Oracle® Identity Manager

Connector Guide for Microsoft Active Directory

Release 9.0.2

B32157-01

September 2006

ORACLE®

Oracle Identity Manager Connector Guide for Microsoft Active Directory, Release 9.0.2

B32157-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

Contents

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 set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade 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 Connector Guide for BMC Remedy User Management*
- *Oracle Identity Manager Connector Guide for CA-ACF2 Advanced*
- *Oracle Identity Manager Connector Guide for CA-Top Secret Advanced*
- *Oracle Identity Manager Connector Guide for Database Application Table*s
- *Oracle Identity Manager Connector Guide for Database User Management*
- *Oracle Identity Manager Connector Guide for IBM RACF*
- *Oracle Identity Manager Connector Guide for IBM RACF Advanced*
- *Oracle Identity Manager Connector Guide for IBM Lotus Notes and Domino*
- *Oracle Identity Manager Connector Guide for Microsoft Active Directory*
- *Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide*
- *Oracle Identity Manager Connector Guide for Microsoft Exchange 2000 and 2003*
- *Oracle Identity Manager Connector Guide for Microsoft Exchange 5.5*
- *Oracle Identity Manager Connector Guide for Microsoft Windows 2000*
- *Oracle Identity Manager Connector Guide for Microsoft Windows NT 4.0*
- *Oracle Identity Manager Connector Guide for Novell eDirectory*
- *Oracle Identity Manager Connector Guide for Novell GroupWise*
- *Oracle Identity Manager Connector Guide for Oracle e-Business Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for Oracle e-Business User Management*
- *Oracle Identity Manager Connector Guide for Oracle Internet Directory*
- *Oracle Identity Manager Connector Guide for PeopleSoft Employee Reconciliation*

- *Oracle Identity Manager Connector Guide for PeopleSoft User Management*
- *Oracle Identity Manager Connector Guide for Siebel Enterprise Applications*
- *Oracle Identity Manager Connector Guide for RSA Authentication Manager*
- *Oracle Identity Manager Connector Guide for RSA ClearTrust*
- *Oracle Identity Manager Connector Guide for SAP CUA*
- *Oracle Identity Manager Connector Guide for SAP Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for SAP Enterprise Portal*
- *Oracle Identity Manager Connector Guide for SAP User Management*
- *Oracle Identity Manager Connector Guide for Sun Java System Directory*
- *Oracle Identity Manager Connector Guide for UNIX SSH*
- *Oracle Identity Manager Connector Guide for UNIX Telnet*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.2 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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in 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 9.0.2 of the Oracle Identity Manager connector pack.

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 the following software updates implemented in this release of the connector.

Incorporation of Multilanguage Support

In addition to English, this release of the connector supports the French and Japanese languages. The following are documentation updates pertaining to the incorporation of this feature:

- The installation media directory includes resource bundle files for the languages supported by the connector. These resource bundle files are described in the "Files and Directories That Comprise the Connector" section on page 1-4.

  Some other changes have also been made in this section.

- The "Step 3: Copying the Connector Files and External Code" section on page 2-2 specifies the destination directory into which you must copy the resource bundle files during the deployment procedure.

- The "Step 4: Configuring the Oracle Identity Manager Server" section on page 2-2 describes the procedure to change to the required input locale and to clear content related to connector resource bundles from the server cache.

- Two new IT resource parameters have been added to carry country code and language code information to the target system. These parameters are described in the "Defining IT Resources" section on page 2-5.

- Chapter 4, "Known Issues" discusses two new issues related to the use of non-English locales.

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.

Changes in the Known Issues List

The following issues have been added to the Known Issues list in Chapter 4:

- An issue pertaining to the entry of mandatory user field values.
- An error may be thrown during the password change operation on a Microsoft Windows 2003 server on which service pack 1 has not been installed.
- You can provision an organization through Oracle Identity Manager on Microsoft Active Directory. However, you cannot change the name this organization through Oracle Identity Manager.

Changes in Supported Functionality

The Change Organization Name function has been removed from the "Supported Functionality" section on page 1-1.

Changes Related to the User's Name Attribute in Microsoft Active Directory

The following changes have been made in the display and storage of the user's name:

- The display name for a user shows the first name, middle name, and last name.
- After provisioning, in addition to the first name and last name, the middle name initials are displayed.
- In the Japanese locale, the display name for a user shows the last name first, followed by the middle name, and then the first name.
- The name that you provide as the logon name is used as the account name. The account name is not dependent on the first name or full name.

Documentation-Specific Updates

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

- Oracle Identity Manager uses a Microsoft Active Directory user account to connect to and exchange data with Microsoft Active Directory. The "Step 1: Verifying Deployment Requirements" section on page 2-1 provides information about the minimum rights that must be assigned to this user account.
- In the "Step 3: Copying the Connector Files and External Code" section on page 2-2:
  - Changes have been made in the destination directory specified for some of the files.
  - Instructions to change the values specified in the `install.bat` (and `install.sh`) file so that they match the Oracle Identity Manager operating environment parameters have been added.
- In the following sections, instructions to copy the connector JAR files and adapter files to all the nodes of a clustered environment have been added:

  - Step 3: Copying the Connector Files and External Code on page 2-2
  - Step 4: Configuring the Oracle Identity Manager Server on page 2-2
  - Step 7: Compiling Adapters on page 2-13

  In the "Importing the Microsoft Active Directory Certificate" section on page 2-15, instructions to perform the procedure on all the nodes of a cluster have been added.

- In the "Step 5: Importing the Connector XML Files" section on page 2-4, the `XliActiveDirectoryScheduleTask_DM.xml` file has been added to the list of XML files to be imported. The fact that importing this XML file results in the creation of reconciliation scheduled tasks has been mentioned in the "Step 6: Configuring Reconciliation" section on page 2-7.
- Detailed instructions on configuring reconciliation have been moved from Appendix A to the "Step 6: Configuring Reconciliation" section on page 2-7. The revised Appendix A describes only the attributes of the reconciliation scheduled task.

  In addition, the acceptable values of some of the reconciliation scheduled task attributes have been changed from `Yes` and `No` to `True` and `False`.
- Instructions and pointers to information about configuring trusted source reconciliation have been moved to the "Configuring Trusted Source Reconciliation" section on page 2-9.
- In the "Lookup Fields Reconciliation Scheduled Task" section on page 2-10, the default value of the `LookupCodeName` attribute is `Lookup.ADReconliation.GroupLookup`. In this default value, the word "reconciliation" has been misspelled. This will be fixed in the next release.
- Instructions to enable reconciliation in Oracle Identity Manager release 9.0.1 have been added in the "Enabling Reconciliation in Oracle Identity Manager Release 9.0.1" section on page 2-12.
- While performing the procedure described in the "Installing Certificate Services" section on page 2-14, you must first insert the operating system installation media into the CD-ROM or DVD drive. This step has been added at the start of the procedure.
- Instructions to use Oracle Identity Manager for linking multiple installations of Microsoft Active Directory are given in the "Configuring the Connector for Multiple Installations of the Target System" section on page 2-17.

1

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

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 Xellerate 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

In addition to English, this release of the connector supports the following languages:

- French
- Japanese

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.ADReconliation.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 in order 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 in order 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
- 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 compressed in the following ZIP file on the installation media:

```
Directory Servers\Microsoft Active Directory\Microsoft Active Directory Rev
4.5.0.zip
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
xml\xliADOrganizationObject_DM.xml	This XML file contains definitions for the connector components related to AD Organization provisioning. These components include: ■ 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\xliADGroupObject_DM.xml	This XML file contains definitions for the connector components related to AD Group provisioning. These components include: ■ 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\xliADUserObject_DM.xml	This XML file contains definitions for the connector components related to AD User provisioning. These components include: ■ 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
xml\xliActiveDirectoryScheduleTask_DM.xml	This XML file contains definitions for the Oracle Identity Manager components of the connector related to the reconciliation module.
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.
ext\ldapsdk-4.1.jar	This external JAR file contains the JNDI LDAP booster package that is required for the connector.
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.
Files in the resources directory	Each of these files contains locale-specific information that is used by the connector.

File in the Installation Media Directory	Description
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.
docs\B32157_01.pdf	This guide, which provides instructions to deploy the connector.

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 the connector:

1. Extract the contents of the xliActiveDirectory.jar file. This file is in the lib directory inside the installation media directory.
2. Open the manifest.mf file in a text editor, which 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.

2

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

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: ■ 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.jar`)
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 2-5.

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 2-5 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 ZIP file on the installation media:

`Directory Servers\Microsoft Active Directory\Microsoft Active Directory Rev 4.5.0.zip`

Refer to the "Files and Directories That Comprise the Connector" section on page 1-4 for more information about these files.

File in the Installation Media Directory	Destination Directory
Files in the `xml` directory	*OIM_home*`\xellerate\XLIntegrations\Active Directory\xml`
`lib\xliActiveDirectory.jar`	*OIM_home*`\xellerate\JavaTasks` *OIM_home*`\xellerate\ScheduleTask`
`lib\xliADRecon.jar`	*OIM_home*`\xellerate\JavaTasks` *OIM_home*`\xellerate\ScheduleTask`
`ext\ldapsdk-4.1.jar`	*OIM_home*`\xellerate\ThirdParty`
Files in the `scripts` directory	*OIM_home*`\xellerate\scripts` After you copy the `install.bat` (or `install.sh`) file, use a text editor to open the file and specify the actual location of the JDK directory in the file.
Files in the `resources` directory	*OIM_home*`\xellerate\connectorResources`
Directories and files in the `test` directory	*OIM_home*`\xellerate\test`
`docs\B32157_01.pdf`	*OIM_home*`\xellerate\docs\ActiveDirectory`

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

Changing to the Required Input Locale

Changing to the required input locale 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 file in the *OIM_home*\xellerate\connectorResources directory or make a change in an existing resource bundle file, 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.

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 2-5 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 need to 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 2-7.

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. Value: `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`

Parameter	Description
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
Use SSL	Specifies whether or not to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory Default value: false
SSL Port Number	Port at which SSL is running on the Microsoft Active Directory server Default value: 636
AtMap ADUser	Attribute map name for the Microsoft Active Directory user Default value: AtMap.AD
AtMap Group	Attribute map name for the Microsoft Active Directory group Default value: AtMap.ADGroup
Target Locale: Country	Country code Default value: US **Note:** You must specify the value in uppercase.
Target Locale: Language	Language code Default value: en **Note:** You must specify the value in lowercase.

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	Fully qualified domain name corresponding to the administrator Format: *ADMIN_LOGIN@DOMAIN* Sample value: administrator@adomain.com
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	Usually, 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,dc=com

Parameter	Description
Server Address	Host name or IP address of the target Microsoft Windows 2000 computer on which Microsoft Active Directory is installed Sample value: w2003host
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
Use SSL	Specifies whether or not to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory Default value: false
SSL Port Number	Port at which SSL is running on the Microsoft Active Directory server Default value: 636
AtMap ADUser	Attribute map name for the Microsoft Active Directory user Default value: AtMap.AD
AtMap Group	Attribute map name for the Microsoft Active Directory group Default value: AtMap.ADGroup
Country	Country code Default value: US **Note:** You must specify the value in uppercase.
Language	Language code Default value: en **Note:** You must specify the value in lowercase.

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 2-4.

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
   - 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 2-10 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 2-12.

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 objectGUIDs	Lookup.ADReconliation.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 A 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 It 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
Object	Name of the AD User resource object in Oracle Identity Manager on which reconciliation is performed If you want AD User reconciliation to be performed, then change the value to AD User. Otherwise, change the value to False. You must specify a value for this attribute.	AD User

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

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 Process Definition form for the AD User. This form is in the Process Management folder.
2. Click the **Reconciliation Field Mappings** tab.
3. 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. Then, restart each node.

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.

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 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.
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	*JAVA_HOME*\jre\lib\security\cacerts
BEA WebLogic	*BEA_HOME*\java\jre\lib\security\cacerts
IBM WebSphere	*WS_HOME*\java\jre\lib\security\cacerts *WS_HOME*\etc\DummyServerTrustFile.jks

   Note: For IBM WebSphere, you must also copy the jnet.jar, jsse.jar, and jcert.jar files to the *WS_HOME*\java\jre\lib\ext directory. You can download these JAR files from the Sun Web site at

   http://java.sun.com/

   - *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 a number that is not in use in the file.

6. Restart the Oracle Identity Manager server and the application server.

Note: The user password cannot be set unless 128-bit SSL is being used. In addition, the computer on which Microsoft Active Directory is installed must have Microsoft Windows 2000 Service Pack 2 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 2-7 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 the trusted source.

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.

3

Testing the Connector

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.

A test from the connector to the target resource is known as an I-T provisioning testing.

Note: In earlier releases of this guide, the connector was referred to as the *integration.*

I-T Provisioning Test

To perform an I-T provisioning test:

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 as part of the I-T 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.

Enabling Logging

Logging can be enabled by making an appropriate entry in the `log.properties` file at the following location:

`OIM_home``\xellerate\test\config`

The following are the different log levels for which logging can be enabled:

- `DEBUG`
- `INFO`

- WARN
- ERROR
- FATAL

Note: The check for these values is case-sensitive. You must specify a value in uppercase only.

For example, if the log level for DEBUG is to be enabled, then you must add the following entry in the log.properties file:

```
log4j.logger.ADAPTERS.ACTIVEDIRECTORY=DEBUG
```

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.mspx?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.

Therefore, if you want to configure this setting correctly for a Microsoft Active Directory user, then perform the following steps:

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.

- If the `Use SSL` attribute of the IT resource is set to `false` while provisioning the Microsoft Active Directory user, then 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.**

- 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 2-8 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 locale 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

- 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/`

- 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.

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

- When provisioning users in Japanese, given names (first names) are listed before family names (last names) instead family names being listed before given names.

A

Attributes of the Reconciliation Scheduled Task

The following are the attributes of the reconciliation scheduled task:

- **DeleteRecon**

  This attribute is used to enable Delete reconciliation. 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 B

- **`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.

B

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

M

O

P

R

S

T

U

V

X