Oracle® Identity Manager

Connector Guide for Microsoft Active Directory

Release 9.0.4

E10158-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for Microsoft Active Directory, Release 9.0.4

E10158-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

Contents

3 Configuring the Connector

4 Testing and Troubleshooting

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 Connector Pack Release 9.0.4 documentation library, 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 software and documentation for the Microsoft Active Directory connector in release 9.0.4 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3.1 release of this guide for information about updates that were new for the 9.0.3.1 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.

Configuring the Reconciliation of User Account Status

If you want to configure the reconciliation of user account status from Microsoft Active Directory to Oracle Identity Manager, then perform the procedure described in the "Configuring the Connector for Oracle Identity Manager Release 9.0.1.3" section on page 3-11.

Changes in the Connector Files on the Installation Media

The "Files and Directories That Comprise the Connector" section on page 1-5 reflects the changes made to the connector files bundled on the installation media.

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-5, you can configure the generation of log information that is specific to the target system.

Partial Reconciliation

The `CustomizedReconQuery` parameter has been added to the IT resource definition. You can use this parameter to customize the query that the reconciliation module uses to determine the records to be retrieved from the target system. The `CustomizedReconQuery` parameter is explained in the following sections:

- Defining IT Resources on page 2-8
- Partial Reconciliation on page 3-2

Batched Reconciliation

In this release of the connector, user reconciliation schduled task is added with attributes such as `StartRecord`, `BatchSize`, and `NumberofBatches`. By specifying values for these attributes, you can reconcile users in various batches. These attributes are discussed in the following sections:

- User Reconciliation Scheduled Task on page 3-5
- Batched Reconciliation on page 3-4

Documentation-Specific Updates

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

- Instructions in the "Determining the Release Number of the Connector" section on page 1-6 have been revised.
- The "Adding Custom Attributes for Provisioning" section on page 3-10 describes the procedure to add add custom attributes for provisioning.
- Some of the content from the Chapter 2 of the earlier release of this guide has been moved to Chapter 3.

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:

- Reconciliation Module
- Provisioning Module
- Supported Functionality
- Multilanguage Support
- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector

> **Note:** At some places in this guide, Microsoft Active Directory has been referred to as the *target system.*

Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager additions of and modifications to user accounts on the target system. It is an automated process initiated by a scheduled task that you configure.

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

- Lookup Fields Reconciliation
- Group Reconciliation

- User Reconciliation

Lookup Fields Reconciliation

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

- sAMAccountName
- objectGUID

Group Reconciliation

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

- sAMAccountName
- objectGUID
- Organization Name
- instanceType
- cn

User Reconciliation

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

Provisioning involves creating or modifying a user's access rights on the target system through Oracle Identity Manager. You use the Administrative and User Console to perform provisioning operations.

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about provisioning

For this target system, provisioning is divided into the following types:

- Organization Provisioning
- Group Provisioning
- User Provisioning

Organization Provisioning

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.

Group Provisioning

The following fields are provisioned:

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

User Provisioning

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

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
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

The connector supports the following languages:

- Chinese Simplified

- Chinese Traditional
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

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

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
`lib/xliActiveDirectory.jar`	This JAR file contains the class files required for reconciliation and provisioning.
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.

File in the Installation Media Directory	Description
xml/xliADResourceObject.xml	This XML file contains definitions for the connector components related to reconciliation and provisioning. These components include: ■ All resource objects for reconciliation and provisioning ■ IT resource types ■ Custom process forms ■ Process task and adapters (along with their mappings) ■ Login resource objects ■ Provisioning process ■ Pre-populate rules
xml/xliADXLResourceObject.xml	This XML file contains the configuration for the objects, such as Xellerate User and Xellerate Organization, which are specific to trusted sources. You must import this file only if you plan to use the connector in trusted source reconciliation mode.

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 Files" section on page 2-3 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

You can use any one of the following methods to determine the release number of the connector.

Before Deployment

To determine the release number of a connector:

1. Extract the contents of the `xliActiveDirectory.jar` file. This file is in the following directory on the installation media:

   ```
   Directory Servers/Microsoft Active Directory/Microsoft Active Directory
   Base/lib
   ```

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.

Note: If you maintain a copy of the `xliActiveDirectory.jar` file after deployment, you can use this method to determine the release number of the connector at any stage. After you deploy the connector, it is recommended that you use the "After Deployment" method, which is described in the following section.

After Deployment

To determine the release number of a connector that has already been deployed:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

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 Files
- Step 4: Configuring the Oracle Identity Manager Server
- Step 5: Importing the Connector XML Files
- Step 6: Configuring SSL

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, 2003)
Target system host platforms	The target system host platform can be any one of the following: ■ Microsoft Windows 2000 with Service Pack 4 ■ 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 2-8. If the specified user account is not used, then an authentication error message is displayed.

Step 2: Configuring the Target System

Configuring the target system involves performing the following procedures:

- Ensuring That the Parent Organization Exists in Microsoft Active Directory
- Enabling or Disabling Password Policies on Microsoft Active Directory

Ensuring That the Parent Organization Exists in Microsoft Active Directory

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 IT resource definition. Refer to the "Defining IT Resources" section on page 2-8 for more information about this parameter.

Enabling or Disabling Password Policies on Microsoft Active Directory

On Microsoft Active Directory, the "Passwords must meet complexity requirements" policy setting is used to enable or disable password policies. You can choose whether or not you want to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory.

> **Note:** The procedure to configure SSL is discussed later in this guide.

The procedure that you must perform depends on whether or not you configure SSL and enforce password policies.

If you do not configure SSL and try to provision a Microsoft Active Directory user through Oracle Identity Manager, then the user's password cannot be updated by using Oracle Identity Manager. Therefore, if the communication is not secured by SSL, then you must disable any existing password policies in Microsoft Active Directory. This is achieved by disabling the "Passwords must meet complexity requirements" policy setting.

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

To enable or disable the "Passwords must meet complexity requirements" policy setting:

1. On the Microsoft Windows computer hosting the Active Directory domain controller on which you are installing the password synchronization module, start the Domain Security Policy application.

   To do this, on the Microsoft Windows computer, click the **Start** menu, **Programs**, **Administrative Tools**, and **Domain Security Policy**.

2. If you are using Microsoft Active Directory 2003, then directly proceed to the next step.

   If you are using Microsoft Active Directory 2000, then select **Window Settings** on the left pane of the Domain Security Policy application window and then proceed to the next step.

3. Select **Security Settings**, expand **Account Policies**, and then click **Password Policy**.

4. Double-click **Passwords must meet complexity requirements**.

5. In the Password Must Meet Complexity Requirements Properties dialog box, select **Define this policy setting** and then select:

   - **Enabled**, if you want to enable password policies

- **Disable**, if you do not want to enable password policies

6. Click **OK**.

Step 3: Copying the Connector Files and External Code Files

The connector 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
`lib/xliActiveDirectory.jar`	*`OIM_home`*`/xellerate/JavaTasks`
Files in the `resources` directory	*`OIM_home`*`/xellerate/connectorResources`
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.
Directories and files in the `test` directory	*`OIM_home`*`/xellerate/test`
Files in the `xml` directory	*`OIM_home`*`/xellerate/XLIntegrations/Active Directory/xml`

To copy the `ldapbp.jar` and `ldapsdk-4.1.jar` files into the required directory:

1. Log on the Sun Web site at

   `http://java.sun.com/products/jndi/downloads/index.html`

2. Click the **Download JNDI 1.2.1 & More** button.

3. From the table on the page that is displayed, select and download the file containing the `ldapbp.jar` and `ldapsdk-4.1.jar` files.

4. Copy the `ldapbp.jar` and `ldapsdk-4.1.jar` files into the *`OIM_home`*`/xellerate/JavaTasks` directory on the Oracle Identity Manager server.

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

> **Note:** In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.

Configuring the Oracle Identity Manager server involves performing 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.

You may require the assistance of the system administrator to change to the required input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 3: Copying the Connector Files and External Code Files" section on page 2-3, you copy files from the `resources` directory on the installation media into the *`OIM_home`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the *`OIM_home`*`/xellerate/bin` directory.

   > **Note:** You must perform Step 1 before you perform Step 2. If you run the command described in Step 2 as follows, then an exception is thrown:
   >
   > *`OIM_home`*`/xellerate/bin/`*`batch_file_name`*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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
```

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:

- **BEA WebLogic**

  To enable logging:

  1. Add the following lines in the *`OIM_home`*`/xellerate/config/log.properties` file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.ACTIVEDIRECTORY=log_level
     ```

  2. In these lines, replace *`log_level`* with the log level that you want to set.

     For example:

```
log4j.logger.XELLERATE=INFO
log4j.logger.XL_INTG.ACTIVEDIRECTORY=INFO
```

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

WebLogic_home/user_projects/domains/*domain_name*/*server_name*/*server_name*.log

- **IBM WebSphere**

  To enable logging:

  1. Add the following lines in the *OIM_home*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.ACTIVEDIRECTORY=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.ACTIVEDIRECTORY=INFO
     ```

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

  WebSphere_home/AppServer/logs/*server_name*/startServer.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBoss_home*/server/default/conf/log4j.xml file, locate or add the following lines:

     ```
     <category name="XELLERATE">
        <priority value="log_level"/>
     </category>

     <category name="XL_INTG.ACTIVEDIRECTORY">
        <priority value="log_level"/>
     </category>
     ```

  2. In the second XML code line of each set, replace *log_level* with the log level that you want to set. For example:

     ```
     <category name="XELLERATE">
        <priority value="INFO"/>
     </category>

     <category name="XL_INTG.ACTIVEDIRECTORY">
        <priority value="INFO"/>
     </category>
     ```

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

  JBoss_home/server/default/log/server.log

- **OC4J**

  To enable logging:

  1. Add the following lines in the *OIM_home*/xellerate/config/log.properties file:

```
log4j.logger.XELLERATE=log_level
log4j.logger.XL_INTG.ACTIVEDIRECTORY=log_level
```

2. In these lines, replace `log_level` with the log level that you want to set.

   For example:

   ```
   log4j.logger.XELLERATE=INFO
   log4j.logger.XL_INTG.ACTIVEDIRECTORY=INFO
   ```

After you enable logging, the 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

As mentioned in the "Files and Directories That Comprise the Connector" section on page 1-5, the connector XML files contains definitions of the components of the connector. By importing the connector XML files, you create these components in Oracle Identity Manager.

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 `xliADResourceObject.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 2-8 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. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.

12. Click **Import**. The connector file is imported into Oracle Identity Manager.

After you import the connector XML file, proceed to the "Step 6: Configuring SSL" section on page 2-13.

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`	Specifies whether or not to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory Default value: `true` **See Also:** The Known Issues list in Chapter 5 for information about a limitation arising from setting this parameter to `false`. **Note:** It is recommended that you enable SSL to secure communication with the target system.
`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.
`CustomizedReconQuery`	Specify the LDAP query that you want to use to customize reconciliation. The reconciliation engine uses this LDAP query to filter the records that must be fetched from the target system. Sample value: `memberOf=cn=AcmeAdmin,cn=Users,dc=GLOBAL,dc=com` **Note:** You can use this value in conjunction with the `GroupObject` attribute defined in the "User Reconciliation Scheduled Task" section on page 3-5.
`ADDisableAttr Lookup Definition`	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. **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. Refer to *Oracle Identity Manager Design Console Guide* for information about creating the lookup definition.

Parameter	Description
Use Disable Attr	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. **Note:** You can use this parameter only if you specify a value for the ADDisableAttr Lookup Definition parameter.
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.

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

Parameter	Description
`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`
`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: `true` **See Also:** The Known Issues list in Chapter 5 for information about a limitation arising from setting this parameter to `false`. **Note:** It is recommended that you enable SSL to secure communication with the target system.
`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.

Parameter	Description
CustomizedReconQuery	Specify the LDAP query that you want to use to customize reconciliation. The reconciliation engine uses this LDAP query to filter the records that must be fetched from the target system. Sample value: memberOf=cn=AcmeAdmin,cn=Users,dc=GLOBAL,dc=com **Note:** You can use this value in conjunction with the GroupObject attribute defined in the "User Reconciliation Scheduled Task" section on page 3-5.
ADDisableAttr Lookup Definition	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. **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. Refer to *Oracle Identity Manager Design Console Guide* for information about creating the lookup definition.
Use Disable Attr	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. **Note:** You can use this parameter only if you specify a value for the ADDisableAttr Lookup Definition parameter.
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.

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

Step 6: Configuring SSL

> **Note:** Although this is an optional step of the deployment procedure, it is recommended that you configure SSL communication between Microsoft Active Directory and Oracle Identity Manager.

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 `jcert.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	`JBoss_home/jre/lib/security/cacerts`
BEA WebLogic	`BEA_home/java/jre/lib/security/cacerts`

IBM WebSphere	For a nonclustered configuration of IBM WebSphere, you must import the files into the following certificate stores:
	`WS_home/java/jre/lib/security/cacerts`
	For a clustered configuration of IBM WebSphere, you must import the files into the following certificate stores on each node of the cluster:
	`WS_home/java/jre/lib/security/cacerts`
	`WS_home/etc/DummyServerTrustFile.jks`

Oracle Containers for J2EE (OC4J)	`OC4J_home/jdk/jre/lib/security/cacerts`

- *`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.

3

Configuring the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

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

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Oracle Identity Manager Release 9.0.1.3
- Configuring the Connector for Multiple Installations of the Target System
- Configuring the Connector and Password Synchronization Module

Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager additions of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Configuring Trusted Source Reconciliation
- Partial Reconciliation
- Batched Reconciliation
- Configuring the Reconciliation Scheduled Tasks
- Enabling Reconciliation in Oracle Identity Manager Release 9.0.1
- Adding Custom Attributes for Reconciliation

Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

> **Note:** You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

To import the XML file for trusted source reconciliation:

> **Note:** Only one target system can be designated as a trusted source. If you import the `xliADXLResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

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

After you import the XML file for trusted source reconciliation, you must set the value of the `TrustedSource` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-4.

Partial Reconciliation

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

For this connector, you create a filter by specifying values for the `CustomizedReconQuery` IT resource parameter while performing the procedure described in the "Defining IT Resources" section on page 2-8.

The following table lists the Microsoft Active Directory attributes, and the corresponding Oracle Identity Manager attributes, that you can use to build the query condition. You specify this query condition as the value of the `CustomizedReconQuery` parameter.

Oracle Identity Manager Attribute	Microsoft Active Directory Attribute
User ID	sAMAccountName
First Name	givenName
Last Name	sn

Oracle Identity Manager Attribute	Microsoft Active Directory Attribute
Middle Name	initials
Full Name	displayName
Groups	memberOf

The following are sample query conditions:

- `givenName=John&sn=Doe`

  With this query condition, records of users whose first name is John and last name is Doe are reconciled.

- `givenName=John&sn=Doe|initials=JD`

  With this query condition, records of users who meet either of the following conditions are reconciled:

  - The user's first name is `John` or last name is `Doe`.
  - The user's initials are `JD`.

If you do not specify values for the `CustomizedReconQuery` parameter, then all the records in the target system are compared with existing Oracle Identity Manager records during reconciliation.

The following are guidelines to be followed while specifying a value for the `CustomizedReconQuery` parameter:

- For the Microsoft Active Directory attributes, you must use the same case (uppercase or lowercase) as given in the table shown earlier in this section. This is because the attribute names are case-sensitive.

- You must not include unnecessary blank spaces between operators and values in the query condition.

  A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

  ```
  givenname=John&sn=Doe
  ```

  ```
  givenname= John&sn= Doe
  ```

  In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

  > **Note:** An exception is thrown if you include special characters other than the equal sign (=), ampersand (&), and vertical bar (|).

You specify a value for the `CustomizedReconQuery` parameter while performing the procedure described in the "Defining IT Resources" section on page 2-8.

Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- `StartRecord`: Use this attribute to specify the record number from which batched reconciliation must begin.
- `BatchSize`: Use this attribute to specify the number of records that must be included in each batch.
- `NumberOfBatches`: Use this attribute to specify the total number of batches that must be reconciled. If you do not want to use batched reconciliation, specify `All Available` as the value of this attribute.

> **Note:** If you specify `All Available` as the value of this attribute, then the values of the `StartRecord` and `BatchSize` attributes are ignored.

You specify values for these attributes by following the instructions described in the "User Reconciliation Scheduled Task" section on page 3-5.

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then refer to the log file for information about the batch at which reconciliation has failed.

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 5: Importing the Connector XML Files" section on page 2-7, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure these 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 3-5 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 create the second scheduled task.

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

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

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 source reconciliation is to be performed If you want trusted source 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
Server	Name of the IT resource representing 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 This attribute 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

Attribute	Description	Default/Sample Value
XellerateOrg	Oracle Identity Manager organization in which reconciled users are to be created You must specify a value for this attribute.	Xellerate Users
MultiValueAttributes	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
StartRecord	Specifies the start record for batching process The default value is 0. This attribute is also discussed in the "Batched Reconciliation" section on page 3-4.	1
BatchSize	Specifies how many records must be there in a batch The default value is 0. This attribute is also discussed in the "Batched Reconciliation" section on page 3-4.	3
NumberOfBatches	Specifies the number of batches that must be reconciled If you specify the default value (All Available), then batched reconciliation is not performed. This attribute is also discussed in the "Batched Reconciliation" section on page 3-4.	Default value: All Available (for reconciling all the users) Sample value: 50

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**.

Adding Custom Attributes for Reconciliation

> **Note:** This section describes an optional procedure. You need not perform this procedure if you do not want to add new attributes for provisioning.

By default, the attributes listed in the "Reconciliation Module" section on page 1-1 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation.

To add a custom attribute for reconciliation:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

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 (This is a mandatory field; it must be present in the field map)
   - distinguishedName
   - initials
   - displayName
   - Employee Type
   - userAccountControl
   - User Type

Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. Refer to the "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector.

> **Note:** You must perform the procedure described in this section if you want to use the provisioning features of the connector.

Configuring provisioning involves compiling the adapters that are used to implement provisioning functions.

> **See Also:** The "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector

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 they can be used in provisioning operations.

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.

If you want to compile one adapter at a time, then use the Adapter Factory form.

> **See Also:** *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms

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.

Adding Custom Attributes for Provisioning

> **Note:** This section describes an optional procedure. You need not perform this procedure if you do not want to add new attributes for provisioning.

By default, the attributes listed in the "Provisioning Module" section on page 1-2 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a custom attribute for provisioning:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Add the attribute as a field in the `UD_ADUSER` or `UD_ADGRP` process form.
2. Add the attribute in the `AtMap.AD` or `AtMap.ADGroup` lookup definition.

Configuring the Connector for Oracle Identity Manager Release 9.0.1.3

> **Note:** You must perform this procedure only if you are using Oracle Identity Manager release 9.0.1.3.

In Oracle Identity Manager release 9.0.1.3, user accounts that are disabled or enabled are not reconciled correctly into Oracle Identity Manager during nontrusted (target resource) reconciliation. If you are using this release of Oracle Identity Manager, then you must perform the following procedure to resolve this problem:

1. Log in to the Design Console.
2. Create the `userAccountControl` reconciliation field in the `AD User` resource object as follows:
   a. Expand the **Resource Management** folder.
   b. Open the **Resource Objects** form.
   c. Click the Search button.
   d. From the list of resource objects that is displayed, double-click **AD User**.
   e. On the Object Reconciliation tab, select the **Reconciliation Fields** tab.
   f. On the Reconciliation Fields tab, click **Add Field** and then enter the following values:
      – **Field Name**: Enter **userAccountControl**.
      – **Field Type**: Select **String**.
      – **Required**: Select this check box.
   g. Save the changes.
3. Map the `userAccountControl` reconciliation field to the `OIM_OBJECT_STATUS` field as follows:
   a. Expand the **Process Management** folder.
   b. Open the **Process Definition** form.
   c. Click the Search button.
   d. From the list of process definitions that is displayed, double-click the **AD User** process definition.
   e. On the Reconciliation Field Mappings tab, double-click **userAccountControl** and then enter the following values:

- **Field Name**: Select **userAccountControl**.
- **Field Type**: Select **String**.
- **Process Data Field**: Enter **OIM_OBJECT_STATUS**.

f. Save the changes.

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.

You may want to configure the connector for multiple installations of Microsoft Active Directory. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Acme Multinational Inc. have their own installations of Microsoft Active Directory. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of Microsoft Active Directory.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of Microsoft Active Directory.

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 "Configuring Reconciliation" section on page 3-1 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.

See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

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 password synchronization 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 release 9.0.3 of the connector and password synchronization module.

- Creating a Custom Attribute in Microsoft Active Directory to Track Password Changes
- Creating a Custom Attribute in Oracle Identity Manager
- Specifiying Values for IT Resource Parameters
- Sequence of Events That Occur During a Password Change

Creating a Custom Attribute in Microsoft Active Directory to Track Password Changes

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**.

Specifiying Values for IT Resource Parameters

While performing the procedure described in the "Defining IT Resources" section on page 2-8, 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 action 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 action 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*.

4

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 you set the `Use SSL` IT resource parameter to `false.` When you provision a Microsoft Active Directory user through Oracle Identity Manager, the password cannot be 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.

Refer to the "Enabling or Disabling Password Policies on Microsoft Active Directory" section on page 2-2 for information about the procedure that you must perform to fix this limitation.

This problem is also mentioned in the Known Issues list in Chapter 5.

5 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.

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 you set the `Use SSL` IT resource parameter to `false.` When you provision a Microsoft Active Directory user through Oracle Identity Manager, the password cannot 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.

  Refer to the "Enabling or Disabling Password Policies on Microsoft Active Directory" section on page 2-2 for information about the procedure that you must perform to fix this limitation.

  This limitation is also described in the "Troubleshooting" section on page 4-1.

- 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 "Adding Custom Attributes for Reconciliation" section on page 3-8 for information about using the `Lookup.ADReconciliation.FieldMap` field map to suppress such fields.

- The `MaintainHeirarchy` option with a value `true` reconciles organizational 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.

A

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

B

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 source reconciliation, the users that are reconciled using the Delete Reconciliation function are marked as deleted by Oracle Identity Manager. In the case of nontrusted source 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 5.

- **`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 source reconciliation is to be performed.

  The value must be `Xellerate User`. If you do not want trusted source 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 source 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 `Employee Type` or `User 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, "Code for a Sample Transformation Class"

- **`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 source reconciliation to be performed, then change the value to `false.`

  You must specify a value for this attribute.

C

Code for a Sample Transformation Class

When you use this connector, you can transform reconciled data according to your requirements. This feature has been described earlier in Appendix B, 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