Oracle® Identity Manager

Connector Guide for Microsoft Active Directory

Release 9.0.4

E10429-13

July 2014

ORACLE®

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

E10429-13

Primary Author: Gowri.G.R

Contributing Authors: Debapriya Datta, Alankrita Prakash, Deena Purushothaman

Contents

3 Configuring the Connector

4 Testing and Troubleshooting

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Microsoft Active Directory.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://www.oracle.com/technology/documentation/oim.html

Documentation Updates

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

http://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 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 9.0.4.17.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following sections discuss software updates:

Software Updates in Release 9.0.4.1_6742854

The following are software updates in release 9.0.4.1_6742854:

- Support for Lookup Field Reconciliation of Security Groups and Organizations
- Support for New Provisioning Operations
- Changes in the IT Resource Definition
- Separate Scheduled Tasks for Trusted Source and Target Resource Reconciliation
- Change in the Requirement for External Code Files
- Support for the Application of Native LDAP Queries During Reconciliation
- Support for Mapping New Attributes for Reconciliation and Provisioning

Support for Lookup Field Reconciliation of Security Groups and Organizations

The functionality of the scheduled task has been extended to cover lookup field reconciliation of security groups and organizations.

See "Lookup Fields Reconciliation" for more information. See "Lookup Fields Reconciliation Scheduled Task" for information about the scheduled tasks that automate reconciliation of these lookup fields.

Support for New Provisioning Operations

The connector now supports the following provisioning operations (functions):

- Lock User
- Unlock User
- Update First Name
- Update Last Name
- Move Group

See "Supported Functionality" for information about these functions.

Changes in the IT Resource Definition

Parameters to track the time at which reconciliation runs end have been added to the IT resource. In earlier releases, parameters that used to accept `true` and `false` now accept `yes` and `no`.

The `isOrgLookupDN` parameter has been added to the IT resource definition. You use this parameter to specify whether DN or relative DN values must be stored in the `Lookup.ADReconciliation.Organization` lookup definition during lookup reconciliation.

See "Defining IT Resources" for more information.

Separate Scheduled Tasks for Trusted Source and Target Resource Reconciliation

These scheduled tasks are discussed in the "User Reconciliation Scheduled Task" section.

Change in the Requirement for External Code Files

From this release onward, the `ldapbp.jar` file is the only external code file required for connector operations.

See "Copying the Connector Files and External Code Files" for information about downloading and using this file.

Support for the Application of Native LDAP Queries During Reconciliation

In the earlier release, you specify the query condition for limited reconciliation by using operators that are not native to the target system. You can now specify the query condition using either non-native or native operators. You use the `CustomizedReconQuery` and `isNativeQuery` attributes of the user reconciliation scheduled task for this purpose.

See "Partial Reconciliation" for more information.

Support for Mapping New Attributes for Reconciliation and Provisioning

You can map new target system attributes with Oracle Identity Manager attributes for reconciliation and provisioning. See the following sections for more information:

- Adding Custom Attributes for Reconciliation
- Adding Custom Attributes for Provisioning

Software Updates in Releases 9.0.4.2 Through 9.0.4.4

There are no software updates in releases 9.0.4.2 through 9.0.4.4.

Software Updates in Release 9.0.4.5

The following are issues resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
6989471	An attempt by a user to change a password by using the Forgot Password self-service feature would always fail, even if the user correctly answered the challenge questions. The "Invalid user found" message is displayed as the outcome of this operation.	This issue has been fixed, and you can now change the password by using the Forgot Password feature.

Software Updates in Release 9.0.4.6

The following are issues resolved in release 9.0.4.6:

Bug Number	Issue	Resolution
6976717	During a Create User provisioning operation, if you entered a comma in the `Full Name` field, then the operation would fail. This was because the `Full Name` field of Oracle Identity Manager was mapped to the `cn` field of the target system.	In the `AtMap.AD` lookup definition, the cn field of the target system has been mapped to the `User ID` field of Oracle Identity Manager. If required, you can change this mapping in the lookup definition so that the `cn` field is mapped to a different Oracle Identity Manager field. See *Oracle Identity Manager Design Console Guide* for information about modifying lookup definitions.

Software Updates in Release 9.0.4.7

There are no software updates in release 9.0.4.7.

Software Updates in Release 9.0.4.8

There are no software updates in release 9.0.4.8.

Software Updates in Release 9.0.4.9

There are no software updates in release 9.0.4.9.

Software Updates in Release 9.0.4.10

The following are issues resolved in release 9.0.4.10:

Bug Number	Issue	Resolution
7031943	Suppose the target system contains two domains that are configured as a parent-child pair. Groups `grp1` and `grp2` are created on the parent and child domain, respectively. User John Doe is a member of both groups. Through group reconciliation, groups `grp1` and `grp2` have been created in Oracle Identity Manager. During user reconciliation, reconciliation of John's record failed because user matching was based on the `objectGUID` and `cn`. attributes	This issue has been resolved. User matching during reconciliation is now based on the DN of the user. Therefore, user reconciliation is successful even when a user is a member of groups on both parent and child Microsoft Active Directory domains.

Software Updates in Release 9.0.4.10.1

The following are issues resolved in release 9.0.4.10.1:

Bug Number	Issue	Resolution
7112864	The name of an OU created in Oracle Identity Manager through reconciliation was converted to lowercase letters. For example, if you created the `MyOrg` OU in the target system, then the OU created in Oracle Identity Manager through reconciliation was named `myorg`. During subsequent user reconciliation runs, the target system OU could not be matched with its corresponding OU in Oracle Identity Manager. Therefore, reconciliation of users belonging to the OU failed.	This issue has been resolved. The case (uppercase and lowercase) of the name of an OU created in Oracle Identity Manager through reconciliation is the same as the case of the OU name on the target system.

Software Updates in Release 9.0.4.11

The following are issues resolved in release 9.0.4.11:

Bug Number	Issue	Resolution
7314549	A provisioning operation failed if you entered the slash character (/) in the Full Name field.	This issue has been resolved. During a provisioning operation, you can now enter the slash character in the Full Name fields.

Software Updates in Release 9.0.4.12

The following are issues resolved in release 9.0.4.12:

Bug Number	Issue	Resolution
7336488	During group lookup reconciliation, target system groups were reconciled under a single organization in Oracle Identity Manager.	You can now specify whether each target system group must be reconciled into an organization of its own or all target system groups must be reconciled into a single organization. To implement this feature, the following attributes have been introduced in the `ActiveDirectoryReconTask` scheduled task: ■ `UseOrgNameForGroupRecon` ■ `OrganizationNameForGroupRecon` See "User Reconciliation Scheduled Task" on page 3-8 for information about these attributes.

In addition, Arabic and Danish have been added to the list of supported languages.

Software Updates in Release 9.0.4.13

The following are issues resolved in release 9.0.4.13:

Bug Number	Issue	Resolution
7449155	During a Create User provisioning operation, if you entered a comma in the `Full Name` field, then the operation would fail. This was because the `Full Name` field of Oracle Identity Manager was mapped to the `cn` field of the target system.	This issue has been resolved. See "User Provisioning" on page 1-5 for information about special characters that are supported in the Full Name field.
7328972	During a provisioning operation, a user could not be made a member of a group whose name contained special characters.	This issue has been resolved. See "User Provisioning" on page 1-5 for information about special characters that are supported in the Group Name field.
7320836	During reconciliation of a large number of records, the reconciliation run would sometimes stop automatically and no error was thrown. In addition, no attempt was made to reestablish the connection to resume the reconciliation run.	This issue has been resolved. The number of records to be reconciled is determined at the start of a reconciliation run. Whenever the connection fails during the reconciliation run, an attempt is made to reestablish the connection and resume reconciliation. This process is repeated until the number of records reconciled is equal to the number of records identified for reconciliation at the start of the run.
7235815	Reconciliation of a user record failed if the Full Name field contained commas.	This issue has been resolved. You can now reconcile records even if the Full Name field contains commas.

Bug Number	Issue	Resolution
7450317	On the target system, if you do not want to set an expiry date for a user's account, then you enter `Never` in the Expiry Date field. This action is the same as setting the expiry date to `1-Jan-1970`. Similarly, on Oracle Identity Manager, you leave the Expiry Date process form field empty if you do not want to set an expiry date for the user's target system account. If the client computer and the target system host are set to different time zones, then the connector converts time stamp values sent from the client computer to GMT-relative time stamp values before storing them in the target system database. This conversion sometimes caused the `1-Jan-1970` value to be changed to `31-Dec-1969`. When this happened, the user account was created and disabled at the same time.	The `Target Locale: TimeZone` parameter has been added in the IT resource. You use this parameter to specify the time zone of the target system. See "Defining IT Resources" on page 2-7 for more information about this parameter.
7502026	The following is the format of the time-stamp filter applied to each target system record during reconciliation: *timestamp_record_updated* >= *last_reconciliation_run_timestamp* When this filter was applied, a record that was added or modified at the instant the reconciliation run ended was also reconciled. However, the application of the time-stamp filter caused the same record to be reconciled during the next reconciliation run.	This issue has been resolved. The time-stamp filter cannot be changed to the following: *timestamp_record_updated* > *last_reconciliation_run_timestamp* As a workaround, one second is added to the time stamp recorded in the IT resource before the filter is applied during a reconciliation run. In other words, the filter is changed to the following: *timestamp_record_updated* + 1 second >= *last_reconciliation_run_timestamp* Application of this filter ensures that a record reconciled at the end of a reconciliation run is not reconciled during the next reconciliation run.
7314549	A provisioning operation failed if you entered the comma (,) or slash (/) character in the Full Name field.	This issue has been resolved. You can now enter special characters in the Full Name field during provisioning operations.

Software Updates in Release 9.0.4.14

The following are issues resolved in release 9.0.4.14:

Bug Number	Issue	Resolution
7509116	The following problem was observed in earlier releases if you used this connector in conjunction with the password synchronization module: You created a custom attribute in Microsoft Active Directory to track password changes that came from Oracle Identity Manager. This attribute did not work.	This issue has been resolved. The custom attribute that is created in Oracle Identity Manager when you deploy this patch set captures password change events originating from both Microsoft Active Directory and Oracle Identity Manager. You do not have to create a custom attribute in Microsoft Active Directory. **Note:** For information about implementing this solution, see the release 9.0.4.14 readme for the password synchronization module.
7449155	If a target system record contained a comma in the cn field, then the organization name was not correctly reconciled.	This issue has been resolved. See "User Provisioning" on page 1-5 for information about supported special characters.

In the "Known Issues" chapter, the following point has been added:

- **Bug 7612861**

  The following tasks of the Create User provisioning operation fail if the last name specified ends in a comma (,):

  - User must change password at next logon Updated
  - Password never expires Updated

Software Updates in Release 9.0.4.15

The following is a software update in release 9.0.4.15:

Support for Specification of LDAP Query for Group Reconciliation

From this release onward, you can use an LDAP query to specify the groups that must be reconciled. You specify the LDAP query as the value of the `CustomizedGroupReconQuery` attribute of the `ActiveDirectoryReconTask` scheduled task. See "CustomizedGroupReconQuery Attribute" on page 3-4 for information about this attribute.

Software Updates in Release 9.0.4.16

The following are issues resolved in release 9.0.4.16:

Bug Number	Issue	Resolution
7719525 and 7685400	The connector did not support reconciliation or provisioning of multivalued attributes.	This issue has been resolved. The connector now supports reconciliation and provisioning of multivalued attributes. To enable provisioning of multivalued attributes, the `AD Multi Value Attribtes`, `AD Remove Multi Value Attributes`, and `AD Update Multi Value Attributes` adapters have been added. To enable reconciliation of multivalued attributes, the `GroupMultiValueAttributes` attribute has been added in the `ActiveDirectoryReconTask` scheduled task. See "User Reconciliation Scheduled Task" for more information about this attribute. In addition, you can now add new multivalued fields for reconciliation and provisioning. See the following sections for more information: ▪ Adding New Multivalued Fields for Target Resource Reconciliation ▪ Adding New Multivalued Fields for Provisioning
7722041	The connector could not be installed on Oracle Identity Manager release 9.0.3.x.	This issue has been resolved. The connector can now be installed on Oracle Identity Manager release 9.0.3.x and later releases.
8216540	A case-sensitive check was performed on attribute names in the Code Key column of the `Lookup.ADReconciliation.FieldMap` lookup definition. If the case (uppercase or lowercase) of an attribute name did not match the case of the attribute name on the target system, then reconciliation failed.	This issue has been resolved. A case-sensitive check is not performed on attribute names in the `Lookup.ADReconciliation.FieldMap` lookup definition.
8236103	During trusted source reconciliation, the `Email ID` field of the `Xellerate User` was not updated.	This issue has been resolved. The `Email ID` field of the `Xellerate User` is now updated during trusted source reconciliation.

Software Updates in Release 9.0.4.17

The following are issues resolved in release 9.0.4.17:

Bug Number	Issue	Resolution
8420393	During a group reconciliation run, only a maximum of 1000 groups could be reconciled.	This issue has been resolved. You can now reconcile more than 1000 groups during the same reconciliation run. In addition, you can reconcile group records in which each group has more than 1000 members. Similarly, you can reconcile user records in which each user contains more than 1000 entries for multivalued attributes. For example, you can reconcile the record of a user who is a member of more than 1000 groups. The EnableRange attribute has been introduced to enable the reconciliation of user and group records that contain more than 1000 entries.

Documentation-Specific Updates

The following are documentation-specific updates in revision "13" of release 9.0.4.17:

- Section 2.1, "Verifying Deployment Requirements" has been removed and all the contents of this section have been moved to Section 1.1, "Certified Components" in order to make it consistent with other connector guides.
- The "Usage Recommendation" section has been added.

The following are documentation-specific updates in earlier revisions of release 9.0.4.17:

- In the following sections, the version of one of the external JAR files has been changed from `ldapsdk-4.17.jar` to `ldapsdk-4.1.jar`:
  - Certified Components on page 1-1
  - Copying the Connector Files and External Code Files on page 2-2
- In the "User Reconciliation Scheduled Task" section on page 3-8, the description of the `Object` attribute has been modified.
- In the "Known Issues" chapter, the following point has been added:

  If you modify the group membership of a user (assign to or unassign from a group) in Microsoft Active Directory, this change in group membership is not reconciled into Oracle Identity Manager during the next reconciliation run. This is because group membership changes cannot be detected by the reconciliation scheduled task. This known issue will be addressed in a future release of Oracle Identity Manager.
- In the "User Reconciliation" section, the list of fields reconciled during target resource and trusted source reconciliation have been added.
- Microsoft Windows 2000 is no longer a supported host for the target system. All occurrences of "Microsoft Windows 2000" have been removed from this guide.
- In the "Certified Components" section, changes have been made in the "Target systems" row.
- From this release onward:

  The minimum certified release of Oracle Identity Manager is release 9.0.1.

  The minimum certified release of JDK is release 1.4.2.

  See "Certified Components" section for the complete listing of certified components.

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. This guide discusses the procedure to deploy the connector that 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:

> **Note:** In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.
>
> At some places in this guide, Microsoft Active Directory has been referred to as the *target system*.

1.1 Certified Components

Table 1–1 lists the certified components for this connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager Release 9.1.0.1 and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector supports.
Target systems	Microsoft Windows Server 2003 Active Directory
Target system host platforms	Microsoft Windows Server 2003 with SP1 and later service packs On a Microsoft Windows 2003 server on which Service Pack 1 has not been installed, you might come across the "WILL_NOT_PERFORM" error message during the password change operation. You can access information about one of the causes of and a solution for this error on the Microsoft Knowledge Base Web site at `http://support.microsoft.com`
Other software	Certificate Services
External code	`ldapbp.jar`
Target system user account	Microsoft Windows 2003 Server (Domain Controller) administrator You provide the credentials of this user account while performing the procedure in Section 2.4.1, "Defining IT Resources." If the specified user account is not used, then an authentication error message is displayed.

1.2 Usage Recommendation

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

- If you are using an Oracle Identity Manager release that is 9.1.0.1 or later and earlier than Oracle Identity Manager Release 9.1.0.2, then you must use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager Release 9.1.0.2 or later and earlier than, Oracle Identity Manager 11*g* Release 1 PS1 (11.1.1.5.6), then use the latest 9.1.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 (11.1.1.5.6) or later, or Oracle Identity Manager 11*g* Release 2 BP06 (11.1.2.0.6) or later, then use the latest 11.1.1.*x* version of this connector.
- If you are using the Microsoft Exchange 9.1.*x* connector, then you must use the Microsoft Active Directory 9.1.*x* connector, and if you are using the Microsoft Exchange 11.1.1.*x* connector, then you must use the Microsoft Active Directory 11.1.1.*x* connector.

1.3 Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager the creation 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 Concepts 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

1.3.1 Lookup Fields Reconciliation

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

- sAMAccountName
- objectGUID

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

- sAMAccountName
- primaryGroupToken

To populate the `Lookup.ADReconciliation.Organization` lookup definition, the following field of AD Organizations is reconciled:

- distinguishedName

1.3.2 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

1.3.3 User Reconciliation

Fields that are mapped for reconciliation depend on the type of reconciliation that you configure:

Reconciled Resource Object Fields

If you configure the connector for target resource reconciliation, then the following fields are reconciled:

Note: You can map other fields of the target system for reconciliation. Instructions are provided later in this guide.

- sAMAccountName

  Note: The sAMAccountName field must be reconciled from the target system during user reconciliation.

- objectGUID
- name
- memberOf
- sn
- cn
- Initials

Reconciled Xellerate User Fields

If you configure the connector for trusted source reconciliation, then the following fields are reconciled:

- User Login (mandatory field)
- First Name (mandatory field)
- Last Name (mandatory field)
- Xellerate Type (mandatory field)
- Organization Name (mandatory field)
- Middle Name
- Role
- Password
- Start Date
- End Date
- Email
- Status

1.4 Provisioning Module

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

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

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

- Organization Provisioning
- Group Provisioning
- User Provisioning

1.4.1 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.

1.4.2 Group Provisioning

The following fields are provisioned:

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

1.4.3 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

The following table lists special characters that are supported in process form fields:

Note: The following special characters are *not* supported in process form fields:

- Single quotation mark (')
- Double quotation mark (")

Name of the Character	Character
ampersand	&
asterisk	*
at sign	@
caret	^
comma	,
dollar sign	$
equal sign	=
exclamation point	!
hyphen	-
left brace	{
left bracket	[
left parenthesis	(
number sign	#
percent sign	%
period	.
plus sign	+
question mark	?
right brace	}
right bracket	]
right parenthesis	)
slash	/
underscore	_

1.5 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

Function	Type	Description
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
Lock User	Provisioning	Locks the user
Unlock User	Provisioning	Unlocks the user
Update First Name	Provisioning	Updates a user's profile according to a change in the First Name attribute
Update Last Name	Provisioning	Updates a user's profile according to a change in the Last Name attribute
Move Group	Provisioning	Moves a group from one organization to another
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)

1.6 Multilanguage Support

The connector supports the following languages:

- Arabic

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

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

1.7 Files and Directories on the Installation Media

The files and directories on the installation media 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 provisioning.
`lib/xliADRecon.jar`	This JAR file contains the class files required for reconciliation.
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
`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/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 (OIM 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 "Copying the Connector Files and External Code Files" section on page 2-2 provides instructions to copy these files into the required directories.

1.8 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME/xellerate/JavaTasks/xliActiveDirectory.jar

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.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Configuring the Target System
- Copying the Connector Files and External Code Files
- Configuring the Oracle Identity Manager Server
- Importing the Connector XML Files
- Configuring SSL

2.1 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

2.1.1 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 2-7 for more information about this parameter.

2.1.2 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. Select **Security Settings**, expand **Account Policies**, and then click **Password Policy**.
3. Double-click **Passwords must meet complexity requirements**.
4. 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
5. Click **OK**.

2.2 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.

See Also: "Files and Directories on the Installation Media" on page 1-8 for more information about these files

File in the Installation Media Directory	Destination Directory
`lib/xliActiveDirectory.jar`	*OIM_home*`/xellerate/JavaTasks`
`lib/xliADRecon.jar`	*OIM_home*`/xellerate/ScheduleTask`
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/ActiveDirectory/xml`

To copy the `ldapbp.jar` file 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` file.
4. Copy the `ldapbp.jar` file into the *`OIM_home`*`/xellerate/ThirdParty` 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 contents of the `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

2.3 Configuring the Oracle Identity Manager Server

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

2.3.1 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.

2.3.2 Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Copying the Connector Files and External Code Files" section on page 2-2, 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. An exception is thrown if you run the command described in Step 2 as follows:
>
> *`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`

2.3.3 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:

- **Oracle 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, log information is displayed on the server console.

- **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, log information is written to the following file:

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/SystemOut.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBoss_home*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

```
<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

2.4 Importing the Connector XML Files

As mentioned in the "Files and Directories on the Installation Media" section on page 1-8, 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 opening 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 ADITResource IT resource is displayed.
8. Specify values for the parameters of the ADITResource IT resource. See the "Defining IT Resources" section on page 2-7 for information about the values to be specified.
9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the AD Server IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

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

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. 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 "Configuring SSL" section on page 2-9.

2.4.1 Defining IT Resources

The following table provides values for the parameters of the `ADITResource` IT resource.

Parameter	Description
`Admin FQDN`	Fully qualified domain name corresponding to the administrator Format 1: `cn=`*`ADMIN_LOGIN`*`,cn=Users,dc=`*`DOMAIN`* Sample value 1: `cn=administrator,cn=Users,dc=adomain` Format 2: *`ADMIN_LOGIN@DOMAIN`* Sample value 2: `administrator@adomain.com`
`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 2003 computer on which Microsoft Active Directory is installed Sample value: `w2khost`
`Last Modified Time Stamp AD`	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`
`Last Modified Time Stamp TrustedAD`	Date and time at which the last AD User trusted source 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`
`Use SSL`	Specifies whether or not to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory Default value: `yes` **See Also:** The Known Issues list in Chapter 5 for information about a limitation arising from setting this parameter to `no`. **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`

Parameter	Description
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.
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 yes or no. The default value is no. **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.
isOrgLookupDN	Specify whether you want the Lookup.ADReconciliation.Organization lookup definition to be populated with distinguished names (DNs) or relative DNs during lookup field synchronization: ■ Enter yes if you want the lookup field to be populated with DNs. ■ Enter no if you want the lookup field to be populated with relative DNs.
ADGroup LookUp Definition	This parameter holds the name of the lookup definition in which the names of group fields are stored during group lookup synchronization. Value: Lookup.ADReconliation.GroupLookup This value is the same as that of the Lookup Code Name attribute of the AD Group Lookup Recon scheduled task, which is discussed in "Lookup Fields Reconciliation Scheduled Task". Note: You must not change the value of this parameter.

Parameter	Description
`Target Locale: TimeZone`	Specify the time zone of the target system. For example: `GMT-08:00` and `GMT+05:30` During a provisioning operation, the connector uses this time zone information to convert date-time values entered on the process form to date-time values relative to the time zone of the target system. Default value: `GMT`

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

2.5 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

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.5.3.1 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.

2.5.3.2 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
Oracle WebLogic Server	*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 Application Server	*ORACLE_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 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
- Adding a Custom Object Class for Provisioning
- Adding New Multivalued Fields for Target Resource Reconciliation
- Adding New Multivalued Fields for 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

3.1 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation 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

3.1.1 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 during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

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 opening 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 `yes`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-6.

3.1.2 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 specifying the queries that must be applied during reconciliation. You specify these queries as the values of the following scheduled task attributes:

- CustomizedReconQuery Attribute
- CustomizedGroupReconQuery Attribute

3.1.2.1 CustomizedReconQuery Attribute

For this connector, you create a filter by specifying values for the `CustomizedReconQuery` attribute while performing the procedure described in the "Defining IT Resources" section on page 2-7.

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` attribute.

Oracle Identity Manager Attribute	Microsoft Active Directory Attribute
User ID	sAMAccountName
First Name	givenName
Last Name	sn
Middle Name	initials
Full Name	displayName
Groups	memberOf

The `CustomizedReconQuery` attribute is used in conjunction with the `isNativeQuery` attribute. You use the `isNativeQuery` attribute to specify whether or not the query condition is in the native format.

The following are sample `CustomizedReconQuery` attribute values when the `isNativeQuery` attribute is set to `yes`:

Note: These queries are in the native format.

- `(&(objectclass=user)(givenName=John))`

  With this query condition, records of users belonging to the user object class and whose first name is John are reconciled.

- `(&(objectClass=user)(memberOf=CN=grp123,CN=Users,DC=corp,DC=com))`

  With this query condition, records of all users who belong to the user object class and the grp123 group are reconciled.

- `(&(&(objectClass=user)(memberOf=CN=group1,CN=Users,DC=corp,DC=com))(givenName=Richard))`

  With this query condition, records of all users who belong to the group1 group and user object class and whose first name is Richard are reconciled.

- `(&(objectclass=user)(sn=Roe))`

  With this query condition, records of all users who belong to the user object class and whose last name is Roe are reconciled.

The following are sample CustomizedReconQuery attribute values when the isNativeQuery attribute is set to no:

- objectClass=user&givenName=John&sn=Doe

  With this query condition, records of users who belong to the user object class and whose first name is John and last name is Doe are reconciled.

- givenName=John|sn=Doe

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

  – First name is John.

  – Last name is Doe.

- objectClass=user&memberOf=CN=grp123,CN=Users,DC=Globalsv,DC=com

  With this query condition, records of all users who belong to the grp123 group and the user object class are reconciled.

If the value of the CustomizedReconQuery attribute is [NONE], 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 when the isNativeQuery attribute is set to no (that is, when you want to use a non-native format query):

- 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 must enclose the query condition in parentheses, for example:

  (&(objectClass=user)(sn!=Doe))

3.1.2.2 CustomizedGroupReconQuery Attribute

You use the CustomizedGroupReconQuery attribute to specify the groups that must be reconciled. The value of this attribute is an LDAP query that you specify.

You can use any one or a combination of the following group fields to create the LDAP query:

- name
- instanceType
- groupType
- objectSid
- sAMAccountType
- member
- uSNCreated
- uSNChanged
- objectClass
- distinguishedName
- objectCategory
- sAMAccountName
- objectGUID
- cn
- whenCreated
- whenChanged

The following are sample LDAP queries:

Note:

As shown in these samples, individual conditions must be enclosed in parentheses. For example: `(groupType=2)`

Only queries in native LDAP format are supported.

- `(&(|(groupType=2)(name=MyGrp))(objectClass=group))`
- `(&(&(groupType=2)(name=MyGrp))(objectClass=group))`
- `(&(objectclass=group)(name=MyGrp))`
- `(|(groupType=2)(name=MyGrp))`

3.1.3 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 3-8.

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.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML Files" section on page 2-6, 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 3-7 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.

3.1.4.1 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

3.1.4.1.1 Lookup Fields Reconciliation Scheduled Task The following lookup field reconciliation scheduled tasks have the same attributes:

- `ADGroupLookupReconTask`
- `AD Security Group Global Lookup Recon`
- `ADOrganizationLookupReconTask`

These attributes are described in the following table:

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	`ADITResource`
`LookupCodeName`	Name of the lookup definition	▪ For group lookup reconciliation: `Lookup.ADReconliation.GroupLookup` ▪ For security group lookup reconciliation: `Lookup.AD.PrimaryGroupList` ▪ For organization lookup reconciliation: `Lookup.ADReconciliation.Organization`
`AttrNameForDecodeValueInLookup`	Decode value of the attribute name for lookup reconciliation	▪ For group lookup reconciliation: `cn` ▪ For security group lookup reconciliation: `cn` ▪ For organization lookup reconciliation: `distinguishedName`

Attribute	Description	Default/Sample Value
AttrNameForCodeValueInLookup	Code Key value of the attribute name for lookup reconciliation	■ For group lookup reconciliation: objectGUID ■ For security group lookup reconciliation: primaryGroupToken ■ For organization lookup reconciliation: distinguishedName
FilterForLookupRecon	Search filter for lookup reconciliation	■ For group lookup reconciliation: (objectclass=group) ■ For security group lookup reconciliation: (&(groupType=-2147483646)(objectclass=group)) ■ For organization lookup reconciliation: (objectclass=OrganizationalUnit)
OverWriteLookup	Enter yes as the value of this attribute if you want the following events to occur during lookup field reconciliation: ■ Existing values of the Oracle Identity Manager lookup definition are deleted. ■ All the values in the target system lookup field are copied into the Oracle Identity Manager lookup definition. Enter no as the value of this attribute if you want the following events to occur during lookup field reconciliation: ■ Existing values in the Oracle Identity Manager lookup definition are updated with changes made to the target system lookup field. ■ New values in the target system lookup field are copied into the Oracle Identity Manager lookup definition. Default value: yes	yes

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

3.1.4.1.2 User Reconciliation Scheduled Task The following table describes attributes of these user reconciliation scheduled tasks:

- ActiveDirectoryReconTask
- TrustedADReconTask

Note:

- Most of the attributes are common to both scheduled tasks.
- See Appendix B, "Attributes of the Reconciliation Scheduled Task" for more information about these attributes.
- 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 yes or no. 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. You must specify a value for this attribute.	yes
FieldLookupCode	Name of the lookup definition that is used for custom reconciliation See Appendix B, "Attributes of the Reconciliation Scheduled Task" for more information about this attribute.	Lookup.ADReconciliation.FieldMap
MaintainHierarchy	Specifies whether or not organization hierarchy must be maintained in Microsoft Active Directory See Appendix B, "Attributes of the Reconciliation Scheduled Task" for more information about this attribute. The default value is no. If required, you can set it to yes. **Note:** This attribute is used only in the TrustedADReconTask scheduled task.	no
XellerateObject	Name of the OIM 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 no. You must specify a value for this attribute. **Note:** This attribute is used only in the TrustedADReconTask scheduled task.	'
XellerateOrg	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. The default value of this attribute is Xellerate Users. Do not change the default value. **Note:** This attribute is used only in the TrustedADReconTask scheduled task.	Xellerate Users

Attribute	Description	Default/Sample Value
Object	Name of the AD User resource object in Oracle Identity Manager on which reconciliation is performed The default value is AD User. You must not change this value. **Note:** This attribute is used only in the ActiveDirectoryReconTask scheduled task.	AD User
Server	Name of the IT resource representing the Microsoft Active Directory server You must specify a value for this attribute.	ADITResource
TransformLookupCode	Lookup code used for the transformation class map stored in the lookup tables See Appendix B, "Attributes of the Reconciliation Scheduled Task" for more information about this attribute. This attribute is valid only when the UseTransformMapping attribute is set to yes.	Lookup.ADReconciliation.TransformationMap
UseTransformMapping	Specifies whether or not transform mappings accessed by using the TransformLookupCode attribute must be used The value can be yes or no.	yes
MultiValueAttributes	Comma-delimited list of all the multivalued Microsoft Active Directory attributes that must be reconciled For AD Group reconciliation, enter member. See Appendix B, "Attributes of the Reconciliation Scheduled Task" for more information about this attribute. You must specify a value for this attribute.	member
GroupObject	**For target resource reconciliation:** Name of the AD Group resource object in Oracle Identity Manager on which group reconciliation is to be performed If you want AD Group reconciliation to be performed, then change the value to AD Group. Otherwise, change the value to no. You must specify a value for this attribute. The value can be yes or no. **For trusted source reconciliation:** Accept the default value, no.	no
LastTimeStampAttrName	The attribute holds the name of the IT resource time-stamp parameter that is updated after this scheduled task is run. For example, if the IT resource time-stamp parameter is Last Modified TimeStampTrustedAD, then specify Last Modified TimeStampTrustedAD as the value of this attribute.	Last Modified Time Stamp TrustedAD

Attribute	Description	Default/Sample Value
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. If you do not want to fetch records based on the filter provided as the value of the CustomizedReconQuery attribute, then specify [NONE] as the value. See "Partial Reconciliation" for more information about this attribute. Sample values: ■ If isNativeQuery is set to no: sn=last&givenName=first ■ If isNativeQuery is set to yes: (&(sn=last)(given=first))	[NONE]
isNativeQuery	Enter yes to specify that the value of the CustomizedReconQuery attribute is in native LDAP format. Enter no to specify that the value of the CustomizedReconQuery attribute is in native LDAP format.	yes
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 3-5.	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 3-5.	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 3-5.	Default value: All Available (for reconciling all the users) Sample value: 50
LookupForPrimaryGroup	Name of the lookup definition that is used for primary group reconciliation This attribute is used only when the isReconPrimaryGroups attribute is set to yes. **Note:** This attribute is used only in the ActiveDirectoryReconTask scheduled task.	Lookup.AD.PrimaryGroupList
isReconPrimaryGroups	Specifies whether or not primary groups accessed by using the LookupForPrimaryGroup attribute must be used **Note:** This attribute is used only in the ActiveDirectoryReconTask scheduled task.	yes
UseOrgNameForGroupRecon	This attribute is used only during group reconciliation. You can set this attribute to one of the following values: ■ If you want each target system group to be reconciled into an organization of its own, then set the value of this attribute to No. ■ If you want all target system groups to be reconciled into a single organization, then set the value of this attribute to Yes.	No

Attribute	Description	Default/Sample Value
OrganizationNameForGroupRecon	This attribute is used only during group reconciliation. ■ If you want each target system group to be reconciled into an organization of its own, then accept the default value of this attribute ([NONE]). **Note:** In addition, set the AD Group Recon reconciliation rule to the following: *ORGANIZATION_NAME* (from organization data) <equals> *USER_ID* (from the reconciliation event) See *Oracle Identity Manager Design Console Guide* for information about modifying reconciliation rules. ■ If you want all target system groups to be reconciled into a single organization, then set the value of this attribute to the name of the Oracle Identity Manager organization under which groups must be created. **Note:** In addition, set the AD Group Recon reconciliation rule to the following: *ORGANIZATION_NAME* (from organization data) <equals> *ORGANIZATION_NAME* (from the reconciliation event) See *Oracle Identity Manager Design Console Guide* for information about modifying reconciliation rules.	[NONE]
CustomizedGroupReconQuery	Specifies the LDAP query that you want to use for determining groups that must be reconciled See "Partial Reconciliation" for more information about this attribute. **Note:** Only queries in native LDAP format are supported. Sample values: ■ (&(|(groupType=2)(name=MyGrp))(objectClass=group)) ■ (&(&(groupType=2)(name=MyGrp))(objectClass=group)) ■ (&(objectclass=group)(name=MyGrp)) ■ (|(groupType=2)(name=MyGrp))	[NONE]
GroupMultiValueAttributes	Specifies the comma-separated list of multivalued group attributes that you want to reconcile **Note:** This attribute is specific to the ActiveDirectoryReconTask scheduled task. Sample value: member	[NONE]
EnableRange	Enter yes if you want to enable the reconciliation of user and group records that contain more than 1000 entries for the multivalued attributes. Otherwise, enter no.	no

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

3.1.5 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**.

3.1.6 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 1-2 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation.

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

1. Install the target system schema, if it is not already installed.

   Refer to the Microsoft Web site for information about installing the schema.

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

2. Open the target system schema.
3. Expand the **Console Root** folder, expand the target system schema, and then double-click **Classes**.
4. Right-click **user**, and then select **Properties**.

   The Attributes tab displays the attributes (that is, fields) that are currently in use on the target system.
5. Note down the name of the field that you want to add, and then click **Cancel**.

   For example, if you want to add the Employee ID field for reconciliation, then note down `employeeID`.

To add a new field for target resource reconciliation:

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

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new field on the process form as follows:

a. Expand **Development Tools**.

b. Double-click **Form Designer.**

c. Search for and open the **UD_ADUSER** process form.

d. Click **Create New Version**, and then click **Add**.

e. Enter the details of the field.

   For example, if you are adding the Employee ID field, enter `UD_ADUSER_EMPLOYEE_ID` in the **Name** field and then enter other details such as Variable Type, Length, Field Label, and Field Type.

f. Click **Save**, and then click **Make Version Active.**

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

   a. Expand **Resource Management**.

   b. Double-click **Resource Objects.**

   c. Search for and open the **AD User** resource object.

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

   e. Enter the details of the field.

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

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

   f. Click **Save**.

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

   a. Expand **Process Management**.

   b. Double-click **Process Definition**.

   c. Search for and open the **AD User** provisioning process.

   d. On the **Reconciliation Field Mappings** tab of the **AD User** provisioning process, click **Add Field Map**.

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

   f. Double-click the **Process Data Field** field, and then select **UD_ADUSER_EMPLOYEE_ID**.

   g. Click **Save**.

5. Create an entry for the field in the lookup definition for reconciliation as follows:

   a. Expand **Administration**.

   b. Double-click **Lookup Definition.**

   c. Open **Lookup.ADReconciliation.FieldMap**.

   d. Click **Add** and enter the Code Key and Decode values for the field. The Code Key value must be the name of the field on the target system, which you determined at the start of this procedure. The Decode value is the name that you provide for the reconciliation field in Step 3.e.

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

e. Click **Save**.

3.2 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.

Note: You must perform the procedure described in this section if you want to use the provisioning features of Oracle Identity Manager for this target system.

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

See Also: The "Supported Functionality" section on page 1-6 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 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`
- `AD Get ObjectGUID`
- `AD Enable User`
- `AD Disable User`
- `AD Delete User`

- AD Create User
- AD Change Attribute
- AD Change User Password
- 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.

3.2.1 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 1-4 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

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

1. Install the target system schema, if it is not already installed.

   Refer to the Microsoft Web site for information about installing the schema.

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

2. Open the target system schema.
3. Expand the **Console Root** folder, expand the target system schema, and then double-click **Classes**.
4. Right-click **user**, and then select **Properties**.

   The Attributes tab displays the attributes (that is, fields) that are currently in use on the target system.
5. Note down the name of the field that you want to add, and then click **Cancel**.

   For example, if you want to add the Employee ID field for reconciliation, then note down `employeeID`.

To add a new field for provisioning:

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

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new field on the process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer.**
   c. Search for and open the **UD_ADUSER** process form.
   d. Click **Create New Version**, and then click **Add**.
   e. Enter the details of the field.

      For example, if you are adding the Employee ID field, enter `UD_ADUSER_EMPLOYEE_ID` in the Name field, and then enter the rest of the details of this field.
   f. Click **Save** and then click **Make Version Active.**
3. Create an entry for the field in the lookup definition for provisioning as follows:
   a. Expand **Administration**.
   b. Double-click **Lookup Definition.**
   c. If the field that you want to add is *not* an Environment, Remote Control, or Sessions field, then search for and open the AtMap.AD lookup definition.

d. Cick **Add** and then enter the Code Key and Decode values for the field. The Decode value must be the name of the field on the target system, which you determined at the start of this procedure.

   For example, enter `UD_ADUSER_EMPLOYEE_ID` in the **Code Key** field and then enter `employeeID` in the **Decode** field.

Enabling Update of New Fields for Provisioning

After you add a field for provisioning, you must enable update operations on the field. If you do not perform this procedure, then you will not be able to modify the value of the field after you set a value for it during the Create User provisioning operation.

To enable the update of a new field for provisioning:

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

1. Log in to the Oracle Identity Manager Design Console.
2. In the provisioning process, add a new task for updating the field as follows:
   a. Expand **Process Management**.
   b. Double-click **Process Definition** and open **the AD User** provisioning process.
   c. Click **Add** and enter the task name and the task description.
   d. In the Task Properties section, select the following fields:
      – Conditional
      – Required for Completion
      – Allow Cancellation while Pending
      – Allow Multiple Instances
   e. Click **Save**.
3. In the AD User provisioning process, select the adapter name in the Handler Type section as follows:
   a. Go to the Integration tab, click **Add** and select **Adapter**.
   b. In the Handler Type section, select **adpADCSCHANGEATTRIBUTE**.
   c. Click **Save**.
4. Double-click the **Variable Name** field to get the value and map the adapter variable to **Response Code**.
5. Double-click the **Variable Name** field to get the value and map the adapter variable to a process data field.
6. Double-click the **Variable Name** field to get the value and map the adapter variable to a process data field.
7. Double-click the **Variable Name** field to get the value and map the adapter variable with the corresponding field on the target system. For example, enter employeeID for updating Employee ID.
8. Click **Save**.

3.3 Adding a Custom Object Class for Provisioning

By default, newly created users on the target system are assigned to the user object class. The user object class is the value of the `LdapUserObjectClass` field in the `Atmap.AD` lookup definition. If you want to assign new users to additional object classes, then enter the list of object classes in the Decode column for this field. Use the vertical bar (`|`) to separate the object class names in the value that you specify.

The following are sample values for the LdapUserObjectClass entry:

- `user`
- `coperson`
- `user|coperson`

In the third sample value, the vertical bar (`|`) is used as the delimiting character.

This parameter is used only during provisioning.

Note:

- When you create an object class, set the `user` object class as the parent object class.
- You can provision users with user-defined object classes in addition to the user object class. However you cannot provision the user with object classes such as contact and computer because they are not treated as user objects by Microsoft Active Directory.

3.4 Adding New Multivalued Fields for Target Resource Reconciliation

Note:

This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for reconciliation.

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

If required, you can add new multivalued fields for target resource reconciliation.

To add a new multivalued field for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued field as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Create a form by specifying a table name and description, and then click **Save**.
   d. Click **Add** and enter the details of the field.
   e. Click **Save** and then click **Make Version Active.**
3. Add the form created for the multivalued field as a child form of the process form as follows:

a. Search for and open the **UD_ADUSER** or **UD_ADGROUP** process form.

b. Click **Create New Version**.

c. Click the **Child Table(s)** tab.

d. Click **Assign**.

e. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.

f. Click **Save** and then click **Make Version Active.**

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

a. Expand **Resource Management**.

b. Double-click **Resource Objects**.

c. Search for and open the **AD User** or **AD Group** resource object.

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

e. In the Add Reconciliation Fields dialog box, enter the details of the field.

For example, enter `carLicense` in the **Field Name** field and select **Multi Valued Attribute** from the Field Type list.

f. Click **Save** and then close the dialog box.

g. Right-click the newly created field.

h. Select **Define Property Fields**.

i. In the Add Reconciliation Fields dialog box, enter the details of the newly created field.

For example, enter `carLicense` in the Field Name field and select **String** from the Field Type list.

j. Click **Save**, and then close the dialog box.

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

a. Expand **Process Management**.

b. Double-click **Process Definition**.

c. Search for and open the **AD User** or **AD Group** process definition.

d. On the Reconciliation Field Mappings tab of the AD User or AD Group process definition, click **Add Table Map**.

e. In the Add Reconciliation Table Mapping dialog box, select the field name and table name from the list, click **Save**, and then close the dialog box.

f. Right-click the newly created field, and select **Define Property Field Map**.

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

h. Double-click the Process Data Field field, and then select the column that you want to add, for example, **UD_CAR_LICENSE**.

i. Select **Key Field for Reconciliation Field Matching** and click **Save**.

6. Create an entry for the field in the lookup definition for reconciliation as follows:

a. Expand **Administration**.

b. Double-click **Lookup Definition.**

c. Search for and open the **Lookup.ADReconciliation.FieldMap** lookup definition.

d. Cick **Add** and enter the Code Key and Decode values for the field, and then Click **Save**. The Code Key value must be the name of the attribute field on the target system.

For example, enter `carLicense` in the Code Key field and then enter `carLicense` in the Decode field.

3.5 Adding New Multivalued Fields for Provisioning

Note: This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for reconciliation.

To add new multivalued fields for provisioning:

Note: Before starting the following procedure, perform Steps 1 through 3 as described in the "Adding New Multivalued Fields for Target Resource Reconciliation" section. If these steps have been performed while adding new multivalued fields for target resource reconciliation, then you need not repeat the steps.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Process Management**.
3. In the process definition, add the task for provisioning multivalued attributes as follows:
   a. Double-click **Process Definition**.
   b. Search for and open the **AD User** or **AD Group** process definition.
   c. Click **Add** and enter the task name and the description.
   d. In the Task Properties section, select the following:
      – Conditional
      – Required for Completion
      – Retry Count
      – Allow Multiple Instances
      – Child table name from the Child Table list
      – **Insert**, if you want to add the data, from the Trigger Type list
      – **Delete**, if you want to remove the data, from the Trigger Type list.
   e. Click **Save**.
4. Select the adapter as follows:
   a. On the Integration tab in the AD User or AD Group provisioning Process, click **Add** and then select **Adapter**. From the list of adapters:

- If you want to add multivalued data, then select **adpADCSAddMultiAttributeData** and click **Save**.
- If you want to remove multivalued data, then select **adpADCSRemoveMultiAttributeData** and click **Save**.

5. Double-click and map the adapter variable to a process data field and click **Save**.
6. Double-click and map the adapter variable to a literal and specify the name of the attribute to be updated in the Literal Value field, and then click **Save**.
7. Double-click and map the adapter variable to a process data field of the newly created form. If you are removing the attribute, then select **Old Value** and click **Save**.
8. Double-click and map the adapter variable to a process data field and click **Save**.
9. Double-click and map the adapter variable to a response code field and click **Save**.
10. Click **Save** on Process Task.

Note: During a provisioning operation, you can either add or remove values of multivalued fields. You cannot update these values.

3.6 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.

3.7 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.

3.8 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 Oracle Identity Manager
- Specifying Values for IT Resource Parameters
- Sequence of Events That Occur During a Password Change
- Configuring the xlconfig.xml File for the Password Synchronization Module

3.8.1 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**.

3.8.2 Specifying Values for IT Resource Parameters

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

- AD Sync installed (yes/no)

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

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

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

  Note: You must specify the column name and not the field label that you enter while adding the custom attribute in Oracle Identity Manager. For example, if you enter the label PWDCHANGEDINDICATION, then the column name that you must specify is USR_UDF_PWDCHANGEDINDICATION. Oracle Identity Manager adds the USR_UDF_ prefix while creating a column.

3.8.3 Sequence of Events That Occur During a Password Change

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

When you change the password on Oracle Identity Manager:

1. Oracle Identity Manager sets the value of the USR_UDF_PWDCHANGEDINDICATION field to 1.
2. The new password is propagated to the target system.
3. The password synchronization module detects the password change.
4. The password synchronization module checks the value of the USR_UDF_PWDCHANGEDINDICATION field, sets the field to 0, and then performs no further action.

Note: When you perform a Create User provisioning operation, the value of the field is NULL. The password synchronization module treats the NULL value the same as it would treat a value of 1.

When you change the password on the target system:

1. The password synchronization module sets the value of the `USR_UDF_PWDCHANGEDINDICATION` field to 1.
2. The new password is set in the USR table.
3. Oracle Identity Manager detects the password change.
4. Oracle Identity Manager checks the value of the `USR_UDF_PWDCHANGEDINDICATION` field, sets the field to 0, and then performs no further action.

3.8.4 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" section 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.

4.1 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.

4.2 Troubleshooting

Suppose you set the `Use SSL` IT resource parameter to `no`. 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 2-1 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 the current release of the connector:

- **Bug 7226547**

  If you do not want to enable SSL communication between Oracle Identity Manager and Microsoft Active Directory, then you set the `Use SSL` IT resource parameter to `no`. Now, when you provision a Microsoft Active Directory user through Oracle Identity Manager, the password cannot be updated by using Oracle Identity Manager. To enable updates of passwords when the communication is not secured by SSL, you must disable any existing password policies in Microsoft Active Directory.

  See "Enabling or Disabling Password Policies on Microsoft Active Directory" for information about the procedure that you must perform to address this limitation.

  This limitation is also described in the "Troubleshooting" section.

- **Bug 7226622**

  If the `MaintainHierarchy` attribute is set to `yes` and the `Root Context` IT resource parameter does not begin with `ou`, then organization hierarchy might not be maintained during reconciliation. Therefore, to ensure that the `MaintainHierarchy` attribute works as expected, the value that you specify for the `Root Context` parameter must begin with `ou`.

- **Bug 7237564**

  Suppose password policies are enabled on the target system. On the Administration and User Console page, at the end of the Create User provisioning operation, the status of the AD User resource is Provisioned and the status of the Create User task is Completed even when the following tasks are rejected:

  - Password never expires Updated
  - User must change password at next logon Updated
  - Get Object GUID Created

- **Bug 7237572**

  If an invalid value is entered in the `CustomizedReconQuery` attribute of the `ActiveDirectoryReconTask` and `TrustedADReconTask` scheduled tasks, then a corresponding error message is not written to the log file during reconciliation.

- **Bug 7237580**

During a particular reconciliation run, suppose all the created and modified user records are successfully reconciled. Now, suppose there are no user record changes on the target system up to the next reconciliation run.

During the next reconciliation run, the last user record that was reconciled in the previous reconciliation run is reconciled again.

- **Bug 7612861**

  The following tasks of the Create User provisioning operation fail if the last name specified ends in a comma (,):

  - User must change password at next logon Updated
  - Password never expires Updated

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

This appendix provides additional information about the following attributes of the reconciliation scheduled task:

- **DeleteRecon**

  This attribute is used to enable the Delete Reconciliation feature. The value can be `yes` or `no`. 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.

- **FieldLookupCode**

  This attribute provides the name of the lookup definition that holds mappings 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 `yes` or `no`.

  If this attribute is set to `yes`, 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.

- **`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 D, "Code for a Sample Transformation Class"

- **`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.

C

Special Characters Supported for Passwords

Table C–1 lists the special characters supported by Oracle Identity Manager and Microsoft Active Directory for password field. You can use these characters in combination with letters (alphabets) while specifying a password.

Table C–1 Special Characters That Can Be Used in the Password Field

Name of the Character	Character
at sign	@
percent sign	%
plus sign	+
backslash	\
slash	/
single quotation mark	'
exclamation point	!
number sign	#
dollar sign	$
caret	^
question mark	?
colon	:
comma	.
left parenthesis	(
right parenthesis	)
left brace	{
right brace	}
left bracket	[
right bracket	]
tilde	~
grave accent This character is also known as the backquote character.	The grave accent cannot be reproduced in this document.
hyphen	-

Table C–1 (Cont.) Special Characters That Can Be Used in the Password Field

Name of the Character	Character
underscore	_

D

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

O

P

R

S

T

U

X