Oracle® Identity Manager

Connector Guide for Microsoft Active Directory

Release 9.0.1

B31119-01

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for Microsoft Active Directory, Release 9.0.1

B31119-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

Contents

Preface

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

Note: This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

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

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Connector Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.1 connector documentation set, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation/index.html`

Conventions

The following text conventions are used in this document:

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

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector forMicrosoft Active Directory is used to integrate Oracle Identity Manager withMicrosoft Active Directory.

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

This chapter contains the following sections:

Supported Functionality

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

Function	Type	Description
Create User	Provisioning	Creates a user
Delete user	Provisioning	Deletes a provisioned user
Get Organization USN	Provisioning	Retrieves the USN of an existing organization
Create Organization	Provisioning	Creates an organization
Change Organization Name	Provisioning	Updates the organization name
Get Organization USN Changed	Provisioning	Retrieves the USN of an existing organization after an update
Move Organization	Provisioning	Moves an organization from one root to another
Delete Organization	Provisioning	Deletes an existing organization
Get User ObjectGUID	Provisioning	Retrieves the ObjectGUID of an existing user

Function	Type	Description
User Must Change Password at Next Logon Updated	Provisioning	Updates the configuration of a user according to a change in the User Must Change Password at Next Logon attribute
Set Account Expiration Date	Provisioning	Updates the configuration of a user according to a change in the Account Expiration Date attribute
Password Never Expires Updated	Provisioning	Updates the configuration of a user according to a change in the Password Never Expires attribute
Update User ID	Provisioning	Updates the configuration of a user according to a change in the User ID attribute
Move User	Provisioning	Moves a user from one organization to another
Delete User	Provisioning	Deletes an existing user
Enable User	Provisioning	Enables a disabled existing user
Disable User	Provisioning	Disables an existing user
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 existing AD group
Update Group Name	Provisioning	Updates an AD group name
Get Group ObjectGUID	Provisioning	Retrieves the ObjectGUID of an existing group
Trusted Reconciliation for User	Reconciliation	Creates Xellerate User accounts corresponding to reconciled Microsoft Active Directory accounts
Create User	Reconciliation	Reconciles Microsoft Active Directory accounts
Create Organization	Reconciliation	Creates organizations along with users in Oracle Identity Manager corresponding to reconciled Microsoft Active Directory accounts (and their root organizations)
Create Group	Reconciliation	Creates groups along with users in Oracle Identity Manager corresponding to reconciled Microsoft Active Directory accounts (and their parent groups)

Reconciliation Module

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

- AD Lookup Fields
- AD User
- AD Group

AD Lookup Fields

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

- sAMAccountName
- objectGUID

AD User

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

- sAMAccountName
- objectGUID
- name
- memberOf
- sn
- cn

AD Group

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

- sAMAccountName
- objectGUID
- Organization Name
- instanceType
- cn

Provisioning Module

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

- AD User
- AD Group
- AD Organization

AD User

The following fields are provisioned:

- User ID
- Password
- Object GUID
- 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

AD Group

The following fields are provisioned:

- Group Name
- Organization Name
- Object GUID
- Group Type
- Group Display Name

AD Organization

The following fields are provisioned:

- USN Create
- USN Change
- Object GUID
- Organization Name (extracts the value from the Name field in the Create Organization form of the Oracle Identity Manager Administrative and User Console)

Files and Directories That Comprise the Connector

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

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

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
xml\xliADOrganizationObject_DM.xml	This XML file contains the Oracle Identity Manager components of the connector related to AD Organization provisioning. These components include: ■ Resource object for AD Organization provisioning ■ IT resource type ■ Custom process form ■ Process task and rule-generator adapters (along with their mappings) ■ Login resource object ■ Provisioning process ■ Pre-populate rules
xml\xliADGroupObject_DM.xml	This XML file contains the Oracle Identity Manager components of the connector related to AD Group provisioning. These components include: ■ Resource object for AD Group provisioning ■ IT resource type ■ Custom process form ■ Process task and adapters (along with their mappings) ■ Login resource object ■ Provisioning process ■ Pre-populate rules
xml\xliADUserObject_DM.xml	This XML file contains the Oracle Identity Manager components of the connector related to AD User provisioning. These components include: ■ Resource object for AD User provisioning ■ IT resource type ■ Custom process form ■ Process task and adapters (along with their mappings) ■ Login resource object ■ Provisioning process ■ Pre-populate rules
xml\xliActiveDirectoryScheduleTask_DM.xml	This XML file contains the Oracle Identity Manager components of the connector related to the Database Access reconciliation module. These components include: ■ Reconciliation scheduled task ■ Reconciliation scheduled task attributes
lib\xliActiveDirectory.jar	This JAR file contains the class files required for provisioning.
lib\xliADRecon.jar	This JAR file contains the class files required for reconciliation.
ext\ldapsdk-4.1.jar	This external JAR file contains the JNDI LDAP booster package that is required for the Active Directory connector.
scripts\install.bat	This batch file is used to add a certificate to the keystore if Oracle Identity Manager is installed on a Microsoft Windows operating system.

File in the Installation Media Directory	Description
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 Microsoft Active Directory connector test suite.
test\lib\xliADTest.jar	This JAR file contains the class files required for the Microsoft Active Directory connector test suite.
test\logs	This directory is used by the Microsoft Active Directory connector test suite to log the results of the tests.
test\scripts\runADTest.bat	This file is used to run a test using the connector test suite.
docs\B31119_01.pdf docs\html	These are PDF and HTML versions of this guide, which provides instructions to deploy the connector.

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

The "Step 3: Copying the Connector Files and External Code" section on page 2-1 provides instructions to copy these files into the required directories.

2

Deploying the Connector

Deploying the connector involves the following steps:

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target systems	Microsoft Active Directory Server (Microsoft Windows 2000 or 2003)
Target system host platforms	The target system host platform can be any one of the following: ■ Microsoft Windows 2000 SP 4 ■ Microsoft Windows 2003
Other systems	Certificate services
External code	JNDI LDAP Booster package (`ldapsdk-4.1.jar`)

Step 2: Configuring the Target System

You must ensure that the parent organization exists in the target server installation. The parent organization is specified as the Root Context parameter in the relevant IT resource.

Step 3: Copying the Connector Files and External Code

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

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

`Directory Servers\Microsoft Active Directory\Microsoft Active Directory Rev 4.4.0.zip`

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

File in the Installation Media Directory	Destination Directory

The following files in the `xml` directory:
`xliADOrganizationObject_DM.xml`
`xliADGroupObject_DM.xml`
`xliADUserObject_DM.xml`
`xliActiveDirectoryScheduleTask_DM.xml`
	xellerate_home`\XLIntegrations\ActiveDirectory\xml`

`lib\xliActiveDirectory.jar`	*xellerate_home*`\xellerate\JavaTasks`
`lib\xliADRecon.jar`	*xellerate_home*`\xellerate\ScheduleTask`
`ext\ldapsdk-4.1.jar`	*xellerate_home*`\xellerate\XLIntegrations\ActiveDirectory\lib`

The following files in the `scripts` directory:
`install.bat`
`install.sh`
	xellerate_home`\xellerate\scripts`

The following contents of the `test` directory:
`config\config.properties`
`lib\xliADTest.jar`
`logs`
`scripts\runADTest.bat`
	xellerate_home`\xellerate\test`

The following contents of the `docs` directory:
`B31119_01.pdf`
`html`
	xellerate_home`\xellerate\docs`

Step 4: Importing the Connector XML Files

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

1. `xliADOrganizationObject_DM.xml`
2. `xliADGroupObject_DM.xml`
3. `xliADUserObject_DM.xml`

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

To import the connector XML files into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `xliADOrganizationObject_DM.xml` file, which is in the *`xellerate_home`*`\xellerate\XLIntegrations\ActiveDirectory\xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the `AD Server` IT resource is displayed.
8. Specify values for the parameters of the `AD Server` IT resource. Depending on whether the operating system is Microsoft Windows 2000 or Microsoft Windows 2003, refer to the appropriate table in the "Defining IT Resources" section on page 2-3 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. You must remove these nodes. To do this, right-click each such node and then select **Remove.**
12. Click **Import**. The connector file is imported into Oracle Identity Manager.

Defining IT Resources

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

- Microsoft Windows 2000
- Microsoft Windows 2003

Microsoft Windows 2000

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

Parameter Name	Parameter Description
`Admin FQDN`	Fully qualified domain name corresponding to the admin user Format: `cn=ADMIN_LOGIN,cn=Users,dc=`*`DOMAIN`* Sample value: `cn=administrator,cn=Users,dc=adomain`

Parameter Name	Parameter Description
Admin Login	User ID of the admin account that is used to create the OU/user Sample value: administrator
Admin Password	Password of the admin account that is used to create the OU/user Sample value: password
Root Context	Usually, this is the fully qualified domain name of the parent or root organization. For example, the root suffix. Value: ou=*ORGANIZATION_NAME*,dc=*DOMAIN* Sample value: ou=Adapters, dc=adomain
Server Address	Host name or the IP address of the target Microsoft Windows 2000 computer where the Microsoft Active Directory server is installed Sample value: w2khost
Last Modified Time Stamp	Date and time at which the last AD User reconciliation run was completed The reconciliation engine automatically fills a value in this attribute each time it runs the AD User reconciliation. Default value: 0
Last Modified Time Stamp Group	Date and time at which the last AD Group reconciliation run was completed The reconciliation engine automatically fills a value in this attribute each time it runs AD Group reconciliation. Default value: 0
Use SSL	Specifies whether or not to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory Default value: false
SSL Port Number	Port at which SSL is running on the Microsoft Active Directory server Default value: 636
AtMap ADUser	Attribute map name for the Microsoft Active Directory user Default value: AtMap.AD
AtMap Group	Attribute map name for the Microsoft Active Directory group Default value: AtMap.ADGroup

Microsoft Windows 2003

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

Parameter Name	Parameter Description
Admin FQDN	Fully qualified domain name corresponding to the admin user Format: *ADMIN_LOGIN@DOMAIN* Sample value: administrator@adomain.com
Admin Login	User ID of the administrator account that is used to create the OU/user Sample value: administrator
Admin Password	Password of the administrator account that is used to create the OU/user Sample value: password
Root Context	Usually, this is the fully qualified domain name of the parent or root organization. For example, the root suffix. Format: ou=*ORGANIZATION_NAME*,dc=*DOMAIN* Sample value: ou=Adapters,dc=adomain,dc=com
Server Address	Host name or IP address of the target Microsoft Windows 2000 computer on which Microsoft Active Directory is installed Sample value: w2003host
Last Modified Time Stamp	Date and time at which the last AD User reconciliation run was completed The reconciliation engine automatically fills a value in this attribute each time it runs the AD User reconciliation. Default value: 0
Last Modified Time Stamp Group	Date and time at which the last AD Group reconciliation run was completed The reconciliation engine automatically fills a value in this attribute each time it runs AD Group reconciliation. Default value: 0
Use SSL	Specifies whether or not to use SSL to secure communication between Oracle Identity Manager and Microsoft Active Directory Default value: false
SSL Port Number	Port at which SSL is running on the Microsoft Active Directory server Default value: 636
AtMap ADUser	Attribute map name for the Microsoft Active Directory user Default value: AtMap.AD
AtMap Group	This is the attribute map name for the Microsoft Active Directory group. Default value: AtMap.ADGroup

Step 5: Configuring Reconciliation

Configuring reconciliation involves performing the following tasks:

- Adding Prerequisites for Reconciliation

- Creating Scheduled Tasks for Reconciliation

Adding Prerequisites for Reconciliation

Microsoft Active Directory reconciliation provides a mechanism for customizing the list of fields that are reconciled. Refer to Appendix A for information about this feature. To use this feature, you must perform the following prerequisite steps:

1. Open **Lookup.ADReconciliation.FieldMap** from the Lookup Definition form in the Oracle Identity Manager Design Console.
2. Add the required fields to the field map.

In addition, this connector also supports trusted source reconciliation. Before you implement trusted source reconciliation, you must perform the following prerequisite steps:

1. Open the Resource Object form.
2. Search for the Xellerate User.
3. On the Object Reconciliation tab, add reconciliation fields as required. You must add all the reconciliation fields that are required to provide input for mandatory fields on the Xellerate User form. For example, fields like User Login and First Name. Although the Password field is a mandatory field, you can ignore it.
4. Open the Process Definition form.
5. Search for the Xellerate User.
6. On the Reconciliation Field Mappings tab, add the reconciliation field mappings as required. All the mandatory fields of the User Defined process form must be mapped.
7. Open the Reconciliation Rules form.
8. Create a new rule for Object Xellerate User, with a rule element as required.
9. After you create the rule, select the **Active** check box.

Creating Scheduled Tasks for Reconciliation

Configuring reconciliation involves creating scheduled tasks for lookup fields and user reconciliations. To create 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. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager should attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.
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 appropriate table in the "Specifying Values for the Scheduled Task Attributes"section on page 2-7 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 define the second scheduled task.

After you define both scheduled tasks, proceed to the "Step 6: Compiling Adapters" section on page 2-9.

Specifying Values for the Scheduled Task Attributes

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

- Lookup Fields Reconciliation Scheduled Task
- User Reconciliation Scheduled Task

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

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

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

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

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

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

Attribute Name	Description	Default/Sample Value
DeleteRecon	Boolean field that specifies whether the reconciliation is an add, update, or delete reconciliation The IT resource instance for the Delete reconciliation function must point to a root context where deleted users are stored on the Microsoft Active Directory server. A value must be specified for this attribute.	Yes
FieldLookupCode	Lookup definition used for customized reconciliation Refer to Appendix A for more information. It is valid only when the UseFieldMapping attribute is set to true.	Lookup.ADReconciliation.FieldMap
MaintainHierarchy	Specifies whether or not organization hierarchy must be maintained in Microsoft Active Directory If this field is set to true, then the reconciliation scheduled task first creates an organization hierarchy similar to the organization hierarchy for Microsoft Active Directory in Oracle Identity Manager. It then performs reconciliation of users into the specific organization. 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. A value must be specified for this attribute.	Yes
XellerateObject	Name of the resource object in Oracle Identity Manager on which trusted reconciliation is to be performed This value must be Xellerate User. If you do not want trusted reconciliation to be performed, then change the value to false. A value must be specified for this attribute.	Xellerate User
Object	Name of the AD User resource object in Oracle Identity Manager on which reconciliation is performed. For example, AD User. If AD User reconciliation need not be performed, then change the value to false. A value must be specified for this attribute.	AD user
Server	IT resource instance name of the Microsoft Active Directory server A value must be specified for this attribute.	AD Server

Attribute Name	Description	Default/Sample Value
TransformLookupCode	Lookup code used for the transformation class map kept in the lookup tables It is valid only when the UseTransformMapping attribute is set to true. Refer to Appendix B for more information.	Lookup.ADReconciliation.TransformationMap
UseFieldMapping	Specifies whether or not the field mappings from the FieldLookupCode attribute must be used This is used for customized reconciliation. Refer to the "Step 5: Configuring Reconciliation" section on page 2-5 for more information.	Yes
UseTransformMapping	Specifies whether or not the transform mappings from the TransformLookupCode attribute must be used	Yes
XellerateOrg	Oracle Identity Manager organization in which reconciled users are to be stored A value must be specified for this attribute.	Xellerate Users
MultiValueAttributes	A comma-delimited list of all the multivalued Microsoft Active Directory attributes that must be reconciled For AD User Group reconciliation, enter memberOf. A value must be specified for this attribute.	memberOf
GroupObject	Name of the AD Group resource object in Oracle Identity Manager on which reconciliation is being performed If AD Group reconciliation need not be performed, then change the value to false. A value must be specified for this attribute.	AD Group

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

Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file. You must compile these adapters before you can use them to provision accounts on the target system.

- Chk Process Parent Org
- AD Move OU
- AD Get USNChanged
- AD Get OU USNCR
- Update AD Group Details
- Get Group ObjectGUID Created
- AD Delete Group
- AD Create Group

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

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 the **Compile All** option.

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

   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 adapters that you specify.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.

3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

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

Step 7: Configuring SSL

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

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

1. Installing Certificate Services
2. Enabling LDAPS
3. Setting Up the Microsoft Active Directory Certificate As a Trusted Certificate

Installing Certificate Services

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

1. Click **Start,** and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Select **Certificate Services**.
5. Follow the instructions to start Certificate Services.

Enabling LDAPS

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

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

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

7. Use the wizard to add a policy with the **Domain Controller** template.

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

Setting Up the Microsoft Active Directory Certificate As a Trusted Certificate

If the Microsoft Active Directory certificate is not issued or certified by a certification authority (CA), then set it up as a trusted certificate.

To make the Microsoft Active Directory certificate a trusted certificate, you first export the certificate and then import it into the keystore of the Oracle Identity Manager server as a trusted CA certificate.

Exporting the Microsoft Active Directory Certificate

To export the Microsoft Active Directory certificate:

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

Importing the Microsoft Active Directory Certificate

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

1. Copy the certificate to the Oracle Identity Manager server.
2. Change to the directory where you copy the certificate file, and then enter a command similar to the following:

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

   In this command:

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

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

Application Server	Certificate Store Location
JBoss Application Server	*JAVA_HOME*\jre\lib\security\cacerts
BEA WebLogic	*BEA_HOME*\java\jre\lib\security\cacerts
IBM WebSphere	*WS_HOME*\java\jre\lib\security\cacerts *WS_HOME*\etc\DummyServerTrustFile.jks

Note: For IBM WebSphere, you must also copy the `jnet.jar`, `jsee.jar`, `jcert.jar` files to the *`WS_HOME`*`\java\jre\lib\ext` directory.

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

  For example:

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

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

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

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

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

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

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

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

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

   In this line, *`N`* is a number that is not in use in the file.

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

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

3

Testing the Connector

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

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

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

I-T Provisioning Test

To perform an I-T provisioning test:

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

   ```
   set XL_HOME = xellerate_home
   ```

2. Update the `config.properties` file in the *`xellerate_home`*`\xellerate\test\config` directory. In this file, specify the values of attributes for the AD user that would get created in Microsoft Active Directory as part of the I-T test.

3. Run the `runADTest.bat` script.

   For example:

   ```
   D:\eclipse\workspace\XLIntegrations\package\ActiveDirectory\test\scripts>runADT
   est
   ```

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

Logging for Microsoft Active Directory Connectors

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

`xellerate_home``\xellerate\test\config`

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

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

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

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

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

4

Known Issues

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

- A Microsoft Active Directory user can be migrated from one Microsoft Windows Server (2000 or 2003) domain controller to another. However, if you want to move a user from one domain to another, then the organization must remain the same.
- The field name defined in the Xellerate User Reconciliation Fields form for user login must be `sAMAccountName`, so that it is consistent with the entry in Microsoft Active Directory.
- If the date field is not directly reconciled from Microsoft Active Directory, then you must set a transform mapping between the Oracle Identity Manager date field and the Microsoft Active Directory date field.
- A problem may occur when provisioning Oracle Identity Manager users to Microsoft Active Directory using Microsoft Windows 2003. The user's password must meet the minimum length requirement of 7 characters for the user to be provisioned. In addition, the password complexity requirement that is enabled must be set for the target Microsoft Windows 2003 system. Therefore, the user's password must also meet this complexity requirement. To enable the password complexity requirement, perform the following procedure:

  1. Click **Start, Settings,** and **Control Panel**.
  2. Double-click **Administrative Tools, Local Security Policy, Account Policies,** and **Password Policy**.
  3. Double-click **Password must meet complexity requirements**.
  4. In the Domain Security Policy Setting dialog box, select **Enabled** and then click **OK**.
- A problem may occur when provisioning Oracle Identity Manager users to Microsoft Active Directory using Microsoft Windows 2003. You must either select **Password Never Expires** or specify a valid date in the **Account Expiry Date** field. Otherwise, the user will be created and disabled immediately.
- During reconciliation, the actual Microsoft Active Directory user password is not reconciled. Instead, a dummy value is inserted in the User Password field in the process form.
- There is a limitation in the Create User function. When this function is run, if the **User must change password at next logon** check box is selected in the User Defined process form, then the corresponding change does not get reflected in Microsoft Active Directory.

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

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

1. Run the Create User function with the default settings in the User Defined process form.
2. After the Microsoft Active Directory user is created, in the process form, select the **User must change password at next logon** check box, and then click **Save.** This will trigger the relevant update task, and the setting gets correctly configured in Microsoft Active Directory.

- If the `Use SSL` attribute of the IT resource is set to `false` while provisioning the Microsoft Active Directory user, then the password cannot be set and updated by using Oracle Identity Manager. Therefore, if there are any existing password policies in the Microsoft Active Directory server, then you must disable them if the communication is not secured by SSL.

  To disable a password policy, perform the following procedure:

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

- While provisioning an AD User or AD Group, if the organization is not selected, then the user or group is created in the static container `CN=Users`.
- While reconciling a Microsoft Active Directory user, you can ignore the following attributes related to the Microsoft Exchange mailbox:
  - `msExchMailboxSecurityDescriptor`
  - `msExchMailboxGuid`
  - `showInAddressBook`
  - `msExchPoliciesIncluded`
  - `textEncodedORAddress`
  - `proxyAddresses`
- The `MaintainHeirarchy` option with a value `true` reconciles organization units from Microsoft Active Directory. It is recommended that you use this option with a root context in which the parent attribute is `ou`. This means that the DN of a root context must start with `ou=`. For a root context starting with elements like `dc=`, the `MaintainHeirarchy` option would not work as expected.
- To run the Move User function, you must ensure that the following prerequisite is addressed:

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

organization must be inside the `Integrations` organization in Oracle Identity Manager.

A

Installing and Deploying the Reconciliation Scheduled Task

This chapter describes the procedures involved in installing and deploying the reconciliation scheduled task. It includes the following sections:

Installing the Reconciliation Scheduled Task

The reconciliation scheduled task is completely independent of provisioning. There is no code that is common to both reconciliation and provisioning.

You must perform the following steps before you can successfully run the reconciliation scheduled task:

1. Ensure that the connector XML file is imported by performing the procedure described in the "Step 4: Importing the Connector XML Files" section on page 2-2. This step is required because the Microsoft Active Directory reconciliation scheduled task uses the IT resource that is defined in the connector XML file.
2. Import the sample Microsoft Active Directory Reconciliation task. In addition, ensure that all the required attributes in the task are correctly configured.
3. Import the `ADGroup Lookup Reconciliation` sample task. In addition, ensure that all the required attributes in the task are correctly configured.
4. If there are any transformation classes to be applied, then you must place them in a JAR file in the `JavaTasks` directory.

Deploying the Reconciliation Scheduled Task

This section describes the following task attributes from the deployment perspective:

- **`DeleteRecon:`** This attribute can be set to `true` or `false`. It is not case-sensitive. While using this attribute, 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) has to be implemented by the directory administrator. In addition, in the case of trusted reconciliation, the users that are reconciled using the Delete Reconciliation function are marked as

deleted by Oracle Identity Manager. In the case of nontrusted reconciliation, the Microsoft Active Directory resource object is revoked for such users.

- **MaintainHierarchy:** This attribute can be set to `true` or `false`. It is not case-sensitive. While using this attribute, you must ensure that no two organizations have the same name in Microsoft Active Directory, because this is a constraint in Oracle Identity Manager. If this attribute is set to `true`, then the value of the `XellerateOrg` attribute is ignored.
- **UseFieldMapping:** This attribute can be set to `true` or `false`. It is not case-sensitive. If it is set to `true`, then the value of the `FieldLookupCode` attribute is used to find the field mappings stored in the lookup tables.
- **UseTransformMapping:** This attribute can be set to `true` or `false`. It is not case-sensitive. If it is set to `true`, then the value of the `TransformLookupCode` attribute is used to get the transform mappings stored in the lookup tables.
- **FieldLookupCode:** This attribute specifies the mapping between the Microsoft Active Directory fields and virtual fields in Oracle Identity Manager. It also specifies the fields that are imported in Oracle Identity Manager during reconciliation. It 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 current reconciliation scheduled task. Therefore, you must specify the mappings between the Microsoft Active Directory fields and virtual Oracle Identity Manager fields.

  These virtual fields are then mapped to the actual fields on the process form.

  For example:

  Suppose you have two systems S1 and S2 that are being reconciled against a resource object called `ADObject`. In addition, assume that 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 -> x1
  p2 -> x2
  p3 -> x3
  q1 -> x1
  q2 -> x2
  q3 -> x3

- **TransformLookupCode:** This attribute specifies the mapping between the Microsoft Active Directory fields and the transformation to be applied to them. It is used if the values from the external systems must be modified before they can be entered into Oracle Identity Manager. There is no restriction on custom modification. The following are examples of custom modifications:
  - Append a number at the end of the user ID.
  - Look up the field name from some external system, and set the value based on the field name.

  - Set custom types, such as `Role` or `Xellerate Type` in Oracle Identity Manager, based on the value of a field in Microsoft Active Directory.

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

- **`Server:`** This attribute specifies the IT resource for the Microsoft Active Directory server from which reconciliation is to be carried out.
- **`XellerateObject:`** This attribute specifies the `Xellerate User` resource object on which trusted reconciliation is to be carried out.
- **`Object:`** This attribute specifies the `AD User` resource object on which reconciliation is to be carried out.
- **`XellerateOrg:`** This attribute gives the name of the Oracle Identity Manager organization in which reconciled users will be created. The name of this organization will be used by default unless either the `MaintainHierarchy` or the `ProcessOrg` attribute is set.
- **`MultiValueAttributes:`** The value of this attribute is interpreted as a comma-separated list of the multivalued attributes in Microsoft Active Directory, which 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.
- **`GroupObject:`** This attribute specifies the Oracle Identity Manager resource object on which reconciliation is to be carried out. The fields and mappings must be correctly created on the resource object and provisioning process for successful reconciliation. The default value of this attribute is `AD Group`.

User-Defined Reconciliation Fields

If only selective parameters need to be reconciled, then first check if the `Lookup.ADReconciliation.FieldMap` field map is present in the Lookup Definition form. If it is not present, then create it. In addition, you must add the parameters mentioned in the preceding list. The `whenChanged` parameter is a mandatory field, which means that it must be present in the field map.

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

- `sAMAccountName`
- `IT Resource`
- `objectGUID`
- `name`
- `sn`
- `cn`

- whenChanged
- distinguishedName

The UseFieldMapping attribute of the scheduled task must be set to true for selective parameter reconciliation.

Note: If the UseFieldMapping parameter is set to false, then some fields with binary values would be reconciled. This is not handled by the current release of Oracle Identity Manager.

The following are some fields that have binary values:

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

B

Code For a Sample Transformation Class

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

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

The following is one such sample class.

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

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

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

Index

P

R

S

T

U

X