

Oracle® Identity Manager

Connector Guide for Microsoft Active Directory

Release 9.0.3

B32355-01

February 2007

Copyright © 1991, 2007, Oracle. All rights reserved.

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

| | |
|------------------------------------------------------------------------------------------------------|-----|
| Preface | v |
| Audience | v |
| Documentation Accessibility | v |
| Related Documents | vi |
| Documentation Updates | vi |
| Conventions | vi |
| What's New in the Oracle Identity Manager Connector for Microsoft Active Directory? | vii |
| Software Updates | vii |
| Documentation-Specific Updates..... | ix |
| 1 About the Connector | |
| Supported Functionality | 1-1 |
| Multilanguage Support | 1-2 |
| Reconciliation Module | 1-3 |
| AD Lookup Fields..... | 1-3 |
| AD Group | 1-3 |
| AD User | 1-3 |
| Provisioning Module | 1-4 |
| AD Organization | 1-4 |
| AD Group | 1-4 |
| AD User | 1-4 |
| Files and Directories That Comprise the Connector | 1-5 |
| Determining the Release Number of the Connector | 1-6 |
| 2 Deploying the Connector | |
| Step 1: Verifying Deployment Requirements | 2-1 |
| Step 2: Configuring the Target System | 2-2 |
| Step 3: Copying the Connector Files and External Code | 2-2 |
| Step 4: Configuring the Oracle Identity Manager Server | 2-3 |
| Changing to the Required Input Locale..... | 2-3 |
| Clearing Content Related to Connector Resource Bundles from the Server Cache | 2-3 |
| Enabling Logging | 2-4 |
| Step 5: Importing the Connector XML Files | 2-6 |

| | |
|----------------------------------------------------------------------------------------|-------------|
| Defining IT Resources | 2-7 |
| Microsoft Windows 2000 | 2-7 |
| Microsoft Windows 2003 | 2-9 |
| Step 6: Configuring Reconciliation..... | 2-12 |
| Specifying the Fields to Be Reconciled | 2-12 |
| Configuring Trusted Source Reconciliation | 2-13 |
| Creating Scheduled Tasks for Reconciliation..... | 2-14 |
| Specifying Values for the Scheduled Task Attributes | 2-14 |
| Lookup Fields Reconciliation Scheduled Task..... | 2-15 |
| User Reconciliation Scheduled Task..... | 2-15 |
| Enabling Reconciliation in Oracle Identity Manager Release 9.0.1 | 2-16 |
| Step 7: Compiling Adapters | 2-17 |
| Step 8: Configuring SSL..... | 2-18 |
| Installing Certificate Services | 2-18 |
| Enabling LDAPS..... | 2-19 |
| Setting Up the Microsoft Active Directory Certificate As a Trusted Certificate..... | 2-19 |
| Exporting the Microsoft Active Directory Certificate..... | 2-19 |
| Importing the Microsoft Active Directory Certificate | 2-20 |
| Configuring the Connector for Multiple Installations of the Target System | 2-21 |
| Configuring the Connector and Password Synchronization Module | 2-22 |
| Creating a Custom Attribute in Microsoft Active Directory | 2-22 |
| Ensuring That the Microsoft Active Directory Schema Snap-In Is Installed | 2-23 |
| Creating a Custom Attribute | 2-23 |
| Creating a Custom Attribute in Oracle Identity Manager | 2-24 |
| Specifying Values for IT Resource Parameters | 2-24 |
| Sequence of Events That Occur During a Password Change | 2-25 |
| Configuring the xlconfig.xml File for the Password Synchronization Module | 2-25 |

3 Testing and Troubleshooting

| | |
|----------------------------|-----|
| Testing Provisioning | 3-1 |
| Troubleshooting..... | 3-1 |

4 Known Issues

A Attribute Mappings Between Oracle Identity Manager and Microsoft Active Directory

B Attributes of the Reconciliation Scheduled Task

C Code for a Sample Transformation Class

Index

Preface

Oracle Identity Manager Connector Guide for Microsoft Active Directory provides information about integrating Oracle Identity Manager with Microsoft Active Directory.

Note: Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for Microsoft Active Directory.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

<http://www.oracle.com/accessibility/>

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation library:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.3 connector documentation set, visit Oracle Technology Network at

<http://www.oracle.com/technology/documentation/index.html>

Conventions

The following text conventions are used in this document:

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

What's New in the Oracle Identity Manager Connector for Microsoft Active Directory?

This chapter provides an overview of the updates made to the connector and documentation for Microsoft Active Directory in release 9.0.3 of the Oracle Identity Manager connector pack.

See Also: The 9.0.2 release of this guide for information about updates that were new for the 9.0.2 release

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

- [Software Updates](#)

These include updates made to the connector software.

- [Documentation-Specific Updates](#)

These include major changes made to the connector documentation. These changes are not related to software updates.

See Also: *Oracle Identity Manager Release Notes*

Software Updates

This section discusses updates made to this release of the connector software.

Enhancement in the Multilanguage Support Feature

In addition to the three languages supported by the earlier release, this release of the connector supports seven new languages. All the supported languages are listed in the ["Multilanguage Support"](#) section on page 1-2.

Query-Based Reconciliation

In reconciliation performed by using the earlier release of the connector, all target system records that have been added or updated after the last reconciliation run are reconciled during the current reconciliation run. This release of the connector provides features that enable you to specify the subset of records to be reconciled.

You can specify an LDAP query that the reconciliation engine must use while fetching records from the target system. You specify this LDAP query as the value of the CustomizedReconQuery IT resource parameter, which is listed in the table in the ["Defining IT Resources"](#) section on page 2-7.

You can also specify whether the query that you provide must be run on records for all user groups or only on the user group specified in the LDAP query. To do this, you use

the `GroupObject` attribute defined in the ["User Reconciliation Scheduled Task"](#) section on page 2-15.

No Limit on the Number of Users That Can Be Reconciled During a Single Reconciliation Run

With the earlier release of this connector, you could not reconcile more than 1000 users during any particular reconciliation run. This release of the connector can reconcile any number of users during a reconciliation run.

Display of the Group Name Values

In the earlier release of this connector, group ID (`objectGUID`) values were displayed in the Design Console and Administrative and User Console after group lookup reconciliation. From this release onward, the group names (`sAMAccountName`) of the reconciled groups are displayed. This makes it easier to identify the groups that have been reconciled.

Determining the Release Number of the Connector

Instructions to determine the release number of the connector are given in the ["Determining the Release Number of the Connector"](#) section on page 1-6.

Support for OC4J

Earlier releases of the connector supported the following application servers:

- JBoss Application Server
- BEA WebLogic
- IBM WebSphere

This release of the connector also supports Oracle Containers for J2EE (OC4J). Instructions pertaining to OC4J have been added at the required places in the guide.

Setting Non-Mandatory User Attributes to NULL During a Disable User Provisioning Operation

This release of the connector provides a feature that enables you to automatically set to NULL the value of nonmandatory user attributes while performing a Disable User provisioning operation. To enable this feature, you use the following new parameters of the IT resource definition:

- `ADDisableAttr Lookup Definition`
- `Use Disable Attr`

These parameters are discussed in the ["Defining IT Resources"](#) section on page 2-7.

New Field in the Lookup.ADReconciliation.FieldMap Field Map

In the ["Specifying the Fields to Be Reconciled"](#) section on page 2-12, the password field has been added to the list of fields provided by default in the `Lookup.ADReconciliation.FieldMap` field map.

Changes in the Known Issues

The following issues have been added to the Known Issues list in [Chapter 4](#):

- A limitation of Microsoft Active Directory that restricts the number of characters in the user ID field to 20 characters.

- In this release of the connector, a problem involving the use of the connector and the password synchronization module has been resolved. The procedure to address this problem is described in the ["Configuring the Connector and Password Synchronization Module"](#) section on page 2-22.

As part of the solution, you must also specify values for the following parameters that have been added to the IT resource definition in the ["Defining IT Resources"](#) section on page 2-7:

- AD Sync installed (yes/no)
- OIM User UDF
- Custom Attribute Name

Documentation-Specific Updates

The following documentation-specific updates have been made in this release of the guide:

- The `ldapbp.jar` has been added in the following sections:
 - The ["Files and Directories That Comprise the Connector"](#) section on page 1-5
 - The ["Step 3: Copying the Connector Files and External Code"](#) section on page 2-2
- In Steps 1 and 2 of the procedure in the ["Importing the Microsoft Active Directory Certificate"](#) section on page 2-20, information has been added about what needs to be done for nonclustered and clustered configurations of IBM WebSphere.
- In the ["Step 7: Compiling Adapters"](#) section on page 2-17, the instruction about restarting the node has been removed from Step 4 of the procedure to compile adapters.
- In the "Testing and Troubleshooting" chapter, the ["Troubleshooting"](#) section on page 3-1 has been added. The content for this section is the same as the procedure described in the Known Issues chapter about the limitation that is observed when you set the `Use SSL IT resource` parameter to `false`.
- Instructions to enable logging have been moved from the "Testing and Troubleshooting" chapter to the "Deploying the Connector" chapter. In the revised ["Enabling Logging"](#) section on page 2-4, instructions have been added for each of the application servers that are supported by this release of the connector.
- [Appendix A](#) provides information about attribute mappings between Oracle Identity Manager and Microsoft Active Directory.

About the 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 third-party applications. The connector for Microsoft Active Directory is used to integrate Oracle Identity Manager with Microsoft Active Directory.

Note: Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

This chapter contains the following sections:

- [Supported Functionality](#)
- [Multilanguage Support](#)
- [Reconciliation Module](#)
- [Provisioning Module](#)
- [Files and Directories That Comprise the Connector](#)
- [Determining the Release Number of the Connector](#)

Supported Functionality

The following table lists the functions that are available with this connector.

| Function | Type | Description |
|------------------------------|--------------|------------------------------------------------------|
| Create User | Provisioning | Creates a user |
| Move User | Provisioning | Moves a user from one organization to another |
| Delete User | Provisioning | Deletes a user |
| Enable User | Provisioning | Enables a disabled user |
| Disable User | Provisioning | Disables a user |
| Get Organization USN | Provisioning | Retrieves the USN of an organization |
| Create Organization | Provisioning | Creates an organization |
| Get Organization USN Changed | Provisioning | Retrieves the USN of an organization after an update |

| Function | Type | Description |
|-------------------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete Organization | Provisioning | Deletes an organization |
| Get User objectGUID | Provisioning | Retrieves the objectGUID of a user |
| User Must Change Password at Next Logon Updated | Provisioning | Updates a user's profile according to a change in the User Must Change Password at Next Logon attribute |
| Set Account Expiration Date | Provisioning | Updates a user's profile according to a change in the Account Expiration Date attribute |
| Password Never Expires Updated | Provisioning | Updates a user's profile according to a change in the Password Never Expires attribute |
| Update User ID | Provisioning | Updates a user's profile according to a change in the User ID attribute |
| Add User to Group | Provisioning | Adds a user to a group |
| Remove User from Group | Provisioning | Removes a user from a group |
| Create AD Group | Provisioning | Creates an AD group |
| Delete AD Group | Provisioning | Deletes an AD group |
| Update Group Name | Provisioning | Updates an AD group name |
| Get Group objectGUID | Provisioning | Retrieves the objectGUID of a group |
| Trusted Reconciliation for User | Reconciliation | Creates OIM User accounts corresponding to reconciled Microsoft Active Directory accounts |
| Create User | Reconciliation | Reconciles Microsoft Active Directory accounts |
| Create Organization | Reconciliation | Creates organizations along with users in Oracle Identity Manager corresponding to reconciled Microsoft Active Directory accounts (and their root organizations) |
| Create Group | Reconciliation | Creates groups along with users in Oracle Identity Manager corresponding to reconciled Microsoft Active Directory accounts (and their parent groups) |

Multilanguage Support

This release of the connector supports the following languages:

- English
- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish

- Traditional Chinese

See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

Reconciliation Module

This section discusses the elements that the reconciliation module extracts from the target system to construct reconciliation event records. This section discusses the following reconciliation types:

- [AD Lookup Fields](#)
- [AD Group](#)
- [AD User](#)

AD Lookup Fields

To populate the `Lookup.ADReconciliation.GroupLookup` lookup definition, the following fields of AD Groups are reconciled:

- `sAMAccountName`
- `objectGUID`

AD Group

The reconciliation module extracts the following elements from the target system to construct AD Group reconciliation event records:

- `sAMAccountName`
- `objectGUID`
- `Organization Name`
- `instanceType`
- `cn`

AD User

The reconciliation module extracts the following elements from the target system to construct AD User reconciliation event records:

- `sAMAccountName`
- `objectGUID`
- `name`
- `memberOf`
- `sn`
- `cn`
- `Initials`

Provisioning Module

In Microsoft Active Directory, the provisioning module can be divided into the following:

- [AD Organization](#)
- [AD Group](#)
- [AD User](#)

AD Organization

The following fields are provisioned:

- USN Create
- USN Change
- objectGUID
- Organization Name

This is the value of the Name field in the Create Organization form of the Oracle Identity Manager Administrative and User Console.

AD Group

The following fields are provisioned:

- Group Name
- Organization Name
- objectGUID
- Group Type
- Group Display Name

AD User

The following fields are provisioned:

- User ID

Note: Microsoft Active Directory restricts the number of characters in the user ID field to 20 characters. Therefore, while provisioning a user through Oracle Identity Manager, you must not enter more than 20 characters in this field.

- Password
- objectGUID
- Organization Name
- First Name
- Last Name
- Middle Name
- User Must Change Password at Next Logon

- Password Never Expires
- Account Expiration Date
- Full Name
- Group Name

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are in the following directory on the installation media:

Directory Servers\Microsoft Active Directory\Microsoft Active Directory Base

These files and directories are listed in the following table.

| File in the Installation Media Directory | Description |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ext\ldapsdk-4.1.jar | This external JAR file contains the JNDI LDAP booster package that is required for the connector. |
| ext\ldapbp.jar | This external JAR file is used for batched reconciliation. |
| lib\xliActiveDirectory.jar | This JAR file contains the class files required for provisioning. |
| lib\xliADRecon.jar | This JAR file contains the class files required for reconciliation. |
| Files in the resources directory | Each of these resource bundle files contains language-specific information that is used by the connector. Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console. |
| scripts\install.bat | This batch file is used to add a certificate to the keystore if Oracle Identity Manager is installed on a Microsoft Windows operating system. |
| scripts\install.sh | This file is used to add a certificate to the keystore if Oracle Identity Manager is installed on a UNIX-based system. |
| test\config\config.properties | This file is used to set input test data for the connector test suite. |
| test\lib\xliADTest.jar | This JAR file contains the class files required for the connector test suite. |
| test\logs | This directory is used by the connector test suite to log the results of the tests. The log files are created in this directory. |
| test\scripts\runADTest.bat | This file is used to run a test using the connector test suite. |
| xml\xliActiveDirectoryScheduleTask_DM.xml | This XML file contains definitions for the Oracle Identity Manager components of the connector related to the reconciliation module. |

| File in the Installation Media Directory | Description |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| xml\xliADGroupObject_DM.xml | <p>This XML file contains definitions for the connector components related to AD Group provisioning. These components include:</p> <ul style="list-style-type: none">▪ Resource object for AD Group provisioning▪ IT resource type▪ Custom process form▪ Process task and adapters (along with their mappings)▪ Login resource object▪ Provisioning process▪ Pre-populate rules |
| xml\xliADOrganizationObject_DM.xml | <p>This XML file contains definitions for the connector components related to AD Organization provisioning. These components include:</p> <ul style="list-style-type: none">▪ Resource object for AD Organization provisioning▪ IT resource type▪ Custom process form▪ Process task and adapters (along with their mappings)▪ Login resource object▪ Provisioning process▪ Pre-populate rules |
| xml\xliADUserObject_DM.xml | <p>This XML file contains definitions for the connector components related to AD User provisioning. These components include:</p> <ul style="list-style-type: none">▪ Resource object for AD User provisioning▪ IT resource type▪ Custom process form▪ Process task and adapters (along with their mappings)▪ Login resource object▪ Provisioning process▪ Pre-populate rules |

Note: The files in the test directory are used only to run tests on the connector.

The "[Step 3: Copying the Connector Files and External Code](#)" section on page 2-2 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

To determine the release number of a connector that you have deployed:

1. Extract the contents of the xliActiveDirectory.jar file. For a connector that has been deployed, this file is in the following directory:

`OIM_home\xellerate\JavaTasks`

2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `xliActiveDirectory.jar` file.

In the `manifest.mf` file, the release number of the connector is displayed as the value of the `Version` property.

See Also: *Oracle Identity Manager Design Console Guide*

Deploying the Connector

Deploying the connector involves the following steps:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Configuring the Target System](#)
- [Step 3: Copying the Connector Files and External Code](#)
- [Step 4: Configuring the Oracle Identity Manager Server](#)
- [Step 5: Importing the Connector XML Files](#)
- [Step 6: Configuring Reconciliation](#)
- [Step 7: Compiling Adapters](#)
- [Step 8: Configuring SSL](#)

If you want to configure the connector for multiple installations of Microsoft Active Directory, then perform the following procedure:

- [Configuring the Connector for Multiple Installations of the Target System](#)

If you are going to install and use the password synchronization module for Microsoft Active Directory, then perform the following procedure:

- [Configuring the Connector and Password Synchronization Module](#)

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

| Item | Requirement |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Oracle Identity Manager | Oracle Identity Manager release 8.5.3 or later |
| Target systems | Microsoft Active Directory Server (Microsoft Windows 2000 or 2003) |
| Target system host platforms | The target system host platform can be any one of the following: <ul style="list-style-type: none">■ Microsoft Windows 2000 with Service Pack 4 or later■ Microsoft Windows 2003 |
| Other software | Certificate Services |
| External code | JNDI LDAP Booster package (ldapsdk-4.1.1.jar) |

| Item | Requirement |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target system user account | Microsoft Windows 2000/2003 Server (Domain Controller) administrator You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-7. |

Step 2: Configuring the Target System

You must ensure that the parent organization exists in the target server installation. The parent organization is specified as the value of the `Root_Context` parameter in the relevant IT resource. Refer to the ["Defining IT Resources"](#) section on page 2-7 for more information about this parameter.

Step 3: Copying the Connector Files and External Code

The connector files and external code files to be copied and the directories to which you must copy them are given in the following table.

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:

Directory Servers\Microsoft Active Directory\Microsoft Active Directory Base

Refer to the ["Files and Directories That Comprise the Connector"](#) section on page 1-5 for more information about these files.

| File in the Installation Media Directory | Destination Directory |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Files in the <code>ext</code> directory | <code>OIM_home\xellerate\ThirdParty</code> |
| <code>lib\xliActiveDirectory.jar</code> | <code>OIM_home\xellerate\JavaTasks</code> <code>OIM_home\xellerate\ScheduleTask</code> |
| <code>lib\xliADRecon.jar</code> | <code>OIM_home\xellerate\JavaTasks</code> <code>OIM_home\xellerate\ScheduleTask</code> |
| Files in the <code>resources</code> directory | <code>OIM_home\xellerate\connectorResources</code> |
| Files in the <code>scripts</code> directory | <code>OIM_home\xellerate\scripts</code> |
| | After you copy the <code>install.bat</code> (or <code>install.sh</code>) file, use a text editor to open the file and specify the actual location of the JDK directory in the file. |
| Directories and files in the <code>test</code> directory | <code>OIM_home\xellerate\test</code> |
| Files in the <code>xml</code> directory | <code>OIM_home\xellerate\XLIntegrations\Active Directory\xml</code> |

Note: While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

Step 4: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

Note: In a clustered environment, you must perform this step on each node of the cluster.

- [Changing to the Required Input Locale](#)
- [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)
- [Enabling Logging](#)

Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

To set the required input locale:

Note: Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.
2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle in the `OIM_home\xellerate\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, change to the `OIM_home\xellerate\bin` directory.
2. Enter one of the following commands:

Note: You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:

`OIM_home\xellerate\bin\batch_file_name`

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

- **On UNIX:**

```
PurgeCache.sh ConnectorResourceBundle
```

In this command, `ConnectorResourceBundle` is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

```
OIM_home\xellerate\config\xlConfig.xml
```

Note: You can ignore the exception that is thrown when you perform Step 2.

Enabling Logging

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- **ALL**
This level enables logging for all events.
- **DEBUG**
This level enables logging of information about fine-grained events that are useful for debugging.
- **INFO**
This level enables logging of informational messages that highlight the progress of the application at coarse-grained level.
- **WARN**
This level enables logging of information about potentially harmful situations.
- **ERROR**
This level enables logging of information about error events that may still allow the application to continue running.
- **FATAL**
This level enables logging of information about very severe error events that could cause the application to stop functioning.
- **OFF**
This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **For JBoss Application Server**

To enable logging:

1. Add the following line in the
`OIM_home\xellerate\config\log.properties` file:

```
log4j.logger.XELLERATE=log_level
```

2. In this line, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.XELLERATE=INFO
```

After you enable logging, log information is written to the following file:

```
JBoss_home\server\default\log\server.log
```

■ For IBM WebSphere:

To enable logging:

1. Add the following line in the

OIM_home\xellerate\config\log.properties file:

```
log4j.logger.XELLERATE=log_level
```

2. In this line, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.XELLERATE=INFO
```

After you enable logging, log information is written to the following file:

```
WebSphere_home\AppServer\logs\server_name\startServer.log
```

■ For BEA WebLogic

To enable logging:

1. Add the following line in the

OIM_home\xellerate\config\log.properties file:

```
log4j.logger.XELLERATE=log_level
```

2. In this line, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.XELLERATE=INFO
```

After you enable logging, log information is written to the following file:

```
WebLogic_home\user_projects\domains\domain_name\server_name\server_name.log
```

■ For OC4J

To enable logging:

1. Add the following line in the

OIM_home\xellerate\config\log.properties file:

```
log4j.logger.XELLERATE=log_level
```

2. In this line, replace *log_level* with the log level that you want to set.

For example:

```
log4j.logger.XELLERATE=INFO
```

After you enable logging, log information is written to the following file:

```
OC4J_home\opmn\logs\default_group~home~default_group~1.log
```

Step 5: Importing the Connector XML Files

You must import the connector XML files in the following sequence:

1. xliADOrganizationObject_DM.xml
2. xliADGroupObject_DM.xml
3. xliADUserObject_DM.xml
4. XliActiveDirectoryScheduleTask_DM.xml

Caution: If you do not import the connector files in the specified sequence, then the connector may not work.

To import the connector XML files into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the xliADOrganizationObject_DM.xml file, which is in the *OIM_home\xellerate\XLIntegrations\ActiveDirectory\xml* directory. 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 **Next**. The Provide IT Resource Instance Data page for the AD Server IT resource is displayed.
8. Specify values for the parameters of the AD Server IT resource. Depending on whether the operating system is Microsoft Windows 2000 or Microsoft Windows 2003, refer to the appropriate table in the "[Defining IT Resources](#)" section on page 2-7 for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the AD Server IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

See Also: If you want to define another IT resource, then refer to *Oracle Identity Manager Tools Reference Guide* for instructions.

11. Click **View Selections**.

The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. Remove these nodes by right-clicking each node and then selecting **Remove**.

12. Click **Import**. The connector file is imported into Oracle Identity Manager.
13. Perform the same procedure to import the remaining connector XML files, in the specified order.

Note: The IT resources that you must define are the same, regardless of the XML file that you import. Therefore, you only need to define the IT resources for the first XML file that you import.

After you import the connector XML file, proceed to the ["Step 6: Configuring Reconciliation"](#) section on page 2-12.

Defining IT Resources

This section provides IT resource parameter values for the following operating systems:

- [Microsoft Windows 2000](#)
- [Microsoft Windows 2003](#)

Microsoft Windows 2000

The following table provides values for the parameters of the AD Server IT resource, for Microsoft Windows 2000.

| Parameter | Description |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin FQDN | Fully qualified domain name corresponding to the administrator Format: cn=ADMIN_LOGIN, cn=Users, dc=DOMAIN Sample value: cn=administrator, cn=Users, dc=adomain |
| Admin Login | User ID of the administrator account that is used to create the OU/user |
| Admin Password | Password of the administrator account that is used to create the OU/user |
| Root Context | This is the fully qualified domain name of the parent or root organization. For example, the root suffix. Format: ou=ORGANIZATION_NAME, dc=DOMAIN Sample value: ou=Adapters, dc=adomain |
| Server Address | Host name or IP address of the target Microsoft Windows 2000 computer on which Microsoft Active Directory is installed Sample value: w2khost |
| Last Modified Time Stamp | Date and time at which the last AD User reconciliation run was completed The reconciliation engine automatically fills a value in this attribute each time it runs the AD User reconciliation. Default value: 0 |
| Last Modified Time Stamp Group | Date and time at which the last AD Group reconciliation run was completed The reconciliation engine automatically fills a value in this attribute each time it runs AD Group reconciliation. Default value: 0 |

| Parameter | Description |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use SSL | <p>Specifies whether or not to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory</p> <p>Default value: <code>false</code></p> <p>See Also: The Known Issues list in Chapter 4 for information about a limitation arising from setting this parameter to <code>false</code>.</p> <p>Note: It is recommended that you enable SSL to secure communication with the target system.</p> |
| SSL Port Number | <p>Port at which SSL is running on the Microsoft Active Directory server</p> <p>Default value: <code>636</code></p> |
| AtMap ADUser | <p>Attribute map name for the Microsoft Active Directory user</p> <p>Default value: <code>AtMap.AD</code></p> |
| AtMap Group | <p>Attribute map name for the Microsoft Active Directory group</p> <p>Default value: <code>AtMap.ADGroup</code></p> |
| Target Locale: Country | <p>Country code</p> <p>Default value: <code>US</code></p> <p>Note: You must specify the value in uppercase.</p> |
| Target Locale: Language | <p>Language code</p> <p>Default value: <code>en</code></p> <p>Note: You must specify the value in lowercase.</p> |
| CustomizedReconQuery | <p>Specify the LDAP query that you want to use to customize reconciliation. Refer to the "Query-Based Reconciliation" section in the "What's New" chapter for information about this parameter.</p> <p>Sample value: <code>memberOf=cn=AcmeAdmin,cn=Users,dc=GLOBAL,dc=com</code></p> <p>Note: You can use this value in conjunction with the <code>GroupObject</code> attribute defined in the "User Reconciliation Scheduled Task" section on page 2-15.</p> |
| ADDisableAttr Lookup Definition | <p>Specify the name of the lookup table that lists the nonmandatory user attributes defined in Microsoft Active Directory. This attribute is used in conjunction with the <code>Use Disable Attr</code> parameter.</p> <p>Note: Nonmandatory attributes of Microsoft Active Directory can accept <code>NULL</code> values during provisioning. You must manually create the lookup definition containing the nonmandatory attributes of Microsoft Active Directory. For each attribute that you add to this lookup definition, you must ensure that both the code key and decode key values are set to the name of the attribute.</p> <p>Refer to <i>Oracle Identity Manager Design Console Guide</i> for information about creating the lookup definition.</p> |

| Parameter | Description |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use Disable Attr | <p>Specifies whether or not nonmandatory attributes defined in Microsoft Active Directory must be set to NULL when a user is disabled through a provisioning operation. The value of this parameter can be True or False. The default value is False.</p> <p>Note: You can use this parameter only if you specify a value for the ADDisableAttr Lookup Definition parameter.</p> |
| AD Sync installed (yes/no) | <p>If you are going to install and use the Microsoft Active Directory Password Synchronization module, then specify yes as the value of this parameter. Otherwise, specify no. The default value is no.</p> |
| OIM User UDF | <p>Specify the name of the user-defined field that you create in Oracle Identity Manager.</p> <p>You must specify a value for this parameter only if you specify yes as the value of the AD Sync installed (yes/no) parameter.</p> <p>Note: You must specify the column name and not the field label that you enter while adding the custom attribute in Oracle Identity Manager. For example, if you enter the label PWDCHANGEDINDICATION, then the column name that you must specify is USR_UDF_PWDCHANGEDINDICATION. Oracle Identity Manager adds the USR_UDF_ prefix while creating a column.</p> |
| Custom Attribute Name | <p>Specify the name of the custom attribute that you create in Microsoft Active Directory.</p> <p>You must specify a value for this parameter only if you specify yes as the value of the AD Sync installed (yes/no) parameter.</p> |

After you specify values for these IT resource parameters, proceed to Step 9 of the procedure to import connector XML files.

Microsoft Windows 2003

The following table provides values for the parameters of the AD Server IT resource, for Microsoft Windows 2003.

| Parameter | Description |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin FQDN | <p>Fully qualified domain name corresponding to the administrator</p> <p>Format: <i>ADMIN_LOGIN@DOMAIN</i></p> <p>Sample value: administrator@adomain.com</p> |
| Admin Login | <p>User ID of the administrator account that is used to create the OU/user</p> |
| Admin Password | <p>Password of the administrator account that is used to create the OU/user</p> |

| Parameter | Description |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root Context | <p>Usually, this is the fully qualified domain name of the parent or root organization.</p> <p>For example, the root suffix.</p> <p>Format: ou=<i>ORGANIZATION_NAME</i>,dc=<i>DOMAIN</i></p> <p>Sample value: ou=Adapters,dc=adomain,dc=com</p> |
| Server Address | <p>Host name or IP address of the target Microsoft Windows 2000 computer on which Microsoft Active Directory is installed</p> <p>Sample value: w2003host</p> |
| Last Modified Time Stamp | <p>Date and time at which the last AD User reconciliation run was completed</p> <p>The reconciliation engine automatically fills a value in this attribute each time it runs the AD User reconciliation.</p> <p>Default value: 0</p> |
| Last Modified Time Stamp Group | <p>Date and time at which the last AD Group reconciliation run was completed</p> <p>The reconciliation engine automatically fills a value in this attribute each time it runs AD Group reconciliation.</p> <p>Default value: 0</p> |
| Use SSL | <p>Specifies whether or not to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory</p> <p>Default value: false</p> <p>See Also: The Known Issues list in Chapter 4 for information about a limitation arising from setting this parameter to false.</p> <p>Note: It is recommended that you enable SSL to secure communication with the target system.</p> |
| SSL Port Number | <p>Port at which SSL is running on the Microsoft Active Directory server</p> <p>Default value: 636</p> |
| AtMap ADUser | <p>Attribute map name for the Microsoft Active Directory user</p> <p>Default value: AtMap.AD</p> |
| AtMap Group | <p>Attribute map name for the Microsoft Active Directory group</p> <p>Default value: AtMap.ADGroup</p> |
| Country | <p>Country code</p> <p>Default value: US</p> <p>Note: You must specify the value in uppercase.</p> |
| Language | <p>Language code</p> <p>Default value: en</p> <p>Note: You must specify the value in lowercase.</p> |

| Parameter | Description |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CustomizedReconQuery | <p>Specify the LDAP query that you want to use to customize reconciliation. Refer to the "Query-Based Reconciliation" section in the "What's New" chapter for information about this parameter.</p> <p>Sample value: <code>memberOf=cn=AcmeAdmin,cn=Users,dc=GLOBAL,dc=com</code></p> <p>Note: You can use this value in conjunction with the GroupObject attribute defined in the "User Reconciliation Scheduled Task" section on page 2-15.</p> |
| ADDisableAttr Lookup Definition | <p>Specify the name of the lookup table that lists the nonmandatory user attributes defined in Microsoft Active Directory. This attribute is used in conjunction with the Use Disable Attr parameter.</p> <p>Note: Nonmandatory attributes of Microsoft Active Directory can accept NULL values during provisioning. You must manually create the lookup definition containing the nonmandatory attributes of Microsoft Active Directory. For each attribute that you add to this lookup definition, you must ensure that both the code key and decode key values are set to the name of the attribute.</p> <p>Refer to <i>Oracle Identity Manager Design Console Guide</i> for information about creating the lookup definition.</p> |
| Use Disable Attr | <p>Specifies whether or not nonmandatory attributes defined in Microsoft Active Directory must be set to NULL when a user is disabled through a provisioning operation. The value of this parameter can be True or False.</p> <p>Note: You can use this parameter only if you specify a value for the ADDisableAttr Lookup Definition parameter.</p> |
| AD Sync installed (yes/no) | <p>If you are going to install and use the Microsoft Active Directory Password Synchronization module, then specify yes as the value of this parameter. Otherwise, specify no. The default value is no.</p> |
| OIM User UDF | <p>Specify the name of the user-defined field that you create in Oracle Identity Manager.</p> <p>You must specify a value for this parameter only if you specify yes as the value of the AD Sync installed (yes/no) parameter.</p> <p>Note: You must specify the column name and not the field label that you enter while adding the custom attribute in Oracle Identity Manager. For example, if you enter the label PWDCHANGEDINDICATION, then the column name that you must specify is USR_UDF_PWDCHANGEDINDICATION. Oracle Identity Manager adds the USR_UDF_ prefix while creating a column.</p> |
| Custom Attribute Name | <p>Specify the name of the custom attribute that you create in Microsoft Active Directory.</p> <p>You must specify a value for this parameter only if you specify yes as the value of the AD Sync installed (yes/no) parameter.</p> |

After you specify values for these IT resource parameters, proceed to Step 9 of the procedure to import connector XML files.

Step 6: Configuring Reconciliation

The scheduled tasks for reconciliation are created when you import the `XliActiveDirectoryScheduleTask_DM.xml` file as part of the procedure described in the ["Step 5: Importing the Connector XML Files"](#) section on page 2-6.

Additional tasks that you need to perform to configure reconciliation are described in the following sections:

- [Specifying the Fields to Be Reconciled](#)
- [Configuring Trusted Source Reconciliation](#)
- [Creating Scheduled Tasks for Reconciliation](#)

If you are using Oracle Identity Manager release 9.0.1, then you must perform the following procedure to enable reconciliation:

- [Enabling Reconciliation in Oracle Identity Manager Release 9.0.1](#)

Specifying the Fields to Be Reconciled

You can select the fields that must be reconciled. To do this:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Double-click **Lookup Definition**.
4. Search for the `Lookup.ADReconciliation.FieldMap` lookup definition by entering the name in the **Code** field and then clicking the **Query** icon.
5. To open the `Lookup.ADReconciliation.FieldMap` field map, double-click **Lookup.ADReconciliation.FieldMap**.
6. Add the required fields to the `Lookup.ADReconciliation.FieldMap` field map.

The following fields are provided by default in the `Lookup.ADReconciliation.FieldMap` field map:

- `memberOf`
- `instanceType`
- `Organization`
- `givenName`
- `sAMAccountName`
- `IT Resource`
- `objectGUID`
- `name`
- `password`

Note: The connector does not reconcile and store passwords in Oracle Identity Manager. Refer to [Chapter 4, "Known Issues"](#) for an explanation of this functionality of the connector.

- `sn`

- cn
- whenChanged
- distinguishedName
- initials
- displayName

Note: The whenChanged field is a mandatory field, which means that it must be present in the field map.

Configuring Trusted Source Reconciliation

Note: Perform this step of the procedure only if you want to configure trusted source reconciliation. Only one connector can be configured for trusted source reconciliation. If you configure trusted source reconciliation for this connector while you have another trusted source configured, then both connector reconciliations would stop working.

Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

Use the Oracle Identity Manager Design Console to configure trusted source reconciliation as follows:

1. In the Resource Objects form, select the fields that you want to reconcile as follows:
 - a. Expand the **Resource Management** folder.
 - b. Double-click **Resource Objects**.
 - c. Enter `Xellerate User` in the Name field and then click the **Query** icon.
 - d. Double-click **Xellerate User** in the list that is displayed.
 - e. On the Object Reconciliation tab, add reconciliation fields as required. You must add all the reconciliation fields that are required to provide input for mandatory fields on the Xellerate User form, for example, fields such as User Login and First Name. However, you need not specify a value in the Password field, although it is a mandatory field.
2. In the Process Definition form, create reconciliation field mappings as follows:
 - a. Expand the **Process Management** folder.
 - b. Double-click **Process Definition**.
 - c. Enter `Xellerate User` in the **Name** field and then click the **Query** icon.
 - d. On the Reconciliation Field Mappings tab, add reconciliation field mappings as required. All the mandatory fields of the User Defined process form must be mapped.
3. In the Reconciliation Rules form, create a rule for the `Xellerate User` object as follows:
 - a. Expand the **Development Tools** folder.

- b. Double-click **Reconciliation Rules**.
- c. Create a rule for the Xellerate User object, with a rule element as required.

See: *Oracle Identity Manager Design Console Guide* for instructions
- d. Select the **Active** check box to enable the rule.

Creating Scheduled Tasks for Reconciliation

To create the reconciliation scheduled tasks:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler**.
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
 - To set the task to run on a recurring basis, select the **Daily, Weekly, Recurring Intervals, Monthly, or Yearly** option.

If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
 - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task. Refer to the "[Specifying Values for the Scheduled Task Attributes](#)" section on page 2-14 for information about the values to be specified.

See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.
11. Repeat Steps 5 through 10 to define the second scheduled task.

After you define both scheduled tasks, proceed to the "[Enabling Reconciliation in Oracle Identity Manager Release 9.0.1](#)" section on page 2-16.

Specifying Values for the Scheduled Task Attributes

This section provides information about the attribute values to be specified for the following scheduled tasks:

- [Lookup Fields Reconciliation Scheduled Task](#)
- [User Reconciliation Scheduled Task](#)

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the lookup fields reconciliation scheduled task.

Note: Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

| Attribute | Description | Default/Sample Value |
|----------------|---------------------------------------------------------------------------------------------|-------------------------------------|
| Server | IT resource instance name of the Microsoft Active Directory server | AD Server |
| LookupCodeName | Lookup code that contains all the reconciled group names and the corresponding object GUIDs | Lookup.ADReconciliation.GroupLookup |

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

User Reconciliation Scheduled Task You must specify values for the following attributes of the user reconciliation scheduled task.

Note: Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change. Refer to [Appendix B](#) for more information about these attributes.

| Attribute | Description | Default/Sample Value |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| DeleteRecon | Specifies whether or not Delete reconciliation is enabled The value can be True or False. You must specify a value for this attribute. | True |
| UseFieldMapping | Specifies whether or not field mappings from the FieldLookupCode attribute must be used This attribute is used to enable the reconciliation of specific fields. The value can be True or False. | True |
| FieldLookupCode | Name of the lookup definition that is used for custom reconciliation This attribute is valid only when the UseFieldMapping attribute is set to True. | Lookup.ADReconciliation.FieldMap |
| MaintainHierarchy | Specifies whether or not organization hierarchy must be maintained in Microsoft Active Directory The value can be True or False. You must specify a value for this attribute. | True |
| XellerateObject | Name of the Xellerate User resource object in Oracle Identity Manager on which trusted reconciliation is to be performed If you want trusted reconciliation to be performed, then change the value to Xellerate User. Otherwise, change the value to False. You must specify a value for this attribute. | Xellerate User |

| Attribute | Description | Default/Sample Value |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Object | <p>Name of the AD User resource object in Oracle Identity Manager on which reconciliation is performed</p> <p>If you want AD User reconciliation to be performed, then change the value to <code>AD User</code>. Otherwise, change the value to <code>False</code>.</p> <p>You must specify a value for this attribute.</p> | <code>AD User</code> |
| Server | <p>Name of the IT resource representing the Microsoft Active Directory server</p> <p>You must specify a value for this attribute.</p> | <code>AD Server</code> |
| TransformLookupCode | <p>Lookup code used for the transformation class map kept in the lookup tables</p> <p>This attribute is valid only when the <code>UseTransformMapping</code> attribute is set to <code>True</code>.</p> | <code>Lookup.ADReconciliation.TransformationMap</code> |
| UseTransformMapping | <p>Specifies whether or not transform mappings accessed by using the <code>TransformLookupCode</code> attribute must be used</p> <p>The value can be <code>True</code> or <code>False</code>.</p> | <code>True</code> |
| XellerateOrg | <p>Oracle Identity Manager organization in which reconciled users are to be created</p> <p>You must specify a value for this attribute.</p> | <code>Xellerate Users</code> |
| MultiValueAttributes | <p>Comma-delimited list of all the multivalued Microsoft Active Directory attributes that must be reconciled</p> <p>For AD Group reconciliation, enter <code>memberOf</code>.</p> <p>You must specify a value for this attribute.</p> | <code>memberOf</code> |
| GroupObject | <p>Name of the AD Group resource object in Oracle Identity Manager on which group reconciliation is being performed</p> <p>If you want AD Group reconciliation to be performed, then change the value to <code>AD Group</code>. Otherwise, change the value to <code>False</code>.</p> <p>You must specify a value for this attribute.</p> | <code>AD Group</code> |

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

Enabling Reconciliation in Oracle Identity Manager Release 9.0.1

If you are using Oracle Identity Manager release 9.0.1, then you must perform the following procedure to enable reconciliation:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Design Console.
2. Expand the **Process Management** folder.
3. Open the Process Definition form for the AD User.
4. Click the **Reconciliation Field Mappings** tab.
5. For each field that is of the IT resource type:

- a. Double-click the field to open the Edit Reconciliation Field Mapping window for that field.
- b. Deselect **Key Field for Reconciliation Matching**.

Step 7: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- Chk Process Parent Org
- AD Move OU
- AD Get USNChanged
- AD Get OU USNCR
- Update AD Group Details
- Get Group ObjectGUID Created
- AD Delete Group
- AD Create Group
- Prepopulate AD Group Display Name
- Prepopulate AD Group Name
- check process organization
- AD Set User Password
- AD Set User CN Standard
- AD Set Account Exp Date
- AD remove User From Group
- AD Pwd Never Expires
- AD Must Change PWD
- AD Move User New
- AD Move User
- AD Get ObjectGUID
- AD Enable User
- AD Disable User
- AD Delete User
- AD Create User
- AD Change Attribute
- AD Add User To Group
- AD Prepopulate User Last Name
- AD Prepopulate User Login
- AD Prepopulate User Full Name
- AD Prepopulate User Middle Name
- AD Prepopulate User First Name

You must compile these adapters before you can use them to provision accounts on the target system.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you import into the current database, select **Compile All**.

To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.

Note: Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an OK compilation status.

3. Click **Start**. Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the `OIM_home\xellerate\Adapter` directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

Note: To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

Step 8: Configuring SSL

Note: This is an optional step of the deployment procedure.

This section covers the procedure to enable SSL on Microsoft Active Directory.

To configure SSL connectivity between Oracle Identity Manager and the target Microsoft Active Directory server, you must perform the following tasks:

1. [Installing Certificate Services](#)
2. [Enabling LDAPS](#)
3. [Setting Up the Microsoft Active Directory Certificate As a Trusted Certificate](#)

Installing Certificate Services

The connector requires Certificate Services to be running on the host computer. To install Certificate Services:

1. Insert the operating system installation media into the CD-ROM or DVD drive.
2. Click **Start**, **Settings**, and **Control Panel**.
3. Double-click **Add/Remove Programs**.
4. Click **Add/Remove Windows Components**.
5. Select **Certificate Services**.
6. Follow the instructions to start Certificate Services.

Enabling LDAPS

The target Microsoft Active Directory server must have LDAP over SSL (LDAPS) enabled. To enable LDAPS, generate a certificate as follows:

Note: Use the Enterprise CA option when you perform the following steps.

1. On the Active Directory Users and Computers console, right-click the domain node, and select **Properties**.
2. Click the **Group Policy** tab.
3. Select **Default Domain Policy**.
4. Click **Edit**.
5. Click **Computer Configuration, Windows Settings, Security Settings, and Public Key Policies**.
6. Right-click **Automatic Certificate Request Settings**, and then select **New** and **Automatic Certificate Request**. A wizard is started.
7. Use the wizard to add a policy with the **Domain Controller** template.

At the end of this procedure, the certificate is created and LDAP is enabled using SSL on port 636.

Setting Up the Microsoft Active Directory Certificate As a Trusted Certificate

If the Microsoft Active Directory certificate is not issued or certified by a certification authority (CA), then set it up as a trusted certificate. To do this, you first export the certificate and then import it into the keystore of the Oracle Identity Manager server as a trusted CA certificate.

Exporting the Microsoft Active Directory Certificate

To export the Microsoft Active Directory certificate:

1. Click **Start**, **Programs**, **Administrative Tools**, and **Certification Authority**.
2. Right-click the Certification Authority that you create, and then select **Properties**.
3. On the **General** tab, click **View Certificate**.
4. On the **Details** tab, click **Copy To File**.
5. Use the wizard to create a certificate (.cer) file using base-64 encoding.

Importing the Microsoft Active Directory Certificate

To import the Microsoft Active Directory certificate into the certificate store of the Oracle Identity Manager server:

Note: In a clustered environment, you must perform this procedure on all the nodes of the cluster.

1. Copy the certificate to the Oracle Identity Manager server.

If you use IBM WebSphere, then you must also copy the following files:

- For a nonclustered configuration of IBM WebSphere:

Copy the `jsse.jar` file into the `WS_home\java\jre\lib\ext` directory.

- For a clustered configuration of IBM WebSphere:

Copy the `jnet.jar`, `jsse.jar`, and `jcrt.jar` files into the `WS_home\java\jre\lib\ext` directory.

You can download these JAR files from the Sun Web site at

<http://java.sun.com/>

2. Change to the directory where you copy the certificate file, and then enter a command similar to the following:

```
keytool -import -alias alias -file cer_file -keystore my_cacerts -storepass
password
```

In this command:

- *alias* is the alias for the certificate (for example, the server name)
- *cer_file* is the full path and name of the certificate (`.cer`) file
- *my_cacerts* is the full path and name of the certificate store (the default is `cacerts`)

The path of the certificate store depends on the application server as shown in the following table.

| Application Server | Certificate Store Location |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| JBoss Application Server | <code>JBoss_home\jre\lib\security\cacerts</code> |
| BEA WebLogic | <code>BEA_home\java\jre\lib\security\cacerts</code> |
| IBM WebSphere | <p>For a nonclustered configuration of IBM WebSphere, you must import the files into the following certificate stores:</p> <p><code>WS_home\java\jre\lib\security\cacerts</code></p> <p>For a clustered configuration of IBM WebSphere, you must import the files into the following certificate stores on each node of the cluster:</p> <p><code>WS_home\java\jre\lib\security\cacerts</code> <code>WS_home\etc\DummyServerTrustFile.jks</code></p> |
| Oracle Containers for J2EE (OC4J) | <code>OC4J_home\jdk\jre\lib\security\cacerts</code> |

- `password` is the keystore password (the default is `changeit`)

For example:

```
keytool -import -alias thorADCert -file c:\thor\ActiveDir.cer -keystore  
C:\mydir\java\jre\lib\security\cacerts -storepass changeit
```

Note: `changeit` is the default password for the `cacerts` file stored in the Sun JVM. This may change depending on the JVM that you are using.

3. In the command prompt window, when you are prompted to specify whether or not you want to trust this certificate, enter `YES`.
4. To confirm whether or not the certificate has been imported successfully, enter a command similar to the following:

```
keytool -list -alias alias -keystore mycacerts -storepass password
```

In the example given in Step 2, to confirm that the certificate has been successfully imported, use the following command and look for the certificate name, `thorADCert`, that you provide while importing the certificate into the keystore:

```
keytool -list -alias thorADCert -keystore  
C:\mydir\java\jre\lib\security\cacerts -storepass changeit
```

5. Perform this step only if you are registering the certificate file in a new certificate store.

Add the following line in the `jre\lib\security\java.security` file:

```
security.provider.N=com.sun.net.ssl.internal.ssl.Provider
```

In this line, `N` is any number that is not used in the file.

6. Restart the application server.

Note: The user password cannot be set unless 128-bit SSL is used. In addition, the computer on which Microsoft Active Directory is installed must have Microsoft Windows 2000 Service Pack 2 (or later) or Microsoft Windows 2003 running on it.

Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of Microsoft Active Directory. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

To configure the connector for multiple installations of the target system:

1. Create and configure one IT resource for each target system installation.

The IT Resources form is in the Resource Management folder. An IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

2. Configure reconciliation for each target system installation. Refer to the "[Step 6: Configuring Reconciliation](#)" section on page 2-12 for instructions. Note that you only need to modify the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.

You can designate either a single or multiple installations of Microsoft Active Directory as trusted sources.

3. If required, modify the fields to be reconciled for the Xellerate User resource object.

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.

Configuring the Connector and Password Synchronization Module

The connector for Microsoft Active Directory performs the following functions:

- Updates Microsoft Active Directory with user account attributes (except for passwords) changed in Oracle Identity Manager
- Updates Oracle Identity Manager with user account attributes (except for passwords) changed in Microsoft Active Directory
- Updates Microsoft Active Directory with passwords changed in Oracle Identity Manager (requires LDAP over SSL)

The password synchronization module for Microsoft Active Directory updates Oracle Identity Manager with passwords changed in Microsoft Active Directory.

The connector is deployed on the Oracle Identity Manager server, and the module is deployed on the Microsoft Active Directory server. When they are deployed together (along with LDAP over SSL), the connector and the password synchronization module provide full, bidirectional synchronization of all user attributes, including passwords.

See Also: *Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide*

The instructions in this section are aimed at solving a problem that was observed in the release 9.0.3 of the connector and password synchronization module.

- [Creating a Custom Attribute in Microsoft Active Directory](#)
- [Creating a Custom Attribute in Oracle Identity Manager](#)
- [Specifying Values for IT Resource Parameters](#)
- [Sequence of Events That Occur During a Password Change](#)

Creating a Custom Attribute in Microsoft Active Directory

You must create a custom attribute in Microsoft Active Directory to act as a flag for tracking password changes initiated by Oracle Identity Manager.

The following sections describe this procedure:

- [Ensuring That the Microsoft Active Directory Schema Snap-In Is Installed](#)
- [Creating a Custom Attribute](#)

Ensuring That the Microsoft Active Directory Schema Snap-In Is Installed

The Microsoft Active Directory Schema snap-in is required to create a custom attribute. Before you can create the custom attribute, you must ensure that this snap-in is installed.

To check if the snap-in is installed:

1. On the Microsoft Active Directory server, click **Start** and then click **Run**.
2. Enter the following command, and then click **OK**:

```
mmc /a
```

If the Microsoft Active Directory Schema snap-in is already installed, then its console is displayed when you run this command.

If the console is not displayed, then you must install the Microsoft Active Directory Schema snap-in as follows:

1. Log in to the Microsoft Active Directory server as the administrator.
2. Insert the Windows 2000 Server compact disc into your compact disc drive, and then click **Browse this CD**.
3. Double-click the **I386** folder, double-click **Adminpak**, and then follow the instructions displayed in the Windows 2000 Administration Tools Setup Wizard.
4. Open the Microsoft Active Directory Schema snap-in console as follows:
 - a. Click **Start**, and then click **Run**.
 - b. Enter the following command, and then click **OK**:

```
mmc /a
```

5. On the Console menu, click **Add/Remove Snap-in** and then click **Add**.
6. Double-click **Active Directory Schema**, and then click **Close**.
7. To specify that you do not want to add any more snap-ins, click **OK**.
8. To save the changes that you make, click **Save**.

Creating a Custom Attribute

After you ensure that the Microsoft Active Directory Schema snap-in is installed, add the custom attribute in Microsoft Active Directory as follows:

1. Open the Active Directory Schema snap-in as follows:
 - a. On the Microsoft Active Directory server, click **Start** and then click **Run**.
 - b. Enter the following command, and then click **OK**:

```
mmc /a
```

2. In the console tree, right-click **Attributes** and then select **Create Attribute**.
3. Set the attribute type to **Integer**.
4. In the console tree, select **Classes**.
5. Right-click **User**, and then select **Properties**.

6. On the Attribute tab, select **Add** to add the attribute to the "User" class.

Creating a Custom Attribute in Oracle Identity Manager

You must create a custom attribute in Oracle Identity Manager to act as a flag for tracking password changes initiated by Microsoft Active Directory.

To create a custom attribute (user-defined field) in Oracle Identity Manager:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Design Console.
2. Expand the **Administration** folder.
3. Select **User Defined Field Definition**.
4. Click the Search icon.
5. Select **USR** from the results that are displayed, and then click **Add**.
6. In the User Defined Fields dialog box, enter the following values:
 - **Label:** Enter a label for the field. For example: PWDCHANGEDINDICATION
 - **Field Size:** 20

The user-defined field that you create will hold either `ADSYNC_TRUE` or `ADSYNC_FALSE`.
 - **DataType:** String
 - **Column Name:** Enter a column name for the field.

It is recommended that you enter the same value as that you enter in the Label field. For example: PWDCHANGEDINDICATION

Oracle Identity Manager automatically appends `USR_UDF_` to the column name that you specify. So, for example, if you specify `PWDCHANGEDINDICATION` as the column name, then the actual column name is changed to `USR_UDF_PWDCHANGEDINDICATION`.
7. Click **Save**.

Specifying Values for IT Resource Parameters

While performing the procedure described in the ["Defining IT Resources"](#) section on page 2-7, you must specify values for the following parameters:

- `AD Sync installed (yes/no)`

If you are going to install and use the Microsoft Active Directory Password Synchronization module, then specify `yes` as the value of this parameter. Otherwise, specify `no`. The default value is `no`.
- `OIM User UDF`

Specify the name of the user-defined field that you create in Oracle Identity Manager.

You must specify a value for this parameter only if you specify `yes` as the value of the `AD Sync installed (yes/no)` parameter.

Note: You must specify the column name and not the field label that you enter while adding the custom attribute in Oracle Identity Manager. For example, if you

enter the label `PWDCHANGEDINDICATION`, then the column name that you must specify is `USR_UDF_PWDCHANGEDINDICATION`. Oracle Identity Manager adds the `USR_UDF_` prefix while creating a column.

- Custom Attribute Name

Specify the name of the custom attribute that you create in Microsoft Active Directory.

You must specify a value for this parameter only if you specify `yes` as the value of the `AD Sync installed (yes/no)` parameter.

Sequence of Events That Occur During a Password Change

This section describes the sequence of events that take place during a password change operation.

Suppose user John Doe changes his password in Microsoft Active Directory. This events initiates the following sequence of events:

1. The password synchronization module changes the user's password in Oracle Identity Manager.
2. The password synchronization module changes the value of the Oracle Identity Manager user-defined field to `ADSYNC_TRUE`.
3. Because the value of the Oracle Identity Manager user-defined field is `ADSYNC_TRUE`, the Password Updated process task does not change the password in Microsoft Active Directory.
4. The password synchronization module changes the value of the Oracle Identity Manager user-defined field back to `ADSYNC_FALSE`.

Suppose user Jane Doe changes her password in Oracle Identity Manager. This events initiates the following sequence of events:

1. The Password Updated process task changes the user's password in Microsoft Active Directory.
2. The Password Updated process task changes the value of the Microsoft Active Directory custom attribute to 1.
3. Because the value of the Microsoft Active Directory custom attribute is 1, the password synchronization module does not change the password in Oracle Identity Manager.
4. The Password Updated process task changes the value of the Microsoft Active Directory custom attribute back to 0.

Configuring the `xlconfig.xml` File for the Password Synchronization Module

After you install the Microsoft Active Directory connector, you must make changes in the `xlconfig.xml` of the password synchronization to reflect the properties of the connector.

This is part of the installation procedure for the password synchronization module. It is described in the "Configuring the `xlconfig.xml` File After Installing the Connector" of *Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide*.

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. You can conduct provisioning tests on the connector. This type of test involves using Oracle Identity Manager to provision one of its users or organizations with a target resource. In other words, Oracle Identity Manager is the starting point of the connector and the target resource is the end point.

Testing Provisioning

To test provisioning:

1. Update the following entry in the `runADTest.bat` script file. This file is in the `OIM_home\xellerate\test\scripts` directory.

```
set XL_HOME = OIM_home
```

2. Update the `config.properties` file in the `OIM_home\xellerate\test\config` directory. In this file, specify values for the attributes of the AD user that is created in Microsoft Active Directory during the provisioning test.

3. Run the `runADTest.bat` script. This file is in the following directory:

```
OIM_home\xellerate\test\scripts
```

If the script runs without any error, then verify that the user has been created on the Microsoft Active Directory server.

Troubleshooting

Suppose the `Use SSL IT resource` parameter is set to `false`. When you provision a Microsoft Active Directory user through Oracle Identity Manager, the password cannot be set and updated by using Oracle Identity Manager. Therefore, if there are any existing password policies in the Microsoft Active Directory server, then you must disable them if the communication is not secured by SSL.

To disable a password policy, perform the following procedure:

1. Click **Start, Settings, and Control Panel**.
2. Double-click **Administrative Tools, Local Security Policy, Account Policies, and Password Policy**.
3. Double-click **Password must meet complexity requirements**.
4. In the Domain Security Policy Setting dialog box, select **Disabled** and then click **OK**.

This limitation is also mentioned in the Known Issues list in [Chapter 4](#).

Known Issues

The following are known issues associated with this release of the connector:

- A Microsoft Active Directory user can be migrated from one Microsoft Windows Server (2000 or 2003) domain controller to another. However, if you want to move a user from one domain to another, then the organization must remain the same.
- The field name defined in the Xellerate User Reconciliation Fields form for user login must be `sAMAccountName`, so that it is consistent with the entry in Microsoft Active Directory.
- A problem may occur when provisioning Oracle Identity Manager users to Microsoft Active Directory installed on Microsoft Windows 2003 with password complexity set for user accounts. In this case, passwords for user accounts provisioned from Oracle Identity Manager must adhere to the password policy set in Microsoft Active Directory.

In Microsoft Active Directory, password policies are controlled through password complexity rules. Complexity requirements are enforced when passwords are changed or created.

See Also: For more information about password guidelines, refer to the following page on the Microsoft TechNet Web site:

<http://technet2.microsoft.com/WindowsServer/en/library/d406b824-857c-4c2a-8de2-9b7ecbfa6e511033.msp?mfr=true>

- A problem may occur when provisioning Oracle Identity Manager users to Microsoft Active Directory using Microsoft Windows 2003. You must either select **Password Never Expires** or specify a valid date in the **Account Expiry Date** field. Otherwise, the user will be created and disabled immediately.
- During reconciliation, the actual Microsoft Active Directory user password is not reconciled. Instead, a dummy value is inserted in the User Password field in the process form.

You can install and use the password synchronization module for Microsoft Active Directory if you want to synchronize passwords between Oracle Identity Manager and Microsoft Active Directory.

See Also: *Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide*

- There is a limitation in the Create User function. When this function is run, if the **User must change password at next logon** check box is selected in the User

Defined process form, then the corresponding change does not get reflected in Microsoft Active Directory.

After the user is created in Microsoft Active Directory and the Create User function is run successfully, the same check box remains deselected in the target system.

Perform the following steps to configure this setting correctly for a Microsoft Active Directory user:

1. Run the Create User function with the default settings in the User Defined process form.
 2. After the Microsoft Active Directory user is created, in the process form, select the **User must change password at next logon** check box, and then click **Save**. This will trigger the relevant update task, and the setting gets correctly configured in Microsoft Active Directory.
- Suppose the Use SSL IT resource parameter is set to `false`. When you provision a Microsoft Active Directory user through Oracle Identity Manager, the password cannot be set and updated by using Oracle Identity Manager. Therefore, if there are any existing password policies in Microsoft Active Directory, then you must disable them if the communication is not secured by SSL.

This limitation is also described in the "[Troubleshooting](#)" section on page 3-1.

To disable a password policy, perform the following procedure:

1. Click **Start, Settings, and Control Panel**.
 2. Double-click **Administrative Tools, Local Security Policy, Account Policies, and Password Policy**.
 3. Double-click **Password must meet complexity requirements**.
 4. In the Domain Security Policy Setting dialog box, select **Disabled** and then click **OK**.
- While provisioning an AD User or AD Group, if the organization is not selected, then the user or group is created in the static container `CN=Users`.
 - Suppose the operating environment consists of a Microsoft Active Directory installation on a server on which Microsoft Exchange has also been installed. If reconciliation with Microsoft Active Directory carries user fields with binary values, then these fields must be suppressed before the reconciliation records are passed on to Oracle Identity Manager. This is because Oracle Identity Manager cannot handle fields with binary values.

The following are examples of fields with binary values:

- `msExchMailboxSecurityDescriptor`
- `msExchMailboxGuid`
- `showInAddressBook`
- `msExchPoliciesIncluded`
- `textEncodedORAddress`
- `proxyAddresses`

Refer to "[Specifying the Fields to Be Reconciled](#)" section on page 2-12 for information about using the `Lookup.ADReconciliation.FieldMap` field map to suppress such fields.

- The `MaintainHeirarchy` option with a value `true` reconciles organization units from Microsoft Active Directory. It is recommended that you use this option with a root context in which the parent attribute is `ou`. This means that the DN of the root context must start with `ou=`. For a root context starting with elements like `dc=`, the `MaintainHeirarchy` option would not work as expected.

- To run the Move User function, you must ensure that the following prerequisites are addressed:

The destination organization, where you want to move the user, must have the same hierarchical structure in Oracle Identity Manager as in the target Microsoft Active Directory. For example, if you want to move the user to a destination organization `ou=AcmeWidgets`, `ou=Integrations`, then the `AcmeWidgets` organization must be inside the `Integrations` organization in Oracle Identity Manager.

Then, update the organization name in the AD process form, not in the Oracle Identity Manager user form.

- Some Asian languages use multibyte character sets. If the character limit for the fields in 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 limitation:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

- The connector does not support the use of security certificates that contain non-English characters.
- When you create a user account directly on Microsoft Active Directory, you need not specify values for some user fields, such as First Name and Last Name. However, while provisioning a user on Microsoft Active Directory through Oracle Identity Manager, you must enter values for the User ID, First Name, Last Name, and Full Name fields in the AD User form (User Process form).

In addition, if the pre-populated values are to be changed, then the Full Name field value must be a combination of the First name, Middle Name, and Last Name field values separated by white spaces. The format is as follows:

First_Name Middle_Name Last_Name

- During reconciliation, if a user in Microsoft Active Directory has not been assigned values for the First Name or Last Name fields, then these fields in Oracle Identity Manager are updated with the Full Name field value. This is because Full Name is a mandatory field in Microsoft Active Directory.
- On a Microsoft Windows 2003 server on which Service Pack 1 has not been installed, you may 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

<http://support.microsoft.com/kb/889100/>

- You can provision an organization through Oracle Identity Manager on Microsoft Active Directory. However, you cannot change the name of this organization through Oracle Identity Manager.

-
- While provisioning a user in the Japanese language, the given name (first name) is listed before the family name (last name) instead of the family name being listed before the given name.
 - Microsoft Active Directory restricts the number of characters in the user ID field to 20 characters. Therefore, while provisioning a user through Oracle Identity Manager, if you enter more than 20 characters as the user ID, then the user ID created on Microsoft Active Directory is truncated to the first 20 characters.

Attribute Mappings Between Oracle Identity Manager and Microsoft Active Directory

The following table discusses attribute mappings between Oracle Identity Manager and Microsoft Active Directory.

| Oracle Identity Manager Attribute | Microsoft Active Directory Attribute | Description |
|-----------------------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password | unicodePwd | User's password in UTF-8 format This is a write-only attribute. |
| User must change password at next logon | pwdLastSet | Flag that indicates the last time users modified their passwords If this attribute is set to zero and the Password Never Expires property of the user account is set to false, then the user must set the password at next logon. |
| Password never expires | userAccountControl | Flag that controls the Password Never Expires property |
| Account Expiration Date | accountExpires | Date when the account expires |
| Object GUID | objectGUID | GUID that is based on the current time stamp assigned to an object |
| Organization Name | Organization | Name of the organization |
| First Name | givenName | First name |
| Last Name | sn | Last name |
| Middle Name | middleName, initials | Initials for the user's middle name This is used as the middle initial in the Microsoft Windows Address Book. |
| Full Name | cn, displayName | Display name for a user This is usually a combination of the user's first name, middle initial, and last name. |
| User ID | sAMAccountName, userPrincipalName | User's logon name Note: Microsoft Active Directory restricts the number of characters in the user ID field to 20 characters. Therefore, while provisioning a user through Oracle Identity Manager, you must not enter more than 20 characters in this field. |
| Group Name | memberOf | Distinguished name of the groups to which an object belongs |

| Oracle Identity Manager Attribute | Microsoft Active Directory Attribute | Description |
|-----------------------------------|--------------------------------------|------------------------------------------------------------------------------------------------------------|
| Group Type | instanceType | Type of group For example, Global Security Group and Local Distribution Group. |
| Group Display Name | cn | Display name for the group object |
| USN Create | uSNCreated | USN value assigned by the local directory for the object during creation This is a read-only attribute. |
| USN Change | uSNChanged | USN-changed value assigned for every change to the object |

Attributes of the Reconciliation Scheduled Task

The following are the attributes of the reconciliation scheduled task:

- **DeleteRecon**

This attribute is used to enable the Delete Reconciliation feature. The value can be `True` or `False`. If you enable Delete reconciliation, then you must ensure that the `Server` attribute points to the Microsoft Active Directory root context where information about deleted users is stored.

Because Microsoft Active Directory does not keep track of deleted users, this mechanism (of moving deleted users to a specific OU) must be implemented by the directory administrator. In addition, in the case of trusted reconciliation, the users that are reconciled using the Delete Reconciliation function are marked as deleted by Oracle Identity Manager. In the case of nontrusted reconciliation, the Microsoft Active Directory resource object is revoked for such users.

You must specify a value for this attribute.

- **UseFieldMapping**

This attribute is used to enable the reconciliation of specific fields. The value can be `True` or `False`. If it is set to `True`, then the value of the `FieldLookupCode` attribute is used to find the field mappings stored in the lookup tables.

Note: If the `UseFieldMapping` parameter is set to `False`, then some fields with binary values would be passed on to Oracle Identity Manager. The current release of Oracle Identity Manager cannot handle binary values.

The following are some of the fields that have binary values:

- `msExchMailboxSecurityDescriptor`
- `msExchMailboxGuid`
- `showInAddressBook`
- `msExchPoliciesIncluded`
- `textEncodedORAddress`
- `proxyAddresses`

The same issue is discussed in the Known Issues list in [Chapter 4](#).

- **FieldLookupCode**

This attribute provides the name of the lookup definition that provides the mapping between Microsoft Active Directory fields and virtual fields in Oracle Identity Manager.

This attribute is used when there are multiple external systems that are being reconciled against a single Oracle Identity Manager resource object. In such a situation, it is not possible to use the existing reconciliation scheduled task. Therefore, you must specify the mappings between Microsoft Active Directory fields and virtual Oracle Identity Manager fields. These virtual fields are then mapped to the actual fields on the process form.

This is illustrated by the following example:

Suppose there are two systems, S1 and S2, that are being reconciled against a resource object called `ADObject`. In addition, the reconciliation parameters are p1, p2, and p3 for S1 and q1, q2, and q3 for S2. Because they are being reconciled against the same resource object, Oracle Identity Manager does not allow multiple mappings of the same field. For instance, if p1 and q1 both correspond to the user ID, then both of them cannot be mapped at the same time. To avoid this, you can use virtual mappings, in which case, p1, p2, p3, q1, q2, and q3 are mapped to the same virtual Oracle Identity Manager attributes. These attributes in turn are mapped on the resource object and provisioning process. Therefore, if the virtual Oracle Identity Manager attributes are x1, x2, and x3, then the mapping in the field maps is as follows:

p1 is mapped to x1
p2 is mapped to x2
p3 is mapped to x3
q1 is mapped to x1
q2 is mapped to x2
q3 is mapped to x3

- **MaintainHierarchy**

This attribute is used to specify whether or not organization hierarchy must be maintained in Microsoft Active Directory. The value can be `True` or `False`.

If this attribute is set to `True`, then the reconciliation scheduled task first creates an organization hierarchy similar to the organization hierarchy for Microsoft Active Directory in Oracle Identity Manager. It then performs reconciliation of users into the appropriate organization. The value of the `XellerateOrg` attribute is ignored.

While using this option, you must ensure that duplicate organization names are not created. This is because Oracle Identity Manager does not allow duplicate organization names, even in separate organization trees.

You must specify a value for this attribute.

- **XellerateObject**

This attribute is used to specify the name of the Xellerate User resource object in Oracle Identity Manager on which trusted reconciliation is to be performed.

The value must be `Xellerate User`. If you do not want trusted reconciliation to be performed, then change the value to `false`.

You must specify a value for this attribute.

- **Object**

This attribute is used to specify the name of the AD User resource object in Oracle Identity Manager on which reconciliation is to be performed.

The value must be `AD User`. If you do not want trusted reconciliation to be performed, then change the value to `false`.

You must specify a value for this attribute.

- **Server**

This attribute specifies the IT resource for the Microsoft Active Directory server from which reconciliation is to be carried out.

You must specify a value for this attribute.

- **TransformLookupCode**

This attribute specifies the mapping between Microsoft Active Directory fields and the transformation to be applied to them. It is used if the values from external systems must be modified before they can be entered into Oracle Identity Manager. There is no restriction on custom modification. The following are examples of custom modifications:

- Append a number at the end of the user ID.
- Look up the field name from some external system, and set the value based on the field name.
- Set custom types, such as `Role` or `Xellerate Type` in Oracle Identity Manager, based on the value of a field in Microsoft Active Directory.

Because there can be a different transformation for every field reconciled from Microsoft Active Directory, the transform map gives a flexible way of specifying the field and the Java class that is used to transform it. The custom transformation classes must be compiled and kept in a JAR file in the `JavaTasks` directory.

See Also: [Appendix C](#)

- **UseTransformMapping**

This attribute is used to specify whether or not transform mappings accessed by using the `TransformLookupCode` attribute must be used. The value can be `True` or `False`.

You must specify a value for this attribute.

- **XellerateOrg**

This attribute specifies the name of the Oracle Identity Manager organization in which reconciled users are to be created. The name of this organization is used by default unless either the `MaintainHierarchy` attribute is set.

You must specify a value for this attribute.

- **MultiValueAttributes**

The value of this attribute is interpreted as a comma-separated list of the multivalued attributes in Microsoft Active Directory that must be imported in Oracle Identity Manager during reconciliation. When you use this value, remember that:

- The corresponding child table (used to store the value of the multivalued field) must exist on the form for the resource object against which reconciliation takes place.

-
- The name of the multivalued attribute field and its subfields must be the same as the name of the multivalued field.

You must specify a value for this attribute.

- **GroupObject**

This attribute is used to specify the name of the AD Group resource object in Oracle Identity Manager on which reconciliation is to be performed.

The value must be `AD Group`. If you do not want trusted reconciliation to be performed, then change the value to `false`.

You must specify a value for this attribute.

Code for a Sample Transformation Class

In this connector, a feature has been introduced for transformation of reconciled data according to your requirement. This has been described earlier in this guide along with the discussion on the `TransformLookupCode` attribute.

If you want to apply a certain transformation on a specific attribute, then you must incorporate the required logic in a Java class. Such a transformation class must implement the `com.thortech.xl.schedule.tasks.AttributeTransformer` interface and the `transform` method.

The following is one such sample class.

```
package com.thortech.xl.schedule.tasks;

public class AttributeTransformer implements AttributeTransformer {
    public AttributeTransformer(){
    }
    /**
     * @param inValue: This is the input string to be transformed.
     * @return String: This is the string that is returned.
     */
    public String transform(String inValue){
        return inValue;
    }
}
```

This sample class contains the method that must be implemented for reconciliation. The method defined in this class accepts, transforms, and returns a string value.

Index

A

- AD Group
 - provisioning, 1-4
 - reconciliation, 1-3
 - XML files for provisioning, 1-6
- AD lookup fields
 - reconciliation, 1-3
- AD Organization
 - provisioning, 1-4
 - XML files for provisioning, 1-6
- AD User
 - provisioning, 1-4
 - reconciliation, 1-3
 - XML files for provisioning, 1-6
- Adapter Factory form, 2-18
- Adapter Manager form, 2-18
- adapters, compiling, 2-17
- additional files, 2-1
- Administrative and User Console, 2-6
- attributes
 - lookup fields reconciliation scheduled task, 2-15
 - user reconciliation scheduled task, 2-15
- attributes mappings, A-1

C

- Certificate Services, 2-18
- changing input locale, 2-3
- clearing server cache, 2-3
- compiling adapters, 2-17
- configuring
 - connector for multiple installations of the target system, 2-21
 - Oracle Identity Manager server, 2-3
 - reconciliation, 2-12
 - SSL, 2-18
 - target system, 2-2
 - trusted source reconciliation, 2-13
- connector files and directories
 - copying, 2-2
 - description, 1-5
 - destination directories, 2-2
 - installation media directory, 1-5, 2-2
- connector release number, determining, 1-6
- connector testing, 3-1

- connector XML files
 - See* XML files
- creating scheduled tasks, 2-12

D

- defining
 - IT resources, 2-7
 - scheduled tasks, 2-12
- deployment requirements, 2-1
- Design Console, 2-14
- determining release number of connector, 1-6

E

- enabling logging, 2-4
- external code files, 2-1

F

- files
 - additional, 2-1
 - external code, 2-1
 - See also* XML files
- files and directories of the connector
 - See* connector files and directories
- functionality supported, 1-1
- functions available, 1-1

G

- globalization features, 1-2

I

- importing connector XML files, 2-6
- input locale, changing, 2-3
- issues, 4-1
- I-T provisioning test, 3-1
- IT resources
 - AD Server, 2-6, 2-7, 2-9, 2-15, 2-16
 - defining, 2-7
 - parameters, 2-7
 - types, AD Server, 2-6

L

- LDAP over SSL, 2-19
- LDAPS, 2-19
- limitations, 4-1
- logging enabling, 2-4
- lookup fields reconciliation scheduled task, 2-15

M

- mapping between attributes of target system and Oracle Identity Manager, A-1
- Microsoft Active Directory certificate
 - exporting, 2-19
 - importing, 2-20
 - setting up as trusted certificate, 2-19
- multilanguage support, 1-2

O

- Oracle Identity Manager Administrative and User Console, 2-6
- Oracle Identity Manager Design Console, 2-14
- Oracle Identity Manager Release 9.0.1, 2-16
- Oracle Identity Manager server, configuring, 2-3

P

- parameters of IT resources, 2-7
- password synchronization module, 2-22
- process tasks, 1-1
- provisioning
 - AD Group, 1-4
 - AD Organization, 1-4
 - AD User, 1-4
 - fields, 1-4
 - functions, 1-1
 - module, 1-4

R

- reconciliation
 - AD Group, 1-3
 - AD lookup fields, 1-3
 - AD User, 1-3
 - configuring, 2-12
 - customizing, 2-12
 - enabling in Oracle Identity Manager Release 9.0.1, 2-16
 - functions, 1-1
 - module, 1-3
 - scheduled task attributes, B-1
 - scheduled tasks, 2-14
- release number of connector, determining, 1-6
- requirements for deploying, 2-1

S

- scheduled tasks, 2-14
 - attributes, 2-14
 - defining, 2-12

- lookup fields reconciliation, 2-15
 - user reconciliation, 2-15
- server cache, clearing, 2-3
- SSL, configuring, 2-18
- supported
 - functionality, 1-1
 - languages, 1-2
 - releases of Oracle Identity Manager, 2-1
 - target system host platforms, 2-1
 - target systems, 2-1

T

- target system, multiple installations, 2-21
- target systems
 - configuration, 2-2
 - host platforms supported, 2-1
 - supported, 2-1
- testing the connector, 3-1
- transformation class, sample code, C-1
- troubleshooting, 3-1
- trusted source reconciliation, configuring, 2-13

U

- user attribute mappings, A-1
- user reconciliation scheduled task, 2-15

X

- XML files
 - description, 1-6
 - importing, 2-6
 - provisioning, 1-6