalUnits</td>
<td>The distinguishedName field of organizations</td>
<td>You use the Active Directory Organization Lookup Recon scheduled job to synchronize this lookup definition. This scheduled job is discussed in Scheduled Jobs for Lookup Field Synchronization.</td>
<td></td>
</tr>
</tbody>
</table>

1.7.2 Preconfigured Lookup Definitions for the Microsoft Active Directory User Management Connector

This section discusses the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed. The other lookup definitions are as follows:

- Preconfigured Lookup Definitions for User Operations
- Preconfigured Lookup Definitions for Group Operations
- Preconfigured Lookup Definitions for Organizational Unit Operations
- Preconfigured Lookup Definitions for AD LDS

1.7.2.1 Lookup.Configuration.ActiveDirectory

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

Table 1-3 lists the default entries in this lookup definition.

Note:

- If you want to use dynamic auxiliary object classes, then you must add a new entry to this lookup definition. See Adding Dynamic Auxiliary Object Classes and Their Attributes to Users for more information.
- If you want to use user-defined object classes, then you must update this lookup definition. See Configuring the Connector for User-Defined Object Classes for more information.
Table 1-3  Entries in the Lookup.Configuration.ActiveDirectory Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
</table>
| ADLDSLockoutThreshold      | 5      | This entry holds the number of unsuccessful login attempts after which a user’s account must be locked.  
**Note:** This entry is applicable only for the Microsoft AD LDS target system. |
| AlwaysUseObjectGUID         | yes    | This entry specifies whether the GUID of an object must be used for searching records during reconciliation.  
**Note:** Do not change the value of this entry.                              |
| Bundle Name                 | ActiveDirectory.Connector | This entry holds the name of the connector bundle package. Do not modify this entry.                                                             |
| Bundle Version              | 1.1.0.6380 | This entry holds the version of the connector bundle class. Do not modify this entry.                                                       |
| Connector Name              | Org.IdentityConnectors.ActiveDirectory.ActiveDirectoryConnector | This entry holds the name of the connector class. Do not modify this entry.                                                                       |
| CreateHomeDirectory         | yes    | This entry holds information whether a home directory must be created.  
Enter yes if you want the connector to create a home directory for user accounts. Otherwise, enter no. |
| Group Configuration Lookup  | Lookup.ActiveDirectory.Group.Configuration | This entry holds the name of the lookup definition that contains group-specific configuration properties. Do not modify this entry. |
| NativeGuidConvention        | true   | This entry specifies whether GUID is stored in its native format. This entry is used by the connector internally.  
**Note:** Do not change the value of this entry.                              |
| ObjectClass                 | User   | This entry holds the name of the object class to which newly created users on the target system are assigned.  
If you create a custom object class, then specify the name of that object class. For example, InetOrgPerson. |
| organizationalUnit          | Lookup.ActiveDirectory.Group.Configuration | This entry holds the name of the lookup definition that contains organization-specific configuration properties.  
This lookup definition is used as the configuration lookup definition when you perform reconciliation of organizational units.  
**Do not modify this entry.** |

Chapter 1  Lookup Definitions Used During Reconciliation and Provisioning
<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PageSize</td>
<td>1000</td>
<td>This entry holds the page size of records fetched 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. 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 the more expensive operation for simple searches. While it is possible to specify a PageSize greater than the MaxPageSize of the target system, the Active Directory server will ignore it and use the MaxPageSize instead. No exception will be generated in this case. 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.</td>
</tr>
<tr>
<td>Recon Date Format</td>
<td>yyyyMMddHHmmss.0Z</td>
<td>This entry holds the format in which the last reconciliation run timing must be displayed.</td>
</tr>
<tr>
<td>SearchChildDomains</td>
<td>no</td>
<td>This entry determines the search scope of users, groups, or organizational units within the domain name specified as the value of the DomainName attribute. Enter no 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 parameter of the IT resource. Note that records are fetched from the domain controller specified as the value of the SyncDomainController parameter of the IT Resource. Enter yes 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 SyncGlobalCatalogServer parameter of the IT Resource. <strong>Note:</strong> If you enter yes, then do not enter a value for LDAPHostName parameter of the IT resource. The connector will automatically find the right domain controller to fetch complete user information after obtaining the distinguished name from the global catalog server.</td>
</tr>
</tbody>
</table>
Table 1-3  (Cont.) Entries in the Lookup.Configuration.ActiveDirectory Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseDeleteTreeForAccounts</td>
<td>false</td>
<td>This entry specifies whether the associated leaf nodes of an <strong>ACCOUNT</strong> object to be deleted are to be removed along with the object. If the value of this entry is not true and the <strong>ACCOUNT</strong> object to be deleted has leaf nodes, then the operation fails and an error message is displayed. If you set the value of this entry to false, then the <strong>ACCOUNT</strong> objects are removed from the child list of its parent only. Otherwise, regardless of the object class, the whole tree is removed recursively.</td>
</tr>
</tbody>
</table>

User Configuration Lookup
Lookup.ActiveDirectory.U M.Configuration
This entry holds the name of the lookup definition that contains user-specific configuration properties. Do not modify this entry.

1.7.2.2 Lookup.Configuration.ActiveDirectory.Trusted

The Lookup.Configuration.ActiveDirectory.Trusted lookup definition holds connector configuration entries that are used during trusted source reconciliation.

Table 1-4 lists the default entries in this lookup definition.

Table 1-4  Entries in the Lookup.Configuration.ActiveDirectory.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADLDSLockoutThreshold</td>
<td>5</td>
<td>This entry holds the number of unsuccessful login attempts after which a user’s account must be locked. <strong>Note:</strong> This entry is applicable only for the Microsoft AD LDS target system.</td>
</tr>
<tr>
<td>AlwaysUseObjectGUID</td>
<td>yes</td>
<td>This entry specifies whether the GUID of an object must be used for searching records during reconciliation. If the object class is of a non-account type and if you set the value of this entry to no, then the DN of the non-account object is used as the UID instead of GUID.</td>
</tr>
<tr>
<td>Bundle Name</td>
<td>ActiveDirectory.Connector</td>
<td>This entry holds the name of the connector bundle package. Do not modify this entry.</td>
</tr>
<tr>
<td>Bundle Version</td>
<td>1.1.0.6380</td>
<td>This entry holds the version of the connector bundle class. Do not modify this entry.</td>
</tr>
<tr>
<td>Connector Name</td>
<td>Org.IdentityConnectors.Act iveDirectory.ActiveDirector yConnector</td>
<td>This entry holds the name of the connector class. Do not modify this entry.</td>
</tr>
<tr>
<td>MaintainHierarchy</td>
<td>no</td>
<td>Enter yes to specify that you want to maintain in Oracle Identity Manager the same organization hierarchy that is maintained on the target system. Otherwise, enter no.</td>
</tr>
<tr>
<td>NativeGuidConvention</td>
<td>true</td>
<td>This entry specifies whether GUID is stored in its native format. This entry is used by the connector internally. <strong>Note:</strong> Do not change the value of this entry.</td>
</tr>
</tbody>
</table>
Table 1-4  (Cont.) Entries in the Lookup.Configuration.ActiveDirectory.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ObjectClass</td>
<td>User</td>
<td>This entry holds the name of the object class to which newly created users on the target system are assigned. If you create a custom object class, then specify the name of that object class. For example, InetOrgPerson.</td>
</tr>
<tr>
<td>organizationalUnit</td>
<td>Lookup.ActiveDirectory.OM.Configuration.Trusted</td>
<td>This entry holds the name of the lookup definition that contains organization-specific configuration properties. This lookup definition is used as the configuration lookup definition when you perform reconciliation of organizational units. Do not modify this entry.</td>
</tr>
<tr>
<td>PageSize</td>
<td>1000</td>
<td>This entry holds the page size of records fetched 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. 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 the more expensive operation for simple searches. While it is possible to specify a PageSize greater than the MaxPageSize of the target system, the Active Directory server will ignore it and use the MaxPageSize instead. No exception will be generated in this case. 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.</td>
</tr>
<tr>
<td>Recon Date Format</td>
<td>yyyyMMddHHmmss.0Z</td>
<td>This entry holds the format in which the last reconciliation run timing must be displayed.</td>
</tr>
<tr>
<td>SearchChildDomains</td>
<td>no</td>
<td>This entry determines the search scope of users, groups, or organizational units within the domain name specified as the value of the DomainName attribute. Enter no 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 records are fetched from the domain controller specified as the value of the SyncDomainController parameter of the IT Resource. Enter yes 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 SyncGlobalCatalogServer parameter of the IT resource.</td>
</tr>
<tr>
<td>User Configuration Lookup</td>
<td>Lookup.ActiveDirectory.UM.Configuration.Trusted</td>
<td>This entry holds the name of the lookup definition that contains user-specific configuration properties. Do not modify this entry.</td>
</tr>
</tbody>
</table>
1.7.2.3 Preconfigured Lookup Definitions for User Operations

This section discusses the following lookup definitions for user operations:

- Lookup.ActiveDirectory.UM.Configuration
- Lookup.ActiveDirectory.UM.Configuration.Trusted
- Lookup.ActiveDirectory.UM.ProvAttrMap
- Lookup.ActiveDirectory.UM.ReconAttrMap
- Lookup.ActiveDirectory.UM.ProvValidation
- Lookup.ActiveDirectory.UM.ReconTransformation
- Lookup.ActiveDirectory.UM.ReconValidation

1.7.2.3.1 Lookup.ActiveDirectory.UM.Configuration

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

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

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Attribute Map</td>
<td>Lookup.ActiveDirectory.UM.ProvAttrMap</td>
<td>This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.ActiveDirectory.UM.ProvAttrMap for more information about this lookup definition.</td>
</tr>
<tr>
<td>Provisioning Validation</td>
<td>Lookup.ActiveDirectory.UM.ProvValidation</td>
<td>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 Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.</td>
</tr>
<tr>
<td>Recon Attribute Map</td>
<td>Lookup.ActiveDirectory.UM.ReconAttrMap</td>
<td>This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.ActiveDirectory.UM.ReconAttrMap for more information about this lookup definition.</td>
</tr>
<tr>
<td>Recon Transformation Lookup</td>
<td>Lookup.ActiveDirectory.UM.ReconTransformation</td>
<td>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 Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition.</td>
</tr>
</tbody>
</table>
Table 1-5 (Cont.) Entries in the Lookup.ActiveDirectory.UM.Configuration Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recon Validation Lookup</td>
<td>Lookup.ActiveDirectory.UM.ReconValidation</td>
<td>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 Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.</td>
</tr>
</tbody>
</table>

1.7.2.3.2 Lookup.ActiveDirectory.UM.Configuration.Trusted

The Lookup.ActiveDirectory.UM.Configuration.Trusted lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during trusted source user reconciliation runs.

Table 1-6 lists the default entries in this lookup definition.

Table 1-6 Entries in the Lookup.ActiveDirectory.UM.Configuration.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recon Attribute Map</td>
<td>Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted</td>
<td>This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.ActiveDirectory.UM.ReconAttrMap for more information about this lookup definition.</td>
</tr>
</tbody>
</table>

1.7.2.3.3 Lookup.ActiveDirectory.UM.ProvAttrMap

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

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

Table 1-7 Default Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Code key (Process Form Field)</th>
<th>Decode (Target System Field)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager Name</td>
<td>manager</td>
<td>Manager name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must enter the manager name in the DN format. For example: cn=abc,ou=lmn,dc=corp,dc=com</td>
</tr>
<tr>
<td>Code key (Process Form Field)</td>
<td>Decode (Target System Field)</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Terminal Home Directory</td>
<td>TerminalServicesHomeDirectory</td>
<td>Full path of the home directory for the Terminal Server userSample value: c:\MyDirectory During a provisioning operation, you must enter the full, absolute path of the home directory, as shown in the sample value.</td>
</tr>
<tr>
<td>UD_ADUSRC~Group Name[Lookup]</td>
<td><strong>GROUPS</strong></td>
<td>Group name</td>
</tr>
<tr>
<td>Terminal Profile Path</td>
<td>TerminalServicesProfilePath</td>
<td>Profile that is used when the user logs on to a Terminal Server The profile can be roaming or mandatory. A roaming profile remains the same, regardless of the computer from which the user logs in. The user can make changes to a roaming profile, but not to a mandatory profile. Any changes a user makes while logged in with a mandatory profile are retained only for that Terminal Services session. The changes are lost when the user starts another Terminal Services session.</td>
</tr>
<tr>
<td>Account Expiration Date[DATE]</td>
<td><strong>PASSWORD_EXPIRATION_DATE</strong></td>
<td>Date when the account expires</td>
</tr>
<tr>
<td>Street</td>
<td>streetAddress</td>
<td>Street address</td>
</tr>
<tr>
<td>Zip</td>
<td>postalCode</td>
<td>ZIP code</td>
</tr>
<tr>
<td>Middle Name</td>
<td>middleName</td>
<td>Initials for the user’s middle name</td>
</tr>
<tr>
<td>User Must Change Password At Next Logon</td>
<td><strong>PASSWORD_EXPIRED</strong></td>
<td>Flag that indicates whether or not the user must change the password at next logon. If the value is yes (check box is selected), then the user must change the password at next logon.</td>
</tr>
<tr>
<td>Office</td>
<td>physicalDeliveryofficeName</td>
<td>Office Location</td>
</tr>
<tr>
<td>Home Phone</td>
<td>homePhone</td>
<td>Home phone number</td>
</tr>
<tr>
<td>City</td>
<td>I</td>
<td>City</td>
</tr>
<tr>
<td>Code key (Process Form Field)</td>
<td>Decode (Target System Field)</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Account is Locked out This is a check box</td>
<td><em>LOCK_OUT</em></td>
<td>Specifies whether the user account must be locked or unlocked</td>
</tr>
<tr>
<td>Last Name This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the Last Name field on the process form is prepopulated with the value entered in the Last Name field on</td>
<td>sn</td>
<td>Last name</td>
</tr>
<tr>
<td>IP Phone</td>
<td>ipPhone</td>
<td>IP phone number</td>
</tr>
<tr>
<td>Mobile</td>
<td>mobile</td>
<td>Mobile number</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>telephoneNumber</td>
<td>Telephone number</td>
</tr>
<tr>
<td>State</td>
<td>st</td>
<td>State</td>
</tr>
<tr>
<td>Fax</td>
<td>facsimileTelephoneNumber</td>
<td>Fax number</td>
</tr>
<tr>
<td>First Name This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the First Name field on the process form is prepopulated with the value entered in the First Name field on the OIM User form.</td>
<td>givenName</td>
<td>First name</td>
</tr>
<tr>
<td>Password This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the Password field on the process form is prepopulated with the value entered in the Password field on the OIM User form. If SSL is configured between Oracle Identity Manager and the target system, then the Password field on the process form is a mandatory field.</td>
<td><em>PASSWORD</em></td>
<td>User's password in UTF-8 format</td>
</tr>
</tbody>
</table>

This connector uses ADSI to set the password of the user. It uses the IADsUser#SetPassword API. This API sets the user's unicodePwd attribute. See the following URL for more information: [http://msdn.microsoft.com/en-us/library/ms677943(v=vs.85).aspx#unicodepwd](http://msdn.microsoft.com/en-us/library/ms677943(v=vs.85).aspx#unicodepwd)
### Table 1-7 (Cont.) Default Entries in the Lookup.ActiveDirectory.UMProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Code key (Process Form Field)</th>
<th>Decode (Target System Field)</th>
<th>Description</th>
</tr>
</thead>
</table>
| Full Name                     | displayName                   | Display name for a user  
During a Create User provisioning operation, the `cn` and `displayName` fields are populated with a combination of the user's first name, middle initial, and last name entered on the OIM User form.  
The full name is displayed in the following format on the process form:  
`FIRSTNAME MIDDLE_INITIAL. LASTNAME`  
For example: John M. Doe  
If the middle initial is not entered, then the name is displayed as, for example, John Doe.  
During an Update provisioning operation, only the value in the `displayName` field is updated. |
| Redirection Mail Id           | ___MAILREDIRECTION__           | E-mail address to which e-mail sent to the user must be redirected  
This e-mail address overrides the one set in the E Mail field. |
| ___NAME___                    | NAME_="CN=$ (Common_Name),$ (Organization_Name)" | User name with full DN |
| Password Not Required         | PasswordNotRequired            | Specifies whether or not Password is required. If it is true, then there is no need to specify the password. If it is false, then password is required. |
| Terminal Allow Login          | AllowLogon                    | Specifies whether or not the user is permitted to log on to the Terminal Server |
| Country                       | c                             | Country |
| User Id                       | sAMAccountName                | User’s logon name  
This field is on both the process form and the OIM User form. It is a mandatory field.  
During a provisioning operation, the User ID field on the process form is prepopulated with the value entered in the User  
This field does not exist in Microsoft ADAM and AD LDS. |
| Pager                         | pager                         | Pager number |
| Organization Name[LOOKUP,IGNORE] | IGNORED                     | Name of the organization |
Table 1-7  (Cont.) Default Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Code key (Process Form Field)</th>
<th>Decode (Target System Field)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
<td>Object GUID of the user</td>
</tr>
<tr>
<td>E Mail</td>
<td>mail</td>
<td>Email address</td>
</tr>
<tr>
<td>Common Name[IGNORE]</td>
<td>IGNORED</td>
<td>Common name of the user</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
<td>Title</td>
</tr>
<tr>
<td>Company</td>
<td>company</td>
<td>Company</td>
</tr>
<tr>
<td>Password Never Expires</td>
<td>PasswordNeverExpires</td>
<td>Flag that controls the Password Never Expires property</td>
</tr>
<tr>
<td>Department</td>
<td>department</td>
<td>Department</td>
</tr>
<tr>
<td>User Principal Name</td>
<td>userPrincipalName</td>
<td>The user principal name is the domain-specific name of the user. This field is pre-populated on the Administrative and User Console. The format is as follows: USER_ID_VALUE@UPN_DOMAIN_VALUE</td>
</tr>
<tr>
<td>Homedirectory</td>
<td>homeDirectory</td>
<td>Home directory of the user</td>
</tr>
<tr>
<td>Post Office Box</td>
<td>postOfficeBox</td>
<td>Post-office box</td>
</tr>
</tbody>
</table>

1.7.2.3.4 Lookup.ActiveDirectory.UM.ReconAttrMap

The Lookup.ActiveDirectory.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is preconfigured and is used during target resource reconciliation.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

Table 1-8  Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Code Key (Resource Object Field)</th>
<th>Decode (Target System Field)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>department</td>
<td>Department</td>
</tr>
</tbody>
</table>
Table 1-8  (Cont.) Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Code Key (Resource Object Field)</th>
<th>Decode (Target System Field)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>displayName</td>
<td>Full name</td>
</tr>
<tr>
<td>Terminal Home Directory</td>
<td>TerminalServicesHomeDirectory</td>
<td>Full path of the home directory for the Terminal Server user. This field does not exist in Microsoft AD LDS. <strong>Note:</strong> Reconciliation of values in this field is enabled by the Remote Manager.</td>
</tr>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
<td>GUID of each user on the target system</td>
</tr>
<tr>
<td>Mobile</td>
<td>mobile</td>
<td>Mobile number</td>
</tr>
<tr>
<td>Terminal Profile Path</td>
<td>TerminalServicesProfilePath</td>
<td>Profile that is used when the user logs on to a Terminal Server. This field does not exist in Microsoft AD LDS. The profile can be roaming or mandatory. A roaming profile remains the same, regardless of the computer from which the user logs in. The user can make changes to a roaming profile, but not to a mandatory profile. Any changes a user makes while logged in with a mandatory profile are retained only for that Terminal Services session. Changes are lost when the user starts another Terminal Services session.</td>
</tr>
<tr>
<td>Home Phone</td>
<td>homePhone</td>
<td>Home phone number</td>
</tr>
<tr>
<td>Company</td>
<td>company</td>
<td>Company</td>
</tr>
<tr>
<td>Account is Locked out</td>
<td><strong>LOCK_OUT</strong></td>
<td>Specifies whether the user account must be locked or unlocked.</td>
</tr>
<tr>
<td>Middle Name</td>
<td>middleName</td>
<td>Initials for the user's middle name</td>
</tr>
<tr>
<td>Organization Name[LOOKUP]</td>
<td>ad_container</td>
<td>Organization name on the target system</td>
</tr>
<tr>
<td>IP Phone</td>
<td>ipPhone</td>
<td>IP phone number</td>
</tr>
<tr>
<td>Common Name</td>
<td>cn</td>
<td>Common name on the target system. You can change the value of this field.</td>
</tr>
<tr>
<td>State</td>
<td>st</td>
<td>State</td>
</tr>
<tr>
<td>Country</td>
<td>c</td>
<td>Country</td>
</tr>
<tr>
<td>Street</td>
<td>streetAddress</td>
<td>Street address</td>
</tr>
<tr>
<td>City</td>
<td>l</td>
<td>City</td>
</tr>
<tr>
<td>User Principal Name</td>
<td>userPrincipalName</td>
<td>The user principal name is the domain-specific name of the user. This is a mandatory field.</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Last name</td>
</tr>
<tr>
<td>E Mail</td>
<td>mail</td>
<td>Email address</td>
</tr>
<tr>
<td>User Must Change Password At Next Logon</td>
<td><strong>PASSWORD_EXPIRED</strong></td>
<td>Flag that indicates whether or not the user must change the password at next logon. If the value is yes (check box is selected), then the user must change the password at next logon.</td>
</tr>
</tbody>
</table>
Table 1-8  (Cont.) Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Code Key (Resource Object Field)</th>
<th>Decode (Target System Field)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax</td>
<td>facsimileTelephoneNumber</td>
<td>Fax number</td>
</tr>
<tr>
<td>Homedirectory</td>
<td>homeDirectory</td>
<td>Home directory for each user on the target system.</td>
</tr>
<tr>
<td>Manager Name</td>
<td>manager</td>
<td>Manager name</td>
</tr>
<tr>
<td>Password Never Expires</td>
<td>PasswordNeverExpires</td>
<td>Flag that controls the Password Never Expires property</td>
</tr>
<tr>
<td>Terminal Allow Login</td>
<td>AllowLogon</td>
<td>Specifies whether or not the user is permitted to log on to the Terminal Server</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
<td>First name</td>
</tr>
<tr>
<td>Pager</td>
<td>pager</td>
<td>Pager number</td>
</tr>
<tr>
<td>Account Expiration Date[DATE]</td>
<td><strong>PASSWORD_EXPIRATION_DATE</strong></td>
<td>Date when the account expires</td>
</tr>
<tr>
<td>Office</td>
<td>physicalDeliveryofficeName</td>
<td>Office location</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>telephoneNumber</td>
<td>Telephone number</td>
</tr>
<tr>
<td>Post Office Box</td>
<td>postOfficeBox</td>
<td>Post-office box</td>
</tr>
<tr>
<td>User Id</td>
<td>sAMAccountName</td>
<td>User's logon name</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
<td>Title</td>
</tr>
<tr>
<td>Status</td>
<td><strong>ENABLE</strong></td>
<td>The value that controls the account is enabled or disabled</td>
</tr>
</tbody>
</table>

1.7.2.3.5 Lookup.ActiveDirectory.UM.ProvValidation

The Lookup.ActiveDirectory.UM.ProvValidation lookup definition is used to configure validation of attribute values entered on the process form during provisioning operations. See Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.

1.7.2.3.6 Lookup.ActiveDirectory.UM.ReconTransformation

The Lookup.ActiveDirectory.UM.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 more information about adding entries in this lookup definition.
1.7.2.3.7 Lookup.ActiveDirectory.UM.ReconValidation

The Lookup.ActiveDirectory.UM.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 more information about adding entries in this lookup definition.

1.7.2.3.8 Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted

The Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is preconfigured and used during trusted source user reconciliation runs.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

Table 1-9   Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>Code Key (OIM User Form Field)</th>
<th>Decode (Target System Field)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E Mail</td>
<td>mail</td>
<td>Email address</td>
</tr>
<tr>
<td>Employee Type</td>
<td>OIM Employee Type</td>
<td>Employee type of the OIM User</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
<td>First name</td>
</tr>
<tr>
<td>This is a mandatory field.</td>
<td>This is a mandatory field.</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Last name</td>
</tr>
<tr>
<td>This is a mandatory field.</td>
<td>sn</td>
<td>For a record fetched during trusted source reconciliation, if there is no value in this attribute, then the value from the Common Name attribute is populated in the Last Name field on the process form.</td>
</tr>
<tr>
<td>Manager ID</td>
<td>Manager Id</td>
<td>Manager name</td>
</tr>
<tr>
<td>Middle Name</td>
<td>middleName</td>
<td>Middle name</td>
</tr>
<tr>
<td>objectGUID</td>
<td><strong>UID</strong></td>
<td>Object GUID of each user on the target system</td>
</tr>
<tr>
<td>Organization</td>
<td><strong>PARENTCN</strong></td>
<td>This is the name of the organization to which users belong if you set the value of the MaintainHierarchy entry of the Lookup.Configuration.ActiveDirectory.Trusted lookup definition to yes. See Lookup.Configuration.ActiveDirectory.Trusted for more information. If Maintain Hierarchy is set to no, then the default organization in Oracle Identity Manager, Xellerate Users, is used.</td>
</tr>
<tr>
<td>TrustedStatus[TRUSTED]</td>
<td><strong>ENABLE</strong></td>
<td>This field stores the status of the user account.</td>
</tr>
</tbody>
</table>
Table 1-9 (Cont.) Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>Code Key (OIM User Form Field)</th>
<th>Decode (Target System Field)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Id</td>
<td>sAMAccountName</td>
<td>User’s logon name</td>
</tr>
<tr>
<td>User Type</td>
<td>OIM User Type</td>
<td>Type of the OIM User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Values can be one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Full-Time Employee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Contractor</td>
</tr>
</tbody>
</table>

1.7.2.3.9 Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted.Defaults

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

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

- **Code Key**: Name of the reconciliation field of the AD User resource object
- **Decode**: Corresponding default value to be displayed

For example, assume a field named Preferred Language is a mandatory field on the OIM User form. Suppose the target system contains no field that stores information about the preferred language of communication for a user account. During reconciliation, no value for the Preferred Language field is fetched from the target system. However, as the Preferred Language 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 Preferred Language and Decode value set to English. This implies that the value of the Preferred Language field on the OIM User form displays English for all user accounts reconciled from the target system.

1.7.2.4 Preconfigured Lookup Definitions for Group Operations

This section discussed the following lookup definitions for group operations:

- 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.GroupTypes
1.7.2.4.1 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 1-5 lists the default entries in this lookup definition.

Table 1-10 Entries in the Lookup.ActiveDirectory.GM.Configuration Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Attribute Map</td>
<td>Lookup.ActiveDirectory.GM.ProvAttrMap</td>
<td>This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.ActiveDirectory.GM.ProvAttrMap for more information about this lookup definition.</td>
</tr>
<tr>
<td>Provisioning Validation Lookup</td>
<td>Lookup.ActiveDirectory.GM.ProvValidation</td>
<td>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 Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.</td>
</tr>
<tr>
<td>Recon Attribute Defaults</td>
<td>Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults</td>
<td>This entry holds the name of the lookup definition that maps fields on the group form and their default values. See Lookup.ActiveDirectory.GM.ReconAttrMap.Defaults for more information about this lookup definition.</td>
</tr>
<tr>
<td>Recon Attribute Map</td>
<td>Lookup.ActiveDirectory.GM.ReconAttrMap</td>
<td>This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.ActiveDirectory.GM.ReconAttrMap for more information about this lookup definition.</td>
</tr>
<tr>
<td>Recon Transformation Lookup</td>
<td>Lookup.ActiveDirectory.GM.ReconTransformation</td>
<td>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 Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition.</td>
</tr>
<tr>
<td>Recon Validation Lookup</td>
<td>Lookup.ActiveDirectory.GM.ReconValidation</td>
<td>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 Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.</td>
</tr>
</tbody>
</table>

1.7.2.4.2 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. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.
Table 1-11 Default Entries in the Lookup.ActiveDirectory.GM.ProvAttrMap

<table>
<thead>
<tr>
<th>Group Field on Oracle Identity Manager</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAME</strong></td>
<td><strong>NAME</strong>=&quot;CN=${Group_Name},${Organization_Name}&quot;</td>
<td>Group name with full DN</td>
</tr>
<tr>
<td>Display Name</td>
<td>displayName</td>
<td>Display name for a group</td>
</tr>
<tr>
<td>Group Name</td>
<td>sAMAccountName</td>
<td>Group name</td>
</tr>
<tr>
<td>Group Type</td>
<td>groupType</td>
<td>Group type</td>
</tr>
<tr>
<td>Organization Name[LOOKUP,IGNORE]</td>
<td>IGNORED</td>
<td>Name of the organization to which the group belongs</td>
</tr>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
<td>Object GUID of the group</td>
</tr>
</tbody>
</table>

1.7.2.4.3 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 used during reconciliation. This lookup definition is preconfigured. Table 1-15 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

1.7.2.4.4 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 or more information about adding entries in this lookup definition.

1.7.2.4.5 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 more information about adding entries in this lookup definition.

1.7.2.4.6 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 more information about adding entries in this lookup definition.

1.7.2.4.7 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.

1.7.2.4.8 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 Manager. 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

1.7.2.5 Preconfigured Lookup Definitions for Organizational Unit Operations

This section discusses the following lookup definitions for organizational unit operations:

- 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

1.7.2.5.1 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 1-5 lists the default entries in this lookup definition.

### Table 1-12 Entries in the Lookup.ActiveDirectory.OM.Configuration Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Attribute Map</td>
<td>Lookup.ActiveDirectory.OM.ProvAttrMap</td>
<td>This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.ActiveDirectory.OM.ProvAttrMap for more information about this lookup definition.</td>
</tr>
<tr>
<td>Provisioning Validation</td>
<td>Lookup.ActiveDirectory.OM.ProvValidation</td>
<td>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 Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.</td>
</tr>
<tr>
<td>Recon Attribute Defaults</td>
<td>Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults</td>
<td>This entry holds the name of the lookup definition that maps fields on the organizational unit form and their default values. See Lookup.ActiveDirectory.OM.ReconAttrMap.Defaults for more information about this lookup definition.</td>
</tr>
<tr>
<td>Recon Attribute Map</td>
<td>Lookup.ActiveDirectory.OM.ReconAttrMap</td>
<td>This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.ActiveDirectory.OM.ReconAttrMap for more information about this lookup definition.</td>
</tr>
<tr>
<td>Recon Transformation Lookup</td>
<td>Lookup.ActiveDirectory.OM.ReconTransformation</td>
<td>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 Configuring Transformation of Data During Reconciliation for more information about adding entries in this lookup definition.</td>
</tr>
<tr>
<td>Recon Validation Lookup</td>
<td>Lookup.ActiveDirectory.OM.ReconValidation</td>
<td>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 Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.</td>
</tr>
</tbody>
</table>

1.7.2.5.2 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 1-13 lists the default entries in this lookup definition.
### Table 1-13 Entries in the Lookup.ActiveDirectory.OM.Configuration.Trusted Lookup Definition

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

### 1.7.2.5.3 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 used during provisioning. This lookup definition is preconfigured. Table 1-21 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

### 1.7.2.5.4 Lookup.ActiveDirectory.OM.ReconAttrMap

The Lookup.ActiveDirectory.OM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definitions is used during reconciliation of organizational units. This lookup definition is preconfigured. Table 1-16 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

### 1.7.2.5.5 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 more information about adding entries in this lookup definition.

### 1.7.2.5.6 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 more information about adding entries in this lookup definition.
1.7.2.5.7 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 more information about adding entries in this lookup definition.

1.7.2.5.8 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 used during trusted source reconciliation runs for organizational units. This lookup definition is preconfigured. Table 1-23 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

1.7.2.5.9 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.

1.7.2.6 Preconfigured Lookup Definitions for AD LDS

This section discusses the following lookup definitions for AD LDS:

- Lookup.ActiveDirectoryLDS.UM.ProvAttrMap
- Lookup.ActiveDirectoryLDS.UM.ReconAttrMap
- Lookup.ActiveDirectoryLDS.GM.ProvAttrMap
•  Lookup.ActiveDirectoryLDS.GM.ReconAttrMap

1.7.2.6.1 Lookup.ActiveDirectoryLDS.UM.ProvAttrMap

The Lookup.ActiveDirectoryLDS.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes for AD LDS. This lookup definition is used during provisioning. This lookup definition is preconfigured.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

1.7.2.6.2 Lookup.ActiveDirectoryLDS.UM.ReconAttrMap

The Lookup.ActiveDirectoryLDS.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes for AD LDS. This lookup definition is used during reconciliation. This lookup definition is preconfigured.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

1.7.2.6.3 Lookup.ActiveDirectoryLDS.UM.ReconAttrMap.Trusted

The Lookup.ActiveDirectoryLDS.UM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes for AD LDS. This lookup definitions is used during trusted source user reconciliation runs. This lookup definition is preconfigured.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

1.7.2.6.4 Lookup.ActiveDirectoryLDS.GM.ProvAttrMap

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

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.

1.7.2.6.5 Lookup.ActiveDirectoryLDS.GM.ReconAttrMap

The Lookup.ActiveDirectoryLDS.GM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes for AD LDS. This lookup definition is used during reconciliation of groups. This lookup definition is preconfigured.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Extending the Functionality of the Microsoft Active Directory User Management Connector for more information.
1.8 Connector Objects Used During Target Resource Reconciliation

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

The Active Directory User Target Recon scheduled job is used to initiate a target resource reconciliation run. This scheduled task is discussed in Scheduled Jobs for Reconciliation of User Records.

See Also:
Managing Reconciliation in Performing Self Service Tasks with Oracle Identity Manager for conceptual information about reconciliation

This section discusses the following topics:

- User Fields for Target Resource Reconciliation
- Group Fields for Reconciliation
- Organizational Unit Fields for Reconciliation
- Reconciliation Rules for Target Resource Reconciliation
- Viewing Reconciliation Rules for Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation
- Viewing Reconciliation Action Rules for Target Resource Reconciliation

1.8.1 User Fields for Target Resource Reconciliation

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

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

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

Table 1-14 lists the entries in this lookup definition.

<table>
<thead>
<tr>
<th>Resource Object Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>department</td>
<td>Department</td>
</tr>
<tr>
<td>Full Name</td>
<td>displayName</td>
<td>Full name</td>
</tr>
</tbody>
</table>
Table 1-14  (Cont.) Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Resource Object Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Home Directory</td>
<td>TerminalServicesHomeDirectory</td>
<td>Full path of the home directory for the Terminal Server user. <strong>Note:</strong> Reconciliation of values in this field is enabled by the Remote Manager.</td>
</tr>
<tr>
<td>This is a string data type field.</td>
<td>This field does not exist in Microsoft AD LDS.</td>
<td></td>
</tr>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
<td>GUID of each user on the target system.</td>
</tr>
<tr>
<td>Mobile</td>
<td>mobile</td>
<td>Mobile number.</td>
</tr>
<tr>
<td>Terminal Profile Path</td>
<td>TerminalServicesProfilePath</td>
<td>Profile that is used when the user logs on to a Terminal Server. The profile can be roaming or mandatory. A roaming profile remains the same, regardless of the computer from which the user logs in. The user can make changes to a roaming profile, but not to a mandatory profile. Any changes a user makes while logged in with a mandatory profile are retained only for that Terminal Services session. Changes are lost when the user starts another Terminal Services session.</td>
</tr>
<tr>
<td>This is a string data type field.</td>
<td>This field does not exist in Microsoft AD LDS.</td>
<td></td>
</tr>
<tr>
<td>Home Phone</td>
<td>homePhone</td>
<td>Home phone number.</td>
</tr>
<tr>
<td>Company</td>
<td>company</td>
<td>Company.</td>
</tr>
<tr>
<td>Account is Locked out</td>
<td><strong>LOCK_OUT</strong></td>
<td>Specifies whether the user account must be locked or unlocked.</td>
</tr>
<tr>
<td>This is a check box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middle Name</td>
<td>middleName</td>
<td>Initials for the user's middle name.</td>
</tr>
<tr>
<td>Organization Name[LOOKUP]</td>
<td>ad_container</td>
<td>Organization name on the target system.</td>
</tr>
<tr>
<td>IP Phone</td>
<td>ipPhone</td>
<td>IP phone number.</td>
</tr>
<tr>
<td>Common Name</td>
<td>cn</td>
<td>Common name on the target system. You can change the value of this field.</td>
</tr>
<tr>
<td>This is a mandatory field.</td>
<td>This is a mandatory field.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>st</td>
<td>State.</td>
</tr>
<tr>
<td>Country</td>
<td>c</td>
<td>Country.</td>
</tr>
<tr>
<td>Street</td>
<td>streetAddress</td>
<td>Street address.</td>
</tr>
<tr>
<td>City</td>
<td>l</td>
<td>City.</td>
</tr>
<tr>
<td>User Principal Name</td>
<td>userPrincipalName</td>
<td>The user principal name is the domain-specific name of the user.</td>
</tr>
<tr>
<td>This is a mandatory field.</td>
<td>This is a mandatory field.</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Last name.</td>
</tr>
<tr>
<td>This is a mandatory field.</td>
<td>This is a mandatory field.</td>
<td></td>
</tr>
<tr>
<td>E Mail</td>
<td>mail</td>
<td>Email address.</td>
</tr>
<tr>
<td>User Must Change Password At Next Logon</td>
<td><strong>PASSWORD_EXPIRED</strong></td>
<td>Flag that indicates whether or not the user must change the password at next logon. If the value is yes (check box is selected), then the user must change the password at next logon.</td>
</tr>
<tr>
<td>This is a check box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fax</td>
<td>facsimileTelephoneNumber</td>
<td>Fax number.</td>
</tr>
</tbody>
</table>
### Table 1-14  (Cont.) Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Resource Object Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homedirectory</td>
<td>homeDirectory</td>
<td>Home directory for each user on the target system.</td>
</tr>
<tr>
<td>Manager Name</td>
<td>manager</td>
<td>Manager name</td>
</tr>
<tr>
<td>Password Never Expires</td>
<td>PasswordNeverExpires</td>
<td>Flag that controls the Password Never Expires property</td>
</tr>
<tr>
<td>Terminal Allow Login</td>
<td>AllowLogon</td>
<td>Specifies whether or not the user is permitted to log on to the Terminal Server</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
<td>First name</td>
</tr>
<tr>
<td>Pager</td>
<td>pager</td>
<td>Pager number</td>
</tr>
<tr>
<td>Account Expiration</td>
<td><strong>PASSWORD_EXPIRATION_DATE</strong></td>
<td>Date when the account expires</td>
</tr>
<tr>
<td>Office</td>
<td>physicalDeliveryOfficeName</td>
<td>Office location</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>telephoneNumber</td>
<td>Telephone number</td>
</tr>
<tr>
<td>Post Office Box</td>
<td>postOfficeBox</td>
<td>Post-office box</td>
</tr>
<tr>
<td>User Id</td>
<td>sAMAccountName</td>
<td>User's logon name</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
<td>Title</td>
</tr>
<tr>
<td>Status</td>
<td><strong>ENABLE</strong></td>
<td>The value that controls the account is enabled or disabled</td>
</tr>
</tbody>
</table>

#### 1.8.2 Group Fields for Reconciliation

The Lookup.ActiveDirectory.GM.ReconAttrMap lookup definition maps user resource object fields and target system attributes. This lookup definition is used for performing target resource group reconciliation runs.

Table 1-15 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.

### Table 1-15  Entries in the Lookup.ActiveDirectory.GM.ReconAttrMap

<table>
<thead>
<tr>
<th>Group Field on Oracle Identity Manager</th>
<th>Microsoft Active Directory Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>displayName</td>
<td>Display name for a group</td>
</tr>
<tr>
<td>Group name</td>
<td>sAMAccountName</td>
<td>Group name</td>
</tr>
</tbody>
</table>
Table 1-15  (Cont.) Entries in the Lookup.ActiveDirectory.GM.ReconAttrMap

<table>
<thead>
<tr>
<th>Group Field on Oracle Identity Manager</th>
<th>Microsoft Active Directory Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Type</td>
<td>groupType</td>
<td>Group type</td>
</tr>
<tr>
<td>OIM Org Name</td>
<td>sAMAccountName</td>
<td>OIM organization name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that this value does not contain the DN.</td>
</tr>
<tr>
<td>Organization Name[LOOKUP]</td>
<td>ad_container</td>
<td>Organization name with DN format</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, OU=Org1,DC=example,dc=com</td>
</tr>
<tr>
<td>Org Name</td>
<td>sAMAccountName</td>
<td>Organization name without DN format</td>
</tr>
<tr>
<td>Org Type</td>
<td>OIM Organization Type</td>
<td>Organization type</td>
</tr>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
<td>Object GUID of the group</td>
</tr>
</tbody>
</table>

1.8.3 Organizational Unit Fields for Reconciliation

The Lookup.ActiveDirectory.OM.ReconAttrMap lookup definition maps organization resource object fields and target system attributes. This lookup definition is used for performing target resource reconciliation runs for organizational units.

Table 1-16 lists the organizational unit fields of the target system from which values are fetched during reconciliation.

Table 1-16  Entries in the Lookup.ActiveDirectory.OM.ReconAttrMap

<table>
<thead>
<tr>
<th>Organization Field on Oracle Identity Manager</th>
<th>Microsoft Active Directory Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container[LOOKUP]</td>
<td>ad_container</td>
<td>Organization name with DN format For example, OU=Org1,DC=example,dc=com</td>
</tr>
<tr>
<td>Display Name</td>
<td>ou</td>
<td>Display name for an organizational unit</td>
</tr>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
<td>Object GUID of the organizational unit</td>
</tr>
</tbody>
</table>

1.8.4 Reconciliation Rules for Target Resource Reconciliation

See Also:

Reconciliation Engine in *Performing Self Service Tasks with Oracle Identity Manager* for generic information about reconciliation matching and action rules.

The following is the process matching rule:
Rule name: AD User Target Recon Rule

Rule element: (ObjectGUID Equals Unique Id) OR (User Login Equals User Id)

In the first rule component:
- ObjectGUID is the objectGUID of the resource assigned to the OIM User.
- Unique Id is the ID that uniquely identifies a user account. Unique Id is mapped to UID, which is the GUID value of the user account in the target system.

In the second rule component:
- User Login is the User ID field on the OIM User form.
- User Id is the sAMAccountName field of Microsoft Active Directory or the userPrincipalName field of Microsoft ADAM.

This rule supports the following scenarios:
- You can provision multiple Microsoft Active Directory resources to the same OIM User, either on Oracle Identity Manager or directly on the target system.
- You can change the user ID of a user on the target system.

This is illustrated by the following use cases:
- Use case 1: You provision an AD account for an OIM User, and you also create an account for the user directly on the target system.
  When the first rule condition is applied, no match is found. Then, the second rule condition is applied and it is determined that a second account has been given to the user on the target system. Details of this second account are associated with the OIM User by the reconciliation engine.
- Use case 2: An OIM User has an AD account. You then change the user ID of the user on the target system.
  During the next reconciliation run, application of the first rule condition helps match the resource with the record.

1.8.5 Viewing Reconciliation Rules for Target Resource Reconciliation

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

Note:
Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand Development Tools.
4. Search for Target Resource Recon Rule. Figure 1-2 shows the reconciliation rule for target resource reconciliation.
1.8.6 Reconciliation Action Rules for Target Resource Reconciliation

Table 1-17 lists the action rules for target resource reconciliation.

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Matches Found</td>
<td>Assign to Authorizer With Least Load</td>
</tr>
<tr>
<td>One Entity Match Found</td>
<td>Establish Link</td>
</tr>
<tr>
<td>One Process Match Found</td>
<td>Establish Link</td>
</tr>
</tbody>
</table>

**Note:**
No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about setting a reconciliation action rule, see

- Setting a Reconciliation Action Rule (Developing Identity Connectors using Java)
- Setting a Reconciliation Action Rule (Developing Identity Connectors using .net)

in *Developing and Customizing Applications for Oracle Identity Manager*.

1.8.7 Viewing Reconciliation Action Rules for Target Resource Reconciliation

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:
1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **AD User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1-3 shows the reconciliation action rule for target resource reconciliation.

**Figure 1-3 Reconciliation Action Rules for Target Resource Reconciliation**

1.9 Connector Objects Used During Provisioning

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

**See Also:**

Managing Provisioning Tasks in *Performing Self Service Tasks with Oracle Identity Manager* for conceptual information about provisioning.

The following topics are discussed:

- Provisioning Functions
- User Fields for Provisioning
- Group Fields for Provisioning
- Organizational Unit Fields for Provisioning

1.9.1 Provisioning Functions

*Table 1-18* lists the supported user provisioning functions and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.
Table 1-18  Provisioning Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Adapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Provisioning Functions</td>
<td></td>
</tr>
<tr>
<td>Create a user account</td>
<td>ADIDC Create Object</td>
</tr>
<tr>
<td>Delete a user account</td>
<td>ADIDC Delete Object</td>
</tr>
<tr>
<td>Enable a disabled user account</td>
<td>ADIDC Enable User</td>
</tr>
<tr>
<td>Disable a user account</td>
<td>ADIDC Disable User</td>
</tr>
<tr>
<td>Update the password</td>
<td>ADIDC Return Text Value</td>
</tr>
<tr>
<td>Update the redirection e-mail address</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the zip code</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the terminal home directory</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the pager</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the IP phone</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the first name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the title</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the user account principal name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the middle name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the account expiration date</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the password never expires flag</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the password not required flag</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update organization name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the company name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the account is locked flag</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the last name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the user home directory</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the post office box</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the terminal allow login field</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the state</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the mobile number</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the telephone number</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the street</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the country</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the fax</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the e-mail ID</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the terminal profile path</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the department</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the full name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update home phone</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the city</td>
<td>ADIDC Update Attribute Value</td>
</tr>
</tbody>
</table>
Table 1-18  (Cont.) Provisioning Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Adapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update the manager name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the user ID</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update common name</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Update the user must change password at next logon flag</td>
<td>ADIDC Update Attribute Value</td>
</tr>
<tr>
<td>Delete group membership</td>
<td>ADIDC Update Child Table Values</td>
</tr>
<tr>
<td>Create object class</td>
<td>ADIDC Update Child Table Values</td>
</tr>
<tr>
<td>Update group membership</td>
<td>ADIDC Update Child Table Values</td>
</tr>
<tr>
<td>Create group membership</td>
<td>ADIDC Update Child Table Values</td>
</tr>
<tr>
<td>Update object class</td>
<td>ADIDC Update Child Table Values</td>
</tr>
<tr>
<td>Delete object class</td>
<td>ADIDC Update Child Table Values</td>
</tr>
</tbody>
</table>

Group Provisioning Functions

| Create group                                       | ADIDC Create Object                         |
| Delete group                                       | ADIDC Delete Object                         |
| Display Name Updated                               | ADIDC Update Attribute Value                |
| Group Name Updated                                 | ADIDC Update Attribute Value                |
| Group Type Updated                                 | ADIDC Update Attribute Value                |
| Organization Name Updated                          | ADIDC Update Attribute Value                |

Organizational Unit Provisioning Functions

| Create Organizational Unit                         | ADIDC Create Object                         |
| Display Name Updated                               | ADIDC Update Attribute Value                |
| Container Updated                                  | ADIDC Update Attribute Value                |
| Delete Organizational Unit                         | ADIDC Delete Object                         |

1.9.2 User Fields for Provisioning

The Lookup.ActiveDirectory.UM.ProvAttrMap lookup definition maps process form fields with target system attributes. This lookup definition is used for performing user provisioning operations.

Table 1-19 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-19 Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager Name</td>
<td>manager</td>
<td>Manager name You must enter the manager name in the DN format. For example:</td>
</tr>
</tbody>
</table>
### Table 1-19 (Cont.) Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Home Directory</td>
<td>TerminalServicesHomeDirectory</td>
<td>Full path of the home directory for the Terminal Server userSample value: c:\MyDirectory. During a provisioning operation, you must enter the full, absolute path of the home directory, as shown in the sample value.</td>
</tr>
<tr>
<td></td>
<td>Part of the data stored in the userParameters field</td>
<td><strong>Note:</strong> This field does not exist in Microsoft AD LDS. A value that you enter in this field would be ignored during provisioning operations in Microsoft AD LDS.</td>
</tr>
<tr>
<td>UD_ADUSRC~Group Name[Lookup]</td>
<td><strong>GROUPS</strong></td>
<td>Group name</td>
</tr>
<tr>
<td>Terminal Profile Path</td>
<td>TerminalServicesProfilePath</td>
<td>Profile that is used when the user logs on to a Terminal Server. The profile can be roaming or mandatory. A roaming profile remains the same, regardless of the computer from which the user logs in. The user can make changes to a roaming profile, but not to a mandatory profile. Any changes a user makes while logged in with a mandatory profile are retained only for that Terminal Services session. The changes are lost when the user starts another Terminal Services session.</td>
</tr>
<tr>
<td></td>
<td>Part of the data stored in the userParameters field</td>
<td><strong>Note:</strong> This field does not exist in Microsoft AD LDS. A value that you enter in this field would be ignored during provisioning operations in Microsoft AD LDS.</td>
</tr>
<tr>
<td>Account Expiration Date[DATE]</td>
<td><strong>PASSWORD_EXPIRATION_DATE</strong></td>
<td>Date when the account expires</td>
</tr>
<tr>
<td>Street</td>
<td>streetAddress</td>
<td>Street address</td>
</tr>
<tr>
<td>Zip</td>
<td>postalCode</td>
<td>ZIP code</td>
</tr>
<tr>
<td>Middle Name</td>
<td><strong>middleName</strong></td>
<td>Initials for the user's middle name</td>
</tr>
<tr>
<td>This field is on both the process form and the OIM User form. During a provisioning operation, the Middle Name field on the process form is prepopulated with the value entered in the Middle Name field on the OIM User form.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Must Change Password At Next Logon</td>
<td><strong>PASSWORD_EXPIRED</strong></td>
<td>Flag that indicates whether or not the user must change the password at next logon. If the value is yes (check box is selected), then the user must change the password at next logon.</td>
</tr>
<tr>
<td>This is a check box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office</td>
<td>physicalDeliveryofficeName</td>
<td>Office Location</td>
</tr>
<tr>
<td>Home Phone</td>
<td>homePhone</td>
<td>Home phone number</td>
</tr>
<tr>
<td>City</td>
<td>l</td>
<td>City</td>
</tr>
<tr>
<td>Account is Locked out</td>
<td><strong>LOCK_OUT</strong></td>
<td>Specifies whether the user account must be locked or unlocked.</td>
</tr>
<tr>
<td>This is a check box.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table 1-19  (Cont.) Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Last name</td>
</tr>
<tr>
<td>This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the Last Name field on the process form is prepopulated with the value entered in the Last Name field on the OIM User form.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Phone</td>
<td>ipPhone</td>
<td>IP phone number</td>
</tr>
<tr>
<td>Mobile</td>
<td>mobile</td>
<td>Mobile number</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>telephoneNumber</td>
<td>Telephone number</td>
</tr>
<tr>
<td>State</td>
<td>st</td>
<td>State</td>
</tr>
<tr>
<td>Fax</td>
<td>facsimileTelephoneNumber</td>
<td>Fax number</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
<td>First name</td>
</tr>
<tr>
<td>This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the First Name field on the process form is prepopulated with the value entered in the First Name field on the OIM User form.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td><strong>PASSWORD</strong></td>
<td>User's password in UTF-8 format</td>
</tr>
<tr>
<td>This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the Password field on the process form is prepopulated with the value entered in the Password field on the OIM User form. If SSL is configured between Oracle Identity Manager and the target system, then the Password field on the process form is a mandatory field.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This connector uses ADSI to set the password of the user. It uses the IADsUser#SetPassword API. This API sets the user's unicodePwd attribute. See the following URL for more information: <a href="http://msdn.microsoft.com/en-us/library/ms677943%28v=vs.85%29.aspx#unicodepwd">http://msdn.microsoft.com/en-us/library/ms677943%28v=vs.85%29.aspx#unicodepwd</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 1-19  (Cont.) Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Full Name          | displayName         | Display name for a user  
During a Create User provisioning  
operation, the cn and displayName  
fields are populated with a  
combination of the user's first name,  
middle initial, and last name entered  
on the OIM User form.  
The full name is displayed in the  
following format on the process form:  
FIRSTNAME MIDDLE_INITIAL.  
LASTNAME  
For example: John M. Doe  
If the middle initial is not entered,  
than the name is displayed as, for  
example, John Doe.  
During an Update provisioning  
operation, only the value in the  
displayName field is updated. |
| Redirection Mail Id | __MAILREDIRECTION__ | E-mail address to which e-mail sent  
to the user must be redirected  
This e-mail address overrides the one  
set in the E Mail field. |
| __NAME__           | __NAME__="CN=\$  
(Common_Name),\$  
(Organization_Name)" | User name with full DN |
| Password Not Required | PasswordNotRequired | Specifies whether or not Password is  
required. If it is true, then there is no  
need to specify the password. If it is  
false, then password is required. |
| Terminal Allow Login | AllowLogon | Specifies whether or not the user is  
permitted to log on to the Terminal  
Server  
This field does not exist in Microsoft  
ADAM and AD LDS. A value that  
you enter in this field would be  
ignored during provisioning  
operations in Microsoft ADAM and  
AD LDS. |
| Country            | c                   | Country       |
| User Id            | sAMAccountName      | User's logon name  
This field is on both the process form  
and the OIM User form. It is a  
mandatory field.  
During a provisioning operation, the  
User ID field on the process form is  
prepopulated with the value entered in  
the User  
This is a mandatory field in  
Microsoft Active Directory. This field  
does not exist in Microsoft ADAM  
and AD LDS. |
| Pager              | pager               | Pager number   |
| Organization Name[LOOKUP,IGNORE] | IGNORED | Name of the organization |
Table 1-19  (Cont.) Entries in the Lookup.ActiveDirectory.UM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
<td>Object GUID of the user</td>
</tr>
<tr>
<td>This is a hidden field on both the process form and the OIM User form.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E Mail</td>
<td>mail</td>
<td>Email address</td>
</tr>
<tr>
<td>This field is on both the process form and the OIM User form.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Name[IGNORE]</td>
<td>IGNORED</td>
<td>Common name of the user</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
<td>Title</td>
</tr>
<tr>
<td>Company</td>
<td>company</td>
<td>Company</td>
</tr>
<tr>
<td>Password Never Expires</td>
<td>PasswordNeverExpires</td>
<td>Flag that controls the Password Never Expires property</td>
</tr>
<tr>
<td>This is a check box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department</td>
<td>department</td>
<td>Department</td>
</tr>
<tr>
<td>User Principal Name</td>
<td>userPrincipalName</td>
<td>The user principal name is the domain-specific name of the user. This field is pre-populated on the Administrative and User Console. The format is as follows: USER_ID_VALUE@UPN_DOMAIN_VALUE Note: When you update this field, you can change the User ID part but you must not change the domain name. If you change the domain name, then the user will not be matched on the target system.</td>
</tr>
<tr>
<td>This is a mandatory field.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Homedirectory</td>
<td>homeDirectory</td>
<td>Home directory of the user</td>
</tr>
<tr>
<td>Post Office Box</td>
<td>postOfficeBox</td>
<td>Post-office box</td>
</tr>
</tbody>
</table>

1.9.3 Group Fields for Provisioning

The Lookup.ActiveDirectory.GM.ProvAttrMap lookup definition maps user resource object fields and target system attributes. This lookup definition is used for performing group provisioning operations.

Table 1-20 lists the group fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-20  Entries in the Lookup.ActiveDirectory.GM.ProvAttrMap

<table>
<thead>
<tr>
<th>Group Field on Oracle Identity Manager</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAME</strong></td>
<td><strong>NAME</strong>=&quot;CN=$(Group_Name),$(Organization_Name)&quot;</td>
<td>Group name with full DN</td>
</tr>
<tr>
<td>Display Name</td>
<td>displayName</td>
<td>Display name for a group</td>
</tr>
<tr>
<td>Group Name</td>
<td>sAMAccountName</td>
<td>Group name</td>
</tr>
</tbody>
</table>
Table 1-20  (Cont.) Entries in the Lookup.ActiveDirectory.GM.ProvAttrMap

<table>
<thead>
<tr>
<th>Group Field on Oracle Identity Manager</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Type</td>
<td>groupeType</td>
<td>Group type</td>
</tr>
<tr>
<td>Organization Name[LOOKUP,IGNORE]</td>
<td>IGNORED</td>
<td>Name of the organization to which the group belongs</td>
</tr>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
<td>Object GUID of the group</td>
</tr>
</tbody>
</table>

1.9.4 Organizational Unit Fields for Provisioning

The Lookup.ActiveDirectory.OM.ProvAttrMap lookup definition maps organization resource object fields and target system attributes. This lookup definition is used for performing organizational unit provisioning operations.

Table 1-21 lists the organizational unit fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-21  Entries in the Lookup.ActiveDirectory.OM.ProvAttrMap

<table>
<thead>
<tr>
<th>Organizational Unit Field on Oracle Identity Manager</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| __NAME__                                             | NAME__="OU=$(Display_Name),$
(Cont) | Organizational unit name with full DN |
| Container[LOOKUP,IGNORE]                              | IGNORED             | Organization name with DN formatFor 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 |

1.10 Connector Objects Used During Trusted Source Reconciliation

Trusted source reconciliation involves fetching data about newly created or modified accounts on the target system and using that data to create or update OIM Users.

The Active Directory User Trusted Recon scheduled task is used to initiate a trusted source reconciliation run. This scheduled task is discussed in Scheduled Jobs for Reconciliation of User Records.

See Also:

Managing Reconciliation in Performing Self Service Tasks with Oracle Identity Manager for conceptual information about reconciliation
This section discusses the following topics:

- User Fields for Trusted Source Reconciliation
- Organizational Unit Fields for Trusted Source Reconciliation
- Reconciliation Rule for Trusted Source Reconciliation
- Viewing Reconciliation Rules for Trusted Source Reconciliation
- Reconciliation Action Rules for Trusted Source Reconciliation
- Viewing Reconciliation Action Rules for Trusted Source Reconciliation

1.10.1 User Fields for Trusted Source Reconciliation

The Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted lookup definition maps user fields of the OIM User form with corresponding field names in the target system. This lookup definition is used for performing trusted source reconciliation runs.

Table 1-22 lists the user identity fields whose values are fetched from the target system during a trusted source reconciliation run.

<table>
<thead>
<tr>
<th>OIM User Form Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E Mail</td>
<td>mail</td>
<td>Email address</td>
</tr>
<tr>
<td>Employee Type</td>
<td>OIM Employee Type</td>
<td>Employee type of the OIM User</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
<td>First name</td>
</tr>
<tr>
<td></td>
<td>This is a mandatory field.</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Last name</td>
</tr>
<tr>
<td></td>
<td>This is a mandatory field.</td>
<td></td>
</tr>
<tr>
<td>Manager ID</td>
<td>Manager Id</td>
<td>Manager name</td>
</tr>
<tr>
<td>Middle Name</td>
<td>middleName</td>
<td>Middle name</td>
</tr>
<tr>
<td>objectGUID</td>
<td><strong>UID</strong></td>
<td>Object GUID of each user on the target system</td>
</tr>
<tr>
<td>Organization</td>
<td><strong>PARENTCN</strong></td>
<td>This is the name of the organization to which users belong if you set the value of the MaintainHierarchy entry of the Lookup.Configuration.ActiveDirectory.Trusted lookup definition to yes. See Lookup.Configuration.ActiveDirectory.Trusted for more information. If Maintain Hierarchy is set to no, then the default organization in Oracle Identity Manager, Xellerate Users, is used.</td>
</tr>
</tbody>
</table>
Table 1-22  Entries in the Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>OIM User Form Field</th>
<th>Target System Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrustedStatus[TRUSTED]</td>
<td><strong>ENABLE</strong></td>
<td>This field stores the status of the user account.</td>
</tr>
<tr>
<td>User Id</td>
<td>sAMAccountName</td>
<td>User’s logon name</td>
</tr>
<tr>
<td>User Type</td>
<td>OIM User Type</td>
<td>Type of the OIM User&lt;br&gt;Values can be one of the following:&lt;br&gt;• Full-Time Employee&lt;br&gt;• Contractor</td>
</tr>
</tbody>
</table>

1.10.2 Organizational Unit Fields for Trusted Source Reconciliation

The Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted lookup definition maps organizational unit fields of the OIM User form with corresponding field names in the target system. This lookup definition is used for performing trusted source reconciliation runs.

*Table 1-23* lists the organizational unit field whose value is fetched from the target system during a trusted source reconciliation run.

Table 1-23  Entries in the Lookup.ActiveDirectory.OM.ReconAttrMap.Trusted Lookup Definition

<table>
<thead>
<tr>
<th>OIM User Form Field</th>
<th>Target System Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org Name</td>
<td>ou</td>
</tr>
</tbody>
</table>

1.10.3 Reconciliation Rule for Trusted Source Reconciliation

**See Also:**

Reconciliation Engine in *Performing Self Service Tasks with Oracle Identity Manager* for generic information about reconciliation matching and action rules

The following is the entity matching rule:

**Rule name:** AD User Trusted Recon Rule

**Rule:** User Login Equals User Id

In this rule:

- User Login is the User ID field on the OIM User form.
- User Id is the sAMAccountName field of Microsoft Active Directory or the userPrincipalName field of Microsoft AD LDS.
1.10.4 Viewing Reconciliation Rules for Trusted Source Reconciliation

After you deploy the connector, you can view the reconciliation rule for trusted source reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand Development Tools.
4. Search for AD User Trusted Source Recon Rule. Figure 1-4 shows the reconciliation rule for trusted source reconciliation.

Figure 1-4  Reconciliation Rule for Trusted Source Reconciliation

Note: In Microsoft Active Directory, sAMAccountName attribute is a mandatory and unique field.

1.10.5 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1-24 lists the action rules for trusted source reconciliation.
### Table 1-24  Action Rules for Trusted Source Reconciliation

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Matches Found</td>
<td>Create User</td>
</tr>
<tr>
<td>One Entity Match Found</td>
<td>Establish Link</td>
</tr>
<tr>
<td>One Process Match Found</td>
<td>Establish Link</td>
</tr>
</tbody>
</table>

**Note:**

No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See

- Setting a Reconciliation Action Rule (Developing Identity Connectors using Java)
- Setting a Reconciliation Action Rule (Developing Identity Connectors using .net)

in *Developing and Customizing Applications for Oracle Identity Manager* for information about setting a reconciliation action rule.

### 1.10.6 Viewing Reconciliation Action Rules for Trusted Source Reconciliation

After you deploy the connector, you can view the reconciliation action rules for trusted source reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Locate the **AD User Trusted** resource object.
5. Click the **Object Reconciliation** tab, and then the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. *Figure 1-5* shows the reconciliation action rule for trusted source reconciliation.
Figure 1-5  Reconciliation Action Rules for Trusted Source Reconciliation
2

Deploying the Microsoft Active Directory User Management Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, postinstallation. upgrading the Microsoft Active Directory User Management Connector, and cloning the Microsoft Active Directory User Management Connector.

The following topics discuss these stages:

• Preinstallation
• Installation
• Postinstallation
• Upgrading the Microsoft Active Directory User Management Connector
• About Cloning the Microsoft Active Directory User Management Connector

Note:

Some of the procedures described in this chapter are meant to be performed on the target system. The minimum permissions required to perform these procedures depends on the target system that you are using:

• If the target system is Microsoft Active Directory, then the permissions required are those assigned to members of the Domain Admins group.
• If the target system is Microsoft AD LDS, then the permissions required are those assigned to members of the Administrators group.

2.1 Preinstallation

Preinstallation for the Microsoft Active Directory User Management connector involves registering a client application for the connector with the target system. It also involves generating the Client ID and Client Secret values for authenticating to the target system and setting the permissions for the client application.

The preinstallation stage for deploying the AD User Management connector involves performing the following procedures:

• 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
• About the Connector Server
• Managing Logging for Microsoft Active Directory User Management Connector
2.1.1 Creating a Target System User Account for Connector Operations

Oracle Identity Manager requires a target system user account to access the target system during reconciliation and provisioning operations. You provide the credentials of this user account while performing the procedure described in Configuring the IT Resource for Microsoft AD and AD LDS.

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

2.1.1.1 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:

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.

See Also:

Microsoft Active Directory documentation for detailed information about performing this procedure
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.

2.1.1.2 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:

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@mydomain.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 ADLDS instance:

a. Create a user account in the standalone computer.

b. Add the newly created user to the ADLDS Administrators group[CN=Administrators,CN=Roles,DC=X].

2.1.2 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:

   ```
   dsacls DELETED_OBJ_DN /takeownership
   ```

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

   Sample value:

   ```
   dsacls "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:

   ```
   dsacls 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:

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

### 2.1.3 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.
See the Microsoft documentation for detailed instructions to delegate control for an organizational unit or custom object class to a user account.

2.1.4 About the Connector Server

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

You deploy the Active Directory User Management connector remotely in the connector server. A connector server is a Microsoft Windows application that enables remote execution of an Identity Connector.

Connector servers are available in two implementations:

- As a .Net implementation that is used by Identity Connectors implemented in .Net
- As a Java Connector Server implementation that is used by Java-based Identity Connectors

The Active Directory User Management connector is implemented in .Net, so you must deploy this connector to a .Net framework-based connector server.

For detailed instructions about installing, configuring, and upgrading the Microsoft .Net Connector Server, see Using the Microsoft .NET Framework Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.

2.1.5 Managing Logging for Microsoft Active Directory User Management Connector

Logging for the Active Directory User Management connector is enabled and managed on the computer hosting the Connector Server. The following sections contain detailed information:

- Enabling Logging for Microsoft Active Directory User Management Connector
- Configuring Log File Rotation

2.1.5.1 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 Manager. 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

### 2.1.5.2 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 of 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:


2.2 Installation

You must install the Active Directory User Management connector in Oracle Identity Manager and if required, place the connector code bundle in the Connector Server.

The following topics discuss installing the Active Directory User Management connector:

- Installing Microsoft Active Directory User Management Connector in Oracle Identity Manager
- Installing the Microsoft Active Directory User Management Connector in the Connector Server

2.2.1 Installing Microsoft Active Directory User Management Connector in Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

- Running the Connector Installer
- Configuring the IT Resource for Microsoft AD and AD LDS
2.2.1.1 Running the Connector Installer

Note:

In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Administrative and User Console.

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:
   
   \(OIM\_HOME/\text{server/ConnectorDefaultDirectory}\)

2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.x:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector**.
   - For Oracle Identity Manager release 11.1.2.x or later:
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under System Management, click **Manage Connector**.

3. In the Manage Connector page, click **Install**.

4. From the Connector List list, select **ActiveDirectory \text{RELEASE\_NUMBER}**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

   If you have copied the installation files into a different directory, then:
   a. In the **Alternative Directory** field, enter the full path and name of that directory.
   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
   c. From the Connector List list, select **ActiveDirectory \text{RELEASE\_NUMBER}**.

5. Click **Load**.

6. To start the installation process, click **Continue**.

   The following tasks are performed, in sequence:
   a. Configuration of connector libraries
   b. Import of the connector XML files (by using the Deployment Manager)
   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure is displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:
• Retry the installation by clicking Retry.
• Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of steps that you must perform after the installation is displayed. These steps are as follows:
   a. Ensuring that the prerequisites for using the connector are addressed

   **Note:**
   At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Clearing Content Related to Connector Resource Bundles from the Server Cache for information about running the PurgeCache utility.

   There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector
   The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled jobs
   The procedure to configure these scheduled jobs is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–1.

2.2.1.2 Configuring the IT Resource for Microsoft AD and AD LDS

   **Note:**
   If you have configured your target system as a trusted source, then create an IT resource of type Active Directory. For example, Active Directory Trusted. The parameters of this IT resource are the same as the parameters of the IT resources described in Configuring the IT Resource for Microsoft AD and AD LDS of this section. See Creating IT Resources in Administering Oracle Identity Manager for more information about creating an IT resource.

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

You must specify values for the parameters of the Active Directory IT resource as follows:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
• For Oracle Identity Manager release 11.1.1.x:
  Log in to the Administrative and User Console
• For Oracle Identity Manager release 11.1.2.x or later:
  Log in to Oracle Identity System Administration

2. If you are using Oracle Identity Manager release 11.1.1.x, then:
   a. On the Welcome page, click Advanced in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in
      the Configuration region, click Manage IT Resource.

3. If you are using Oracle Identity Manager release 11.1.2.x or later, then in the left
   pane, under Configuration, click IT Resource.

4. In the IT Resource Name field on the Manage IT Resource page, enter Active
   Directory and then click Search. Figure 2-1 shows the Manage IT Resource page.

**Figure 2-1  Manage IT Resource Page**

5. Click the edit icon corresponding to the Active Directory IT resource.
6. From the list at the top of the page, select Details and Parameters.
7. Specify values for the parameters of the Active Directory IT resource. Figure 2-2
   shows the Edit IT Resource Details and Parameters page.
The following list describes each parameter of the Active Directory IT resource

- **ADLDSPort**
  Enter the number of the port at which Microsoft AD LDS is listening.
  Sample value: 50001

  **Note:**
  Do not enter a value for this parameter if you are using Microsoft Active Directory as the target system.

- **BDCHostNames**
  Enter the host name of the backup domain controller to which Oracle Identity Manager must switch to if the primary domain controller becomes unavailable.
  Sample value: mydc1;mydc2;mydc3

  **Note:**
  Multiple backup domain controllers must be separated by semicolon (;).

- **Configuration Lookup**
This parameter holds the name of the lookup definition that stores configuration information used during reconciliation and provisioning.

If you have configured your target system as a target resource, then enter Lookup.Configuration.ActiveDirectory.

If you have configured your target system as a trusted source, then enter Lookup.Configuration.ActiveDirectory.Trusted.


• **Connector Server Name**

Name of the IT resource of the type “Connector Server.” You create an IT resource for the Connector Server in Configuring the IT Resource for the Connector Server.

**Note:**
Enter a value for this parameter only if you have deployed the Active Directory User Management connector in the Connector Server.

Default value: Active Directory Connector Server

• **Container**

Enter the fully qualified domain name of the user container into or from which users must be provisioned or reconciled into Oracle Identity Manager, respectively.

Sample value: DC=example,DC=com

• **DirectoryAdminName**

Enter the user name of account that you create by performing the procedure described in Creating a Target System User Account for Connector Operations.

Enter the value for this parameter in the following format:

`DOMAIN_NAME\USER_NAME`

Sample value: mydomain\admin

**Note:**
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 Creating a Target System User Account for Connector Operations.

Enter a value for this parameter in the following format:

`USER_NAME`

Sample value: admin

• **DirectoryAdminPassword**
Enter the password of the user account that you create by performing the procedure described in Creating a Target System User Account for Connector Operations.

• DomainName

Enter the domain name for the Microsoft Active Directory domain controller on which the connector is being installed.

Sample value: example.com

Note:
This is a mandatory parameter if you are using Microsoft Active Directory as the target system.

• isADLDS

Enter yes to specify that the target system is Microsoft AD LDS.
Enter no to specify that the target system is Microsoft Active Directory.

• LDAPHostName

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.

Note:
If you do not specify a value for this parameter and the BDCHostNames 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.

To determine the host name, on the computer hosting the target system, right-click My Computer and select Properties. 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.

Sample values:

w2khost
172.20.55.120
example.com

• SyncDomainController

Enter the name of the domain controller from which user accounts must be reconciled.
Note:
The value specified in this parameter is used if the value of the SearchChildDomains lookup entry is set to no. If no value is specified for the SyncDomainController parameter and the SearchChildDomains lookup entry is set to no, then the connector automatically finds a domain controller for the target system and reconciles users from it.

Sample value: mynewdc

- SyncGlobalCatalogServer
Enter the host on which the global catalog server is located.

Note:
The value specified in this parameter is used if the value of the SearchChildDomains lookup entry is set to yes. If no value is specified for the SyncGlobalCatalogServer parameter and the SearchChildDomains lookup entry is set to yes, 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 SearchChildDomains lookup entry to yes.

Sample value: myglobalcatalogdc

- UseSSL
Enter yes if the target system has been configured for SSL. This enables secure communication between the Connector Server and target system. Otherwise, enter no.

Default value: no
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 no, it is possible to reset user passwords during provisioning operations because the default communication is secure. See Configuring SSL for Microsoft Active Directory and Microsoft AD LDS for information about configuring SSL.

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 yes to secure communication with Microsoft AD LDS. See Configuring SSL Between Connector Server and Microsoft AD LDS for more information about configuring SSL.

8. To save the values, click Update.

2.2.2 Installing the Microsoft Active Directory User Management Connector in the Connector Server

Installation in the Connector Server consists of the following procedures:

• Copying and Extracting the Connector Bundle to the Connector Server
• Configuring the IT Resource for the Connector Server

2.2.2.1 Copying and Extracting the Connector Bundle to the Connector Server

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

1. Stop the Connector Server.

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-1.1.0.6380.zip file to the CONNECTOR_SERVER_HOME directory.

3. Start the Connector Server for the connector bundle to be picked up by the Connector Server.
2.2.2.2 Configuring the IT Resource for the Connector Server

Note:

A predefined IT resource for the Connector Server by the name Active Directory Connector Server is available after connector installation. The parameters of the predefined IT resource is the same as the parameters described in Table 2-1.

In addition to configuring the Active Directory IT resource, you must configure the IT resource for the Connector Server as follows:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.x:
     Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2.x or later:
     Log in to Oracle Identity System Administration

2. If you are using Oracle Identity Manager release 11.1.1.x, then:
   a. On the Welcome page, click Advanced in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click Manage IT Resource.

3. If you are using Oracle Identity Manager release 11.1.2.x or later, then in the left pane, under Configuration, click IT Resource.

4. In the IT Resource Name field on the Manage IT Resource page, enter Active Directory Connector Server and then click Search.

5. Click the edit icon corresponding to the Active Directory Connector Server IT resource.

6. From the list at the top of the page, select Details and Parameters.

7. Specify values for the parameters of the Active Directory Connector Server IT resource, as described in Table 2-1.

Table 2-1 Parameters of the Active Directory Connector Server IT Resource

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the host name or IP address of the computer hosting the connector server. Sample value: myhost.com</td>
</tr>
<tr>
<td>Key</td>
<td>Enter the key for the connector server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the port at which the connector server is listening. Default value: 8759</td>
</tr>
</tbody>
</table>
Table 2-1  (Cont.) Parameters of the Active Directory Connector Server IT Resource

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: 0 A value of 0 means that the connection never times out.</td>
</tr>
<tr>
<td>UseSSL</td>
<td>Enter true to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter false. Default value: false Note: It is recommended that you configure SSL to secure communication with the connector server. To configure SSL between Oracle Identity Manager and Connector Server, see Configuring SSL Between Oracle Identity Manager and Connector Server.</td>
</tr>
</tbody>
</table>

8. Click Update to save the values.

2.3 Postinstallation

Postinstallation steps are detailed across the following sections:

- Configuring Oracle Identity Manager 11.1.2 or Later
- Localizing Field Labels in UI Forms
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Setting Up the Lookup Definition for Connection Pooling
- Setting Up the Lookup Definition for the Ignore Event API
- Configuring the Connector for the Microsoft AD LDS Target System
- Configuring Oracle Identity Manager for Request-Based Provisioning
- Configuring the Connector for Provisioning Organizations
- Enabling or Disabling Password Policies in Microsoft Active Directory
- Configuring SSL for Microsoft Active Directory and Microsoft AD LDS

2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

- Creating and Activating a Sandbox
- Creating a New UI Form
- Creating an Application Instance
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog
2.3.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see Managing Sandboxes in *Administering Oracle Identity Manager*.

1. Log in to Oracle Identity System Administration.
2. In the upper right corner of the page, click the **Sandbox** link.
   
   The Manage Sandboxes page is displayed.
3. On the toolbar, click **Create Sandbox**.
4. In the Create Sandbox dialog box, enter values for the following fields:
   
   - **Sandbox Name**: Enter a name for the sandbox.
   - **Sandbox Description**: Enter a description of the sandbox.
5. Click **Save and Close**.
6. Click **OK** on the confirmation message that is displayed.

   The sandbox is created and displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
8. On the toolbar, click **Activate Sandbox**.

   The sandbox is activated.

2.3.1.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see Managing Forms in *Administering Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer**. The Form Designer page is displayed.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar.

   The Create Form page is displayed.
3. On the Create Form page, enter values for the following UI fields:
   
   - **Resource Type**: Select the resource object that you want to associate the form with. For example, **AD User**.
   - **Form Name**: Enter a name for the form.
4. Click **Create**.

   A message is displayed stating that the form is created.

2.3.1.3 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see Managing Application Instances in *Administering Oracle Identity Manager*.

1. In the left pane of the System Administration console, under Configuration, click **Application Instances**. The Application Instances page is displayed.
2. From the Actions menu, select **Create**. Alternatively, click **Create** on the toolbar. The Create Application Instance page is displayed.

3. Specify values for the following fields:
   - **Name**: The name of the application instance.
   - **Display Name**: The display name of the application instance.
   - **Description**: A description of the application instance.
   - **Resource Object**: The resource object name. Click the search icon next to this field to search for and select **AD User**.
   - **IT Resource Instance**: The IT resource instance name. Click the search icon next to this field to search for and select **Active Directory**.
   - **Form**: Select the form name (created in Creating a New UI Form).

4. Click Save. The application instance is created.

5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See Managing Organizations Associated With Application Instances in *Administering Oracle Identity Manager* for detailed instructions.

### 2.3.1.4 Publishing a Sandbox

To publish the sandbox that you created in Creating and Activating a Sandbox:

1. Close all the open tabs and pages.

2. In the upper right corner of the page, click the **Sandbox** link. The Manage Sandboxes page is displayed.

3. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Creating and Activating a Sandbox.

4. On the toolbar, click **Publish Sandbox**. A message is displayed asking for confirmation.

5. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

### 2.3.1.5 Harvesting Entitlements and Sync Catalog

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. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in the *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
2.3.2 Localizing Field Labels in UI Forms

**Note:**

Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.x or later and you want to localize UI form field labels.

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand Application Deployments and then select oracle.iam.console.identity.sysadmin.ear.
3. In the right pane, from the Application Deployment list, select MDS Configuration.
4. On the MDS Configuration page, click Export and save the archive to the local computer.
5. Extract the contents of the archive, and open one of the following files in a text editor:
   - For Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):
     
     ```
     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
     ```
   - For releases prior to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):
     
     ```
     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
     ```
6. Edit the BizEditorBundle.xlf file in the following manner:
   a. Search for the following text:
      
      ```
      <file source-language="en"
      original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
      datatype="x-oracle-adf">
      ```
   b. Replace with the following text:
      
      ```
      <file source-language="en" target-language="LANG_CODE"
      original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
      datatype="x-oracle-adf">
      ```
      
      In this text, replace LANG_CODE with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:
      
      ```
      <file source-language="en" target-language="ja"
      original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
      datatype="x-oracle-adf">
      ```
   c. Search for the application instance code. This procedure shows a sample edit for Microsoft Active Directory application instance. The original code is:
      
      ```
      [adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.<Field_Name>__c_description']])
      ```
The sample edit of the code is as follows:

```xml
<trans-unit id="$ {adfBundle["oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle"]
[persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_ADUSER_FULNAME__c_description"]}">
<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_FULNAME=氏名`.

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

```xml
<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>
```

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

```xml
<trans-unit id="$ {adfBundle["oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle"]
[persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_A
DUSER_FULNAME__c_description"]}">
<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.
g. Save the file as BizEditorBundle_{LANG_CODE}.xlf. In this file name, replace {LANG_CODE} with the code of the language to which you are localizing.

Sample file name: BizEditorBundle_ja.xlf.

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

**See Also:**

The Deploying and Undeploying Customizations in *Developing and Customizing Applications for Oracle Identity Manager* for more information about exporting and importing metadata files.

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

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

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

To clear content related to connector resource bundles from the server cache:

1. In a command window, switch to the `OIM_HOME/server/bin` directory.

**Note:**

You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

```bash
OIM_HOME/server/bin/SCRIPT_FILE_NAME
```

2. Enter one of the following commands:

**Note:**

You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat CATEGORY_NAME` on Microsoft Windows or `PurgeCache.sh CATEGORY_NAME` on UNIX. The `CATEGORY_NAME` argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

```
PurgeCache.bat MetaData
PurgeCache.sh MetaData
```
On Microsoft Windows: PurgeCache.bat All

On UNIX: PurgeCache.sh All

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

t3://OIM_HOST_NAME:OIM_PORT_NUMBER

In this format:
- Replace `OIM_HOST_NAME` with the host name or IP address of the Oracle Identity Manager host computer.
- Replace `OIM_PORT_NUMBER` with the port on which Oracle Identity Manager is listening.

2.3.4 Setting Up the Lookup Definition for Connection Pooling

Connection pooling allows reuse of physical connections and reduced overhead for your application. This procedure of setting up the lookup definition for connector pooling can be divided into the following sections:

- **Connection Pooling Properties**
- **Adding Connection Pooling Properties**

2.3.4.1 Connection Pooling Properties

By default, this connector uses the ICF connection pooling. Table 2-2 lists the connection pooling properties, their description, and default values set in ICF:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool Max Idle</td>
<td>Maximum number of idle objects in a pool. Default value: 10</td>
</tr>
<tr>
<td>Pool Max Size</td>
<td>Maximum number of connections that the pool can create. Default value: 10</td>
</tr>
<tr>
<td>Pool Max Wait</td>
<td>Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: 150000</td>
</tr>
<tr>
<td>Pool Min Evict Idle Time</td>
<td>Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: 120000</td>
</tr>
<tr>
<td>Pool Min Idle</td>
<td>Minimum number of idle objects in a pool. Default value: 1</td>
</tr>
</tbody>
</table>

2.3.4.2 Adding Connection Pooling Properties

If you want to add the connection pooling properties to use values that suit requirements in your environment, then perform the following procedure:
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
   A new row is added.
5. In the Code Key column of the new row, enter Pool Max Idle.
6. In the Decode column of the new row, enter a value corresponding to the Pool Max Idle property.
7. Repeat Steps 4 through 6 for adding each of the connection pooling properties listed in Table 2-2 Connection Pooling Properties.
8. Click the Save icon.

2.3.5 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

2.3.5.1 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.

2.3.5.2 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
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.

### 2.3.6 Configuring the Connector for the Microsoft AD LDS Target System

**Note:**

Perform the procedure described in this section **only** if you are using AD LDS as the target system.

Before you start using the connector with the AD LDS target system, you must perform the following procedure:

1. Log in to the Design Console.

2. Expand **Administration**, and then double-click **Lookup Definition**.

3. Modify the **Lookup.ActiveDirectory.UM.Configuration** lookup definition as follows:
   a. Search for and open the **Lookup.ActiveDirectory.UM.Configuration** lookup definition.
   b. Change the **Lookup.ActiveDirectory.UM.ProvAttrMap** Decode value to **Lookup.ActiveDirectoryLDS.UM.ProvAttrMap**.
   c. Change the **Lookup.ActiveDirectory.UM.ReconAttrMap** Decode value to **Lookup.ActiveDirectoryLDS.UM.ReconAttrMap**.

4. Modify the **Lookup.ActiveDirectory.GM.Configuration** lookup definition as follows:
   a. Search for and open the **Lookup.ActiveDirectory.GM.Configuration** lookup definition.
   b. Change the **Lookup.ActiveDirectory.GM.ProvAttrMap** Decode value to **Lookup.ActiveDirectoryLDS.GM.ProvAttrMap**.
   c. Change the **Lookup.ActiveDirectory.GM.ReconAttrMap** Decode value to **Lookup.ActiveDirectoryLDS.GM.ReconAttrMap**.

5. Modify the **Lookup.ActiveDirectory.UM.Configuration.Trusted** lookup definition as follows:
   a. Search for and open the **Lookup.ActiveDirectory.UM.Configuration.Trusted** lookup definition.

6. If you have configured the target system as a target resource, then from the **Lookup.ActiveDirectory.UM.ProvAttrMap** and **Lookup.ActiveDirectory.UM.ReconAttrMap** lookup definitions, remove entries
specific to terminal services fields. For example, the Terminal Home Directory and Terminal Profile Path entries.

7. Click the Save icon.

8. Remove the process form fields and process tasks that are specific to terminal services fields.

2.3.7 Configuring Oracle Identity Manager for Request-Based Provisioning

Note:
Perform the procedures described in this section only if you are using Oracle Identity Manager release 11.1.1.x.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following sections provide more information about configuring request-based provisioning:

- Features of Request-Based Provisioning
- About Request Datasets
- Copying Predefined Request Datasets
- Importing Request Datasets
- Enabling the Auto Save Form Feature
- Running the PurgeCache Utility

2.3.7.1 Features of Request-Based Provisioning

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

Note:
Direct provisioning allows the provisioning of multiple Microsoft Active Directory accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

2.3.7.2 About Request Datasets

Request-based provisioning is performed by using a request dataset. A request dataset is an XML file that specifies the information to be submitted by the requester.
during a provisioning operation. Predefined request datasets are shipped with this
connector. These request datasets specify information about the default set of
attributes for which the requester must submit information during a request-based
provisioning operation. The following is the list of predefined request datasets
available in the dataset directory on the installation media:

For Microsoft Active Directory:
• ProvisionResourceADUser.xml
• ModifyResourceADUser.xml

For Microsoft AD LDS:
• ProvisionResourceADLDSUser.xml
• ModifyResourceADLDSUser.xml

2.3.7.3 Copying Predefined Request Datasets

Copy the predefined request dataset files from the installation media to any directory
on the Oracle Identity Manager host computer. It is recommended that you create a
directory structure as follows:

/custom/connector/RESOURCE_NAME

For example:
E:\MyDatasets\custom\connector\AD

Note:
Until you complete the procedure to configure request-based provisioning,
ensure that there are no other files or directories inside the parent directory
in which you create the directory structure. In the preceding example, ensure
that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into
which these files are imported after you run the Oracle Identity Manager MDS Import
utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request
datasets. In addition, you can modify the information in the request datasets.

2.3.7.4 Importing Request Datasets

There are two ways of importing request datasets:
• Importing Request Datasets Using MDS Import Utility
• Importing Request Datasets Using Deployment Manager
Note:
Request Datasets imported either into MDS or by using Deployment Manager are same.

2.3.7.4.1 Importing Request Datasets Using MDS Import Utility

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility as follows:
   a. Set Environment Variable: Set the `OIM_ORACLE_HOME` environment variable to the Oracle Identity Management Oracle home directory inside the Middleware home directory. For example, for Microsoft Windows, set the `OIM_ORACLE_HOME` environment variable to `C:\Oracle\ Middleware\Oracle_IDM1` directory.
   b. Set Up the Properties File: Set the necessary properties in the `weblogic.properties` file, which is located in the same folder as the utilities.

   Note:
   While setting up the properties in the `weblogic.properties` file, ensure that the value of the `metadata_from_loc` property is the parent directory of the `/custom/connector/RESOURCE_NAME` directory. For example, while performing the procedure in Copying Predefined Request Datasets, if you copy the files to the `E:\MyDatasets\custom\connector\Exchng` directory, then set the value of the `metadata_from_loc` property to `E:\MyDatasets`.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| `wls_server_name`  | Name of the Oracle WebLogic Server on which Oracle Identity Manager is deployed | Value is:  
   • `oim` if importing/exporting an out-of-the-box event handler.  
   • `OIMMetadata` for customizable metadata.  
   If importing or exporting custom data, set `application_name` to `OIMMetadata`. |
<p>| <code>application_name</code> | The application name                                  |                                                            |
| <code>metadata_from_loc</code>| Directory location from which an XML file should be imported. This property is used by <code>weblogicImportMetadata.sh</code> script. | Microsoft Windows paths include <code>//</code> as file or directory separator. |</p>
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>metadata_to_loc</td>
<td>Directory location from which an XML file should be imported. This property is used by weblogicExportMetadata.sh script.</td>
<td>Microsoft Windows paths include // as file or directory separator.</td>
</tr>
<tr>
<td>metadata_files</td>
<td>Full path and name of an XML file. This property is used by weblogicExportMetadata.sh and weblogicDeleteMetadata.sh scripts.</td>
<td>For example, you may specify /file/User.xml to export a user entity definition. You can indicate multiple xml files as comma-separated values.</td>
</tr>
</tbody>
</table>

2. In a command window, change to the OIM_HOME\server\bin directory.

3. Run one of the following commands:
   - On Microsoft Windows
     weblogicImportMetadata.bat
   - On UNIX
     weblogicImportMetadata.sh

4. When prompted, enter the following values:
   - Please enter your username [weblogic]
     Enter the username used to log in to WebLogic server
     Sample value: WL_User
   - Please enter your password [weblogic]
     Enter the password used to log in to WebLogic server
   - Please enter your server URL [t3://localhost:7001]
     Enter the URL of the application server in the following format:
     t3://HOST_NAME_IP_ADDRESS:PORT
     In this format, replace HOST_NAME_IP_ADDRESS with the host name or IP address of the computer on which Oracle Identity Manager is installed, and PORT with the port on which Oracle Identity Manager is listening.

   The request dataset is imported into MDS.

2.3.7.4.2 Importing Request Datasets Using Deployment Manager

The request datasets (predefined or generated) can also be imported by using the Deployment Manager (DM). The predefined request datasets are stored in the xml directory on the installation media.

To import a request dataset definition by using the Deployment Manager:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. On the Welcome page, click Advanced in the upper-right corner of the page.
3. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click Import Deployment Manager File. A dialog box for opening files is displayed.
4. Depending on the target system that you are using, locate and open one of the following files, which is located in the xml directory of the installation media:
   
   **For AD:** ActiveDirectory-Datasets.xml
   **For AD LDS:** ActiveDirectoryLDS-Datasets.xml

   Details of this XML file are shown on the File Preview page.

5. Click **Add File**. The Substitutions page is displayed.

6. Click **Next**. The Confirmation page is displayed.

7. Click **Import**.

8. In the message that is displayed, click **Import** to confirm that you want to import the XML file and then click **OK**.

   The request datasets are imported into MDS.

---

### 2.3.7.5 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.

2. Expand **Process Management** and then double-click **Process Definition**.

3. Search for and open the **AD User** process definition.

4. Select the **Auto Save Form** check box.

5. Click the Save icon.

---

### 2.3.7.6 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See [Clearing Content Related to Connector Resource Bundles from the Server Cache](#) for instructions.

The procedure to configure request-based provisioning ends with this step.

---

### 2.3.8 Configuring the Connector for Provisioning Organizations

Perform the procedure described in this section if you intend to provision organizations to a root DN.

Before you provision organizations to a root DN, you must add the DN to the Lookup.ActiveDirectory.OrganizationalUnits 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 the **Lookup.ActiveDirectory.OrganizationalUnits** lookup definition.

4. Add an entry for the root DN. The following is a sample value for the Code Key and Decode values:

   **Code Key:** 150-DC=childtest,DC=test,DC=idsample,DC=central,DC=example,DC=com

   **Decode:** SamAD-DC=childtest,DC=test,DC=idsample,DC=central,DC=example,DC=com
5. Click Save.

2.3.9 Enabling or Disabling Password Policies in Microsoft Active Directory

In Microsoft Active Directory, the "Passwords must meet complexity requirements" policy setting is used to enable or disable password policies.

The procedure that you must perform depends on whether or not you want to achieve either or both of the following objectives:

• Enable password policies
• Configure SSL between Oracle Identity Manager and the target system

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.

See the Microsoft documentation for detailed instructions to enable or disable 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.

2.3.10 Configuring SSL for Microsoft Active Directory and Microsoft AD LDS

This section discusses the following topics to configure SSL communication between Oracle Identity Manager and the target system:
In this section, Microsoft ADAM and Microsoft AD LDS have both been referred to as Microsoft AD LDS. Therefore, if you are using Microsoft Windows Server 2003 as the target system, then you must consider the term Microsoft AD LDS as Microsoft ADAM while performing the instructions described in this section. Wherever needed, instructions specific to both Microsoft ADAM and Microsoft AD LDS have been called out separately.

- 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 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 Manager and Connector Server

### 2.3.10.1 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.

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.

Before you configure SSL, depending on the target system that you are using, you must install Certificate Services on a Windows Server (2003, 2008, or 2012), and then ensure the following:

- If you are installing Certificate Services on Windows Server 2003, ensure that Active Directory or ADAM is installed on the host computer.
- 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
2.3.10.2 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.

2.3.10.3 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.

### 2.3.10.4 Configuring SSL Between Oracle Identity Manager and Connector Server

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

- Exporting the Certificate
- Configuring the Connector Server for SSL
- Configuring Oracle Identity Manager for SSL

#### 2.3.10.4.1 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.

#### 2.3.10.4.2 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.
2.3.10.4.3 Configuring Oracle Identity Manager for SSL

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

1. Copy the certificate generated in Exporting the Certificate to the computer on which Oracle Identity Manager is running.

2. Import the target system certificate into the JDK used by Oracle Identity Manager (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 changeit

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 of the Connector Server IT resource to true.

2.4 Upgrading the Microsoft Active Directory User Management Connector

If you have already deployed an earlier release of this connector, then upgrade the connector to the current release.

The following sections discuss the procedure to upgrade the connector:
Note:

- Upgrade of the connector from release 9.1.x to 11.1.1.x is supported.
- Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
- As a best practice, first perform the upgrade procedure in a test environment.

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 Manager.
2. Perform the preupgrade procedure documented in Managing Connector Lifecycle of Administering Oracle Identity Manager.
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. Figure 2-3 shows the RootDSE properties dialog box in which the highestCommittedUSN attribute is displayed.
4. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector. See Managing Connector Lifecycle of Administering Oracle Identity Manager for more information.

2.4.2 Upgrade Steps

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 Administering Oracle Identity Manager for detailed information about the wizard and silent modes.

2.4.3 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**
2.4.3.1 Performing Postupgrade Steps

Postupgrade steps involve 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 Manager*.

2. If you are using Oracle Identity Manager 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 Manager 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_USING_THE_SOURCE_CONNECTOR
   ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UPGRADE
   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 Manager administrator, and the logger level and log file location.

See Also:

Using the Form Version Control Utility of Oracle Fusion Middleware Administering Oracle Identity Manager for detailed information about the FVC utility

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
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 Manager 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 Manager. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token attribute.

    See 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.

2.4.3.2 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.

2.4.3.3 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.
2.5 About Cloning the Microsoft Active Directory User Management Connector

You can clone the Microsoft Active Directory User Management connector by setting new names for some of the objects that comprise the connector.

The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

See Also:
Managing Connector Lifecycle of *Administering Oracle Identity Manager* for detailed information about cloning connectors and the steps mentioned in this section

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- **IT Resource**
  The cloned connector has its own set of IT resources. You must configure both the cloned IT resources, Active Directory and Connector Server, and provide the reference of the cloned Connector Server IT Resource in the cloned Active Directory IT resource. Ensure you use the configuration lookup definition of the cloned connector.

- **Scheduled Task**
  The values of the Resource Object Name and IT Resource scheduled task attributes in the cloned connector refer to the values of the base connector. Therefore, these values (values of the Resource Object Name and IT resource scheduled task attributes that refer to the base connector) must be replaced with the new cloned connector artifacts.

- **Lookup Definition**
  Verify the lookup entries in all lookup definitions to ensure that there are no references of old process forms. If there are any, then change it to the corresponding new form.

  For example, after cloning, the *Lookup.ActiveDirectory.UM.ProvAttrMap* lookup definition contains a reference to a child table such as *UD_ADUSRC~Group Name[LOOKUP]*. You must change this to include the new value, for example, *UD_ADUSRC2~Group Name[LOOKUP]*.

- **Process Tasks**
  After cloning, you notice that all event handlers attached to the process tasks are the cloned ones. Therefore, no changes are required for process tasks in parent
forms. This is because the adapter mappings for all process tasks related to parent forms are updated with cloned artifacts.

However, the mapping of the childTableName adapter variable must be updated for all process tasks that are associated with the cloned AD IDC Child Table Update adapter. The following predefined process tasks are associated with the AD IDC Child Table Update adapter:

- Group membership delete
- Group membership insert
- Group membership update
- Object classes delete
- Object classes insert
- Object classes update

• Localization Properties

You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

For example, the process form attributes are referenced in the Japanese properties file, ActiveDirectoryIdC_ja.properties, as global.udf.UD_ADUSER_FULLNAME. During cloning, if you change the process form name from UD_ADUSER to UD_ADUSER1, then you must update the process form attributes to global.udf.UD_ADUSER1_FULLNAME.
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:

- Guidelines on Using the Microsoft Active Directory User Management Connector
- Scheduled Jobs for Lookup Field Synchronization
- Configuring Reconciliation
- Configuring and Running Group Reconciliation
- Configuring and Running Organization Reconciliation
- Configuring Scheduled Jobs
- Action Scripts
- Performing Provisioning Operations in Oracle Identity Manager Release 11.1.1.x
- Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later
- Uninstalling the Microsoft Active Directory User Management Connector

3.1 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
3.1.1 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 Manager 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 Manager.

- 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 Manager.
  - 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 Manager.
  - 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 Manager, then you must set the MaintainHierarchy attribute of the trusted source reconciliation scheduled task to true. In addition, you must configure organization reconciliation to run before trusted source reconciliation.
  - In Oracle Identity Manager, 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 Manager, even if they have different parent OUs on the target system.
  - The name of an organization in Oracle Identity Manager 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.

### 3.1.2 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 Manager 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 Manager, you must ensure that the new password adheres to the password policies on the target system.
For more information about password guidelines applicable on the target system, visit the Microsoft TechNet Web site at

http://technet2.microsoft.com

• 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 Manager fields. For example, ensure that the value you specify for the User Login field in Oracle Identity Manager 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 Manager) 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 Manager, you must enter the DN value.

For example:

\texttt{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 \texttt{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:

\texttt{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

• During a provisioning operation, you can specify multiple auxiliary classes to be attached (to the user account being created) by adding the auxiliary class names as an entry to the Lookup.Configuration.ActiveDirectory lookup definition. See Adding Dynamic Auxiliary Object Classes and Their Attributes to Users for more information.

• 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 Manager. 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 Manager.

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

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 Manager 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 Manager with organization-related data in the target system.

Table 3-1 describes the attributes of both scheduled jobs.

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| Code Key Attribute| 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:  
  - For Active Directory Group Lookup Recon: distinguishedName  
  - For Active Directory Organization Lookup Recon: distinguishedName  
  **Note:** You must not change the value of this attribute. |
| 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). Depending on the scheduled job you are using, the default values are as follows:  
  - For Active Directory Group Lookup Recon: distinguishedName  
  - For Active Directory Organization Lookup Recon: distinguishedName |
| Filter            | Enter a filter to filter out records to be stored in the lookup definition. For more information about the Filter attribute, see Limited Reconciliation. |
| IT Resource Name  | Enter the name of the IT resource for the target system installation from which you want to reconcile records.  
  **Sample value:** Active Directory |
| Lookup Name       | Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system.  
  **Note:** If the lookup name that you specify as the value of this attribute is not present in Oracle Identity Manager, 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:  
  - For Active Directory Organization Lookup Recon: Lookup.ActiveDirectory.OrganizationalUnits |
| 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:  
  - For Active Directory Group Lookup Recon: Group  
  - For Active Directory Organization Lookup Recon: OrganizationalUnit |
3.3 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:

• Full Reconciliation and Incremental Reconciliation
• Limited Reconciliation
• Batched Reconciliation

3.3.1 Full Reconciliation and Incremental Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. 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 Manager.

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

Batch Start
Filter
Latest Token

At the end of the reconciliation run, the Latest Token attribute of the scheduled 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.

3.3.2 Limited Reconciliation

This section discusses the following topics that 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

3.3.2.1 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.
3.3.2.2 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 3-2 lists the filter syntax that you can use and the corresponding description and sample values.

Note: Filters with wildcard characters are not supported.

Table 3-2 Keywords and Syntax for the Filter Attribute

<table>
<thead>
<tr>
<th>Filter Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String Filters</td>
<td></td>
</tr>
<tr>
<td><code>startsWith('ATTRIBUTE_NAME','PREFIX')</code></td>
<td>Records whose attribute value starts with the specified prefix are reconciled.</td>
</tr>
<tr>
<td><strong>Example</strong>: <code>startsWith('userPrincipalName','John')</code></td>
<td>In this example, all records whose userPrincipalName begins with 'John' are reconciled.</td>
</tr>
<tr>
<td><code>endsWith('ATTRIBUTE_NAME','SUFFIX')</code></td>
<td>Records whose attribute value ends with the specified suffix are reconciled.</td>
</tr>
<tr>
<td><strong>Example</strong>: <code>endsWith('sn','Doe')</code></td>
<td>In this example, all records whose last name ends with 'Doe' are reconciled.</td>
</tr>
<tr>
<td><code>contains('ATTRIBUTE_NAME','STRING')</code></td>
<td>Records where the specified string is contained in the attribute's value are reconciled.</td>
</tr>
<tr>
<td><strong>Example</strong>: <code>contains('displayName','Smith')</code></td>
<td>In this example, all records whose display name contains 'Smith' are reconciled.</td>
</tr>
<tr>
<td><code>containsAllValues('ATTRIBUTE_NAME</code>, ['STRING1';'STRING2', . . . ,'STRINGn'])`</td>
<td>Records that contain all the specified strings for a given attribute are reconciled.</td>
</tr>
<tr>
<td><strong>Example</strong>: <code>containsAllValues('objectClass',['person','top'])</code></td>
<td>In this example, all records whose objectClass contains both &quot;top&quot; and &quot;person&quot; are reconciled.</td>
</tr>
<tr>
<td>Equality and Inequality Filters</td>
<td></td>
</tr>
<tr>
<td><code>equalTo('ATTRIBUTE_NAME','VALUE')</code></td>
<td>Records whose attribute value is equal to the value specified in the syntax are reconciled.</td>
</tr>
<tr>
<td><strong>Example</strong>: <code>equalTo('sAMAccountName','Sales Organization')</code></td>
<td>In this example, all records whose sAMAccountName is Sales Organization are reconciled.</td>
</tr>
</tbody>
</table>
### Table 3-2  (Cont.) Keywords and Syntax for the Filter Attribute

<table>
<thead>
<tr>
<th>Filter Syntax</th>
<th>Description</th>
<th>Example 1:</th>
<th>Example 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>greaterThan('ATTRIBUTE_NAME','VALUE')</code></td>
<td>Records whose attribute value (string or numeric) is greater than (in lexicographical or numerical order) the value specified in the syntax are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example 1:</strong> <code>greaterThan('cn','bob')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose common name is present after the common name 'bob' in the lexicographical order (or alphabetical order) are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example 2:</strong> <code>greaterThan('employeeNumber','1000')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose employee number is greater than 1000 are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>greaterThanOrEqualTo('ATTRIBUTE_NAME','VALUE')</code></td>
<td>Records whose attribute value (string or number) is lexographically or numerically greater than or equal to the value specified in the syntax are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example 1:</strong> <code>greaterThanOrEqualTo('sAMAccountName','S')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose sAMAccountName is equal to 'S' or greater than 'S' in lexicographical order are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example 2:</strong> <code>greaterThanOrEqualTo('employeeNumber','1000')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose employee number is greater than or equal to 1000 are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>lessThan('ATTRIBUTE_NAME','VALUE')</code></td>
<td>Records whose attribute value (string or numeric) is less than (in lexicographical or numerical order) the value specified in the syntax are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example 1:</strong> <code>lessThan('sn','Smith')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose last name is present after the last name 'Smith' in the lexicographical order (or alphabetical order) are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example 2:</strong> <code>lessThan('employeeNumber','1000')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose employee number is less than 1000 are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>lessThanOrEqualTo('ATTRIBUTE_NAME','VALUE')</code></td>
<td>Records whose attribute value (string or numeric) is lexographically or numerically less than or equal to the value specified in the syntax are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example 1:</strong> <code>lessThanOrEqualTo('sAMAccountName','A')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose sAMAccountName is equal to 'A' or less than 'A' in lexicographical order are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example 2:</strong> <code>lessThanOrEqualTo('employeeNumber','1000')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose employee number is less than or equal to 1000 are reconciled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Complex Filters</strong></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;FILTER1&gt; &amp; &lt;FILTER2&gt;</code></td>
<td><strong>Example:</strong> <code>startsWith('cn', 'John') &amp; endsWith('sn', 'Doe')</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this example, all records whose common name starts with John and last name ends with Doe are reconciled.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3-2  (Cont.) Keywords and Syntax for the Filter Attribute

<table>
<thead>
<tr>
<th>Filter Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| <FILTER1> | <FILTER2>  | 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.  
  
  **Example:** contains('sAMAccountName', 'Andy') | contains('sn', 'Brown')  
  
  In this example, all records that contain 'Andy' in the sAMAccount Name attribute or records that contain 'Brown' in the last name are reconciled.  

| not(<FILTER>) | Records that do not satisfy the given filter condition are reconciled.  
  
  **Example:** not(contains('cn', 'Mark'))  
  
  In this example, all records that does not contain the common name 'Mark' are reconciled. |

### 3.3.2.3 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 hierarchial structure for objects in Microsoft Active Directory.

### 3.3.3 Batched Reconciliation

This section discusses the Batch Size, Batch Start, Sort By, and Sort Direction attributes of the scheduled jobs for target resource reconciliation (Active Directory User Target Recon) and trusted source reconciliation (Active Directory User Trusted Recon).

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 attributes:

- **Batch Size:** Use this attribute to specify the number of records that must be included in each batch.
- **Batch Start:** Use this attribute to specify the record number from which batched reconciliation must begin.
- **Number of Batches:** Use this attribute to specify the total number of batches that must be reconciled. The default value of this attribute 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 attributes are ignored.
• Sort By: Use this attribute to specify the name of the target system field by which the records in a batch must be sorted.

• Sort Direction: Use this attribute to specify whether records being fetched must be sorted in ascending or descending order. The value of this attribute can be either **asc** or **desc**.

If batched reconciliation fails, then you only need to rerun the scheduled task without changing the values of the task attributes.

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 attribute. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token attribute.

---

**Note:**

Sorting large number of records on the target system fails during batched reconciliation. Therefore, it is recommended that you use the PageSize entry of the Lookup.Configuration.ActiveDirectory or Lookup.Configuration.ActiveDirectory.Trusted lookup definitions to tune fetching of records from the target system.

---

### 3.3.4 Reconciliation Scheduled Jobs

When you run the Connector Installer, the following reconciliation scheduled tasks are automatically created in Oracle Identity Manager:

- **Scheduled Jobs for Reconciliation of User Records**
- **Scheduled Jobs for Reconciliation of Deleted User Records**
- **Scheduled Jobs for Reconciliation of Groups and Organizations**
- **Scheduled Job for Reconciliation of Deleted Groups**

#### 3.3.4.1 Scheduled Jobs for Reconciliation of User Records

Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled jobs:

- See **Active Directory User Target Recon** to implement target resource reconciliation.
- See **Active Directory User Trusted Recon** to implement trusted source reconciliation.

#### 3.3.4.1.1 Active Directory User Target Recon

This scheduled job is used to reconcile user data in the target resource (account management) mode of the connector. **Table 3-3** describes the attributes of this scheduled job.
### Attributes of the Scheduled Job for Reconciliation of User Data from a Target Resource

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Batch Size**             | Enter the number of records that must be included in each batch fetched from the target system.  
  **Default value:** 100  
  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 Batched Reconciliation. |
| **Batch Start**            | Enter the number of the target system record from which a batched reconciliation run must begin.  
  **Default value:** 1  
  This attribute is used in conjunction with the Batch Size, Number of Batches, Sort By, and Sort Direction attributes. All these attributes are discussed in Batched Reconciliation. |
| **Filter**                 | Expression for filtering records. See Performing Limited Reconciliation By Using Filters for more information.  
  **Default value:** None                                                                                                                                                                                                                                                                 |
| **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:** uSNChanged  
  **Note:** Do not change the value of this attribute. |
| **IT Resource Name**       | Name of the IT resource instance that the connector must use to reconcile data.  
  **Sample value:** Active Directory                                                                                                                                                                                                                                                                 |
| **Latest Token**           | This attribute holds the value of the uSNChanged attribute of a domain controller that is used for reconciliation.  
  **Note:** 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 user accounts whose uSNChanged value is greater than the Latest Token attribute value are reconciled. |
| **Number of Batches**      | Enter the number of batches that must be reconciled.  
  **Default value:** All  
  **Sample value:** 20  
  This attribute is used in conjunction with the Batch Size, Batch Start, Sort By, and Sort Direction attributes. All these attributes are discussed in Batched Reconciliation.  
  If you accept the default value (All), then all batches are reconciled. |
| **Object Type**            | This attribute holds the type of object you want to reconcile.  
  **Default value:** User  
  **Note:** If you configure the connector to provision users to a custom class (for example, InetOrgPerson) then enter the value of the object class here.                                                                                                                                                                       |
| **Resource Object Name**   | Enter the name of the resource object against which reconciliation runs must be performed.  
  **Default value:** AD User                                                                                                                                                                                                                                                                                                   |
| **Scheduled Task Name**    | This attribute holds the name of the scheduled task.  
  **Default value:** Active Directory User Target Recon                                                                                                                                                                                                                                                                          |
Table 3-3  (Cont.) Attributes of the Scheduled Job for Reconciliation of User Data from a Target Resource

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Base</td>
<td>Enter the container in which the search for user records must be performed during reconciliation.</td>
</tr>
<tr>
<td></td>
<td>Sample Value: ou=org1,dc=corp,dc=com</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Search Scope</td>
<td>Enter <em>subtree</em> 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 OU=abc,DC=corp,DC=com, then the search would cover the abc OU and all of its child OUs.</td>
</tr>
<tr>
<td></td>
<td>Enter <em>onelevel</em> 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 OU=abc,DC=corp,DC=com, then the search would cover only the abc OU.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you want to enter <em>onelevel</em>, then remember that you must not include a space between &quot;one&quot; and &quot;level.&quot;</td>
</tr>
<tr>
<td></td>
<td>Default value: <em>subtree</em></td>
</tr>
<tr>
<td>Sort By</td>
<td>Enter the name of the target system field by which the records in a batch must be sorted.</td>
</tr>
<tr>
<td></td>
<td>Default value: sAMAccountName</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are using AD LDS as the target system, then change the default value of this attribute to some other attribute (for example, <em>cn</em>) because the sAMAccountName attribute does not exist on the AD LDS target system.</td>
</tr>
<tr>
<td>Sort Direction</td>
<td>Use this attribute to specify whether records being fetched must be sorted in ascending or descending order. The value of this attribute can be either <em>asc</em> or <em>desc</em>.</td>
</tr>
<tr>
<td></td>
<td>Default value: <em>asc</em></td>
</tr>
</tbody>
</table>

### 3.3.4.1.2 Active Directory User Trusted Recon

This scheduled job is used to reconcile user data in the trusted resource (identity management) mode of the connector. Table 3-4 describes the attributes of this scheduled job.

Table 3-4  Attributes of the Scheduled Job for Reconciliation of User Data from a Trusted Source

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Size</td>
<td>Enter the number of records that must be included in each batch fetched from the target system.</td>
</tr>
<tr>
<td></td>
<td>Default value: 100</td>
</tr>
<tr>
<td></td>
<td>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 Batched Reconciliation.</td>
</tr>
<tr>
<td>Batch Start</td>
<td>Enter the number of the target system record from which a batched reconciliation run must begin.</td>
</tr>
<tr>
<td></td>
<td>Default value: 1</td>
</tr>
<tr>
<td></td>
<td>This attribute is used in conjunction with the Batch Size, Number of Batches, Sort By, and Sort Direction attributes. All these attributes are discussed in Batched Reconciliation.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Filter**             | Expression for filtering records. See [Performing Limited Reconciliation By Using Filters](#) for more information.  
                           | Default value: None                                                                          |
| **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: uSNChanged                                                                    |
| **Note:**               | Do not change the value of this attribute.                                                     |
| **IT Resource Name**   | Enter the name of the IT resource instance that you create for trusted source reconciliation in Configuring the IT Resource for Microsoft AD and AD LDS.  
                           | Sample value: Active Directory Trusted                                                        |
| **Latest Token**       | This attribute holds the value of the uSNChanged attribute of a domain controller that is used for reconciliation.  
                           | **Note:** 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 user accounts whose uSNChanged value is greater than the Latest Token attribute value are reconciled. |
| **Maintain Hierarchy** | Enter yes to specify that you want to maintain in Oracle Identity Manager the same organization hierarchy that is maintained on the target system. Otherwise, enter no.  
                           | Default value: no                                                                            |
| **Manager Id**         | Enter the decode value of the User Id Code Key in the lookup definition that holds mappings between resource object fields and target system attributes for trusted source reconciliation.  
                           | If you are using Microsoft Active Directory as the target system, then the default value of this attribute is sAMAccountName.  
                           | If you are using Microsoft AD LDS as the target system, then set the value of this attribute to __UPN_WO_DOMAIN__.  
                           | Default value: sAMAccountName                                                                 |
| **Number of Batches**  | Enter the number of batches that must be reconciled.  
                           | Default value: All                                                                            |
| **Sample value**       | 20                                                                                             |
| **Note:**               | This attribute is used in conjunction with the Batch Size, Batch Start, Sort By, and Sort Direction attributes. All these attributes are discussed in [Batched Reconciliation](#).  
                           | If you accept the default value (All), then all batches are reconciled.                       |
| **Object Type**        | This attribute holds the type of object you want to reconcile.  
                           | Default value: User                                                                            |
| **Note:**               | If you configure the connector to provision users to a custom class (for example, InetOrgPerson) then enter the value of the object class here. |
| **OIM Employee Type**  | Enter the employee type that must be set for OIM Users created through reconciliation.       |
| **Default value**      | Full-Time                                                                                      |
### Table 3-4 (Cont.) Attributes of the Scheduled Job for Reconciliation of User Data from a Trusted Source

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OIM Organization Name</td>
<td>Enter the name of the Oracle Identity Manager organization in which reconciled users must be created. The OIM Organization attribute is taken into account only if you set the MaintainHierarchy attribute to no. If you set the MaintainHierarchy attribute to yes, then the value of the OIM Organization attribute is ignored. Default value: Xellerate Users</td>
</tr>
<tr>
<td>OIM User Type</td>
<td>Enter the role that must be set for OIM Users created through reconciliation. You must select one of the following values: End-User, End-User Administrator. Default value: End-User</td>
</tr>
<tr>
<td>Resource Object Name</td>
<td>Enter the name of the resource object against which reconciliation runs must be performed. Default value: AD User Trusted</td>
</tr>
<tr>
<td>Scheduled Task Name</td>
<td>This attribute holds the name of the scheduled task. Default value: Active Directory User Trusted Recon</td>
</tr>
<tr>
<td>Search Base</td>
<td>Enter the container in which the search for user records must be performed during reconciliation. Sample Value: ou=org1,dc=corp,dc=com. Note: 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.</td>
</tr>
<tr>
<td>Search Scope</td>
<td>Enter subtree 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 OU=abc,DC=corp,DC=com, then the search would cover the abc OU and all of its child OUs. Enter onelevel 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 OU=abc,DC=corp,DC=com, then the search would cover only the abc OU. Note: If you want to enter onelevel, then remember that you must not include a space between “one” and “level.” Default value: subtree</td>
</tr>
<tr>
<td>Sort By</td>
<td>Enter the name of the target system field by which the records in a batch must be sorted. Default value: sAMAccountName. Note: If you are using AD LDS as the target system, then change the default value of this attribute to some other attribute (for example, cn) because the sAMAccountName attribute does not exist on the AD LDS target system.</td>
</tr>
<tr>
<td>Sort Direction</td>
<td>Use this attribute to specify whether records being fetched must be sorted in ascending or descending order. The value of this attribute can be either asc or desc. Default value: asc</td>
</tr>
</tbody>
</table>

#### 3.3.4.2 Scheduled Jobs for Reconciliation of Deleted User Records

Depending on whether you want to implement trusted source or target resource delete reconciliation, you must specify values for the attributes of one of the following scheduled jobs:
Note:

To ensure that the target system user account that you create for performing connector operations has access to the Deleted Objects container in the target system, perform the procedure described in Assigning Permissions to Perform Delete User Reconciliation Runs.

- **Active Directory User Target Delete Recon**
  
  This scheduled job is used to reconcile data about deleted users in the target resource (account management) mode of the connector. During a reconciliation run, for each deleted user account on the target system, the Active Directory resource is revoked for the corresponding OIM User.

- **Active Directory User Trusted Delete Recon**
  
  This scheduled job is used to reconcile data about deleted users in the trusted source (identity management) mode of the connector. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted.

Table 3-5 describes the attributes of both scheduled jobs.

### Table 3-5  Attributes of the Scheduled Jobs for Delete User Reconciliation

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Recon</td>
<td>Specifies whether delete reconciliation must be performed.</td>
</tr>
<tr>
<td></td>
<td>Default value: yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change the value of this attribute.</td>
</tr>
<tr>
<td>IT Resource Name</td>
<td>Name of the IT resource instance that the connector must use to reconcile user data.</td>
</tr>
<tr>
<td></td>
<td>The default value of this attribute in the Active Directory User Target Delete Recon scheduled job is <strong>Active Directory</strong>.</td>
</tr>
<tr>
<td></td>
<td>The default value of this attribute in the Active Directory User Trusted Delete Recon scheduled job is <strong>none</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you have configured your target system as trusted source, then ensure that you specify the name of the IT resource in which the Configuration Lookup parameter is set to <strong>Lookup.Configuration.ActiveDirectory.Trusted</strong>.</td>
</tr>
<tr>
<td>Object Type</td>
<td>This attribute holds the type of object you want to reconcile.</td>
</tr>
<tr>
<td></td>
<td>Default value: <strong>User</strong></td>
</tr>
<tr>
<td>Resource Object Name</td>
<td>Enter the name of the resource object against which reconciliation runs must be performed.</td>
</tr>
<tr>
<td></td>
<td>The default value of this attribute in the Active Directory User Target Delete Recon scheduled job is <strong>AD User</strong>.</td>
</tr>
<tr>
<td></td>
<td>The default value of this attribute in the Active Directory User Trusted Delete Recon scheduled job is <strong>AD User Trusted</strong>.</td>
</tr>
</tbody>
</table>
**Table 3-5 (Cont.) Attributes of the Scheduled Jobs for Delete User Reconciliation**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Task Name</td>
<td>This attribute holds the name of the scheduled task. The default value of this attribute in the Active Directory User Target Delete Recon scheduled job is <em>Active Directory User Target Delete Recon</em>. The default value of this attribute in the Active Directory User Trusted Delete Recon scheduled job is <em>Active Directory User Trusted Delete Recon</em>.</td>
</tr>
<tr>
<td>Sync Token</td>
<td>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 Manager. 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 Manager. This attribute stores values in the following format: `&lt;String&gt;0</td>
</tr>
</tbody>
</table>

**3.3.4.3 Scheduled Jobs for Reconciliation of Groups and Organizations**

Depending on your requirement, you must specify values for the attributes of one of the following scheduled jobs:

- **Active Directory Group Recon**
  This scheduled job is used to reconcile group data from the target system.

- **Active Directory Organization Recon**
  This scheduled job is used to reconcile organization data from the target system.
See Also:
The following sections for information about running group and organization reconciliation:

- Configuring and Running Group Reconciliation
- Configuring and Running Organization Reconciliation

Table 3-6 describes the attributes of both scheduled jobs.

Table 3-6  Attributes of the Scheduled Task for Reconciliation of Group and Organization Data

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Expression for filtering records. See Performing Limited Reconciliation By Using Filters for more information. Default value: None</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> While creating filters, ensure to use attributes specific to Groups or Organizational Units.</td>
</tr>
<tr>
<td>Incremental Recon Attribute</td>
<td>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: uSNChanged</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change the value of this attribute.</td>
</tr>
<tr>
<td>IT Resource Name</td>
<td>Enter the name of the IT resource for the target system installation from which you want to reconcile group or organization data. Default value: Active Directory</td>
</tr>
<tr>
<td>Latest Token</td>
<td>This attribute holds the value of the uSNChanged attribute of a domain controller that is used for reconciliation. Sample value: 0 <strong>Note:</strong> 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 uSNChanged value is greater than the Latest Token attribute value are reconciled.</td>
</tr>
<tr>
<td>Object Type</td>
<td>Type of object to be reconciled. The default value of this attribute in the Active Directory Group Recon scheduled job is Group. The default value of this attribute in the Active Directory Organization Recon scheduled job is organizationalUnit.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Enter the name of the organization to which all groups fetched from the target system is linked. See Configuring and Running Group Reconciliation for more information on the usage of this attribute. <strong>Note:</strong> This attribute is present only in the Active Directory Group Recon scheduled job.</td>
</tr>
<tr>
<td>Organization Type</td>
<td>Type of organization to be created in Oracle Identity Manager. Default value: Company <strong>Note:</strong> This attribute is present only in the Active Directory Group Recon scheduled job.</td>
</tr>
</tbody>
</table>
Table 3-6 (Cont.) Attributes of the Scheduled Task for Reconciliation of Group and Organization Data

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Object Name</td>
<td>Name of the resource object that is used for reconciliation. The default value of this attribute in the Active Directory Group Recon scheduled job is AD Group. The default value of this attribute in the Active Directory Organization Recon scheduled job is Xellerate Organization.</td>
</tr>
<tr>
<td>Scheduled Task Name</td>
<td>Name of the scheduled task used for reconciliation. The default value of this attribute in the Active Directory Group Recon scheduled job is Active Directory Group Recon. The default value of this attribute in the Active Directory Organization Recon scheduled job is Active Directory Organization Recon.</td>
</tr>
<tr>
<td>Search Base</td>
<td>Enter the container in which the search for group or organization records must be performed during reconciliation. Sample Value: ou=org1,dc=corp,dc=com Note: 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.</td>
</tr>
<tr>
<td>Search Scope</td>
<td>Enter subtree 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 OU=abc,DC=corp,DC=com, then the search would cover the abc OU and all of its child OUs. Enter onelevel 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 OU=abc,DC=corp,DC=com, then the search would cover only the abc OU. Note: If you want to enter onelevel, then remember that you must not include a space between &quot;one&quot; and &quot;level.&quot; Default value: subtree</td>
</tr>
</tbody>
</table>

3.3.4.4 Scheduled Job for Reconciliation of Deleted Groups

The Active Directory Group Delete Recon is used to reconcile data about deleted groups.

Table 3-7 describes the attributes of this scheduled job.

Table 3-7 Attributes of the Active Directory Group Delete Recon Scheduled Job

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Recon</td>
<td>Specifies whether delete reconciliation must be performed. Default value: yes Note: Do not change the value of this attribute.</td>
</tr>
<tr>
<td>IT Resource Name</td>
<td>Name of the IT resource instance that the connector must use to reconcile group data. Default value: Active Directory</td>
</tr>
<tr>
<td>Object Type</td>
<td>This attribute holds the type of object you want to reconcile. Default value: Group</td>
</tr>
</tbody>
</table>
### Table 3-7 (Cont.) Attributes of the Active Directory Group Delete Recon Scheduled Job

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Object Name</td>
<td>Enter the name of the resource object against which reconciliation runs must be performed.</td>
</tr>
<tr>
<td></td>
<td><strong>Default value:</strong> AD Group</td>
</tr>
<tr>
<td>Scheduled Task Name</td>
<td>This attribute holds the name of the scheduled task.</td>
</tr>
<tr>
<td></td>
<td><strong>Default value:</strong> Active Directory Group Delete Recon</td>
</tr>
<tr>
<td>Sync Token</td>
<td>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 Manager.</td>
</tr>
<tr>
<td></td>
<td>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 Manager.</td>
</tr>
<tr>
<td></td>
<td>This attribute stores values in the following format:</td>
</tr>
<tr>
<td></td>
<td>(&lt;\text{String}&gt;0</td>
</tr>
<tr>
<td></td>
<td>A value of <strong>True</strong> in the preceding format specifies that the Global Catalog Server is used during delete reconciliation runs. In addition, <strong>DOMAIN_CONTROLLER</strong> is replaced with the name of the domain controller on which the Global Catalog Server is running.</td>
</tr>
<tr>
<td></td>
<td>A value of <strong>False</strong> specifies that the Global Catalog Server is not used during delete reconciliation runs. In addition, <strong>DOMAIN_CONTROLLER</strong> is replaced with the name of the domain controller from which data about deleted records is fetched.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Enter the name of the organization to which data about all deleted groups fetched from the target system is linked. There are two scenarios in which group reconciliation is performed. These scenarios are described in <strong>Configuring and Running Group Reconciliation</strong>.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

### 3.4 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:
3.4.1 Reconciling Target System Groups into Individual Organizations

Create an organizational unit in Oracle Identity Manager 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:

1. Ensure that the value of the Configuration Lookup parameter of the IT resource is set to Lookup.Configuration.ActiveDirectory.
2. Search for and open the Active Directory Group Recon scheduled job.
3. 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.

3.4.2 Reconciling Target System Groups a Single Organization

This section discusses the procedure to perform group reconciliation when all groups available on the target system must be reconciled under the same organizational unit in Oracle Identity Manager. 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.
4. Change the Decode value of the OIM Org Name entry from sAMAccountName to Organization Name.
5. Save and close the lookup definition.
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.

### 3.5 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:


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 Manager 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.


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.
3.6 Configuring Scheduled Jobs

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

You can apply this procedure to configure the scheduled jobs for lookup field synchronization and reconciliation.

To configure a scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1:
   a. Log in to the Administrative and User Console.
   b. On the Welcome to Oracle Identity Manager Self Service page, click Advanced in the upper-right corner of the page.
   c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click Search Scheduled Jobs.

2. If you are using Oracle Identity Manager release 11.1.2.x:
   a. Log in to Oracle Identity System Administration.
   b. In the left pane, under System Management, click Scheduler.

3. Search for and open the scheduled task as follows:
   a. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click Advanced Search and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. On the Job Details tab, you can modify the 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.

   ![Note]

   See Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager for detailed information about schedule types.

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

5. On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.
6. Click **Apply** to save the changes.

**Note:**

The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

### 3.7 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:

- [About Configuring Action Scripts](#)
- [Running a Custom PowerShell Script](#)
- [Running a Script Before a Create Provisioning Operation](#)
- [Running Actions Using Visual Basic Scripts for Users](#)
- [Important Notes on Running Actions Scripts](#)
- [Guidelines on Creating Scripts](#)

#### 3.7.1 About Configuring Action Scripts

The following is a summary of the procedure to configure action scripts:

- On the computer hosting the connector server, create the custom script (for example, PowerShell) in a directory. This script should be self-sufficient, that is, it should be able to create, maintain, and delete sessions with the target AD server and complete all actions against it.
- On the computer hosting Oracle Identity Manager, create a batch (.bat) file. This batch file runs on the computer hosting the connector server, which in turn calls
the custom script (for example, PowerShell) available on the connector server host computer. Even if Oracle Identity Manager is installed on a UNIX-based computer, create a batch file.

For a custom PowerShell script, the batch file runs the custom PowerShell script using the Powershell.exe program. For more information on Powershell.exe, see http://technet.microsoft.com/en-us/library/hh847736.aspx.

• Add entries to the Lookup.ActiveDirectory.UM.Configuration lookup definition.

Table 3-8 describes the entries to be added to the Lookup.ActiveDirectory.UM.Configuration lookup definition for running actions scripts.

Table 3-8 Lookup Entries for Running Action Scripts

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIMING Action Language</td>
<td>Scripting language of the script you want to run. For a custom shell script, enter Shell as the decode value.</td>
</tr>
<tr>
<td>TIMING Action File</td>
<td>Full path and name to the file containing the script to be run. Note that the file containing the script must be located on the computer on which Oracle Identity Manager is running.</td>
</tr>
<tr>
<td>TIMING Action Target</td>
<td>Context in which the script must be run. Enter Resource as the decode value.</td>
</tr>
</tbody>
</table>

In the preceding table, TIMING defines when an action must be performed. An action can be invoked either before or after a create, update, or delete provisioning operation. Therefore, TIMING can be replaced with any of the following values:

Before Create
Before Update
Before Delete
After Create
After Update
After Delete

All the entries in Table 3-8 define an action together. Therefore, to configure action scripts, all the entries must be defined. Otherwise, no action is performed.

3.7.2 Running a Custom PowerShell Script

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 the Lookup.ActiveDirectory.UM.Configuration lookup definition.
3. Add the following new values:
   • Code Key: TIMING Action Language  
     Sample value: Before Create Action Language
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 Manager 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 Manager, create the /scratch/Scripts/InvokeCustomScript.bat file with the following content:

   ```powershell
   Powershell.exe -File NAME_AND_FULL_LOCATION_OF_THE_CUSTOM_SCRIPT
   Exit
   ```

   - **Sample value**:
     ```powershell
     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:

   ```powershell
   $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 Manager, 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 the Lookup.ActiveDirectory.UM.ProvAttrMap lookup definition and be mapped to a corresponding target system attribute. For example, you can pass the First Name process form field (present in the Lookup.ActiveDirectory.UM.ProvAttrMap lookup definition) 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.

3.7.3 Running a Script Before a Create Provisioning Operation

The following is an example procedure for running a script before a create provisioning operation:

1. Create a file named script.bat (extension doesn't matter) with following line:
   
   ```
   echo create >> C:\%givenName%.txt
   ```

2. Log in to the Design Console.

3. Expand Administration and then double-click Lookup Definition.

4. Search for and open the Lookup.ActiveDirectory.UM.Configuration lookup definition and add the following entries:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before Create Action Language</td>
<td>Shell</td>
</tr>
<tr>
<td>Before Create Action File</td>
<td>/scratch/jdoe/script/script.bat</td>
</tr>
<tr>
<td>Before Create Action Target</td>
<td>Resource</td>
</tr>
</tbody>
</table>

   `Figure 3-1` shows the Lookup.ActiveDirectory.UM.Configuration lookup definition with the newly added action script entries.
5. Save and close the lookup definition.
7. Provision a user account. You notice that the script (created in Step 1) is run and a file with the value specified for the givenName attribute is created on the target system.

You can also configure actions by using Visual Basic scripts. Although Visual Basic scripts are not directly supported, a Visual Basic script can be called using a shell script.

### 3.7.4 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 Manager 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:

   ```vbs
   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 Manager.

### 3.7.5 Important Notes on Running Actions Scripts

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 Manager.
- 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.

### 3.7.6 Guidelines on Creating Scripts

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.UM.ProvAttrMap
  - 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.'
Provisioning a resource for an OIM user involves using Oracle Identity Manager to create a Microsoft Active Directory account for the user.

Information pertaining to performing provisioning operations is discussed in the following topics:

- About Performing Provisioning Operations in Oracle Identity Manager
- Direct Provisioning
- Request-Based Provisioning
- Switching Between Request-Based Provisioning and Direct Provisioning

3.8.1 About Performing Provisioning Operations in Oracle Identity Manager

When you install the connector on Oracle Identity Manager, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you configure the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Switching Between Request-Based Provisioning and Direct Provisioning.

This following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

See Also:

Manually Completing a Task in Performing Self Service Tasks with Oracle Identity Manager for information about the types of provisioning

3.8.2 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   a. On the Welcome to Identity Administration page, in the Users region, click Create User.
b. On the user details page, enter values for the OIM User fields, and then click **Save**. Figure 3-2 shows this page.

**Figure 3-2  User Details Page**

3. If you want to provision a target system account to an existing OIM User, then:
   a. On the Welcome to Identity Administration page, search for the OIM User by selecting Users from the list on the left pane.
   b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.

4. On the user details page, click the **Resources** tab.

5. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

6. On the Step 1: Select a Resource page, select **AD User** from the list and then click **Continue**. Figure 3-3 shows the Step 1: Select a Resource page.

**Figure 3-3  Step 1: Select a Resource Page**

7. On the Step 2: Verify Resource Selection page, click **Continue**. Figure 3-4 shows the Step 2: Verify Resource Selection page.
8. On the Step 5: Provide Process Data for Active Directory Users Form page, enter the details of the account that you want to create on the target system and then click Continue. Figure 3-5 shows the user details added.

9. If required, on the Step 5: Provide Process Data for Assigned Groups Form page, search for and select a group for the user on the target system and then click Continue. Figure 3-6 shows this page.
10. On the Step 6: Verify Process Data page, verify the data that you have provided and then click Continue. Figure 3-7 shows Step 6: Verify Process Data page.

11. Close the window displaying the "Provisioning has been initiated" message.

12. On the Resources tab, click Refresh to view the newly provisioned resource.
3.8.3 Request-Based Provisioning

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

Note:
The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- End User's Role in Request-Based Provisioning
- Approver's Role in Request-Based Provisioning

3.8.3.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click Advanced on the top right corner of the page.
3. On the Welcome to Identity Administration page, click the Administration tab, and then click the Requests tab.
4. From the Actions menu on the left pane, select Create Request. The Select Request Template page is displayed.
5. From the Request Template list, select Provision Resource and click Next.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click Search. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the Available Users list, select the user to whom you want to provision the account.
   If you want to create a provisioning request for more than one user, then from the Available Users list, select users to whom you want to provision the account.
8. Click Move or Move All to include your selection in the Selected Users list, and then click Next.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select AD User, move it to the Selected Resources list, and then click Next.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click Next.
If you are setting values for the Terminal Services Profile fields, then you must select the Remote Manager IT resource.

12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
   - Effective Date
   - Justification
   A message confirming that your request has been sent successfully is displayed along with the Request ID.

13. If you click the request ID, then the Request Details page is displayed.

14. To view details of the approval, on the Request Details page, click the **Request History** tab.

### 3.8.3.2 Approver's Role in Request-Based Provisioning

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the Approvals tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.
   A message confirming that the task was approved is displayed.

### 3.8.4 Switching Between Request-Based Provisioning and Direct Provisioning

If you have configured the connector for request-based provisioning, you can always switch to direct provisioning. Similarly, you can always switch back to request-based provisioning any time. This section discusses the following topics:

- **Switching From Request-Based Provisioning to Direct Provisioning**
- **Switching From Direct Provisioning to Request-Based Provisioning**

#### 3.8.4.1 Switching From Request-Based Provisioning to Direct Provisioning

> **Note:**
>
> It is assumed that you have performed the procedure described in Configuring Oracle Identity Manager for Request-Based Provisioning.

If you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **AD User** process definition.
   c. Deselect the Auto Save Form check box.
   d. Click the Save icon.

3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **AD User** resource object.
   c. Deselect the Self Request Allowed check box.
   d. Click the Save icon.

### 3.8.4.2 Switching From Direct Provisioning to Request-Based Provisioning

If you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.

2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **AD User** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.

3. If you want to enable end users to raise requests for themselves, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **AD User** resource object.
   c. Select the Self Request Allowed check box.
   d. Click the Save icon.

### 3.9 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a Microsoft Active Directory account for the user.

To perform provisioning operations in Oracle Identity Manager release 11.1.2 or later:

1. Log in to Oracle Identity Administrative and User console.

2. Create a user. See Managing Users in *Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.

3. On the Account tab, click **Request Accounts**.

4. In the Catalog page, search for and add to cart the application instance created in *Creating an Application Instance*, and then click **Checkout**.

5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.

7. If you want to provision entitlements, then:
   a. On the Entitlements tab, click **Request Entitlements**.
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout**.
   c. Click **Submit**.

### 3.10 Uninstalling the Microsoft Active Directory User Management Connector

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

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

**Note:**

- The connector cannot be uninstalled if a valid access policy is present in Oracle Identity Manager. As a workaround, create a dummy resource type by using the design console. Remove the dependent access policy by directing it to a dummy resource type and then remove the dependency from the resource type that must be deleted.
- Uninstalling the connector removes only those IT resource definitions (and its IT resources) that are attached with the process form. However, the IT resource of the Connector Server IT Resource Type Definition is not removed for Oracle Identity Manager.
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:

**Note:**

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

- Adding Dynamic Auxiliary Object Classes and Their Attributes to Users
- 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
- Configuring the Connector for User-Defined Object Classes
- Adding Dynamic Auxiliary Object Classes and Their Attributes to Users
- Adding the Group Name (pre-Windows 2000) Attribute
- New Fields for Trusted Source Reconciliation
- Configuring Transformation of Data During Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning
- 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
- Configuring the Connector for Provisioning and Reconciling Custom Object Categories
4.1 Adding Custom Fields for Target Resource Reconciliation

You can add additional fields for user, 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.

By default, the fields listed in Table 1-14 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional fields for user, group, or organizational unit reconciliation.

To add a custom field for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the custom field to the list of reconciliation fields in the resource object as follows:
   b. Search for and open one of the following resource objects:
      - For users: AD User
      - 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 users: Lookup.ActiveDirectory.UM.ReconAttrMap
      - 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 users: **UD_ADUSER**
      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_ADUSER_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 Manager 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 users: **AD User**
      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**.
4.2 Adding New Multivalued Fields for Target Resource Reconciliation

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

**Note:**

This procedure can be applied to add either user, 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 Manager natively.

By default, the multivalued fields listed in Table 1-14 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued fields for target resource reconciliation.

To add a new multivalued field for target resource reconciliation:

1. Log in to the Oracle Identity Manager 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**. Figure 4-1 shows the 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 users: UD_ADUSER
      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. Figure 4-2 shows the child form added to the process form.

4. If you are using Oracle Identity Manager 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 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 users: AD User

   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 4-3 shows the new reconciliation field added in the resource object.
Figure 4-3  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 users: **Lookup.ActiveDirectory.UM.ReconAttrMap**
      
      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. **Figure 4-4** shows the lookup code added to the lookup definition.
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 users: **AD User**
      For groups: **AD Group**
      For organizational units: **AD Organizational Unit**
   c. On the Reconciliation Field Mappings tab of the AD User (or 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**. 
      Figure 4-5 shows the new reconciliation field mapped to a process data field in the process definition.
4.3 Adding Custom Fields for Provisioning

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

By default, the attributes listed in Table 1-19 are mapped for provisioning between Oracle Identity Manager and the target system.

To add a custom field for provisioning, 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

4.3.1 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, 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 Manager Design Console.
2. Expand **Development Tools** and then double-click **Form Designer**.

3. Search for and open one of the following process forms:
   - For users: **UD_ADUSER**
   - 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_ADUSER_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**.

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

If you are using Oracle Identity Manager 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 activate a sandbox. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 3.c), and then save the application instance.

5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

6. Run the Form Upgrade Job scheduled task. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for a description of the Form Upgrade Job scheduled task.

### 4.3.3 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 Manager Design Console.

2. Expand **Administration** and then double-click **Lookup Definition**.

3. Search for and open one of the following lookup definitions:
   - For users: **Lookup.ActiveDirectory.UM.ProvAttrMap**
   - 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**.

### 4.3.4 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 users: **AD User**
      - 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 User custom field, then repeat Steps 3 through 5 for the remaining variables listed in the Adapter Variables region. The following table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter Return Variable</td>
<td>Response</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>itResourceFieldName</td>
<td>Literal</td>
<td>String</td>
<td>UD_ADUSER_SERVER</td>
</tr>
<tr>
<td>attrFieldName</td>
<td>Literal</td>
<td>String</td>
<td>Description</td>
</tr>
<tr>
<td>objectType</td>
<td>Literal</td>
<td>String</td>
<td>User</td>
</tr>
</tbody>
</table>

7. 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:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>procInstanceKey</td>
<td>Process</td>
<td>Process</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Data</td>
<td>Instance</td>
<td></td>
</tr>
<tr>
<td>Adapter Return Variable</td>
<td>Response</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>itResourceFieldName</td>
<td>Literal</td>
<td>String</td>
<td>UD_ADGRP_SERVER</td>
</tr>
<tr>
<td>attrFieldName</td>
<td>Literal</td>
<td>String</td>
<td>CUSTOM_FIELD_NAME</td>
</tr>
<tr>
<td>objectType</td>
<td>Literal</td>
<td>String</td>
<td>Group</td>
</tr>
</tbody>
</table>

8. 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:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>procInstanceKey</td>
<td>Process</td>
<td>Process</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Data</td>
<td>Instance</td>
<td></td>
</tr>
<tr>
<td>Adapter Return Variable</td>
<td>Response</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Map To</td>
<td>Qualifier</td>
<td>Literal Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>-----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>itResourceFieldName</td>
<td>Literal</td>
<td>String</td>
<td>UD_ADOU_SERVER</td>
</tr>
<tr>
<td>attrFieldName</td>
<td>Literal</td>
<td>String</td>
<td>CUSTOM_FIELD_NAME</td>
</tr>
<tr>
<td>objectType</td>
<td>Literal</td>
<td>String</td>
<td>organizationalUnit</td>
</tr>
</tbody>
</table>

9. 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**.

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

### 4.3.5 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:

   ```xml
   <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.

4.3.6 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 Purging Cache in Oracle Fusion Middleware Administering Oracle Identity Manager for more information about running the PurgeCache utility.

4.3.7 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.

See Importing Request Datasets for detailed information about the procedure.

4.4 Adding New Multivalued Fields for Provisioning

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. 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
4.4.1 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 Manager Design Console.
2. Expand Administration and double-click Lookup Definition.
3. Search for and open one of the lookup definitions:
   - For a user field on Microsoft Active Directory, open Lookup.ActiveDirectory.UM.ProvAttrMap.
   - For a group field on Microsoft Active Directory, open Lookup.ActiveDirectory.GM.ProvAttrMap.
   - For an 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.

   For example, enter UD_CARLICEN~Car License in the Code Key field and then enter carLicense in the Decode field. Figure 4-6 shows the entry added to the lookup definition.
4.4.2 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 users: **AD User**
   - 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. Figure 4-7 shows the multivalued task added to the process.

![Figure 4-7 Multivalued Field Added to the AD User Provisioning Process](image)

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 User multivalued field, then repeat Steps 8 through 10 for the remaining variables listed in the Adapter Variables region. The following table lists values that you must select from the Map To, Qualifier, and Literal Value lists for each variable:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter Return Variable</td>
<td>Response Code</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>
### Adding New Multivalued Fields for Provisioning

12. 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:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>itResourceFieldName</td>
<td>Literal</td>
<td>String</td>
<td>UD_ADUSER_SERVER</td>
</tr>
<tr>
<td>childTableName</td>
<td>Literal</td>
<td>String</td>
<td>UD_CARLICEN</td>
</tr>
<tr>
<td>objectType</td>
<td>Literal</td>
<td>String</td>
<td>User</td>
</tr>
</tbody>
</table>

13. 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:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>procInstanceKey</td>
<td>Process Data</td>
<td>Process Instance</td>
<td>NA</td>
</tr>
<tr>
<td>Adapter Return Variable</td>
<td>Response Code</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>itResourceFieldName</td>
<td>Literal</td>
<td>String</td>
<td>UD_ADGRP_SERVER</td>
</tr>
<tr>
<td>childTableName</td>
<td>Literal</td>
<td>String</td>
<td>UD_CHILD_PROCES S_FORM_NAME</td>
</tr>
<tr>
<td>objectType</td>
<td>Literal</td>
<td>String</td>
<td>organizationalUnit</td>
</tr>
</tbody>
</table>

14. 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**.

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

16. 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**.

17. 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.

18. Click Save on Process Task.

4.4.3 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:

   ```xml
   <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.

4.4.4 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 *Administering Oracle Identity Manager* for more information about the PurgeCache utility.

4.4.5 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.
See *Importing Request Datasets* for detailed information about the procedure.

4.5 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:
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

### 4.6 Configuring the Connector for User-Defined Object Classes

You can configure the connector for user-defined or custom object class for connector operations.

By default, the Active Directory User Management connector supports the User object class. If you want the connector to use a user-defined or custom object class for connector operations, then:

1. Create the object class and assign mandatory and optional attributes to the object class.
   Refer to Microsoft documentation for information about creating the object class.

   **Note:**
   Assign the user object class as the parent of the object class that you create.

2. Refresh the schema.
3. Add the mandatory and optional attributes of the object class for provisioning.
4. Update the Lookup.Configuration.ActiveDirectory lookup definition as follows:
   b. Search for the ObjectClass code key entry and change its decode value to include the name of the new object class.
   c. If the object class contains more than one mandatory attribute, then add a new lookup entry with the following values:
      Code Key: ObjectClassMandatoryAttributes
      Decode: "CUSTOM_MANDATORY_ATTRIBUTE_NAME"
   d. Click the Save icon.

4.7 Adding Dynamic Auxiliary Object Classes and Their Attributes to Users

You can add dynamic auxiliary object classes and their attributes to users.

To perform the procedure described in this section, all domain controllers in the forest must be running Microsoft Windows Server 2003 or later, and the forest functional mode must be Microsoft Windows Server 2003 or later. For more information on dynamic auxiliary object classes, see "Dynamically Linked Auxiliary Classes (Windows)" at the following Web site:


To add dynamic auxiliary object classes and their attributes to users:

1. Create an entry for the dynamic auxiliary object class in the main configuration lookup definition as follows:
   a. Expand Administration and then double-click Lookup Definition.
   c. Click Add and enter the Code Key and Decode values as follows:
      Code Key: 'AccountObjectClasses'
Decoding: "NAME_OF_THE_CUSTOM_AUXILIARY_OBJECT_CLASS"

**Note:**

While adding the value in the decode column, two or more auxiliary classes must be separated by a comma (,). For example, "AuxIntAttr", "AuxStringAttr".

d. If the dynamic auxiliary class contains more than one mandatory attribute, then add a new lookup entry with the following values:

**Code Key:** ObjectClassMandatoryAttributes

**Decode:** "MANDATORY_ATTRIBUTE_NAME_OF_THE_AUX_CLASS"

**Note:**

Two or more mandatory attributes must be separated by a comma (,). For example, "AuxIntAttr", "AuxStringAttr".

e. Click the Save icon.

2. Run the PurgeCache utility.

To add attributes of the custom auxiliary classes (added in Step 1) for target resource reconciliation and provisioning, perform the procedure described in the following sections:

**Note:**

While performing the procedure described in these sections, ensure that you follow instructions that are specific only to the User object class.

### 4.8 Adding the Group Name (pre-Windows 2000) Attribute

You can add a group name (pre-Windows 200) 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

### 4.8.1 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 Manager 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 Manager for reconciliation and provisioning operations.

### 4.8.2 Adding the Group Name Pre Windows Field for Reconciliation

To add the Group Name Pre Windows field for reconciliation:

1. Log in to the Oracle Identity Manager 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 4-1** lists the updated list of entries in the Lookup.ActiveDirectory.GM.ReconAttrMap lookup definition.

<table>
<thead>
<tr>
<th>Group Field on Oracle Identity Manager</th>
<th>Microsoft Active Directory Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>displayName</td>
</tr>
<tr>
<td>Group name</td>
<td>cn</td>
</tr>
<tr>
<td>Group Name Pre Windows</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>Group Type</td>
<td>groupType</td>
</tr>
<tr>
<td>OIM Org Name</td>
<td>sAMAccountName</td>
</tr>
</tbody>
</table>
Table 4-1  (Cont.) Entries in the Updated Lookup.ActiveDirectory.GM.ReconAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Group Field on Oracle Identity Manager</th>
<th>Microsoft Active Directory Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Name[LOOKUP]</td>
<td>ad_container</td>
</tr>
<tr>
<td>Org Name</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>Org Type</td>
<td>OIM Organization Type</td>
</tr>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
</tr>
</tbody>
</table>

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:
   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.


7. Click Create Reconciliation Profile.

4.8.3 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:
4.8.3.1 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 Manager 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.

4.8.3.2 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 sAMAccountName.
5. In the Code Key column, locate and replace Group Name with Group Name[IGNORE], and change its Decode value to IGNORED. Table 4-1 lists the updated list of entries in the Lookup.ActiveDirectory.GM.ProvAttrMap lookup definition.
Table 4-2  Entries in the Updated Lookup.ActiveDirectory.GM.ProvAttrMap Lookup Definition

<table>
<thead>
<tr>
<th>Group Field on Oracle Identity Manager</th>
<th>Microsoft Active Directory Field</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAME</strong></td>
<td><strong>NAME</strong>=&quot;CN=${Group_Name},${Organization_Name}&quot;</td>
</tr>
<tr>
<td>Display Name</td>
<td>displayName</td>
</tr>
<tr>
<td>Group Name[IGNORE]</td>
<td>IGNORED</td>
</tr>
<tr>
<td>Group Name Pre Windows</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>Group Type</td>
<td>groupType</td>
</tr>
<tr>
<td>Organization Name[LOOKUP,IGNORE]</td>
<td>IGNORED</td>
</tr>
<tr>
<td>Unique Id</td>
<td><strong>UID</strong></td>
</tr>
</tbody>
</table>

6. Click Save.

4.8.3.3 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:
   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 adpADICUPDATEATTRIBUTEVALUE.
   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:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>procInstanceKey</td>
<td>Process Data</td>
<td>Process Instance</td>
<td>NA</td>
</tr>
<tr>
<td>Adapter Return</td>
<td>Response Code</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>itResourceFieldName</td>
<td>Literal</td>
<td>String</td>
<td>UD_ADGRP_SERVER</td>
</tr>
<tr>
<td>attrFieldName</td>
<td>Literal</td>
<td>String</td>
<td>Group Name Pre Windows</td>
</tr>
<tr>
<td>objectType</td>
<td>Literal</td>
<td>String</td>
<td>Group</td>
</tr>
</tbody>
</table>

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.

4.8.3.4 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:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Map To</th>
<th>Qualifier</th>
<th>Literal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>procInstanceKey</td>
<td>Process Data</td>
<td>Process Instance</td>
<td>NA</td>
</tr>
<tr>
<td>Adapter Return</td>
<td>Response Code</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>itResourceFieldName</td>
<td>Literal</td>
<td>String</td>
<td>UD_ADGRP_SERVER</td>
</tr>
<tr>
<td>attrFieldName</td>
<td>Literal</td>
<td>String</td>
<td>Group Name Pre Windows</td>
</tr>
<tr>
<td>objectType</td>
<td>Literal</td>
<td>String</td>
<td>Group</td>
</tr>
</tbody>
</table>
4.8.3.5 Updating the Request Dataset

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:

```xml
<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 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.

4.8.3.6 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 Administering Oracle Identity Manager for more information about the PurgeCache utility.

4.8.3.7 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.

4.9 New Fields for Trusted Source Reconciliation

You can add new fields for trusted source reconciliation.

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

By default, the attributes listed in Table 1-22 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new fields for trusted source reconciliation. This section discusses the following topics:

• Summary of Steps to Add New Fields for Trusted Source Reconciliation
• Determining the Target System Name of the New Field for Trusted Source Reconciliation
• Adding a New Field for Trusted Source Reconciliation
4.9.1 Summary of Steps to Add New Fields for Trusted Source Reconciliation

To add new fields for trusted source reconciliation, you must perform the following steps:

1. Determine the target system name of the new field for trusted source reconciliation. See Determining the Target System Name of the New Field for Trusted Source Reconciliation for detailed information.

2. Add a new field for trusted source reconciliation. See Adding a New Field for Trusted Source Reconciliation for detailed information.

4.9.2 Determining the Target System Name of the New Field for Trusted Source Reconciliation

Before you add a new field for trusted source reconciliation, you must first determine the target system name of the field as follows:

1. Install the target system schema, if it is not already installed.
   Refer to the Microsoft Web site for information about installing the schema.

   Note:
   The ADSIEdit tool provides an alternative to installing and using the target system schema for determining the name of the field that you want to add. The Microsoft Web site provides information about using this tool.

2. Open the target system schema.

3. Expand the Console Root folder, expand the target system schema, and then double-click Classes.

4. Right-click user, and then select Properties.
   The Attributes tab displays the attributes (that is, fields) that are currently in use on the target system.

5. Note down the name of the field that you want to add, and then click Cancel.
   For example, if you want to add the Employee ID field for reconciliation, then note down employeeID.

4.9.3 Adding a New Field for Trusted Source Reconciliation

To add a new field for trusted source reconciliation:

1. Log in to the Oracle Identity Manager Design Console.

2. Add the new field on the OIM User process form as follows:
Note:

- If you are using Oracle Identity Manager 11g Release 1 PS1 or later, then you must use the Oracle Identity Manager Advanced Administration page to create UDFs.
- If you are using Oracle Identity Manager 11g Release 2 or later, then see Configuring Custom Attributes in Administering Oracle Identity Manager for information on creating UDFs.

a. Expand Administration.

b. Double-click User Defined Field Definition.

c. Search for and open the Users form.

d. Click Add and enter the details of the field.

   For example, if you are adding the Employee ID field, then enter Employee ID in the Name field, set the data type to String, enter USR_UDF_EMPLOYEE_ID as the column name, and enter a field size value.

e. Click Save.

3. Add the new field to the list of reconciliation fields in the resource object as follows:

   a. Expand the Resource Management folder.

   b. Double-click Resource Objects.

   c. Search for and open one of the following resource objects:

      For users: AD User Trusted

      For groups: AD Group

      For organizational units: AD Organizational Unit

   d. On the Object Reconciliation tab, click Add Field.

   e. Enter the details of the field and click Save.

      For example, enter Employee ID in the Field Name field and select String from the Field Type list.

      Later in this procedure, you will enter the field name as the Decode value of the entry that you create in the lookup definition for reconciliation.

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

4. Create a reconciliation field mapping for the new field as follows:


   b. Double-click Process Definition.

   c. Search for and open the AD User Trusted process definition.

   d. On the Reconciliation Field Mappings tab, click Add Field Map.

   e. In the Field Name field, select the value for the field that you want to add.

      For example, select Employee ID = Employee ID.
f. Click **Save**.

5. 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 the
      Search for and open the
      **Lookup.ActiveDirectoryLDS.UUM.ReconAttrMap.Trusted** lookup definition if 
      you are using Microsoft AD LDS.
   c. Click **Add** and then enter the Code Key and Decode values for the field. The 
      Code Key value must be the name of the field created in the AD User Trusted 
      resource object. The Decode value is the name of the corresponding field on 
      the target system.

      ![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.

      For example, enter `employeeID` in the Code Key field and then enter `Employee 
      ID` in the Decode field.

   d. Click **Save**.

6. Select **Field Type** and click **Save**.

### 4.10 Configuring Transformation of Data During Reconciliation

You can configure transformation of reconciled single-valued account data according 

You can configure transformation of reconciliation. For example, you can use User Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

![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 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) {}

The following is a sample transformation class:

```java
import java.util.*;
public class MyTransformer {
    /*
     * Description:Abstract method for transforming the attributes
     * param hmUserDetails<String,Object>
     * HashMap containing parent data details
     * param hmEntitlementDetails <String,Object>
     * HashMap containing child data details
     */
    public Object transform(HashMap hmUserDetails, HashMap hmEntitlementDetails, String sField) {
        /*
        * You must write code to transform the attributes.
        * Parent data attribute values can be fetched by
        * using hmUserDetails.get("Field Name").
        * To fetch child data values, loop through the
        * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
        * Return the transformed attribute.
        */
        String firstName= (String)hmUserDetails.get("First Name");
        firstName= "blahPrefix" + firstName + "blahSuffix";
        System.out.println("First Name Value is changed to: " + firstName);
        return firstName;
    }
    } /* End */
```

The method defined in this class transforms the value of the First Name attribute by prefixing the first name with `blahPrefix` and suffixing the first name with `blahSuffix`, and returns the transformed value.

2. Create a JAR file to hold the Java class.

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

   For Microsoft Windows:
   
   `OIM_HOME/server/bin/UploadJars.bat`

   For UNIX:
   
   `OIM_HOME/server/bin/UploadJars.sh`

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host
4. Add an entry in the lookup definition for transformation as follows:
   a. Log in to the Design Console.
   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.UM.Configuration.Trusted` lookup definition:
- **Code Key** value: `Recon Transformation Lookup`
- **Decode** value: `Lookup.ActiveDirectory.UM.ReconTransformation`

### 4.11 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the 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.

**See Also:**
The Javadocs shipped with the connector for more information about this interface

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

```java
package com.validate;
import java.util.*;
public class MyValidation {
    public boolean validate(String attributeName, String attributeValue) {
        // Your validation logic goes here
        return false; // Default return value
    }
}
```
public boolean validate(HashMap hmUserDetails,
HashMap hmEntitlementDetails, String field) {
    /*
    * You must write code to validate attributes. Parent
    * data values can be fetched by using hmUserDetails.get(field)
    * For child data values, loop through the
    * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
    * Depending on the outcome of the validation operation,
    * the code must return true or false.
    */
    /*
    * In this sample code, the value "false" is returned if the field
    * contains the number sign (#). Otherwise, the value "true" is
    * returned.
    */
    boolean valid=true;
    String sUserID=(String) hmUserDetails.get(field);
    for(int i=0;i<sUserID.length();i++){
        if (sUserID.charAt(i) == '#'){
            valid=false;
            break;
        }
    }
    return valid;
}

2. Create a JAR file to hold the Java class.

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

   <Note:
   Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.
   
   For Microsoft Windows:
   OIM_HOME/server/bin/UploadJars.bat
   For UNIX:
   OIM_HOME/server/bin/UploadJars.sh
   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
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 the Lookup.ActiveDirectory.UM.Configuration lookup definition.
f. Ensure that the value of the Recon Validation Lookup entry is set to Lookup.ActiveDirectory.UM.ReconValidation.
g. Save the changes to the lookup definition.

5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Search for and open the Lookup.ActiveDirectory.UM.ProvValidation lookup definition.
   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 the Lookup.ActiveDirectory.UM.Configuration lookup definition.
   f. Ensure that the value of the Provisioning Validation Lookup entry is set to Lookup.ActiveDirectory.UM.ProvValidation.
   g. Save the changes to the lookup definition.

This completes the procedure for configuring validation of data. For data that fails the validation check, the following message is displayed or recorded in the log file:

Value returned for field FIELD_NAME is false.

4.12 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:
4.12.1 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

4.12.1.1 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 Manager, 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 Manager.

4.12.1.2 Enabling Reconciliation Across Multiple Domains

To enable reconciliation across multiple domains:

1. Set the value of the SearchChildDomains entry to yes in one of the following lookup definitions:

2. Specify the name of the domain controller that is hosting the Global Catalog Server as the value of the SyncGlobalCatalogServer IT resource parameter.
### 4.12.2 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 LDAPHostName 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.
4.13 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.

4.14 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
- Prerequisites for Performing Provisioning With Multiple Installations of the Target System
- Performing Provisioning Operations On Oracle Identity Manager
4.14.1 About Multiple Installations of the Target System

Note:

The information in this section also applies to Microsoft AD LDS.

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 Manager release 11.1.1.x, then only the IT resource information must be changed. If you are using Oracle Identity Manager release 11.1.2.x, then the IT resource information must be changed and application instances must be created.

In addition, irrespective of the Oracle Identity Manager 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. For more information about cloning the connector, see About Cloning the Microsoft Active Directory User Management Connector.

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 Manager, and they want to configure Oracle Identity Manager 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.

Summary of steps to configure the connector for multiple installations of the target system is as follows:

1. Configure the connector for multiple installations of the target system.
2. Complete the prerequisite steps for performing provisioning operations with multiple instances of the target system.
3. Perform provisioning operations.

4.14.2 Configuring the Connector for Multiple Installations of the Target System

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
Manager release 11.1.2.x or later, then in addition to creating the IT resource, you must create the application instance.

See Configuring the IT Resource for Microsoft AD and AD LDS for information about the values to be specified for the IT resource parameters.

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.

See Reconciliation Scheduled Jobs for information about the values to be specified for the scheduled task attributes.

3. Manually synchronize the lookup definitions in Oracle Identity Manager with the lookup field values on the target system.

4.14.3 Prerequisites for Performing Provisioning With Multiple Installations of the Target System

The User Principal Name field on the process form is pre-populated with values from the User ID field and the UPN Domain IT resource parameter. Before you perform provisioning operations on Oracle Identity Manager release 11.1.1.x and switch to a different IT resource during a provisioning operation, you must change the IT resource to which the User Principal Name field is mapped.

1. Expand Development Tools, and double-click Form designer.
2. Search for and open the AD User form.
3. On the Pre-Populate tab, double-click the User Principal Name row.
4. In the Pre-Population adapter dialog box, double-click the IT resource that you are currently using (for example, Active Directory).
5. From the Qualifier list in the Map Adapter Variables dialog box, select the IT resource that you want to use. For example, select Active Directory. Then, click the Save icon and close the dialog box.
6. In the Pre-Population adapter dialog box, click the Save icon and close the dialog box.
7. Click the Save icon on the Form Designer form.

4.14.4 Performing Provisioning Operations On Oracle Identity Manager

When you perform provisioning operations:

- On Oracle Identity Manager release 11.1.1.x:
  When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the Microsoft Active Directory installation to which you want to provision the user.

- On Oracle Identity Manager release 11.1.2.x or later:
  Perform the instructions described in Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later.
4.15 Creating a Home Directory After User Create Provisioning Operation

You can initiate the process task for home directory update after the Create User provisioning operation.

The following sections discuss the procedure to initiate the process task for home directory update after the Create User provisioning operation:

• About Creating a Home Directory After User Create Provisioning Operation
• Creating the UpdateHomeDirectoryField Adapter
• Updating the AD User Process Definition
• Updating the Create User Process Task

4.15.1 About Creating a Home Directory After User Create Provisioning Operation

While performing a Create User provisioning operation, you can specify a value for the Home Directory field. However, at times, due to the delay in replicating this information across all domain controllers, the following error is encountered:

The security ID structure is invalid.

To avoid this issue, you can create the home directory after successful completion of the Create User provisioning operation. This is achieved by creating a new process task that will be initiated upon successful completion of the Create User provisioning task.

Note:

During the Create User provisioning operation, do not specify a value for the Home Directory field. After the Create User provisioning operation completes successfully, the UpdateHomeDirTask process task updates the Home Directory field on the process form. This triggers the Homedirectory Updated task, which updates the home directory information for the user and creates it on the target system.

4.15.2 Creating the UpdateHomeDirectoryField Adapter

You must create an adapter (for example UpdateHomeDirectoryField) that can update the home directory for a user. To create the UpdateHomeDirectoryField adapter:

1. Log in to the Design Console.
2. Expand Development Tools, and double-click Adapter Factory.
3. On the Adapter Factory form, in the Adapter Name field, enter the name of the adapter, for example, UpdateHomeDirectoryField.
4. Double-click the Adapter Type lookup field. From the Lookup window that is displayed, select **Process Task**.

5. In the Description field, type a description for the adapter, for example, *This adapter is used to update the home directory for a user*.

6. Click the Save icon.
   
The adapter is created and stored in the Oracle Identity Manager database.

7. Add adapter variables as follows:
   a. On the Adapter Factory form, click the Variable List tab.
   b. Click **Add**.
      
The Add a Variable window is displayed.
   c. In the Variable Name field, enter the name of the adapter variable, for example, *networkShare*.
   d. From the Type menu, select **String**.
   e. From the Map To menu, select **Resolve at runtime**.
   f. Click the Save icon and close the window.
   g. Click **Add** to add another variable.
   h. In the Variable Name field, enter the name of the adapter variable, for example, *sAMAccountName*.
   i. From the Type menu, select **String**.
   j. From the Map To menu, select **Resolve at runtime**.
   k. Click the Save icon and close the window.

8. Create an adapter task of type utility as follows:
   a. On the Adapter Tasks tab, click **Add**.
   b. In the Adapter Task Selection dialog box, select **Utility Task**, ensure that **Utility** is selected from the list of utility tasks, and then click **Continue**.
   c. In the Object Instance Selection dialog box, ensure that **New Object Instance** is selected, and then click **Continue**. The Add An Adapter Factory Task dialog box displays.
   d. In the Task Name field, enter *HomeDirUpdateTask*.
   e. From the Application API list, select *
      
      com.thortech.xl.util.adapters.tcUtilStringOperations*.
   f. From the Methods list, select *
      
      com.thortech.xl.util.adapters.tcUtilStringOperations#performConcat()*.  
   g. Click the Save icon.
   h. Map adapter variables to the method inputs, and map method output to the Adapter return variable.
   i. Click **Set**.
   j. Click the Save icon and close the dialog box.

9. On the Adapter Factory form, click the Build icon.
   
   After the adapter is re-created, the Compile Status field will display the **OK** status.
4.15.3 Updating the AD User Process Definition

After creating the adapter, you must update the AD User process definition to include a new process task that contains the newly created adapter. To do so:

1. Expand **Process Management**, and then double-click **Process Definition**.
2. Search for and open the **AD User** process definition.
3. Create the UpdateHomeDirTask process task as follows:
   a. On the Tasks tab, click **Add**. The Creating New Task dialog box is displayed.
   b. In the Task Name field, enter the name of the process task, for example, **UpdateHomeDirTask**.
   c. In the Task Properties region, select **Conditional** and **Allow Multiple Instances**, and deselect **Required for Completion**.
   d. Click the Save icon.
4. On the Integration tab, in the Event Handler/Adapter region, click **Add**. The Handler Selection dialog box is displayed.
5. Select the **Adapter** option, and then from the list of adapters displayed in the Handler Name region, select **UpdateHomeDirectoryField** (the adapter created in **Creating the UpdateHomeDirectoryField Adapter**). This assigns the UpdateHomeDirectoryField adapter to the UpdateHomeDirTask process task.
6. Click the Save icon and close the dialog box.
7. On the Integration tab, in the Adapter Variables region, select the **networkShare** adapter variable.
8. Click **Map**.
9. In the Edit Data Mapping For Variable dialog box, create the following mapping:
   - **Variable Name**: networkShare
   - **Literal Value**: `\MY_SERVER\MY_SHARED_FOLDER`
10. Click the Save icon and close the dialog box.
11. On the Integration tab, in the Adapter Variables region, select the **sAMAccountName** adapter variable.
12. In the Edit Data Mapping For Variable dialog box, create the following mapping:
   - **Variable Name**: sAMAccountName
   - **Map To**: Process Data
   - **Literal Value**: Any process form field label whose value is the directory name. The literal value is usually the **User ID** field.
13. Click the Save icon and close the Editing Data Mapping for Variable dialog box.
14. Click the Save icon on the Process Definition form.
4.15.4 Updating the Create User Process Task

You must assign the newly created task to the Create User process task as follows:

1. Expand Process Management, and then double-click Process Definition.
2. Search for and open the AD User process definition.
3. On the Tasks tab, double-click Create User.
4. In the Editing Task dialog box, on the Responses tab, select the SUCCESS response code.
5. From the Tasks to Generate region, click Assign.
6. In the Assignment window, select the UpdateHomeDirTask task (created in Updating the AD User Process Definition).
7. Click OK.
   The UpdateHomeDirTask task is assigned to the process task.
8. Click the Save icon on the Process Definition form.

4.16 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 Manager. 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.
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 Manager.

4.17 Configuring the Connector for Provisioning and Reconciling Custom Object Categories

You can provision or reconcile a custom object category.
Note:
The procedure described in this section is applicable only if you are using AD LDS as the target system.

By default, the connector can provision to or reconcile only objects of the Person category. If you want the provision or reconcile custom object category, then perform the procedure discussed in this section. This sections contains the following topics:

- Adding Custom Object Category for Trusted Source Reconciliation
- Adding Custom Object Category for Target Resource Reconciliation
- Adding Custom Object Category for Provisioning

4.17.1 Adding Custom Object Category for Trusted Source Reconciliation

To configure the connector to reconcile records belonging to a custom object category during trusted source reconciliation:

1. Create a new task similar to the Active Directory User Trusted Recon task. In other words, clone the Active Directory User Trusted Recon task.

2. In the newly created scheduled task, add the **objectCategory** attribute.
   
   A new task is ready to perform trusted source reconciliation of a custom object category.

When you perform a trusted source reconciliation by using the scheduled task you created in this section, the connector will retrieve records of custom object that you specify as the value of the objectCategory attribute. If you do not specify a value for the objectCategory attribute, then objects of "Person" category are fetched.

4.17.2 Adding Custom Object Category for Target Resource Reconciliation

To configure the connector to reconcile records belonging to a custom object category during target resource reconciliation:

1. Make the following scheduled task specific changes:
   
   a. Create a new scheduled task similar to the Active Directory User Target Recon task. In other words, clone the Active Directory User Target Recon task.
   
   b. In the newly created scheduled task, add the **objectCategory** attribute.
   
   A new task is ready to perform target resource reconciliation of a custom object category.

2. Modify the process form as follows:
   
   a. Expand **Development Tools** and then double-click **Form Designer**.
   
   b. Search for and open the **UD_ADUSER** process form.
c. Click Create New Version, and then click Add.

d. In the Name field, enter UD_ADUSER_OBJCATEGORY.

e. In the Field Label column, enter Object Category. Then, enter values for the rest of the columns.

f. On the Properties tab, select the Object Category field, and then click Add Property.

g. In the Add Property dialog box, add the Lookup Code property and set its value to Lookup.ActiveDirectory.ObjectCategory.

h. Click Save and then click Make Version Active.


4. Modify the resource object as follows:


b. Search for and open the AD User resource object.

c. On the Object Reconciliation tab, click Add Field.

d. In the Add Reconciliation Field dialog box, enter Object Category in the Field Name field and select String from the Field Type list.

e. Click Save and close the dialog box.

f. Click Save.

5. Modify the process definition:


b. Search for and open the AD User 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 Object Category.

e. Double-click the Process Data field, and then select UD_ADUSER_OBJCATEGORY.

f. Click Save and close the dialog box.

g. Click Save.

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

7. Run the PurgeCache utility.

8. Modify the lookup definition as follows:

a. Expand Administration and then double-click Lookup Definition.

b. Search for and open the Lookup.ActiveDirectoryLDS.UM.ReconAttrMap lookup definition.

c. Click Add to create an entry for the Object Category field.

d. In the Code Key column, enter Object Category. In the Decode column, enter objectCategory.

e. Click Save.
When you perform target resource reconciliation by using the scheduled task you created in this section, the connector will retrieve records of custom object that you specify as the value of the objectCategory attribute. If you do not specify a value for the objectCategory attribute, then objects of "Person" category are fetched.

4.17.3 Adding Custom Object Category for Provisioning

To configure the connector to provision accounts belonging to a custom object category:

1. Create a list (containing distinguished names) of all custom object categories on the target system.

2. Modify the Lookup.ActiveDirectory.ObjectCategory lookup definition as follows:
   a. Expand Administration and then double-click Lookup Definition.
   c. Click Add.
   d. Enter values in the following format:
      
      Code Key: IT_RESOURCE_KEY~CUST_OBJ_CATG_DN
      
      In this format, IT_RESOURCE_KEY is the numeric code assigned to each IT resource in Oracle Identity Manager, and CUST_OBJ_CATG_DN is the distinguished name of a custom object category.
      Sample value:
      23~CN=customPerson,CN=Schema,CN=Configuration,CN={D14B37E9-778C-4312-99B3-FF3A0DE99C6}
      
      Decode: IT_RESOURCE_NAME~CUST_OBJ_CATG_DN
      In this format, IT_RESOURCE_KEY is the name of the IT resource, and CUST_OBJ_CATG_DN is the distinguished name of a custom object category.
      Sample value:
      ADLDSITResource~CN=customPerson,CN=Schema,CN=Configuration,CN={D14B37E9-778C-4312-99B3-FF3A0DE99C6}
      e. Repeat Steps 2.c and 2.d to add all distinguished names collected in Step 1.
      f. Click Save.

3. Modify the Lookup.ActiveDirectoryLDS.UM.ProvAttrMap lookup definition:
   a. Expand Administration and then double-click Lookup Definition.
   b. Search for and open the Lookup.ActiveDirectoryLDS.UM.ProvAttrMap lookup definition.
   c. Click Add.
   d. In the Code Key column, enter Object Category[LOOKUP]. In the Decode column, enter object Category.
   e. Click Save.

4. Run the PurgeCache utility.
**Note:**

After performing the procedure described in this section, during a provisioning operation, you can select the object category from the Object Category lookup field. If you want to enable the update of the Object Category field, then create a process task (for example, *Object Category Updated*) for the *AD User* process definition. Ensure to use the *ADIDC Update Attribute Value* adapter.
This chapter provides solutions to problems you might encounter after you deploy or while using the Microsoft Active Directory User Management connector.

Table 5-1  Troubleshooting the Microsoft Active Directory User Management Connector

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error is encountered: java.net.UnknownHostException:</td>
<td>Ensure that the host name in the IT resource for the Connector Server is specified correctly.</td>
</tr>
<tr>
<td>The following error is encountered: InvalidCredentialException:</td>
<td>Ensure that the value of the Key parameter of the IT resource for the Connector Server is specified</td>
</tr>
<tr>
<td>ConnectorException:</td>
<td>correctly.</td>
</tr>
<tr>
<td>java.net.ConnectException:</td>
<td>Ensure that the port number in the IT resource for the Connector Server is specified correctly.</td>
</tr>
<tr>
<td>The following error is encountered:</td>
<td></td>
</tr>
<tr>
<td>oracle.iam.connectors.icfcommon.exceptions.OIMException:</td>
<td></td>
</tr>
<tr>
<td>Thor.API.Exceptions.tcAPIException:</td>
<td></td>
</tr>
<tr>
<td>Child tables only supported at account-level</td>
<td></td>
</tr>
<tr>
<td>The following error is encountered:</td>
<td></td>
</tr>
<tr>
<td>oracle.iam.connectors.icfcommon.exceptions.OIMException:</td>
<td></td>
</tr>
<tr>
<td>Thor.API.Exceptions.tcAPIException:</td>
<td></td>
</tr>
<tr>
<td>Required column name RECON_UNIQUEID575B37CA and value does not exist.</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-1 (Cont.) Troubleshooting the Microsoft Active Directory User Management Connector

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error is encountered in the scheduled job:</td>
<td>The following are the possible reasons for the occurrence of this error:</td>
</tr>
<tr>
<td>org.identityconnectors.framework.common.exceptions.ConnectorException:</td>
<td>• If the connector is configured for Microsoft AD LDS, then none of the</td>
</tr>
<tr>
<td>The server does not support the requested critical extension.</td>
<td>scheduled job attributes mention the attribute that is not present in</td>
</tr>
<tr>
<td></td>
<td>the Microsoft AD LDS User Schema. For example, the sAMAccountName</td>
</tr>
<tr>
<td></td>
<td>attribute is not a valid attribute on Microsoft AD LDS.</td>
</tr>
<tr>
<td></td>
<td>Therefore, ensure that attributes that are not present on Microsoft AD</td>
</tr>
<tr>
<td></td>
<td>LDS are not specified as values of scheduled job attributes such as Sort</td>
</tr>
<tr>
<td></td>
<td>By.</td>
</tr>
<tr>
<td></td>
<td>• The number of records that are to be fetched are large in number.</td>
</tr>
<tr>
<td></td>
<td>To fix this issue, remove the values specified for the Batch Size,</td>
</tr>
<tr>
<td></td>
<td>Number of Batches, Batch Start, Sort Direction, and Sort By attributes</td>
</tr>
<tr>
<td></td>
<td>of the scheduled jobs.</td>
</tr>
<tr>
<td></td>
<td>You can always use the PageSize entry of the Lookup.Configuration.Active</td>
</tr>
<tr>
<td></td>
<td>definitions for granular-level setting. The connector uses the ICF</td>
</tr>
<tr>
<td></td>
<td>Handler for sending data to Oracle Identity Manager, and the ICF and</td>
</tr>
<tr>
<td></td>
<td>ICFINTG layers take care of processing the data and generating the</td>
</tr>
<tr>
<td></td>
<td>reconciliation event.</td>
</tr>
<tr>
<td></td>
<td>• A multivalued field on the target system is mapped to a single-valued</td>
</tr>
<tr>
<td></td>
<td>field on the AD User form in Oracle Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>To avoid encountering this issue, ensure that multivalued fields on the</td>
</tr>
<tr>
<td></td>
<td>target system are mapped to the corresponding multivalued field on the</td>
</tr>
<tr>
<td></td>
<td>AD User form.</td>
</tr>
</tbody>
</table>

While staring the Connector Server, the following exception is encountered:
Unhandled Exception: System.Net.Sockets.SocketException: Only one usage of each socket address (protocol/network address/port) is normally permitted

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:
• If the Connector Server service is running, then stop it.
• 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.
Table 5-1  (Cont.) Troubleshooting the Microsoft Active Directory User Management Connector

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error is encountered while running the Active Directory Target Reconciliation scheduled job: ADP ClassLoader failed to load: Script1 java.lang.ClassNotFoundException: ADP ClassLoader failed to load: Script1</td>
<td>Ensure that the value for the Filter syntax attribute of the scheduled job is specified correctly. See Performing Limited Reconciliation By Using Filters for more information.</td>
</tr>
<tr>
<td>All reconciliation runs are successful, but the following error is encountered while running provisioning operations: Neither able to connect to Primary Domain Controller nor to any of Back up Domain Controllers.</td>
<td>Ensure that the value of the LDAPHostName parameter of the IT resource is specified correctly. To determine the host name, on the computer hosting the target system, right-click My Computer and select Properties. 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.</td>
</tr>
<tr>
<td>The Connector Server throws an Out of Memory exception.</td>
<td>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: <a href="http://support.microsoft.com/kb/981575">http://support.microsoft.com/kb/981575</a></td>
</tr>
</tbody>
</table>
Table 5-1  (Cont.) Troubleshooting the Microsoft Active Directory User Management Connector

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to start the Connector Server after extracting the contents of the connector bundle into the CONNECTOR_SERVER_HOME directory. The following exception is encountered:</td>
<td></td>
</tr>
<tr>
<td>ConnectorServer.exe Information: 0 : Starting connector server; C:\Program Files\Identity Connectors\Connector Server</td>
<td></td>
</tr>
<tr>
<td>ConnectorServer.exe Error: 0 : Exception occurred starting connector server</td>
<td></td>
</tr>
<tr>
<td>System.IO.FileNotFoundException: Could not load file or assembly 'System.Core, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' or one of its dependencies. The system cannot find the file specified.</td>
<td></td>
</tr>
<tr>
<td>File name: 'System.Core, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' at Org.IdentityConnectors.Common.CollectionUtil.NewSet[T,U](IEnumerable`1 collection)</td>
<td></td>
</tr>
<tr>
<td>Note: This error is encountered only if you use the command prompt to start the Connector Server. If you use services.msc to start the Connector Server, then the Connector Server stops soon after it started.</td>
<td></td>
</tr>
</tbody>
</table>

All connector operations such as reconciliation and provisioning operations fail and the following error is encountered:

oracle.iam.connectors.icfcommon.exceptions.IntegrationException: Connector ConnectorKey( bundleName=ActiveDirectory,Connector bundleVersion=1.1.0.6380 connectorName=Org.IdentityConnectors.ActiveDirectory.ActiveDirectoryConnector) not found

In addition, the same error message is written to the Connector Server log file.

The following are the possible reasons for the occurrence of this error:

- The connector bundle is not extracted in the CONNECTOR_SERVER_HOME directory.
- The Connector Server is started before you extract the contents of the connector bundle.
- Cache-related issue in Oracle Identity Manager.

Perform the following steps to fix this issue:

1. Stop the Connector Server.
2. Extract the contents of the connector bundle into the CONNECTOR_SERVER_HOME directory.
3. Start the Connector Server.
4. Run the PurgeCache utility on the computer hosting Oracle Identity Manager.
5. Restart Oracle Identity Manager.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error is encountered while performing any connector operation: A local error has occurred</td>
<td>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: <code>DOMAIN_NAME\USER_NAME</code></td>
</tr>
</tbody>
</table>
| The computer hosting the Connector Server and target system is unavailable. Nothing works despite specifying a value for the BDCHostNames parameter of the IT resource. | 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:  
  • Have a dedicated computer for the Connector Server. Note that you can specify a value for the BDCHostNames IT resource parameter even if the Connector Server is running on a dedicated computer.  
  • The computer hosting the Connector Server must be in the same domain as the target system.  
  • Deploy the Connector Server and configure the Active Directory Connector Server IT resource. |
| A target resource reconciliation run fails with the following error: Row index out of bounds However, users are brought into Oracle Identity Manager and are linked successfully. | 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. |
| The following error is encountered in the Connector Server log file: org.identityconnectors.framework.common.exceptions.ConnectorException: java.net.ConnectException: Connection timed out | The following are two of the possible reasons for the occurrence of this error:  
  • The connection between the Connector Server and Oracle Identity Manager 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.  
  • 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:  
    <add key="connectorserver.port" value="8759"/>  

Table 5-1  (Cont.) Troubleshooting the Microsoft Active Directory User Management Connector

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>User reconciliation fails with the following error in the log file of Oracle Identity Manager: Required column name RECON_OBJECTGUID and value does not exist</td>
<td>This error is encountered if the value of the Configuration Lookup parameter of the Active Directory IT resource is set to Lookup.Configuration.ActiveDirectory. To avoid this error, while performing trusted user reconciliation, ensure to set the value of the Configuration Lookup parameter of the Active Directory IT resource to Lookup.Configuration.ActiveDirectory.Trusted.</td>
</tr>
<tr>
<td>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): oracle.iam.reconciliation.exception.InvalidDataFormatException: Required column name RECON_ORGNAME4EAE4287 and value does not exist</td>
<td>This error is encountered if value of the Configuration Lookup parameter of the Active Directory IT resource is set to Lookup.Configuration.ActiveDirectory. 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 Lookup.Configuration.ActiveDirectory.Trusted.</td>
</tr>
<tr>
<td>While running the scheduled jobs for lookup field synchronization (groups and organizations), the following exception is encountered: Unable to get the Directory Entry</td>
<td>You can perform one of the following steps to determine the cause for this error:</td>
</tr>
<tr>
<td>In addition, the following error is written to the log file of Oracle Identity Manager: Required column name RECON_ORGNAME&lt;&gt; and value does not exist</td>
<td>• Check for the error message in the log files of the Connector Server to find out the root cause.</td>
</tr>
<tr>
<td>In addition, the following error is written to the Connector Server log file: Org.IdentityConnectors.Framework.Common.Exceptions.ConnectorException: Unable to get the Directory Entry</td>
<td>• Check the Event Viewer. To open the Event Viewer, from the Start menu, select Control Panel, double-click Administrative Tools, and then double-click Event Viewer.</td>
</tr>
<tr>
<td>The following are few of the possible reasons for the occurrence of this error:</td>
<td>The following are few of the possible reasons for the occurrence of this error:</td>
</tr>
<tr>
<td>• 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: DOMAIN_NAME\USER_NAME</td>
<td>• 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.</td>
</tr>
</tbody>
</table>
### Table 5-1 (Cont.) Troubleshooting the Microsoft Active Directory User Management Connector

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error is encountered in the log file of Oracle Identity Manager while running scheduled jobs: java.net.SocketException: Connection reset</td>
</tr>
<tr>
<td>Solution</td>
</tr>
<tr>
<td>The following are two of the possible reasons for the occurrence of this error:</td>
</tr>
<tr>
<td>• LDAPS is not enabled on the domain controllers. To fix this issue, enable LDAPS.</td>
</tr>
<tr>
<td>• Oracle Identity Manager is not set for SSL. In other words, the UseSSL parameter in the IT resources of the target system and Connector 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 in the IT resources of the target system and Connector Server to <code>yes</code> and <code>true</code>, respectively.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any connector operation (reconciliation or provisioning) fails and the following exception is encounter: Domain Controller not found in the domain 'SAMPLEDOMAIN.com'</td>
</tr>
<tr>
<td>In addition, the following error is written to the Connector Server log file: org.identityconnectors.framework.common.exceptions.ConnectorException: Domain controller not found in the domain</td>
</tr>
<tr>
<td>Solution</td>
</tr>
<tr>
<td>The following are two of the possible reasons for the occurrence of this error:</td>
</tr>
<tr>
<td>• 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: <code>DOMAIN_NAME\USER_NAME</code></td>
</tr>
<tr>
<td>• 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>During a provisioning operation, the following error is encountered in the log file of Oracle Identity Manager: java.lang.IllegalArgumentException: Parameter 'lookupName' must not be blank</td>
</tr>
<tr>
<td>Solution</td>
</tr>
<tr>
<td>This error is encountered if the value of the Configuration Lookup parameter of the Active Directory IT resource is set to <code>Lookup.Configuration.ActiveDirectory.Trusted</code> or left blank. To fix this issue, set the value of the Configuration Lookup parameter of the Active Directory IT resource to <code>Lookup.Configuration.ActiveDirectory</code>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error is encountered in the Connector Server log file: org.identityconnectors.framework.common.exceptions.ConnectorException: Neither able to connect to Primary Domain Controller nor to any of Backup Domain Controllers.</td>
</tr>
<tr>
<td>Solution</td>
</tr>
<tr>
<td>This error is encountered if an incorrect value is specified for the LDAPHostName IT resource parameter. To fix this issue, you must specify a correct value for the LDAPHostName IT resource parameter. To determine the correct value for this parameter, on the computer hosting the target system, right-click <strong>My Computer</strong> and select <strong>Properties</strong>. 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.</td>
</tr>
<tr>
<td>Problem</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The following error is encountered in the Connector Server log file:</td>
</tr>
<tr>
<td>System.IO.IOException: The handshake failed due to an unexpected packet format</td>
</tr>
<tr>
<td>The following error is encountered in the Connector Server log file:</td>
</tr>
<tr>
<td>The Active Directory User Target Recon scheduled job for bulk users does not fetch all users from the target system.</td>
</tr>
<tr>
<td>No records are reconciled when the following filter is applied:</td>
</tr>
<tr>
<td>contains('memberOf','PGMGroup')</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>The following error is encountered in the Connector Server log file:</td>
</tr>
<tr>
<td>System.NotSupportedException: The server mode SSL must use a certificate with the associated private key.</td>
</tr>
<tr>
<td>Problem</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>A provisioning operation (either create or update) fails and the following error is written to the Connector Server log file: The specified directory service attribute or value does not exist.</td>
</tr>
<tr>
<td>During a bulk provisioning operation, the following error might be encountered in the Connector Server log file: Max objects exceeded</td>
</tr>
<tr>
<td>Problem</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| OIM 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: 'Data Validation Failed' as the current status and 'Invalid ManagerLogin : <Manager ID>' as Note. | This issue is encountered due to the dependency of manager information of users. OIM User creation fails if the manager of the user is not already present in Oracle Identity Manager. To fix this issue: Log in to the Design Console and remove the manager field mapping as follows:   
   1. Search for and open the **AD User Trusted** process definition. On the Reconciliation Field Mappings tab, remove the mapping for the Manager ID field  
   2. Search for and open the **AD User Trusted** resource object. On the Object Reconciliation tab, delete the Manager ID field.  
   3. Search for and open the **Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted** lookup definition. Delete the entry with code key 'Manager ID' and decode value 'Manager Id'.  

Run the Active Directory User Trusted Recon scheduled job. Log in to the Design Console and add the manager field mapping as follows:  
   1. Search for and open the **AD User Trusted** process definition. On the Reconciliation Field Mappings tab, add the field mapping by specifying Manager ID as the Field Name and Manager Login as the User Attribute.  
   2. Search for and open the **AD User Trusted** resource object. On the Object Reconciliation tab, add the Manager ID field of type string.  
   3. Search for and open the **Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted** lookup definition. Add an entry with code key value Manager ID and decode key value Manager Id.  

Clear the value in the latest token attribute of the Active Directory User Trusted Recon scheduled job and run it.
### Table 5-1  (Cont.) Troubleshooting the Microsoft Active Directory User Management Connector

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error is encountered in the log file of the Connector Server during a provisioning operation: The remote procedure call failed and did not execute. (Exception from HRESULT: 0x800706BF)</td>
<td>This issue is encountered when there are too many requests at the same time during a Create User or Password Update provisioning operation. For example, this issue can be encountered during an access policy-based provisioning operation where too many account creations are triggered. This error can occur on Microsoft Windows 2003, 2008, 2008 R2 or Windows 2012 domain controllers, which includes service packs as well. To fix this issue, you must contact Microsoft Support to apply the hotfix listed on the following Web site: <a href="http://support.microsoft.com/kb/2781049">http://support.microsoft.com/kb/2781049</a> <strong>Note:</strong> Do not apply the hotfix without contacting Microsoft Support.</td>
</tr>
<tr>
<td>The following error is encountered in the Active Directory API which is not meaningful: Encountered DirectoryServicesCOMException: A device attached to the system is not functioning.</td>
<td>Encountered DirectoryServicesCOMException: A device attached to the system is not functioning. This error is encountered when the sAMAccount attribute in the target system (corresponding to the User Loging field in Oracle Identity Manager) contains more than 20 characters. Workaround is to write a validation java code (see Configuring Validation of Data During Reconciliation and Provisioning) 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.</td>
</tr>
</tbody>
</table>
Frequently Asked Questions

This chapter provides 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 2003 or 2008 (both 32-bit or 64-bit), or Microsoft Windows Server 2012, 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 the target system domain.

3. **Is it mandatory to use Oracle Identity Manager 11g Release 1 (1.1.1.5.2) with Active Directory User Management connector release 11.1.1.5.0?**

   Yes. This is because the minimum Oracle Identity Manager version required to install and use Active Directory User Management connector release 11.1.1.5.0 is Oracle Identity Manager 11g Release 1 (11.1.1.5.2) BP02 (with patch 13684913) or later.

4. **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. However, in a forest with disconnected domains, a Connector Server is required for each domain.

5. **Can Active Directory User Management connector release 9.1.x coexist with Active Directory User Management connector release 11.1.x?**

   Yes. Two versions of the same connector can coexist. This can be achieved by cloning the Active Directory User Management 11.x connector XML and using it for installing the connector with the new name.

6. **What are the prerequisites for installing and using the Active Directory User Management connector with Oracle Identity Manager release 11.1.2.x?**

   The following are the prerequisites for installing and using the Active Directory User Management connector with Oracle Identity Manager release 11.1.2.x:
   
   a. Apply patch 14190610 or use Active Directory connector version 11.1.1.6.0 or later.
   b. Create a form in Oracle Identity Manager.
   c. Create an application instance associated with the form (created in Step 2) and IT resource.
d. Run the Entitlement List and Catalog Synchronization Job scheduled jobs to populate the application instance in the catalog.

7. **How to establish a connection between Active Directory User Management connector release 11.1.1.5 and an AD LDS instance?**

The following is the procedure to establish a connection between Active Directory User Management connector release 11.1.1.5 and an AD LDS instance:

a. Set the value of the IsADLDS parameter of the IT resource to yes.

b. Specify a value for the ADLDSPort parameter of the IT resource.


8. **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 IT resource. While providing value for IT resource parameters, ensure that you use the following format to specify a value for the DirectoryAdminName parameter:

```
DOMAIN_NAME\USER_NAME
```

9. **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.

10. **If I customize the connector, should I modify the values in the Decode column (for example, OIM Employee Type, OIM User Type, and __UID__, and __PARENTCN__) of the Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted lookup definition?**

No. The Decode column of the Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted lookup definition 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 Decode column values. The following is a description of each of the attributes in the Decode 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 Manager 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 Manager the same organization hierarchy that is maintained on the target system.

• __ENABLE__: This attribute specifies whether the user in the target system is enabled.

Note:

If you add new attributes for the trusted source reconciliation, then it is expected that you update the Lookup.ActiveDirectory.UM.ReconAttrMap.Trusted lookup definition by creating an entry for the newly added attribute. In the Decode column of this new entry, you specify the name of the newly added target system attribute (for example, middleName, and c). See New Fields for Trusted Source Reconciliation for more information on adding new fields for trusted source reconciliation.

11. Why cannot I see the log files corresponding to the connector operations in the computer hosting Oracle Identity Manager?

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 Managing Logging for Microsoft Active Directory User Management Connector for more information.

12. 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.

13. 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 Manager nor any logs on Oracle Identity Manager. 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 Manager, 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 Manager, 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.

14. **Is Remote Manager required for provisioning and reconciling Terminal Service attributes by using this release of the Active Directory User Management Connector?**

No. For 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.

15. **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 IT resource parameter 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 IT resource 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 of 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.

16. **Can the Active Directory User Management connector version 11.1.1.5.0 manage windows local account?**

No.
17. **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:

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

18. 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.

19. 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 Active Directory Connector IT Resource:

- 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.

20. **Can the Active Directory User Management connector manage a forest containing a single parent domain with many child domains using only one application instance or IT resource?**

Yes, it is possible with a single application instance by performing the following steps:

- 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 `DirectoryAdminName` parameter of the IT resource.

21. **Should the `DirectoryAdminName` parameter of the IT resource 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 Step 7 of Configuring the IT Resource for Microsoft AD and AD LDS for more information about the `DirectoryAdminName` IT resource parameter.
22. 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.

23. 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.

24. What happens when the computer (specified as the value of the LDAPHostName IT resource 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 LDAPHostName IT resource parameter) becomes unavailable, the connector performs in one of the following manners:

- If a value has been specified for the BDCHostNames IT resource parameter, then the connector tries connect to any of the backup domain controllers mentioned in the BDCHostNames parameter. You can configure the connector to be compatible with HA target systems environments by specifying a value for the BDCHostNames IT resource parameter.
- If no value has been specified for the LDAPHostName and BDCHostName IT resource parameters, then the connector connects to any of the domain controllers available in the same domain. This is called serverless bind.

25. What happens when the Connector Server specified in the Active Directory IT resource 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 Manager.

26. Will there be an issue if I specify a value for the ADLDSPort parameter while using Microsoft Active Directory as a target system?  
No. This is because the connector first checks for the value of the isADLDS parameter. If the value of the isADLDS parameter is yes, then the connector uses the value of the ADLDSPort parameter. However, Oracle recommends not to specify a value for ADLDSPort parameter if you are using Microsoft Active Directory as the target system.

27. Can I perform user provisioning operations without configuring SSL between Oracle Identity Manager and Microsoft Active Directory? In addition, is the presence of the SSL certificate of Microsoft Active Directory required in both Oracle Identity Manager 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 Manager 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.

28. **Will changes in AD groups for a user be reconciled during incremental reconciliation?**

No. Group membership changes are not reconciled during incremental reconciliation. This is a target system limitation.

29. **Explain appropriate use of the SyncDomaincontroller and SyncGlobalCatalog parameters of the IT resource.**

The SyncDomaincontroller and SyncGlobalCatalog IT resource parameters are used only during reconciliation. If reconciliation must be performed against a domain controller, then the SyncDomainController parameter is used.

If reconciliation must be performed against the global catalog server, then the SyncGlobalCatalog parameter is used. The following are the steps to be performed for using these parameters:

a. Set the SearchChildDomain entry in the Lookup.Configuration.ActiveDirectory lookup definition to *yes*.

b. Enter the global catalog server host name as the value of the SyncGlobalCatalog IT resource parameter.

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

30. **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.

31. **Where do I find the log files for connector installation?**

You find the log files for connector installation, Oracle Identity Manager server log and diagnostic log, in the following location:

```
DOMAIN_HOME/servers/oim_server1/logs
```

32. **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.

33. **When a group or an OU is created in the target system, will their parent organization be displayed in Oracle Identity Manager?**

When a group or an OU is created in the target system, its parent organization is not displayed in Oracle Identity Manager. 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.

34. **Will a new group or OU be created in Oracle Identity Manager if I rename a group or an OU in the target system?**

Yes.
35. What certificate must be exported while configuring SSL between Oracle Identity Manager and the Connector Server?

While configuring SSL between Oracle Identity Manager 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 Manager is running. Add the certificate to Oracle Identity Manager JDK store and Oracle WebLogic keystore. See Configuring SSL for Microsoft Active Directory and Microsoft AD LDS for more information.

36. Is it correct that all traffic from Oracle Identity Manager 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.

37. What protocol is used for communication between Oracle Identity Manager and the target system?

TCP protocol is used for communication between Oracle Identity Manager and the target system.

38. Architecture of Microsoft Active Directory User Management Connector 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:


If you set the value of the UseSSL IT resource parameter to no, then secure authentication as discussed in the following page:

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

<table>
<thead>
<tr>
<th>Process Form Field and Field Length</th>
<th>Microsoft Active Directory Field and Field Length</th>
<th>Microsoft ADAM Field and Field Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department, 40</td>
<td>department, 64</td>
<td>department, 64</td>
</tr>
<tr>
<td>Fax, 40</td>
<td>facsimileTelephoneNumber, 64</td>
<td>facsimileTelephoneNumber, 64</td>
</tr>
<tr>
<td>Home Phone, 40</td>
<td>homePhone, 64</td>
<td>homePhone, 64</td>
</tr>
<tr>
<td>IP Phone, 40</td>
<td>ipPhone, 64</td>
<td>ipPhone, 64</td>
</tr>
<tr>
<td>Manager Name, 255</td>
<td>manager, Not Specified</td>
<td>manager, Not Specified</td>
</tr>
<tr>
<td>Mobile, 50</td>
<td>mobile, 64</td>
<td>mobile, 64</td>
</tr>
<tr>
<td>Office, 80</td>
<td>physicalDeliveryOfficeName, 128</td>
<td>physicalDeliveryOfficeName, 128</td>
</tr>
<tr>
<td>Organization Name, 400</td>
<td>Distinguished name of the organization, Not Specified</td>
<td>Distinguished name of the organization, Not Specified</td>
</tr>
<tr>
<td>Pager, 40</td>
<td>pager, 64</td>
<td>pager, 64</td>
</tr>
<tr>
<td>Street, 200</td>
<td>StreetAddress, 1024</td>
<td>StreetAddress, 1024</td>
</tr>
<tr>
<td>Terminal Home Directory, 60</td>
<td>Part of the data stored in the userParameters field, 100</td>
<td>NA</td>
</tr>
<tr>
<td>Terminal Profile Path, 60</td>
<td>Part of the data stored in the userParameters field, 100</td>
<td>NA</td>
</tr>
</tbody>
</table>
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:

   ```xml
   <schemaAttributes>
     <schemaAttributes name="givenName" dataType="String" displayName="First Name" length="64" fieldType="TextField" reconcileable="true" provisionable="true" />
   </schemaAttributes>
   ```

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.
Files and Directories On the Installation Media

The contents of the connector installation media directory are described in Table B-1.

Table B-1   Files and Directories On the Installation Media

<table>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle/ActiveDirectory.Connector-1.1.0.6380.zip</td>
<td>This ZIP file contains the connector bundle.</td>
</tr>
<tr>
<td>configuration/ActiveDirectory-CI.xml</td>
<td>This XML file contains configuration information that is used during the connector installation process.</td>
</tr>
</tbody>
</table>

Files in the dataset directory
- ModifyResourceADUser.xml
- ProvisionResourceADUser.xml
- ModifyResourceADLDSUser.xml
- ProvisionResourceADLDSUser.xml

**Note:** The dataset XML files are applicable only if you are using Oracle Identity Manager release 11.1.1.x.

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.

owglue/ActiveDirectoryConnector-idmglue-1.0.12.zip

This ZIP file contains Oracle Waveset metadata for the Microsoft Active Directory User Management connector.

**Note:** This ZIP file is not 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. During connector installation, these resource bundles are copied to the Oracle Identity Manager database.

**Note:** A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings 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>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xml/ActiveDirectory-ConnectorConfig.xml</td>
<td>This XML file contains definitions for the following connector components:</td>
</tr>
<tr>
<td></td>
<td>• Resource objects</td>
</tr>
<tr>
<td></td>
<td>• IT resource types</td>
</tr>
<tr>
<td></td>
<td>• IT resource instance</td>
</tr>
<tr>
<td></td>
<td>• Process forms</td>
</tr>
<tr>
<td></td>
<td>• Process tasks and adapters</td>
</tr>
<tr>
<td></td>
<td>• Process definition</td>
</tr>
<tr>
<td></td>
<td>• Prepopulate rules</td>
</tr>
<tr>
<td></td>
<td>• Lookup definitions</td>
</tr>
<tr>
<td></td>
<td>• Reconciliation rules</td>
</tr>
<tr>
<td></td>
<td>• Scheduled tasks</td>
</tr>
<tr>
<td>xml/ActiveDirectory-Datasets.xml</td>
<td>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.</td>
</tr>
<tr>
<td>xml/ActiveDirectoryLDS-Datasets.xml</td>
<td>Note: The dataset XML files are applicable only if you are using Oracle Identity Manager release 11.1.1.x.</td>
</tr>
</tbody>
</table>
This appendix lists the table that describes the special characters supported in process form fields. Table C-1 lists special characters that are supported in process form fields.

<table>
<thead>
<tr>
<th>Name of the Character</th>
<th>Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>ampersand</td>
<td>&amp;</td>
</tr>
<tr>
<td>asterisk</td>
<td>*</td>
</tr>
<tr>
<td>at sign</td>
<td>@</td>
</tr>
<tr>
<td>backslash</td>
<td>\</td>
</tr>
<tr>
<td>caret</td>
<td>^</td>
</tr>
<tr>
<td>comma</td>
<td>,</td>
</tr>
<tr>
<td>dollar sign</td>
<td>$</td>
</tr>
<tr>
<td>double quotation mark</td>
<td>&quot;</td>
</tr>
<tr>
<td>equal sign</td>
<td>=</td>
</tr>
<tr>
<td>exclamation point</td>
<td>!</td>
</tr>
<tr>
<td>hyphen</td>
<td>-</td>
</tr>
<tr>
<td>left brace</td>
<td>{</td>
</tr>
<tr>
<td>left bracket</td>
<td>[</td>
</tr>
<tr>
<td>left parenthesis</td>
<td>(</td>
</tr>
<tr>
<td>number sign</td>
<td>#</td>
</tr>
<tr>
<td>percent sign</td>
<td>%</td>
</tr>
<tr>
<td>period</td>
<td>.</td>
</tr>
<tr>
<td>plus sign</td>
<td>+</td>
</tr>
<tr>
<td>question mark</td>
<td>?</td>
</tr>
<tr>
<td>right brace</td>
<td>}</td>
</tr>
<tr>
<td>right bracket</td>
<td>]</td>
</tr>
<tr>
<td>right parenthesis</td>
<td>)</td>
</tr>
<tr>
<td>single quotation mark</td>
<td>‘</td>
</tr>
<tr>
<td>slash</td>
<td>/</td>
</tr>
<tr>
<td>underscore</td>
<td>_</td>
</tr>
</tbody>
</table>
Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Table D-1 lists the scheduled jobs that you must configure for lookup field synchronization and reconciliation.

<table>
<thead>
<tr>
<th>Scheduled Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Group Lookup Recon</td>
<td>This scheduled task is used to synchronize the values of group lookup fields between Oracle Identity Manager and the target system. For information about this scheduled task and its attributes, see Scheduled Jobs for Lookup Field Synchronization.</td>
</tr>
<tr>
<td>Active Directory Organization Lookup Recon</td>
<td>This scheduled task is used to synchronize the values of organization lookup fields between Oracle Identity Manager and the target system. For information about this scheduled task and its attributes, see Scheduled Jobs for Lookup Field Synchronization.</td>
</tr>
<tr>
<td>Active Directory User Target Recon</td>
<td>This scheduled task is used to fetch user data during target resource reconciliation. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of User Records.</td>
</tr>
<tr>
<td>Active Directory User Target Delete Recon</td>
<td>This scheduled task is used to fetch data about deleted users during target resource reconciliation. During a reconciliation run, for each deleted user account on the target system, the AD User resource is revoked for the corresponding OIM User. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of Deleted User Records.</td>
</tr>
<tr>
<td>Active Directory Organization Recon</td>
<td>This scheduled task is used to reconcile data about organizations. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of Groups and Organizations.</td>
</tr>
<tr>
<td>Active Directory User Trusted Recon</td>
<td>This scheduled task is used to fetch user data during trusted source reconciliation. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of User Records.</td>
</tr>
<tr>
<td>Active Directory User Trusted Delete Recon</td>
<td>This scheduled task is used to fetch data about deleted users during trusted source reconciliation. During a reconciliation run, for each deleted target system account, the corresponding OIM User is deleted. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of Deleted User Records.</td>
</tr>
<tr>
<td>Active Directory Group Recon</td>
<td>This scheduled task is used to fetch data about groups during target resource reconciliation. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of Groups and Organizations.</td>
</tr>
<tr>
<td>Active Directory Group Delete Recon</td>
<td>This scheduled task is used to reconcile data about deleted groups in the target resource (account management) mode of the connector. For information about this scheduled task and its attributes, see Scheduled Job for Reconciliation of Deleted Groups.</td>
</tr>
</tbody>
</table>