Oracle® Identity Manager

Connector Guide for Microsoft Active Directory User Management

Release 9.1.1

E11197-07

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management, Release 9.1.1

E11197-07

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

2 Deploying the Connector

3 Using the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Microsoft Active Directory and Microsoft Active Directory Application Mode (ADAM).

Audience

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For generic information about connectors, see *Oracle Identity Manager Connector Concepts* in the Oracle Identity Manager Connectors documentation library.

To access the Oracle Identity Manager documents mentioned as references in this guide, visit Oracle Technology Network. The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://www.oracle.com/technology/documentation/index.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 library, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

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

This chapter provides an overview of the updates made to the software and documentation for release 9.1.1 of the Microsoft Active Directory User Management connector.

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

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  This section describes major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

Software Updates

The following software updates have been made in this release of the connector:

- Software Updates in Release 9.1.0
- Software Updates in Release 9.1.0.1
- Software Updates in Release 9.1.1

Software Updates in Release 9.1.0

The following are issues resolved in release 9.1.0:

- Support for Microsoft ADAM
- Introduction of the Connector Installer
- Introduction of Organization Reconciliation
- Introduction of Organization Lookup Synchronization
- Introduction of Scheduled Task for Reconciliation of Deleted User Records
- Introduction of Separate Scheduled Tasks for Target Resource and Trusted Source Reconciliation of User Records

- Support for the Diagnostic Dashboard
- Support for Provisioning Users to User-Defined Object Classes
- Support for Deprovisioning of Users That Have Associated Leaf Nodes on the Target System
- Support for the Application of Native LDAP Queries During Reconciliation
- Support for High-Availability Configuration of the Target System
- Support for Terminal Services Profile Fields of the Target System
- Support for Multivalued (Child) Data Field Mapping
- Support for Multiple Trusted Source Reconciliation
- Support for the E-Mail Redirection Feature in Microsoft Active Directory

Support for Microsoft ADAM

The connector can be used to integrate both Microsoft Active Directory and Microsoft Active Directory Application Mode (ADAM) with Oracle Identity Manager.

Information specific to the Microsoft ADAM has been provided at various places in this guide.

Introduction of the Connector Installer

You can now install the connector by using the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

See "Running the Connector Installer" on page 2-5 for more information.

Introduction of Organization Reconciliation

In the trusted source reconciliation mode, the connector can be configured to reconcile details of organizations on the target system. The AD Organization Recon scheduled task has been introduced to automate organization reconciliation.

See the following sections for more information:

- "Organization Reconciliation" on page 1-28
- "Guidelines on Configuring Reconciliation" on page 3-1
- "AD Organization Recon" on page 3-18

Introduction of Organization Lookup Synchronization

In the target resource mode, the connector can be configured to fetch the names of organizations on the target system and populate a lookup definition in Oracle Identity Manager.

See "Scheduled Tasks for Lookup Field Synchronization" on page 3-8 for more information.

Introduction of Scheduled Task for Reconciliation of Deleted User Records

The connector can be configured to reconcile deleted user data in both account management (target resource) and identity reconciliation (trusted source) modes. The AD User Target Delete Recon and AD User Trusted Delete Recon scheduled tasks have been introduced to automate this process.

See the following sections for more information:

- "Scheduled Tasks for Target Resource Reconciliation" on page 3-13

- "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18

Introduction of Separate Scheduled Tasks for Target Resource and Trusted Source Reconciliation of User Records

In earlier releases, the same scheduled task was used for target resource and trusted source reconciliation. In this release, the following scheduled tasks have been introduced:

- AD User Target Recon

  This scheduled task is used to fetch user data in the target resource mode. See "Scheduled Tasks for Target Resource Reconciliation" on page 3-13 for information about this scheduled task.

- AD User Target Delete Recon

  This scheduled task is used to fetch data about deleted users in the target resource mode. During a reconciliation run, for each deleted user account on the target system, the corresponding AD User resource is revoked for the OIM User. See "Scheduled Tasks for Target Resource Reconciliation" on page 3-13 for information about this scheduled task.

- AD User Trusted Recon

  This scheduled task is used to fetch user data in the trusted source mode. See "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18 for information about this scheduled task and its attributes.

- AD User Trusted Delete Recon

  This scheduled task is used to fetch data about deleted users in the trusted source mode. During a reconciliation run, for each deleted target system account, the corresponding OIM User is deleted. See "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18 for information about this scheduled task and its attributes.

Support for the Diagnostic Dashboard

In addition to support for the traditional testing utility, this connector supports the Diagnostic Dashboard. You can use this tool to test basic functionality of the connector.

See "Using the Diagnostic Dashboard" on page 5-2 for more information.

Support for Provisioning Users to User-Defined Object Classes

By default, the target system uses the user object class. You can use the Lookup.AD.Configuration lookup definition to include user-defined object classes on the target system in reconciliation and provisioning operations.

See "Configuring the Lookup.AD.Configuration Lookup Definition" on page 3-5 for more information.

Support for Deprovisioning of Users That Have Associated Leaf Nodes on the Target System

A user on the target system can have other users defined as its leaf nodes. You can configure the connector to perform one of the following actions when the user is deleted on Oracle Identity Manager:

- Delete the user and its leaf nodes from the target system.
- Display a message stating that the user has leaf nodes.

This feature is implemented through the isUserDeleteLeafNode parameter of the IT resource for the target system. See "Configuring the IT Resource for the Target System" on page 2-7 for information about this parameter.

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.

See "Limited Reconciliation vs. Regular Reconciliation" on page 3-10 for more information.

Support for High-Availability Configuration of the Target System

The connector can be configured for compatibility with high-availability target system environments. It can read information about backup target system hosts from the Lookup.AD.BackupServers lookup definition and apply this information when it is unable to connect to the primary host.

See "Configuring High Availability of the Target System" on page 2-16 for more information.

Support for Terminal Services Profile Fields of the Target System

In the target resource mode, a Remote Manager can be used in conjunction with the connector to enable reconciliation from and provisioning to the Terminal Services fields of the target system. In addition, you can add Environment, Remote Control, and Sessions fields for reconciliation and provisioning.

See the following sections for more information:

- "User Fields for Target Resource Reconciliation" on page 1-8
- "User Fields for Provisioning" on page 1-16
- "Adding New Fields for Target Resource Reconciliation" on page 4-3
- "Adding New Fields for Provisioning" on page 4-14
- "Using Your Own Provisioning Script" on page 4-27
- Appendix C, "Terminal Services Profile Field Names for Reconciliation and Provisioning"

Support for Multivalued (Child) Data Field Mapping

You can add both single-valued and multivalued fields for target resource reconciliation and provisioning.

See the following sections for more information:

- "Adding New Multivalued Fields for Target Resource Reconciliation" on page 4-8
- "Adding New Multivalued Fields for Provisioning" on page 4-21

Support for Multiple Trusted Source Reconciliation

This connector supports the Multiple Trusted Source Reconciliation feature of Oracle Identity Manager release 9.1.0 and later. See "Configuring the Connector for Multiple Trusted Source Reconciliation" on page 4-35 for more information.

Support for the E-Mail Redirection Feature in Microsoft Active Directory

You can use the E-mail Redirection feature to specify an alternative (redirection) e-mail address for a user. E-mail sent to the user is automatically directed to the account specified by the redirection e-mail address.

See "Guidelines on Performing Provisioning Operations" on page 3-3 for more information.

Software Updates in Release 9.1.0.1

The following are software updates in release 9.1.0.1:

Reconciliation of Manager IDs During Trusted Source Reconciliation

You can now enable the reconciliation of manager IDs from the target system during trusted source reconciliation. Manager ID values are stored in the Manager Login field of the OIM User form.

Issues Resolved in Release 9.1.0.1

The following are issues resolved in release 9.1.0.1:

Bug Number	Issue	Resolution
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.
7314549 and 7408391	A provisioning operation failed if you entered the comma (,) or slash (/) characters in the Full Name field.	This issue has been resolved. You can now enter special characters in the Full Name field during provisioning operations.
7324176	If the MaintainHierarchy attribute was set to `yes`, then the value specified for the User Search Base attribute had to be an OU (of the form `ou=abc,dc=...`). If the value of the User Search Base attribute was a domain controller name (of the form `dc=xyz,dc=com`), then organization hierarchy was not maintained during reconciliation.	This issue has been resolved. Organization hierarchy can be maintained during reconciliation even if the value of the User Search Base attribute is a domain controller name. For more information, see the description of the Search Filter attribute in "AD Organization Recon" on page 3-18.
7448615	During target resource reconciliation, if no match was found between a particular target system record and any existing OIM Users, then the RowIndexOutBounds exception was thrown.	This issue has been resolved. If no match is found, then an error message is recorded in the log file and reconciliation continues.

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.	This issue has been resolved. If you do not specify a value in the Expiry Date process form field, then the time zone part of the time stamp value is set to GMT (that is, GMT+00:00). Time zone conversion does not take place before the date value is stored in the target system database. See Bug 7518734 in the "Known Issues" chapter for information about a limitation related to this fix.
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 Table 1–9 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.

Software Updates in Release 9.1.1

The following are software updates in release 9.1.1:

- Microsoft Active Directory 2008 Added to the List of Certified Target Systems
- Change in the Oracle Identity Manager Requirement
- Updates Related to Changes in the Architecture of the Password Synchronization Connector
- Support for Group Provisioning
- Support for Reconciliation of Group Data
- Linking of Entries Stored in Lookup Definitions with Target System Installations
- Support for Specifying a User Principal Name Value
- Support for Creating Copies of the Connector
- No Support for Native Queries
- Introduction of the Lookup.AD.Constants Lookup Definition

- Addition of the Search Base, Search Filter, and Search Scope Attributes in All the Scheduled Tasks
- Issues Resolved in Release 9.1.1

Microsoft Active Directory 2008 Added to the List of Certified Target Systems

From this release onward, Microsoft Active Directory 2008 installed on Microsoft Windows Server 2008 with SP2 and later service packs has been added to the list of certified target systems. This has been mentioned in the "Certified Deployment Configurations" section.

Change in the Oracle Identity Manager Requirement

From this release onward, Oracle Identity Manager release 9.1.0.1 is the minimum supported Oracle Identity Manager release. This is mentioned in the "Certified Deployment Configurations" section.

Updates Related to Changes in the Architecture of the Password Synchronization Connector

The architecture of the password synchronization connector has been completely overhauled in release 9.1.1. The following changes have been made in the IT resource:

- The ADPWSYNCH ADFlag ADPWSYNCH OIMFlag, and ADPWSYNCH Installed parameters have been removed.
- To control propagation of passwords to the target system during provisioning operation, the Allow Password Provisioning parameter has been added.

See "Configuring the IT Resource for the Target System" for more information.

Support for Group Provisioning

From this release onward, the connector supports group provisioning operations. The following changes have been made:

The AtMap ADGroup parameter has been added in the IT resource. This parameter holds the name of the lookup definition that stores group field mappings between Oracle Identity Manager and the target system. These field mappings are listed in the "Group Fields for Provisioning" section.

Support for Reconciliation of Group Data

From this release onward, the connector supports reconciliation of group data. The AD Group Recon scheduled task is used to automate reconciliation of group data.

See the following sections for more information:

- Group Fields for Reconciliation
- Scheduled Tasks for Target Resource Reconciliation

Linking of Entries Stored in Lookup Definitions with Target System Installations

From this release onward, the IT resource name is added as a prefix to values stored in lookup definitions that are synchronized with the target system. During a provisioning operation, lookup fields are populated with values corresponding to the target system installation that you select for the operation.

See "Lookup Fields Used During Connector Operations" for more information.

Support for Specifying a User Principal Name Value

The UPN Domain parameter has been added in the IT resource. You can use this parameter to specify the domain for users. In addition, the User Principal Name field has been added on the process form. This is a mandatory field. See "Configuring the IT Resource for the Target System" for more information.

Support for Creating Copies of the Connector

The AD.Parameters lookup definition has been renamed to "Lookup.AD.Configuration." In addition, new entries that hold the names of the process form and the process form fields used for matching user records have been added in this lookup definition. If you create a copy of the process form, then you can specify details of the new process form in the copy of the Lookup.AD.Configuration lookup definition. This feature enables you to create multiple copies of the connector without making code-level changes.

See the following sections for more information:

- Configuring the Lookup.AD.Configuration Lookup Definition
- Creating Copies of the Connector

No Support for Native Queries

You use the Query attribute of the user reconciliation scheduled tasks to specify the query condition that must be applied during reconciliation. In earlier releases, you used the isNativequery attribute to specify that the query condition was in native LDAP format. From this release onward, you can use only native LDAP queries. The Use Native Query attribute has been removed from the scheduled tasks.

See "Limited Reconciliation vs. Regular Reconciliation" for more information.

Introduction of the Lookup.AD.Constants Lookup Definition

The Lookup.AD.Constants lookup definition stores the constants and variables defined in the Java classes that constitute the connector.

Caution: You must not change any entry in the Lookup.AD.Constants lookup definition. If you change any entry, then the connector will not function correctly.

The name of this lookup definition is specified as the value of the Constants Lookup Code Key in the Lookup.AD.Configuration lookup definition.

Addition of the Search Base, Search Filter, and Search Scope Attributes in All the Scheduled Tasks

From this release onward, you can specify the subset of records that must be reconciled from the target system. The Search Base, Search Filter, and Search Scope attributes have been added in all scheduled tasks except the scheduled tasks for reconciliation of deleted users. See "Reconciliation Scheduled Tasks" for more information.

Issues Resolved in Release 9.1.1

The following are issues resolved in release 9.1.1:

Bug Number	Issue	Resolution
Bugs 7489859 and 7455700	The cn value of a user could not be changed through a provisioning operation on Oracle Identity Manager.	This issue has been resolved. The Common Name field has been introduced on the process form. This field is mapped to the cn field of the target system. Like the Full Name field, the Common Name field is populated with a value in the following format: *FIRST_NAME MIDDLE_NAME LAST_NAME* For example: `John Joseph Doe` You can modify this field through provisioning operations. This field has been added for both Microsoft Active Directory and ADAM. See the following sections for more information: ■ User Provisioning Functions Supported by the Connector ■ User Fields for Provisioning
5404679	If a user was a member of more than 1000 groups, then the user could not be reconciled.	This issue can be resolved by changing the value of the MaxValRange parameter on the target system.
7673487	You could not create and use a new process form. You could only use the predefined process form.	This issue has been resolved. The Lookup.AD.Configuration lookup definition has been extended to include the following entries: ■ ROFormName ■ ROUserGUID ■ ROUserID ■ ROUserManager If you create a process form, then you must provide values for these entries. See "Configuring the Lookup.AD.Configuration Lookup Definition" for more information.
7336488	You could not specify the Oracle Identity Manager organization into which you wanted to reconcile group records. **Note:** This issue was encountered in an earlier patch release of the connector in which group data reconciliation had been implemented.	This issue has been resolved. The following attributes have been included in the AD Group Recon scheduled tasks: ■ Use Organization Name ■ Organization Name See "AD Group Recon" for more information.
7693562 and 8205269	During provisioning operations, the Organization Name field is populated with values from the Lookup.ADReconciliation.Organization lookup definition. In the earlier release, instead of Decode values, Code Key values were displayed in the Organization Name field on the Administrative and User Console.	This issue has been resolved. Decode values of the lookup definition are displayed during provisioning operations.

Bug Number	Issue	Resolution
8269888	You use the LdapUserDNPrefix entry in the Lookup.AD.Configuration lookup definition to specify the LDAP attribute for forming the relative DN or user account DN. This DN value forms the logon attribute for creating the user. In the earlier release, this feature did not work if you changed the value from cn to any other attribute.	This issue has been resolved. You can now change the value of the LdapUserDNPrefix parameter from cn to any other attribute. See "Configuring the Lookup.AD.Configuration Lookup Definition" for information about the LdapUserDNPrefix parameter.
8222203	Suppose you provisioned a Microsoft Active Directory resource to an OIM User and then changed the user ID of the account on the target system. During the next reconciliation run, no match was found with the resource on Oracle Identity Manager.	This issue has been resolved. The reconciliation rule for target resource reconciliation has been modified so that the objectGUID of the account on the target system is first compared with the objectGUID of the resource on Oracle Identity Manager. See "Reconciliation Rules for Target Resource Reconciliation" for more information.
7668437	The Disable User provisioning operation failed if the Full Name field contained the slash (/) character.	This issue has been resolved. The Disable User provisioning operation works even if the Full Name field contains the slash (/) character.
7540967	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.
7384799	During a Create User provisioning operation, if you specified a group to which you wanted to assign the user, then the provisioning operation failed.	This issue has been resolved. You can now specify the group to which you want to assign a user during a provisioning operation.
7320836	Target resource reconciliation in batched mode stopped prematurely, even though no error was encountered.	This issue has been resolved.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Releases 9.1.0 and 9.1.0.1

Documentation-Specific Updates in Releases 9.1.0 and 9.1.0.1

Major changes have been made in the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usabiliy of information provided by the guide.

See "Roadmap for Deploying and Using the Connector" on page 1-30 for detailed information about the organization of content in this guide.

Documentation-Specific Updates in Release 9.1.1

The following are documentation-specific updates in release 9.1.1:

- In the "Known Issues" chapter:
  - Bug 7518734 has been removed. The issue described by this bug was addressed when Bug 7450317 was resolved in release 9.1.0.1.
  - Descriptions for Bugs 7126712, 8346302, 7207232, and 6736667 have been added.
- In the "Installing the Remote Manager" section, information about location for installing Remote Manager has been modified.
- 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 Deployment Configurations" section, changes have been made in the "Target systems and target system host platforms" row.
- In the "User Provisioning Functions Supported by the Connector" section, the following functions have been added to the list of supported provisioning functions:

  Create OU

  Rename OU

  Move OU

  Delete OU

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 external, identity-aware applications. This guide discusses the connector that enables you to use Microsoft Active Directory or Microsoft Active Directory Application Mode (ADAM) either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

> **Note:** At some places in this guide, Microsoft Active Directory and Microsoft ADAM have been referred to as the **target systems.**

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

> **Note:** It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.

This chapter contains the following sections:

1.1 Certified Deployment Configurations

The target system can be Microsoft Active Directory or Microsoft ADAM. Table 1–1 lists the certified deployment configurations for both target systems.

Table 1–1 Certified Deployment Configurations

Item	Requirement for Microsoft Active Directory	Requirement for Microsoft ADAM
Oracle Identity Manager	Oracle Identity Manager release 9.1.0.1 or later	Oracle Identity Manager release 9.1.0.1 or later
Target systems and target system host platforms	The target system can be any one of the following: ■ Microsoft Windows Server 2003 Active Directory installed on Microsoft Windows Server 2003 with SP1 or later service packs **Note:** On a Microsoft Windows 2003 server on which SP1 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 ■ Microsoft Windows Server 2008 Active Directory installed on Microsoft Windows Server 2008	Microsoft Windows Server 2003 Active Directory Application Mode with SP1 installed on Microsoft Windows Server 2003 with SP1 or later service packs **Note:** On a Microsoft Windows 2003 server on which SP1 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	Certificate Services

1.2 Certified Languages

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

1.3 Features of the Connector

This section discusses the following topics:

- The "Connector Architecture" section describes the architecture of the connector.
- The following sections describe features of the target resource mode:
  - Lookup Fields Used During Connector Operations
  - Target Resource Reconciliation
  - Provisioning
- The "Trusted Source Reconciliation" section describes features of the trusted source mode.

1.3.1 Connector Architecture

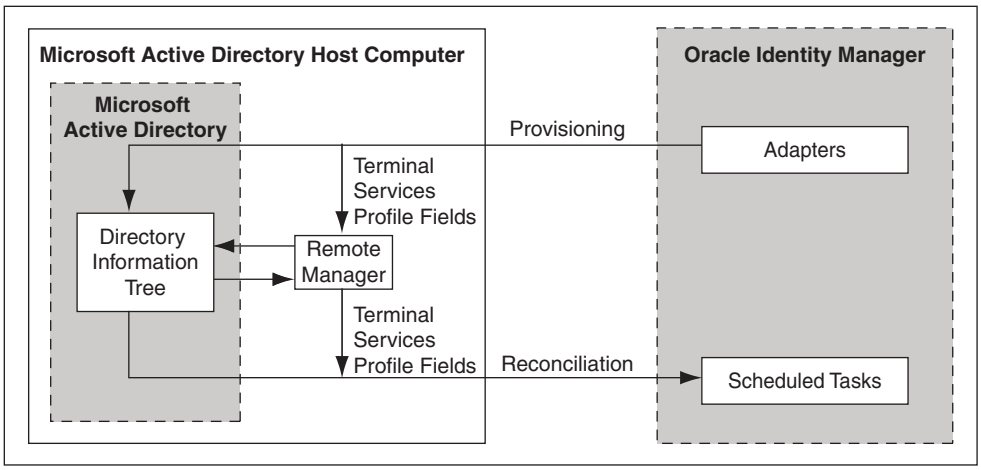
This section discusses the following topics:

- Architecture of the Connector for Microsoft Active Directory
- Connector for Microsoft ADAM

1.3.1.1 Architecture of the Connector for Microsoft Active Directory

Figure 1–1 shows the architecture of the connector for Microsoft Active Directory.

Figure 1–1 Architecture of the Connector for Microsoft Active Directory



The connector can be configured to run in one of the following modes:

- Identity reconciliation

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this form of reconciliation, OIM Users are created or updated corresponding to the creation of and updates to users on the target system. This mode also supports reconciliation of organizations (OUs) created on the target system.

- Account Management

  Account management is also known as target resource management. This mode of the connector enables the following operations:

  - Provisioning

    Provisioning involves creating or updating users on the target system through Oracle Identity Manager. When you allocate (or provision) a Microsoft Active Directory resource to an OIM User, the operation results in the creation of an

account on Microsoft Active Directory for that user. In the Oracle Identity Manager context, the term "provisioning" is also used to mean updates made to the target system account through Oracle Identity Manager.

Users and organizations are organized in hierarchical format on the target system. Before you can provision users to (that is, create users in) the required organizational units (OUs) on the target system, you must fetch into Oracle Identity Manager the list of OUs used on the target system. This is achieved by using a lookup synchronization scheduled task.

The connector enables group assignment provisioning operations in which you set or change the target system group membership profiles of users. The connector also supports provisioning (updating) of the Windows Terminal Services Profile attributes. Accessing these attributes involves the use of components that are native to the Microsoft Windows platform. The connector uses a Remote Manager to update the Terminal Services Profile fields.

– Target resource reconciliation

  The connector applies filters to locate users to be reconciled from the target system and then fetches the attribute values of these users. The Remote Manager used to enable propagation of Terminal Services Profile field values during provisioning is also used to enable the connector to fetch values from these fields during reconciliation.

Password Synchronization

This connector cannot propagate password changes from Microsoft Active Directory to Oracle Identity Manager. To implement this feature, you must install the Microsoft Active Directory password synchronization connector. See *Oracle Identity Manager Connector Guide for Microsoft Active Directory Password Synchronization* for more information. That guide describes scenarios in which both the password synchronization connector and this connector are deployed.

Other Major Features of the Connector

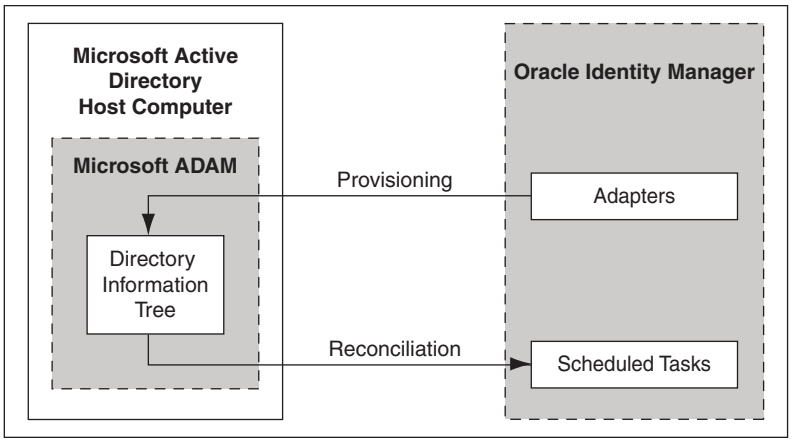
The following are other major features of the connector:

- The connector is compatible with high-availability target system environments. You can store information about backup target system hosts in an Oracle Identity Manager lookup definition. If the connector is unable to connect to the primary host, then it tries to connect to one of the hosts listed in the lookup definition.
- The connector can be configured to reconcile from and provision to user-defined object classes and their attributes. By default, the target system uses the user object class. The connector can be configured to accommodate additional object classes that you define on the target system.

1.3.1.2 Connector for Microsoft ADAM

Figure 1–2 shows the architecture of the connector for Microsoft ADAM.

Figure 1–2 Architecture of the Connector for Microsoft ADAM



There are minor attribute-level and operational differences in the support provided by the connector for Microsoft ADAM and Microsoft Active Directory. The field mappings defined between Oracle Identity Manager and the target system are different. The connector can be configured to integrate Microsoft ADAM for either trusted source reconciliation or account management. For Microsoft ADAM, the connector employs a set of attribute mapping rules for provisioning and reconciliation that is different from the attribute mapping rules employed for Microsoft Active Directory.

Where required, this guide provides information and instructions that are specific to Microsoft ADAM.

1.3.2 Lookup Fields Used During Connector Operations

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Country lookup field to select a country from the list of countries in the lookup field. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

The following is the format in which data is stored after lookup definition synchronization:

Code Key: *<IT_RESOURCE_KEY>~<VALUE_FROM_TARGET_SYSTEM>*

Decode: *<IT_RESOURCE_NAME>~< VALUE_FROM_TARGET_SYSTEM>*

For example, in the Lookup.ADReconciliation.GroupLookup lookup definition, values will be stored in the following format:

Code Key: *<IT_RESOURCE_KEY>~<DISTINGUISHED_NAME>*

Decode: *<IT_RESOURCE_NAME>~<DISTINGUISHED_NAME>*

During a provisioning operation, lookup fields are populated with values corresponding to the target system that you select for the operation.

The "Lookup Definition" column of Table 1–2 lists the Oracle Identity Manager lookup definitions that correspond to target system lookup fields listed in the "Target System Field" column of the table.

Table 1–2 Lookup Definitions Synchronized with the Target System

Lookup Definition	Target System Field	Scheduled Task for Synchronization
Lookup.ADReconciliation.GroupLookup	The distinguishedName field of groups	You use the AD Group Lookup Recon scheduled task to synchronize this lookup definition. This scheduled task is discussed in "Scheduled Tasks for Lookup Field Synchronization" on page 3-8.
Lookup.ADReconciliation.Organization	The distinguishedName field of organizations	You use the AD Organization Lookup Recon scheduled task to synchronize this lookup definition. This scheduled task is discussed in "Scheduled Tasks for Lookup Field Synchronization" on page 3-8.

Table 1–3 describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be entered in them after the connector is deployed.

Table 1–3 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.AD.Configuration	Values of parameters used during reconciliation and provisioning	You use this lookup definition to specify parameters that are used during both reconciliation and provisioning. This lookup definition is discussed in "Configuring the Lookup.AD.Configuration Lookup Definition" on page 3-5.
Lookup.AD.Country	Country codes and names	You manually add or update entries in this lookup definition based on the values in the Country lookup field on the target system. This lookup definition is discussed in "Configuring the Lookup.AD.Country Lookup Definition" on page 3-7.
AtMap.AD.RemoteScriptlookUp	Names of Terminal Services Profile fields of Microsoft Active Directory **Note:** This lookup definition is not used for Microsoft ADAM.	This lookup definition is prepopulated with values. The name of this lookup definition is the default value of the Remote Manager Prov Lookup parameter of the ADITResource IT resource, which is discussed in "Configuring the IT Resource for the Target System" on page 2-7.
Lookup.AD.BackupServers	Information about replicated installations of the target system used for high availability	If you have configured the target system for high availability, then perform the procedure described in "Configuring High Availability of the Target System" on page 2-16 to specify values for this lookup definition.
AtMap.AD	User field mappings between Microsoft Active Directory and Oracle Identity Manager	This lookup definition is prepopulated with values, and it is used during user provisioning operations. You can add values in this lookup definition by performing the procedure described in "Adding New Fields for Provisioning" on page 4-14.

Table 1–3 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
AtMap.ADAM	User field mappings between Microsoft ADAM and Oracle Identity Manager	This lookup definition is prepopulated with values, and it is used during user provisioning operations. You can add values in this lookup definition by performing the procedure described in "Adding New Fields for Provisioning" on page 4-14.
Lookup.ADReconciliation.FieldMap	User field mappings between Microsoft Active Directory and Oracle Identity Manager	This lookup definition is prepopulated with values, and it is used during user reconciliation operations. You can add values in this lookup definition by performing the procedure described in "Adding New Fields for Target Resource Reconciliation" on page 4-3 and "Adding New Fields for Trusted Source Reconciliation" on page 4-29.
Lookup.ADAMReconciliation.FieldMap	User field mappings between Microsoft ADAM and Oracle Identity Manager	This lookup definition is prepopulated with values, and it is used during user reconciliation operations. You can add values in this lookup definition by performing the procedure described in "Adding New Fields for Target Resource Reconciliation" on page 4-3 and "Adding New Fields for Trusted Source Reconciliation" on page 4-29.
AtMap.ADGroup	Group field mappings between Microsoft Active Directory and Oracle Identity Manager	This lookup definition is prepopulated with values, and it is used during group provisioning operations. You can add values in this lookup definition by performing the procedure described in "Adding New Fields for Provisioning" on page 4-14.
AtMap.ADAMGroup	Group field mappings between Microsoft ADAM and Oracle Identity Manager	This lookup definition is prepopulated with values, and it is used during group provisioning operations. You can add values in this lookup definition by performing the procedure described in "Adding New Fields for Provisioning" on page 4-14.
Lookup.AD.Constants	Names of constants and variables defined in the Java classes that constitute the connector	You must not change the predefined values in this lookup definition.

Table 1–3 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.ADGroupReconciliation.FieldMap	Group field mappings between Microsoft Active Directory and Oracle Identity Manager	This lookup definition is prepopulated with values, and it is used during group reconciliation operations. You can add values in this lookup definition by performing the procedure described in "Adding New Fields for Target Resource Reconciliation" on page 4-3.
Lookup.ADAMGroupReconciliation.FieldMap	Group field mappings between Microsoft ADAM and Oracle Identity Manager	This lookup definition is prepopulated with values, and it is used during group reconciliation operations. You can add values in this lookup definition by performing the procedure described in "Adding New Fields for Target Resource Reconciliation" on page 4-3.
AtMap.RM	Names of constants that are used to represent Terminal Services Profile fields of Microsoft Active Directory **Note:** This lookup definition is not used for Microsoft ADAM.	This lookup definition is used to hold names of constants that are used to represent Terminal Services Profile fields of Microsoft Active Directory. You must not change the predefined values in this lookup definition.

1.3.3 Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to OIM Users.

The AD User Target Recon scheduled task is used to initiate a target resource reconciliation run. This scheduled task is discussed in "Scheduled Tasks for Target Resource Reconciliation" on page 3-13.

> **See Also:** The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about target resource reconciliation

This section discusses the following topics:

- User Fields for Target Resource Reconciliation
- Reconciliation Rules for Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation

1.3.3.1 User Fields for Target Resource Reconciliation

Table 1–4 lists the user identity fields whose values are fetched during a target resource reconciliation run. The Remote Manager is used to implement the reconciliation of Terminal Services Profile fields.

Table 1–4 User Fields for Target Resource Reconciliation

Process Form Field	Target System Field	Description
User must change password at next logon This is a check box.	■ pwdLastSet (in Microsoft Active Directory) ■ msDS-UserPasswordExpired (in Microsoft ADAM)	Flag that indicates whether or not the user must change the password at next logon. If the value is `yes` (check box is selected), then the user must change the password at next logon.
Password never expires This is a check box.	■ userAccountControl (in Microsoft Active Directory) ■ msDS-UserDontExpirePassword (in Microsoft ADAM)	Flag that controls the Password Never Expires property
Account Expiration Date This is a date field.	accountExpires On Microsoft ADAM 2003, the value is stored in time-stamp format. For example: `129069486000000000` On Microsoft ADAM 2008, the value is stored in date format. For example: `3-1-2010` This is a mandatory field. On Microsoft ADAM 2003, you can enter **0** while creating an account.	Date when the account expires
First Name	givenName This is a mandatory field.	First name
Last Name This is a mandatory field.	sn This is a mandatory field.	Last name
Middle Name	initials	Initials for the user's middle name
Full Name This is a mandatory field.	displayName This is a mandatory field.	Full name
Telephone Number	telephoneNumber	Telephone number
E Mail	mail	E-mail address
Post Office Box	postOfficeBox	Post-office box
State	st	State
Zip	postalCode	ZIP code
Home Phone	homePhone	Home phone number
Pager	pager	Pager number
Mobile	mobile	Mobile number
Fax	facsimileTelephoneNumber	Fax number
IP Phone	ipPhone	IP phone number
Department	department	Department
Title	title	Title
Company	company	Company
Country This is a lookup field.	c	Country
Street	StreetAddress	Street address

Table 1–4 (Cont.) User Fields for Target Resource Reconciliation

Process Form Field	Target System Field	Description
Manager Name	manager	Manager name
Office	physicalDeliveryOfficeName	Office location
City	l	City
User ID This is a mandatory field.	sAMAccountName This is a mandatory field in Microsoft Active Directory. This field does not exist in Microsoft ADAM.	User's logon name
Terminal Home Directory This is a string data type field.	Part of the data stored in the userParameters field **Note:** This field does not exist in Microsoft ADAM.	Full path of the home directory for the Terminal Server user **Note:** Reconciliation of values in this field is enabled by the Remote Manager.
Terminal Profile Path This is a string data type field.	Part of the data stored in the userParameters field **Note:** This field does not exist in Microsoft ADAM.	Profile that is used when the user logs on to a Terminal Server The profile can be roaming or mandatory. A roaming profile remains the same, regardless of the computer from which the user logs in. The user can make changes to a roaming profile, but not to a mandatory profile. Any changes a user makes while logged in with a mandatory profile are retained only for that Terminal Services session. Changes are lost when the user starts another Terminal Services session. **Note:** Reconciliation of values in this field is enabled by the Remote Manager.
Terminal Services Allow Login This is a check box.	Part of the data stored in the userParameters field **Note:** This field does not exist in Microsoft ADAM.	Specifies whether or not the user is permitted to log on to the Terminal Server **Note:** Reconciliation of values in this field is enabled by the Remote Manager. If the target system is Microsoft Windows 2003, then the "Allow logon to terminal server" check box is used. During a reconciliation run, if the target system check box is selected, then the corresponding process form check box is selected. If the target system is Microsoft Windows 2003 with SP2, then the "Deny this user permissions to log on to any Terminal Server" check box is used. During a reconciliation run, if the target system check box is selected, then the corresponding process form check box is deselected.
Account is Locked Out This is a check box.	lockoutTime	Specifies whether the user account must be locked or unlocked

Table 1–4 (Cont.) User Fields for Target Resource Reconciliation

Process Form Field	Target System Field	Description
Group Name This multivalued field is a lookup field on the process form.	memberOf	Distinguished names of the groups to which a user belongs
User Principal Name This is a mandatory field.	userPrincipalName This is a mandatory field on the target system.	The user principal name is the domain-specific name of the user. The format is as follows: `USER_ID_VALUE@UPN_DOMAIN_VALUE`
Common Name This is a mandatory field.	cn This is a mandatory field.	Common name on the target system You can change the value of this field.
Organization Name	The organization name is extracted from the distinguishedName value.	Organization name on the target system

1.3.3.2 Group Fields for Reconciliation

Table 1–8 lists the group fields of the target system from which values are fetched during reconciliation. The AD Group Recon scheduled task is used to reconcile group data.

Note: While creating a group on Microsoft ADAM, you must provide values for the cn and displayName fields. These are mandatory fields on Microsoft ADAM.

Table 1–5 Group Fields for Reconciliation

Group Field on Oracle Identity Manager	Microsoft Active Directory Field	Microsoft ADAM Field	Description
Organization Name	ou extracted from the distinguishedName of the group	ou extracted from the distinguishedName of the group	Organization name
Group objectGUID	objectGUID	objectGUID	Group objectGUID
Group type	groupType	groupType	Group type
Group name This is a mandatory field.	sAMAccountName This is a mandatory field.	displayName This is a mandatory field.	Group name
Group Display Name	cn	cn	Common name of the group

These field mappings are stored in the following lookup definitions:

- For Microsoft Active Directory: Lookup.ADGroupReconciliation.FieldMap
- For Microsoft ADAM: Lookup.ADAMGroupReconciliation.FieldMap

1.3.3.3 Reconciliation Rules for Target Resource Reconciliation

See Also: *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following is the process matching rule:

Rule name: Target Resource Recon Rule

Rule element: (ObjectGUID Equals objectGUID) OR (User Login Equals User ID)

In the first rule component:

- ObjectGUID to the left of "Equals" is the objectGUID of the resource assigned to the OIM User.
- objectGUID to the right of "Equals" is the objectGUID of the resource on the target system.

In the second rule component:

- User Login is the User ID field on the OIM User form.
- User ID is the sAMAccountName field of Microsoft Active Directory or the userPrincipalName field of Microsoft ADAM.

This rule supports the following scenarios:

- You can provision multiple Microsoft Active Directory resources to the same OIM User, either on Oracle Identity Manager or directly on the target system.
- You can change the user ID of a user on the target system.

This is illustrated by the following use cases:

- Use case 1: You provision an AD account for an OIM User, and you also create an account for the user directly on the target system.

  When the first rule condition is applied, no match is found. Then, the second rule condition is applied and it is determined that a second account has been given to the user on the target system. Details of this second account are associated with the OIM User by the reconciliation engine.
- Use case 2: An OIM User has an AD account. You then change the user ID of the user on the target system.

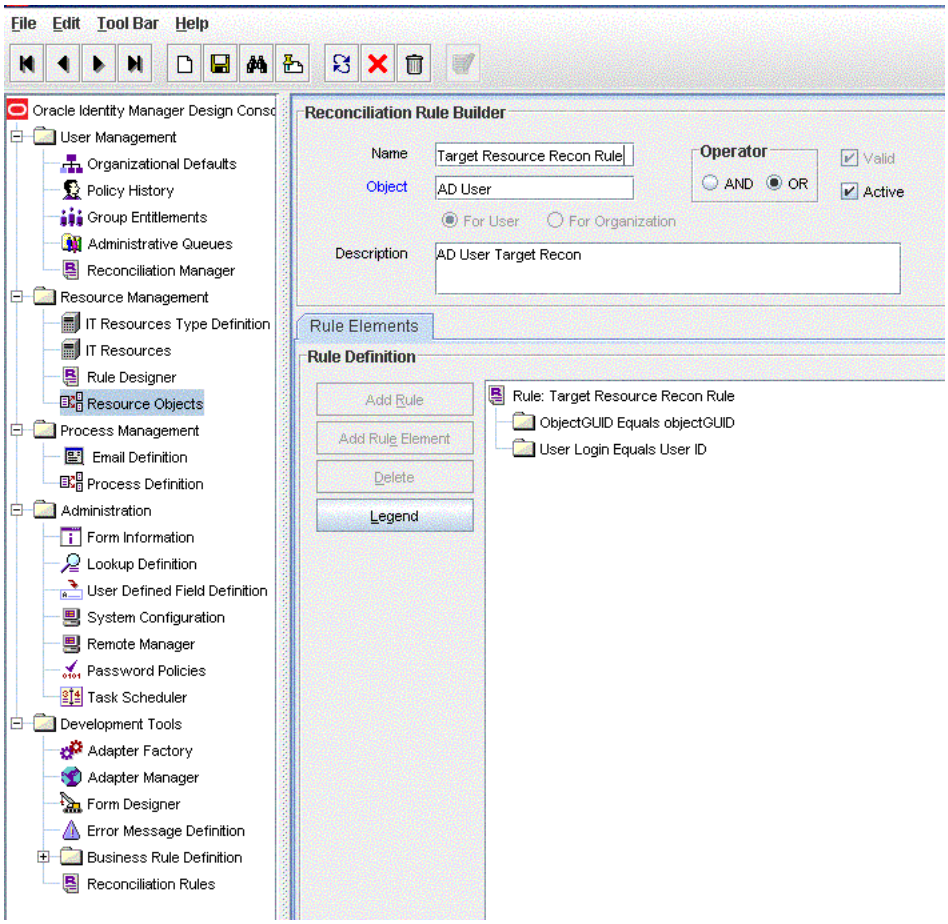
  During the next reconciliation run, application of the first rule condition helps match the resource with the record.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Target Resource Recon Rule**. Figure 1–3 shows the reconciliation rule for target resource reconciliation.

Figure 1–3 Reconciliation Rule for Target Resource Reconciliation



1.3.3.4 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–6 lists the action rules for target resource reconciliation.

Table 1–6 Action Rules for Target Resource Reconciliation

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

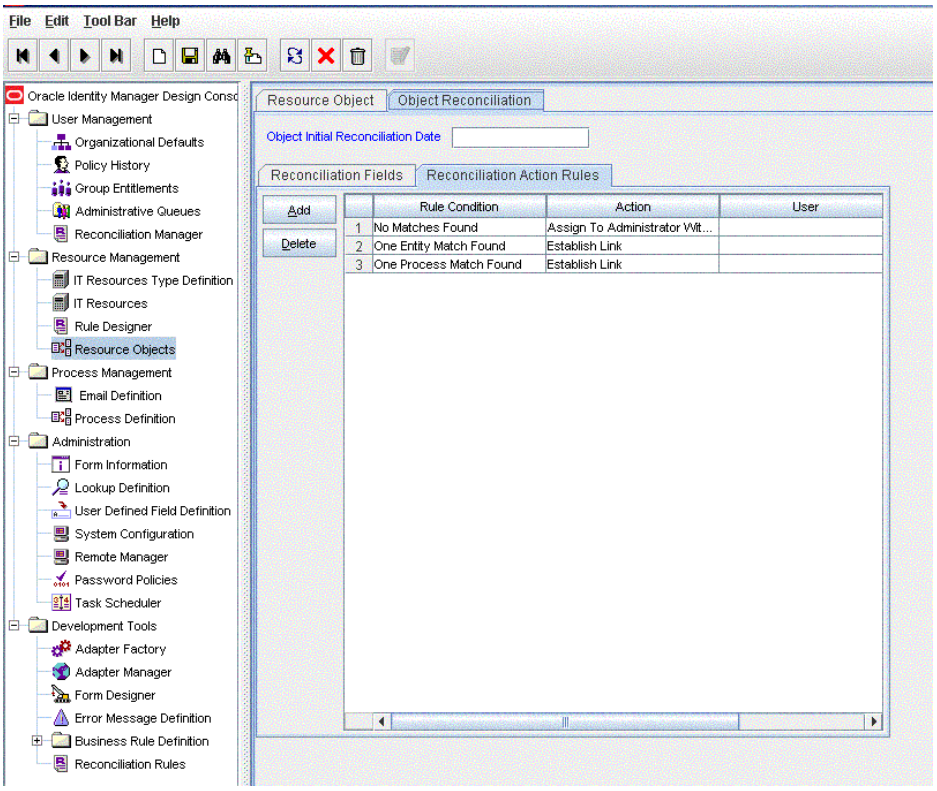
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.

3. Double-click **Resource Objects**.
4. Search for and open the **AD User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–4 shows the reconciliation action rule for target resource reconciliation.

Figure 1–4 Reconciliation Action Rules for Target Resource Reconciliation



1.3.4 Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

> **See Also:** The "Provisioning" section in *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning

This section discusses the following topics:

- User Provisioning Functions Supported by the Connector
- User Fields for Provisioning
- Group Fields for Provisioning

1.3.4.1 User Provisioning Functions Supported by the Connector

Table 1–7 lists the supported user provisioning functions and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

See Also: *Oracle Identity Manager Connector Concepts* for generic information about process tasks and adapters

Table 1–7 User Provisioning Functions Supported by the Connector

Function	Adapter
Create a user account	ADCS Create User If the user is successfully created, then the following adapters are triggered: ■ ADCS Get ObjectGUID ■ ADCS Pwd Never Expires ■ ADCS Must Change PWD ■ ADCS Set Account Exp Date ■ ADCS Execute Remote Script **Note:** If you do not want the ADCS Execute Remote Script adapter to run during the Create User provisioning operation, then see "Removing the ExecuteRemoteScripts Process Task" on page 4-28. The ADCS Execute Remote Script adapter is not used in Microsoft ADAM.
Move a user account from one organization to another in the same domain	ADCS Move User
Delete a user account	ADCS Delete User
Enable a disabled user account	ADCS Enable User
Disable a user account	ADCS Disable User
Lock a user account	ADCS Lock_Unlock User
Unlock a user account	ADCS Lock_Unlock User
Update the "User Must Change Password at Next Logon" flag	ADCS Must Change PWD
Update the account expiration date	ADCS Set Account Exp Date
Update the "Password Never Expires" flag	ADCS Pwd Never Expires
Update the user ID	ADCS Change Attribute
Update the first name	ADCS Change Attribute
Update the last name	ADCS Change Attribute
Update common name	ADCS Rename User Account
Update the password **Note:** The password can be changed only if SSL communication is configured between Oracle Identity Manager and the target system. The procedure to configure SSL is described later in the guide.	ADCS Set User Password
Add a user account to a group	ADCS ADD User To Group
Remove a user account from a group	ADCS Remove User From Group
Update the redirection e-mail address	ADCS Update Redirect Mail ID
Update middle name	ADCS Change Attribute
Update city	ADCS Change Attribute

Table 1–7 (Cont.) User Provisioning Functions Supported by the Connector

Function	Adapter
Update company	ADCS Change Attribute
Update country	ADCS Change Attribute
Update department	ADCS Change Attribute
Update e-mail address	ADCS Change Attribute
Update fax number	ADCS Change Attribute
Update IP phone number	ADCS Change Attribute
Update manager name	ADCS Change Attribute
Update mobile number	ADCS Change Attribute
Update office phone number	ADCS Change Attribute
Create OU	ADCS Create OU
Rename OU	ADCS Change Org Name
Move OU	ADCS Move OU
Delete OU	ADCS Delete OU

1.3.4.2 User Fields for Provisioning

Table 1–8 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations. The Remote Manager is used to implement the provisioning of Terminal Services Profile fields.

Note: The adapters listed in the Adapter column of the table are used during Update User provisioning operations. During a Create User provisioning operation, the ADCS Create User adapter is used to populate values in all the target system user fields.

Table 1–8 User Fields for Provisioning

Process Form Field	Target System Field	Description	Adapter
Password This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the Password field on the process form is prepopulated with the value entered in the Password field on the OIM User form. If SSL is configured between Oracle Identity Manager and the target system, then the Password field on the process form is a mandatory field.	unicodePwd	User's password in UTF-8 format	ADCS Set User Password
User must change password at next logon This is a check box.	▪ pwdLastSet (in Microsoft Active Directory) ▪ msDS-UserPasswordExpired (in Microsoft ADAM)	Flag that indicates whether or not the user must change the password at next logon. If the value is `yes` (check box is selected), then the user must change the password at next logon.	ADCS Must Change PWD
Password never expires This is a check box.	▪ userAccountControl (in Microsoft Active Directory) ▪ msDS-UserDontExpirePassword (in Microsoft ADAM)	Flag that controls the Password Never Expires property	ADCS Pwd Never Expire
Account Expiration Date This is a date field.	accountExpires When you create a user on Microsoft ADAM: ▪ For Microsoft ADAM 2003, the value of this attribute must be `9223372036854775807`. ▪ For Microsoft ADAM 2008, the value of this attribute must be `0`.	Date when the account expires	ADCS Set Account Exp Date
Object GUID This is a hidden field on both the process form and the OIM User form.	objectGUID	Object GUID of the user	ADCS Get ObjectGUID
Organization Name This is a lookup field.	Distinguished name of the organization	Name of the organization The isLookupDN parameter of the target system IT resource is used to specify whether you want DN values or relative DN values to be stored in the Organization Name field. This parameter is described in "Configuring the IT Resource for the Target System" on page 2-7.	ADCS Move User

Table 1–8 (Cont.) User Fields for Provisioning

Process Form Field	Target System Field	Description	Adapter
First Name This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the First Name field on the process form is prepopulated with the value entered in the First Name field on the OIM User form.	givenName	First name	ADCS Change Attribute
Last Name This field is on both the process form and the OIM User form. It is a mandatory field on the OIM User form. During a provisioning operation, the Last Name field on the process form is prepopulated with the value entered in the Last Name field on the OIM User form.	sn	Last name	ADCS Change Attribute
Middle Name This field is on both the process form and the OIM User form. During a provisioning operation, the Middle Name field on the process form is prepopulated with the value entered in the Middle Name field on the OIM User form.	initials	Initials for the user's middle name	ADCS Change Attribute

Table 1–8 (Cont.) User Fields for Provisioning

Process Form Field	Target System Field	Description	Adapter
Full Name This is a mandatory field on the process form.	cn, displayName	Display name for a user During a Create User provisioning operation, the cn and displayName fields are populated with a combination of the user's first name, middle initial, and last name entered on the OIM User form. The full name is displayed in the following format on the process form: *FIRSTNAME MIDDLE_INITIAL. LASTNAME* For example: `John M. Doe` If the middle initial is not entered, then the name is displayed as, for example, `John Doe`. During an Update provisioning operation, only the value in the displayName field is updated.	ADCS Change Attribute
Telephone Number	telephoneNumber	Telephone number	ADCS Change Attribute
E Mail This field is on both the process form and the OIM User form.	mail	E-mail address	ADCS Change Attribute
Post Office Box	postOfficeBox	Post-office box	ADCS Change Attribute
State	st	State	ADCS Change Attribute
Zip	postalCode	ZIP code	ADCS Change Attribute
Home Phone	homePhone	Home phone number	ADCS Change Attribute
Pager	pager	Pager number	ADCS Change Attribute
Mobile	mobile	Mobile number	ADCS Change Attribute
Fax	facsimileTelephoneNumber	Fax number	ADCS Change Attribute
IP Phone	ipPhone	IP phone number	ADCS Change Attribute
Department	department	Department	ADCS Change Attribute
Title	title	Title	ADCS Change Attribute

Table 1–8 (Cont.) User Fields for Provisioning

Process Form Field	Target System Field	Description	Adapter
Company	company	Company	ADCS Change Attribute
Country This is a lookup field.	c	Country	ADCS Change Attribute
Street	StreetAddress	Street address	ADCS Change Attribute
Manager Name	manager	Manager name You must enter the manager name in the DN format. For example: `cn=abc,ou=lmn,dc=corp,dc=com`	ADCS Change Attribute
Office	physicalDeliveryOfficeName	Office Location	ADCS Change Attribute
City	l	City	ADCS Change Attribute
Redirection Mail ID	ProxyAddresses	E-mail address to which e-mail sent to the user must be redirected This e-mail address overrides the one set in the E Mail field.	ADCS Update Redirect Mail ID
Account is Locked out This is a check box.	lockoutTime	Specifies whether the user account must be locked or unlocked	ADCS Lock_Unlock User
User ID This field is on both the process form and the OIM User form. It is a mandatory field. During a provisioning operation, the User ID field on the process form is prepopulated with the value entered in the User ID field on the OIM User form.	sAMAccountName This is a mandatory field in Microsoft Active Directory. This field does not exist in Microsoft ADAM.	User's logon name	ADCS Change Attribute
Group Name This multivalued field is a lookup field on the process form.	memberOf	Distinguished name of the groups to which a user belongs	The following adapters are for provisioning operations that involve changes to the memberOf field: ADCS ADD User To Group ADCS remove User From Group
Common Name	cn	Common name of the user	ADCS Rename User Account

Table 1–8 (Cont.) User Fields for Provisioning

Process Form Field	Target System Field	Description	Adapter
Terminal Home Directory	Part of the data stored in the userParameters field **Note:** This field does not exist in Microsoft ADAM. A value that you enter in this field would be ignored during provisioning operations in Microsoft ADAM.	Full path of the home directory for the Terminal Server user Sample value: `c:\MyDirectory` During a provisioning operation, you must enter the full, absolute path of the home directory, as shown in the sample value. **Note:** The Remote Manager enables provisioning operations on this field.	ADCS ExecuteRemote Script

Table 1–8 (Cont.) User Fields for Provisioning

Process Form Field	Target System Field	Description	Adapter
Terminal Profile Path	Part of the data stored in the userParameters field **Note:** This field does not exist in Microsoft ADAM. A value that you enter in this field would be ignored during provisioning operations in Microsoft ADAM.	Profile that is used when the user logs on to a Terminal Server The profile can be roaming or mandatory. A roaming profile remains the same, regardless of the computer from which the user logs in. The user can make changes to a roaming profile, but not to a mandatory profile. Any changes a user makes while logged in with a mandatory profile are retained only for that Terminal Services session. The changes are lost when the user starts another Terminal Services session. **Note:** The Remote Manager enables provisioning operations on this field.	ADCS ExecuteRemote Script
Terminal Services Allow Login This is a check box.	Part of the data stored in the userParameters field **Note:** This field does not exist in Microsoft ADAM. A value that you enter in this field would be ignored during provisioning operations in Microsoft ADAM.	Specifies whether or not the user is permitted to log on to the Terminal Server **Note:** The Remote Manager enables provisioning operations on this field. If the target system is Microsoft Windows 2003, then the "Allow logon to terminal server" check box is used. During a provisioning operation, if the process form check box is selected, then the target system check box is selected. If the target system is Microsoft Windows 2003 with SP2, then the "Deny this user permissions to log on to any Terminal Server" check box is used. During a provisioning operation, if the process form check box is selected, then the target system check box is deselected.	ADCS ExecuteRemote Script

Table 1–8 (Cont.) User Fields for Provisioning

Process Form Field	Target System Field	Description	Adapter
User Principal Name This is a mandatory field.	userPrincipalName This is a mandatory field. **Note:** The value for UserPrincipalName must be entered in the format shown in the following example: If the root context is `dc=example,dc=com` and the user ID is `user1`, then the userPrincipalName value is `user1@example.com`.	The user principal name is the domain-specific name of the user. This field is pre-populated on the Administrative and User Console. The format is as follows: *USER_ID_VALUE@UPN_DOMAIN_VALUE* **Note:** When you update this field, you can change the User ID part but you must not change the domain name. If you change the domain name, then the user will not be matched on the target system.	ADCS Change Attribute

Table 1–9 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 (")

Table 1–9 Special Characters Supported in Process Form Fields

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	+

Table 1–9 (Cont.) Special Characters Supported in Process Form Fields

Name of the Character	Character
question mark	?
right brace	}
right bracket	]
right parenthesis	)
slash	/
underscore	_

1.3.4.3 Group Fields for Provisioning

Table 1–8 lists the group fields of the target system for which you can specify or modify values during provisioning operations.

Note: The adapters listed in the Adapter column of the table are used during Update Group provisioning operations. During a Create User provisioning operation, the ADCS Create Group adapter is used to populate values in all the target system user fields.

Table 1–10 Group Fields for Provisioning

Group Field on Oracle Identity Manager	Target System Field	Description	Adapter
Organization Name	ou	Organization name	ADCS Move Group
Group Name	For Microsoft Active Directory: sAMAccountName For Microsoft ADAM: displayName	Group name	ADCS Change Group Attribute
Group objectGUID	objectGUID	Group objectGUID	ADCS Get Group ObjectGUID Created
Group Display Name	cn	Group display name	ADCS Rename Group
Group type	groupType	Group type	Not applicable for an existing user

These field mappings are stored in the following lookup definitions:

- For Microsoft Active Directory: AtMap.ADGroup
- For Microsoft ADAM: AtMap.ADAMGroup

1.3.5 Trusted Source Reconciliation

Trusted source reconciliation involves fetching data about newly created or modified accounts on the target system and using that data to create or update OIM Users.

The AD User Trusted Recon scheduled task is used to initiate a trusted source reconciliation run. This scheduled task is discussed in "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18.

> **See Also:** The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about trusted source reconciliation

This section discusses the following topics:

- User Fields for Trusted Source Reconciliation
- Reconciliation Rule for Trusted Source Reconciliation
- Reconciliation Action Rules for Trusted Source Reconciliation
- Organization Reconciliation

1.3.5.1 User Fields for Trusted Source Reconciliation

Table 1–11 lists the user identity fields whose values are fetched from the target system during a trusted source reconciliation run.

> **Note:** While creating a user on Microsoft ADAM, you must provide values for the userPrincipalName, sn, givenName, displayName, cn, and accountExpires fields. These are mandatory fields on Microsoft ADAM.
>
> On Microsoft ADAM 2003, enter 0 as the default value of the accountExpires field.

Table 1–11 User Fields for Trusted Source User Reconciliation

OIM User Form Field	Target System Field	Description
User ID This is a mandatory field.	■ sAMAccountName This is a mandatory field in Microsoft Active Directory. This field does not exist in Microsoft ADAM. ■ userPrincipalName This is a mandatory field in Microsoft ADAM. **Note:** The value for UserPrincipalName must be entered in the format shown in the following example: If the root context is `dc=example,dc=com` and the user ID is `user1`, then the userPrincipalName value is `user1@example.com`.	User's logon name
First Name This is a mandatory field.	givenName This is a mandatory field.	First name
Last Name This is a mandatory field.	sn This is a mandatory field.	Last name
Middle Name	initials	Middle name

Table 1–11 (Cont.) User Fields for Trusted Source User Reconciliation

OIM User Form Field	Target System Field	Description
Organization This is a mandatory field.	The name of the organization is extracted from the distinguished name of the organization.	This is the name of the organization to which users belong if you set the value of the Maintain Hierarchy attribute to `yes` while configuring the AD User Trusted Recon scheduled task. See "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18 for the procedure to configure this scheduled task. If Maintain Hierarchy is set to `no`, then the default organization in Oracle Identity Manager, `Xellerate Users`, is used.
E Mail	mail	E-mail address
Status	▪ userAccountControl (in Microsoft Active Directory) ▪ msDS-UserAccountDisabled (in Microsoft ADAM)	This field stores the status of the user account. See "Guidelines on Configuring Reconciliation" on page 3-1 for information about a guideline related to this field on Microsoft ADAM.

1.3.5.2 Reconciliation Rule for Trusted Source Reconciliation

See Also: *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following is the entity matching rule:

Rule name: Trusted Source Recon Rule

Rule: User Login Equals User ID

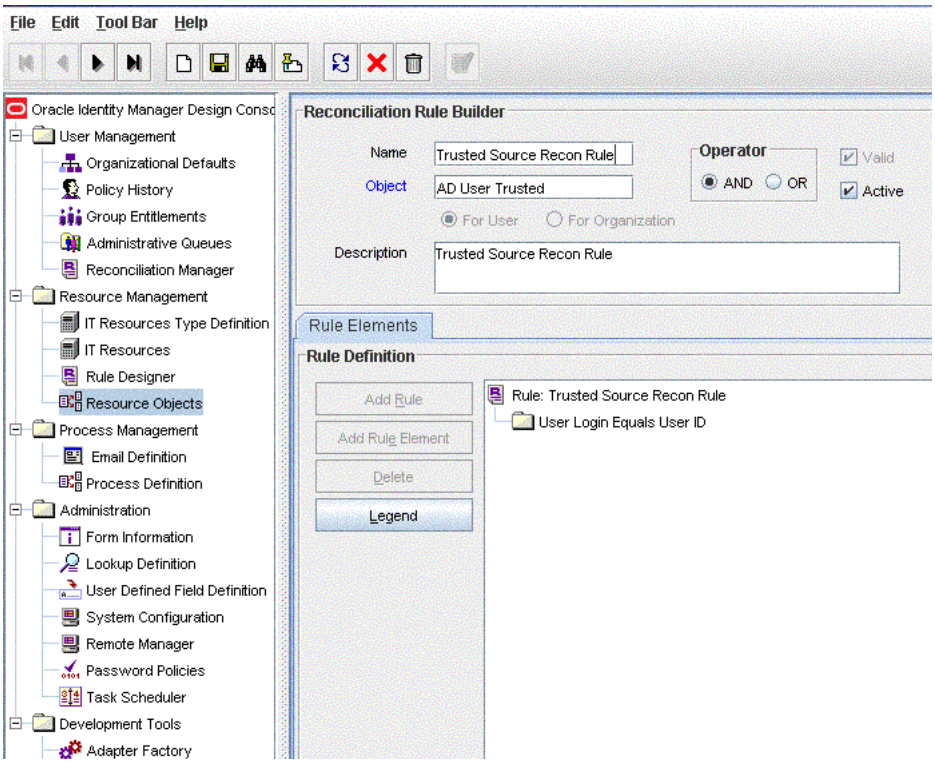
In this rule:

- User Login is the User ID field on the OIM User form.
- User ID is the sAMAccountName field of Microsoft Active Directory or the userPrincipalName field of Microsoft ADAM.

After you deploy the connector, you can view the reconciliation rule for trusted source reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Trusted Source Recon Rule**. Figure 1–5 shows the reconciliation rule for trusted source reconciliation.

Figure 1–5 Reconciliation Rule for Trusted Source Reconciliation



Note: In Microsoft Active Directory, `sAMAccountName` attribute is a mandatory and unique field.

1.3.5.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–12 lists the action rules for trusted source reconciliation.

Table 1–12 Action Rules for Trusted Source Reconciliation

Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

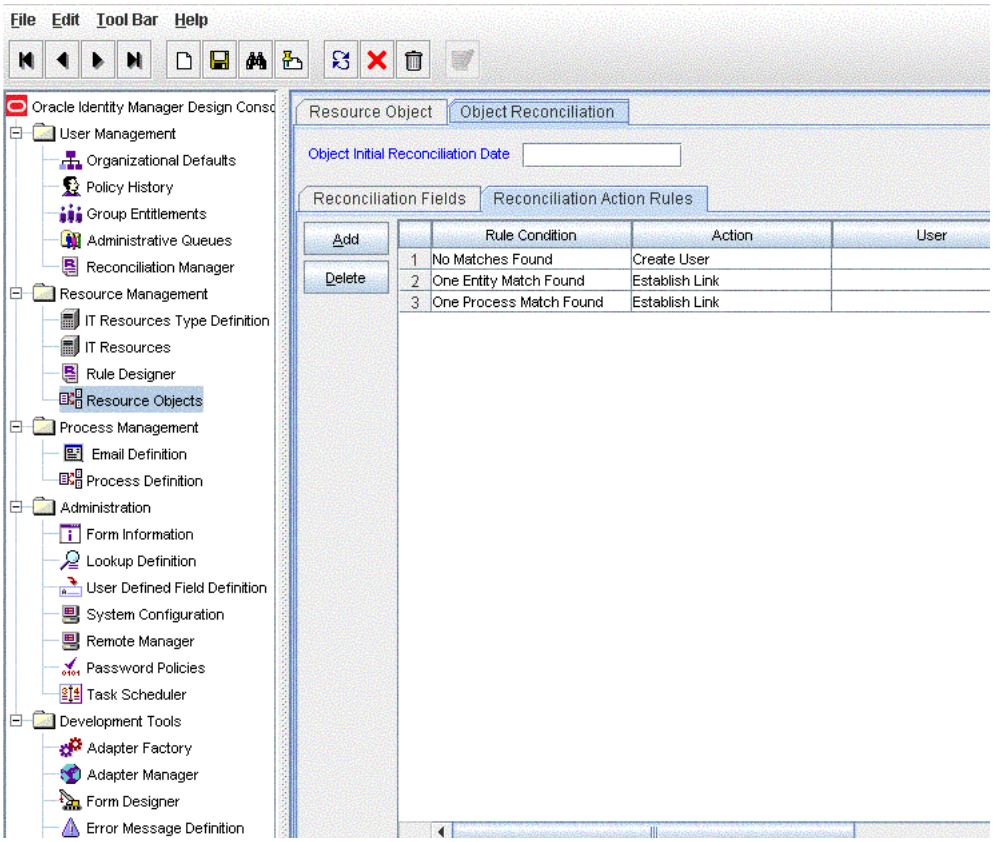
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.

3. Double-click **Resource Objects**.
4. Locate the **AD User** resource object.
5. Click the **Object Reconciliation** tab, and then the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–6 shows the reconciliation action rule for trusted source reconciliation.

Figure 1–6 Reconciliation Action Rules for Trusted Source Reconciliation



1.3.5.4 Organization Reconciliation

As mentioned earlier, trusted source reconciliation fetches data about target system users into Oracle Identity Manager. This data is used to create or update records of OIM Users. You can configure trusted source reconciliation so that newly created OIM Users are placed in OIM Organizations that correspond to users' organizations on the target system. To enable this feature, you set the value of the MaintainHierarchy attribute of the trusted source reconciliation scheduled task (AD User Trusted Recon) to `yes`.

> **Note:** The scheduled tasks mentioned in this section are discussed in detail in "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18.

To ensure that OIM Organizations corresponding to the target system organizations are created and ready for user data fetched during a trusted source reconciliation run, the organization reconciliation scheduled task (AD Organization Recon) must be run

before the scheduled task for trusted source reconciliation. When the AD Organization Recon scheduled task is run, data about target system organizations is fetched and used to create OIM Organizations.

Note:

- It is recommended that you set the MaintainHierarchy attribute to `yes` only if this option is acceptable in your operating environment. Otherwise, the default option of the MaintainHierarchy attribute set to `no` must be used while running the trusted source reconciliation scheduled task.
- The AD Organization Recon scheduled task is independent of the organization lookup synchronization scheduled task (AD Organization Lookup Recon), which is used only in the account management mode.

OIM Organizations cannot completely model the organizational structure that is found on the target system because:

- Although parent-child hierarchical relationships between organizations are supported in Oracle Identity Manager, the OIM Organizations namespace is a flat namespace. Therefore, two target system OUs that have the same name cannot be re-created in Oracle Identity Manager, even if their parent OUs are different.
- In Oracle Identity Manager, organization names cannot contain special characters such as the equal sign (=) and the comma (,). This does not permit the reconciliation of fully qualified distinguished names (FQDNs) of target system OUs into Oracle Identity Manager.
- Organization reconciliation does not cover reconciliation of updates to existing organizations on the target system. If you modify the name of an organization on the target system, then it is reconciled as a new organization in Oracle Identity Manager.

See Also: "Guidelines on Configuring Reconciliation" on page 3-1 for detailed information about guidelines on configuring organization reconciliation. Some of the points mentioned earlier are repeated in that section.

Table 1–13 lists the organization fields whose values are fetched from the target system during organization reconciliation.

Table 1–13 Organization Fields for Trusted Source Organization Reconciliation

Xellerate Organization Form Field	Target System Field	Description
Organization Name	Organization	Distinguished name of the organization
Organization Parent Name	Distinguished name of the parent organization	Name of the parent of the organization
Organization Type	-	This field is not actually reconciled, because there is no corresponding Microsoft Active Directory field. During organization reconciliation, the value of this field is set to `company`.

The following is the reconciliation rule for organization reconciliation:

Rule name: Organization Recon

Rule: Organization Name Equals Organizations.Organization Name

In this rule:

- Organization Name is the Organization Name field on the Xellerate Organization form.
- Organizations.Organization Name is the Organization Name field of Microsoft Active Directory or Microsoft ADAM.

Table 1–12 lists the action rules for organization reconciliation.

Table 1–14 Action Rules for Organization Reconciliation

Rule Condition	Action
No Matches Found	Create Organization
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.4 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 5, "Testing the Connector" describes the procedure to use the connector testing utility and the Diagnostic Dashboard for testing the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.
- Appendix A, "Character Lengths of Target System Fields and Process Form Fields" provides information about the differences in lengths of target system fields and process form fields. This appendix also describes the procedure to change the lengths of process form fields.
- Appendix B, "Special Characters Supported for Passwords" lists special characters that you can use in the Password field on the target system and Oracle Identity Manager.
- Appendix C, "Terminal Services Profile Field Names for Reconciliation and Provisioning" lists the names of special Microsoft Active Directory fields. You use these names if you want to add one of these fields for reconciliation or provisioning.
- Appendix D, "Sample Transformation Class" provides the code for a sample Java class. You can use this sample class to create a class for transforming reconciled data according to your requirements.

2

Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- Preinstallation
- Installation
- Postinstallation

> **Note:** Some of the procedures described in this chapter are meant to be performed on the target system. The minimum permissions required to perform these procedures depends on the target system that you are using:
>
> - If the target system is Microsoft Active Directory, then the permissions required are those assigned to members of the Domain Admins group.
> - If the target system is Microsoft ADAM, then the permissions required are those assigned to members of the Administrators group.

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- Preinstallation on Oracle Identity Manager
- Preinstallation on the Target System

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Files and Directories On the Installation Media
- Determining the Release Number of the Connector

2.1.1.1 Files and Directories On the Installation Media

The contents of the connector installation media directory are described in Table 2–1.

Table 2–1 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
configuration/ActiveDirectory-CI.xml	This XML file contains configuration information that is used during the connector installation process.
lib/xliActiveDirectory.jar	This JAR file contains the class files required for provisioning. During connector installation, this file is copied into the following directory: *OIM_HOME*/xellerate/JavaTasks
lib/xliADRecon.jar	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied into the following directory: *OIM_HOME*/xellerate/ScheduleTask
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied into the following directory: *OIM_HOME*/xellerate/connectorResources **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/ProvTerminalServiceAttr.vbs	This VBScript file is used to set values for Terminal Services Profile fields of the target system during provisioning operations. This script is called by the Remote Manager. While performing the procedure described in "Installing the Remote Manager" on page 2-12, you copy this file into a directory on the target system host computer.
scripts/ReconTerminalServiceAttr.vbs	This VBScript file is used to fetch values from Terminal Services Profile fields of the target system during reconciliation runs. This script is called by the Remote Manager. While performing the procedure described in "Installing the Remote Manager" on page 2-12, you copy this file into a directory on the target system host computer.
test/config/config.properties	This file is used to set input test data for the connector testing utility.
test/config/log.properties	This file is used to set log messages that must be displayed on the console when you run the connector testing utility.
test/lib/xlapiclient.ear	This EAR file contains the JAR files required to run the testing utility for Oracle Identity Manager running on IBM WebSphere Application Server.

Table 2–1 (Cont.) Files and Directories On the Installation Media

File in the Installation Media Directory	Description
test/scripts/runADTest.bat test/scripts/runADtest.sh	These scripts are used to run the testing utility.
test/scripts/wsapiclient.cmd	This file is used by the testing utility if Oracle Identity Manager is running on IBM WebSphere Application Server.
xml/ActiveDirectory-ConnectorConfig.xml	This XML file contains definitions for the connector components. These components include the following: ■ Resource objects ■ IT resource types ■ Process forms ■ Process tasks and adapters ■ Process definition ■ Prepopulate rules ■ Lookup definitions ■ Scheduled tasks

Note: The files in the test directory are used only to run tests on the connector by using the testing utility. The Diagnostic Dashboard is an alternative to the testing utility. Chapter 5, "Testing the Connector" describes both testing options.

2.1.1.2 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.

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the procedure described in the following section.

2.1.2.1 Creating a Target System User Account for Connector Operations

Oracle Identity Manager requires a target system user account to access the target system during reconciliation and provisioning operations. You provide the credentials of this user account while performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7.

In Microsoft Active Directory

You can use a Microsoft Windows 2003 Server (Domain Controller) administrator account. Alternatively, you can create a user account and assign the minimum required rights to the user account.

Note: If you want to enable the reconciliation of deleted target system records, then you must use an administrator account.

To create the Microsoft Active Directory user account for connector operations:

See Also: Microsoft Active Directory documentation for detailed information about performing this procedure

1. Create a group (for example, OIMGroup) on the target system. While creating the group, select **Security Group** as the group type and as **Global** or **Universal** as the group scope.
2. Make this group a member of the Account Operators group.
3. Assign all read permissions to this group.

Note: You assign read permissions on the Security tab of the Properties dialog box for the user account. This tab is displayed only in Advanced Features view. To switch to this view, select Advanced Features from the View menu on the Microsoft Active Directory console.

4. Create a user (for example, OIMUser) on the target system.
5. Make the user a member of the group (for example, OIMGroup) created in Step 1.

In Microsoft ADAM

To create the Microsoft ADAM user account for connector operations:

See Also: Microsoft ADAM documentation for detailed information about these steps

1. Create a user account in Microsoft ADAM.
2. Set a password for the user account.
3. Enable the user account by setting the msDS-UserAccountDisabled field to `false`.
4. Enter a value in the userPrincipalName field.

   The value that you provide must be in the *`user_name`*`@`*`domain_name`* format, for example, `OIMuser@mydomain.com`.
5. Add the distinguished name of the user to the Administrators group.

2.2 Installation

Installation steps are divided across the following sections:

- Installation on Oracle Identity Manager
- Installation on the Target System

2.2.1 Installation on Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

- Running the Connector Installer
- Copying the Connector Files
- Copying the ldapbp.jar File
- Configuring the IT Resource for the Target System

2.2.1.1 Running the Connector Installer

Note: In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Administrative and User Console.

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console Guide*.

3. Click **Deployment Management**, and then click **Install Connector**.

4. From the Connector List list, select **ActiveDirectory 9.1.1**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select **ActiveDirectory 9.1.1**.

5. Click **Load**.

6. To start the installation process, click **Continue**.

   The following tasks are performed, in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (by using the Deployment Manager)

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure is displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

   Note: At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-14 for information about running the PurgeCache utility.

   There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks

   Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–2.

Table 2–2 Files Copied During Connector Installation

File in the Connector 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

Installing the Connector in an Oracle Identity Manager Cluster

While installing the connector in a clustered environment, you must copy all the JAR files and the contents of the resources directory into the destination directories on each node of the cluster. See Table 2–2 for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

2.2.1.2 Copying the Connector Files

Table 2–3 lists the files that you must copy to the Oracle Identity Manager host computer.

Note:

- The directory paths given in the first column of this table correspond to the location of the connector files on the installation media. See "Files and Directories On the Installation Media" on page 2-1 for more information about these files.
- If a particular destination directory does not already exist on the Oracle Identity Manager host computer, then create it.

Table 2–3 Files to Be Copied to the Oracle Identity Manager Host Computer

File in the Installation Media Directory	Destination Directory
Files in the scripts directory	*OIM_HOME*/XLIntegrations/ADUM/scripts
Files in the test directory	*OIM_HOME*/XLIntegrations/ADUM/test

2.2.1.3 Copying the ldapbp.jar File

The ldapbp.jar file is used by the connector to enable LDAP-based search of user records on the target system. You must download this file from the Sun Web site and copy it into the ThirdParty directory as follows:

1. Log on the Sun Web site at

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

2. Click **Download JNDI 1.2.1 & More**.
3. From the table on the page that is displayed, select and download the ldap-1_2_4.zip file.
4. Extract the contents of the ZIP file and copy the ldapbp.jar file from the lib directory to the *OIM_HOME*/xellerate/ThirdParty directory.

> **Note:** In an Oracle Identity Manager cluster, copy this JAR file into the ThirdParty directory on each node of the cluster.

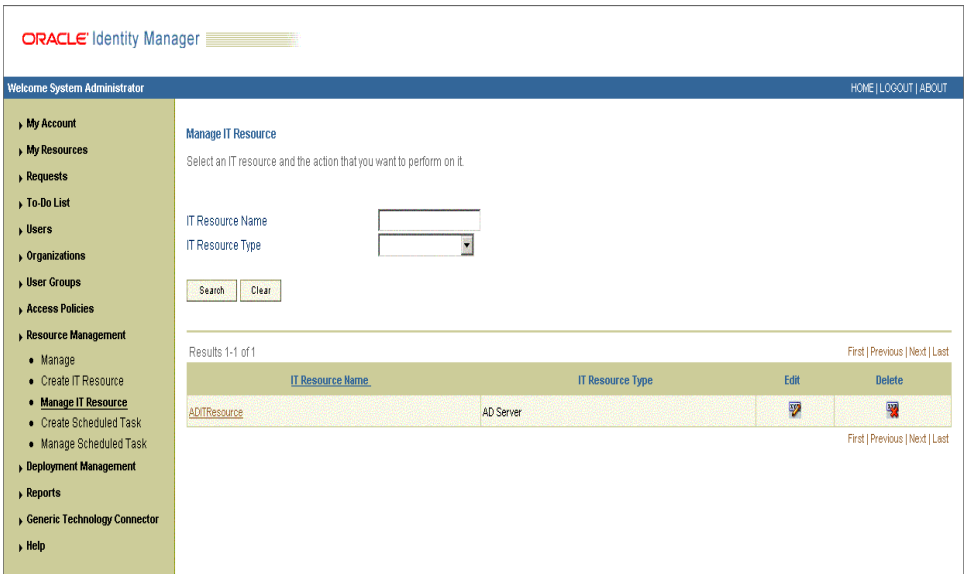
2.2.1.4 Configuring the IT Resource for the Target System

The IT resource for the target system is created during connector installation. This IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

You must specify values for the parameters of the ADITResource IT resource as follows:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter ADITResource and then click **Search**. Figure 2–1 shows the Manage IT Resource page.

Figure 2–1 Manage IT Resource Page



5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. If you are using a Remote Manager to provision to or reconcile from the Terminal Services Profile fields, then select the name of the Remote Manager.
8. Specify values for the parameters of the IT resource. Figure 2–2 shows the Edit IT Resource Details and Parameters page.

Figure 2–2 Edit IT Resource Details and Parameters Page

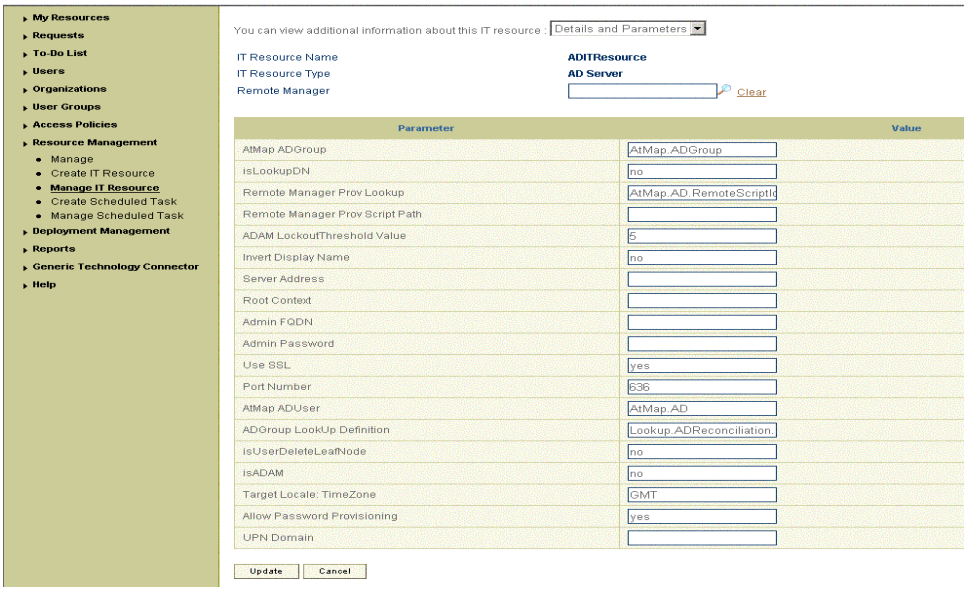


Table 2–4 describes each parameter of the IT resource.

Table 2–4 Parameters of the IT Resource for the Target System

Parameter	Description
ADAM Lockout Threshold Value	If the target system is Microsoft ADAM, then enter the number of unsuccessful login attempts after which a user's account must be locked. If the target system is Microsoft Active Directory, then you need not enter a value. The value set in Microsoft Active Directory is automatically determined and used. Default value: `5`
ADGroup LookUp Definition	This parameter holds the name of the lookup definition in which the names of group fields are stored after group lookup synchronization. Value: `Lookup.ADReconciliation.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 "Scheduled Tasks for Lookup Field Synchronization" on page 3-8. **Note:** You must not change the value of this parameter.

Admin FQDN	Enter the fully qualified domain name of the user account that you create by performing the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-3.
	You can use any one of the following formats to enter the domain name:
	■ *user_login*`@`*domain*`.com`
	■ `cn=`*user_login*`,cn=`*Users*`,dc=`*domain*`,dc=com`
	Sample values:
	`john_doe@example.com`
	`cn=OIMadmin,cn=Users,dc=domain,dc=com`

Admin Password	Enter the password of the user account that you create by performing the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-3.
AtMap ADUser	This parameter holds the name of the lookup definition for user field mappings between Oracle Identity Manager and the target system. This lookup definition is used during user provisioning operations. The default value of this parameter is `AtMap.AD`. Retain this value if the target system is Microsoft Active Directory. If you are using Microsoft ADAM, then change the value to `AtMap.ADAM`.
Port Number	Enter the number of the port at which SSL is running on the target system host computer. Sample values: For Microsoft Active Directory: ■ 636, if the Use SSL parameter is set to `yes` ■ 389, if the Use SSL parameter is set to `no` For Microsoft ADAM: ■ 50000, if the Use SSL parameter is set to `yes` ■ 50001, if the Use SSL parameter is set to `no` The Use SSL parameter is described later in this table. This parameter is also mentioned in "Configuring SSL for Microsoft Active Directory" on page 2-25.

Table 2–4 (Cont.) Parameters of the IT Resource for the Target System

Parameter	Description
Remote Manager Prov Lookup	This parameter holds the name of the lookup definition that stores Terminal Services Profile field mappings between Oracle Identity Manager and the target system. Value: `AtMap.AD.RemoteScriptlookUp` **Note:** You must not change the value of this parameter. If you want to use Environment, Remote Control, or Sessions fields for provisioning operations, then see "Adding New Fields for Provisioning" on page 4-14.
Remote Manager Prov Script Path	Enter the full path and name of the ProvTerminalServiceAttr.vbs script file on the target system host computer. Sample value: RM_HOME\scripts\ProvTerminalServiceAttr.vbs See "Installing the Remote Manager" on page 2-12 for more information. **Note:** ▪ Do not enter a value for this parameter if you do not want to use the Remote Manager. ▪ This parameter is not used for Microsoft ADAM.
Root Context	Enter the base DN on which reconciliation of deleted user data and provisioning are to be carried out. Sample values: `dc=example,dc=com` **Note:** You *must* enter a value for this parameter.

Server Address	Enter the host name or IP address of the Microsoft Windows computer (target system host computer) on which Microsoft Active Directory is installed.
	Sample values:
	`w2khost`
	`172.20.55.120`

Invert Display Name	Enter `yes` if you want the Display Name field to be in the *LAST_NAME FIRST_NAME* format. Enter (or retain) `no` if you want the Display Name field to be in the *FIRST_NAME LAST_NAME* format. For example, if you enter `yes`, then the Display Name field for user John Doe would show `Doe John`. Default value: `no` **Note:** ▪ This parameter is used only during provisioning operations. ▪ If you want to set this parameter to `yes`, then note that it works only with the ADITResource IT resource. It will not work if the IT resource for the target system has a different name. This point has also been mentioned under Bug 7212391 in the "Known Issues" chapter.
Use SSL	Enter `yes` to specify that you will configure SSL between Oracle Identity Manager and the target system. Otherwise, enter `no`. Default value: `yes` **Note:** It is recommended that you configure SSL to secure communication with the target system. You must configure SSL if you want to set or change user passwords during provisioning operations. Refer to "Configuring SSL for Microsoft Active Directory" on page 2-25 for information about enabling SSL.
isADAM	Enter `yes` to specify that the target system is Microsoft ADAM. Enter `no` to specify that the target system is Microsoft Active Directory.

Table 2–4 (Cont.) Parameters of the IT Resource for the Target System

Parameter	Description
isLookupDN	Use this parameter as follows to specify whether you want the Lookup.ADReconciliation.GroupLookup and Lookup.ADReconciliation.Organization lookup definitions to be populated with distinguished names (DNs) or relative DNs during lookup field synchronization: ■ Enter `yes` if you want the lookup fields to be populated with the DNs. ■ Enter `no` if you want the lookup fields to be populated with the relative DNs. Default value: `no` **Note:** The value of this parameter is used during lookup field synchronization, provisioning, and reconciliation. After a lookup field synchronization run, you must not change the value of this parameter. This point is also mentioned in "Guidelines on Using the Connector" on page 3-1.
isUserDeleteLeafNode	In Microsoft Active Directory, a user account can have other user accounts defined as its leaf nodes. Use the isUserDeleteLeafNode parameter to configure one of the following events to take place when a Delete User provisioning operation is carried out on a user account that has leaf nodes: ■ Enter `yes` as the value of the parameter if you want the user account and its leaf nodes to be deleted on the target system. ■ Enter `no` as the value of the parameter if you want a message stating that the user account has leaf nodes to be displayed to the user performing the Delete User provisioning operation. Default value: `no` **Note:** This parameter is not used for Microsoft ADAM. You must not change the default value if the target system is Microsoft ADAM.
Allow Password Provisioning	Enter `yes` as the value of this parameter if you want: ■ Password changes on Oracle Identity Manager to be propagated to the target system. This applies to both trusted source and target resource modes. ■ Password changes for an OIM User to be propagated to all resources allocated (provisioned) to the OIM User. Enter `no` as the value of this parameter if you do not want password changes on Oracle Identity Manager to be propagated to the target system.
AtMap ADGroup	Enter the name of the lookup definition that stores field mappings used for group provisioning: For Microsoft Active Directory: `AtMap.ADGroup` For Microsoft ADAM: `AtMap.ADAMGroup`
UPN Domain	Enter the name of the domain in which you want to provision and reconcile users. Sample value: `example.com` On the Administrative and User Console, the User ID field is prepopulated with the User Login value from the OIM User form. In addition, the User Principal Name field is prepopulated with the concatenated value of the User ID field and UPN Domain parameter value separated by the at sign (@). For example, if you enter `example.com` as the value of the UPN Domain parameter and if the user ID is `jdoe`, then the User Principal Name field is prepopulated with `jdoe@example.com`. If required, you can change the User ID part of the User Principal Name field value during provisioning operations.
Target Locale: TimeZone	Enter the time zone of the target system. For example, enter `GMT-07:00` if the target system is in Arizona in the United States.

9. To save the values, click **Update**.

2.2.2 Installation on the Target System

This section discusses the following topics:

- Installing the Remote Manager
- Enabling Logging in the Remote Manager
- Enabling Client-Side Authentication for the Remote Manager

2.2.2.1 Installing the Remote Manager

The Remote Manager enables you to include the Terminal Services Profile fields of the target system in reconciliation and provisioning operations.

Note:

- Perform the procedure described in this section only if you want to include Terminal Services Profile fields in reconciliation and provisioning operations.
- In this guide, the directory in which you install the Remote Manager is referred to as *RM_HOME*.

To install the Remote Manager:

1. The Remote Manager installation files are shipped along with the Oracle Identity Manager installation files. You can install the Remote Manager on any computer that is a part of the domain. Depending on the application server that you use, perform the procedure to install the Remote Manager by following the instructions given in one of the following guides:
   - *Oracle Identity Manager Installation and Configuration Guide for Oracle WebLogic Server*
   - *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*
   - *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
   - *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*
2. Copy the following JAR files into the *RM_HOME*\xlremote\JavaTasks directory:
   - *OIM_HOME*\xellerate\lib\xlVO.jar
   - *OIM_HOME*\xellerate\lib\xlScheduler.jar
   - *OIM_HOME*\xellerate\lib\xlAPI.jar
   - *OIM_HOME*\xellerate\JavaTasks\xliActiveDirectory.jar
   - *OIM_HOME*\xellerate\ScheduleTask\xliADRecon.jar
3. Copy the ReconTerminalServiceAttr.vbs and ProvTerminalServiceAttr.vbs files from the *OIM_HOME*/XLIntegrations/ADUM/scripts directory to any directory that you create inside the *RM_HOME* directory.

Note:

- Ensure that the directory into which you copy the scripts has the required read and write permissions for the target system user account used by Oracle Identity Manager. This user account is described in "Creating a Target System User Account for Connector Operations" on page 2-3.
- Ensure that the *RM_HOME* directory is secured using Microsoft Windows best practices. Only the target system user account for Oracle Identity Manager must have permissions to access the *RM_HOME* directory.

4. Use the following script to start the Remote Manager:

   RM_HOME\xlremote\remotemanager.bat

5. Note the Remote Manager service name and URL. These values are displayed in the Remote Manager command window. You will need these values while creating the IT resource for the Remote Manager. The default values are `RManager` and `rmi://`*HOST_NAME*`:12346`. For example, for a Remote Manager running on ten.mydomain.com, the default values will be `RManager` and `rmi://ten.mydomain.com:12346`.

2.2.2.2 Enabling Logging in the Remote Manager

To enable logging in the Remote Manager:

1. Add the following lines in the *RM_HOME*\xlremote\config\log.properties file:

   `log4j.logger.OIMCP.ADCS=`*LOG_LEVEL*

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

   For example:

   `log4j.logger.OIMCP.ADCS=INFO`

3. In the log.properties file, use the following parameter to specify the name and location of the file in which you want log information to be recorded:

   `log4j.appender.logfile.File`

2.2.2.3 Enabling Client-Side Authentication for the Remote Manager

To enable client-side authentication for the Remote Manager:

1. Open the *RM_HOME*/xlremote/config/xlconfig.xml file in a text editor.
2. Set the ClientAuth property to `true` as follows:

   `<ClientAuth>`**`true`**`</ClientAuth>`

3. Ensure that the RMIOverSSL property is set to `true` as follows:

   `<RMIOverSSL>`**`true`**`</RMIOverSSL>`

4. Perform Steps 2 through 3 in the *OIM_HOME*/config/xlconfig.xml file.

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Postinstallation on Oracle Identity Manager
- Postinstallation on the Target System
- Configuring the Remote Manager
- Configuring SSL for Microsoft Active Directory
- Configuring SSL for Microsoft ADAM

2.3.1 Postinstallation on Oracle Identity Manager

Configuring Oracle Identity Manager involves performing the following procedures:

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

- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging
- Configuring High Availability of the Target System

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

While you deploy the connector, the resource bundles are copied 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. This exception is different from the one mentioned in Step 1.

In this command, `ConnectorResourceBundle` is the content category that you must delete from the server cache.

> **See Also:** The following file for information about content categories:
>
> *OIM_HOME*/config/xlconfig.xml

2.3.1.2 Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

  This level enables logging of information about fine-grained events that are useful for debugging.

- `INFO`

  This level enables logging of messages that highlight the progress of the application at a 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 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 Server**

  To enable logging:

  1. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.OIMCP.ADCS=LOG_LEVEL
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.ADCS=INFO
     ```

  After you enable logging, the log information is displayed on the server console.

- **IBM WebSphere Application Server**

To enable logging:

1. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

   ```
   log4j.logger.OIMCP.ADCS=LOG_LEVEL
   ```

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

   For example:

   ```
   log4j.logger.OIMCP.ADCS=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, locate or add the following lines:

     ```
     <category name="OIMCP.ADCS">
        <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="OIMCP.ADCS">
        <priority value="INFO"/>
     </category>
     ```

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

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

  1. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.OIMCP.ADCS=LOG_LEVEL
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.ADCS=INFO
     ```

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

  ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log

2.3.1.3 Configuring High Availability of the Target System

Suppose you have set up multiple, replicated installations of the target system for high availability. You can use the Lookup.AD.BackupServers lookup definition to ensure that if the primary target system installation becomes unavailable, then Oracle Identity Manager switches to one of the secondary target system installations. The Lookup.AD.BackupServers lookup definition is one of the lookup definitions created when you deploy the connector.

For a single primary installation, you can have any number of secondary installations. In addition, if you configure the connector to work with multiple primary installations, then you can specify secondary installations for each primary installation.

To use the Lookup.AD.BackupServers lookup definition, open it in the Design Console and enter code key and decode values for each combination of primary and secondary target system installation.

> **See Also:** *Oracle Identity Manager Design Console Guide* for information about working with lookup definitions

Table 2–5 shows samples entries for the Lookup.AD.BackupServers lookup definition.

Table 2–5 Samples Entries for the Lookup.AD.BackupServers Lookup Definition

Code Key	Decode
172.20.55.64	172.20.55.65
172.20.55.64	172.20.55.66
172.20.55.97	172.20.55.98

In this table, the first two entries represent two secondary installations (172.20.55.65 and 172.20.55.66) for one primary installation (172.20.55.64). The third entry shows a one-to-one combination of primary (172.20.55.97) and secondary (172.20.55.98) installations.

2.3.2 Postinstallation on the Target System

Postinstallation on the target system consists of the following procedure.

2.3.2.1 Enabling or Disabling Password Policies in Microsoft Active Directory

In Microsoft Active Directory, the "Passwords must meet complexity requirements" policy setting is used to enable or disable password policies.

The procedure that you must perform depends on whether or not you want to achieve either or both of the following objectives:

- Enable password policies
- Configure SSL between Oracle Identity Manager and the target system

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

Suppose there is a password policy on the target system for enforcing that the password field of user accounts is never left empty. At the same time, suppose you do not configure SSL. Under these conditions, the target system would reject provisioning operations that leave the password field empty. Therefore, you would not be able to perform such provisioning operations from Oracle Identity Manager. To enable provisioning operations under these conditions, you must disable password policies on the target system.

If you configure SSL and you want to enable 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:

Note: If you install Microsoft ADAM in a domain controller then it acquires all the policies of Microsoft Active Directory installed in the same domain controller. If you install Microsoft ADAM in a workgroup, then the local system policies are applied.

1. On the Microsoft Windows computer hosting the target system, 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**.
6. Restart the target system.

2.3.3 Configuring the Remote Manager

This section discusses the following topics:

- Creating the IT Resource for the Remote Manager
- Verifying That the Remote Manager Is Running
- Configuring Oracle Identity Manager to Trust the Remote Manager

2.3.3.1 Creating the IT Resource for the Remote Manager

Note:

- The information in this section does not apply to Microsoft ADAM.
- If the target system is Microsoft Active Directory, then perform this procedure only if you want to use the Terminal Services Profile fields of the target system during reconciliation and provisioning operations.

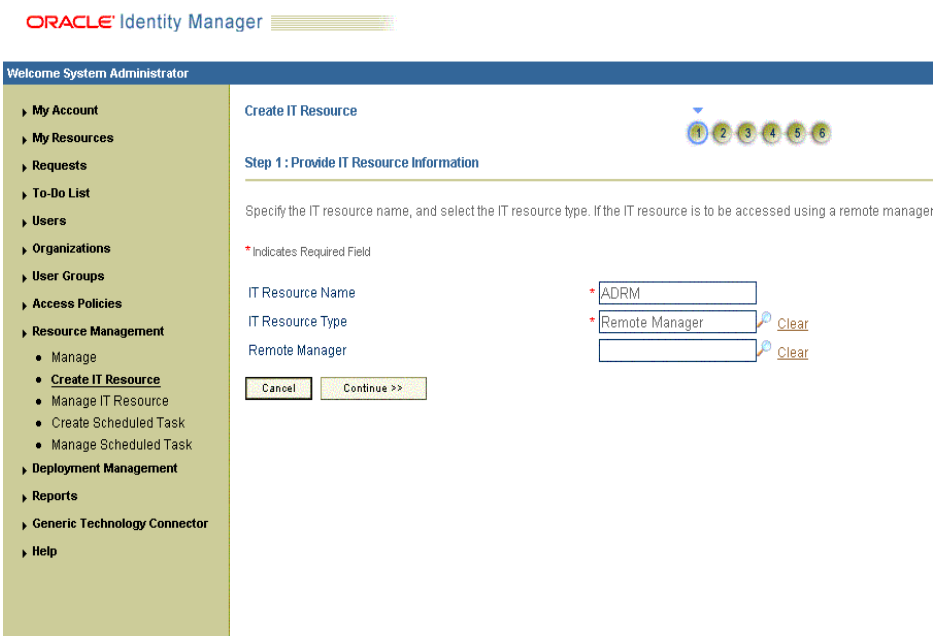
To create the IT resource for the Remote Manager:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Create IT Resource**.
4. On the Step 1: Provide IT Resource Information section, perform the following steps:
   - **IT Resource Name**: Enter a name for the IT resource.

- **IT Resource Type**: Select **Remote Manager** from the IT Resource Type list.
- **Remote Manager**: Do not enter a value in this field.

5. Click **Continue**. Figure 2–3 shows the IT resource values added on the Create IT Resource page.

Figure 2–3 Step 1: Provide IT Resource Information



6. On the Step 2: Specify IT Resource Parameter Values section, specify values for the parameters of the IT resource and then click **Continue**. Figure 2–4 shows the Step 2: Specify IT Resource Parameter Values section.

Figure 2–4 Step 2: Specify IT Resource Parameter Values

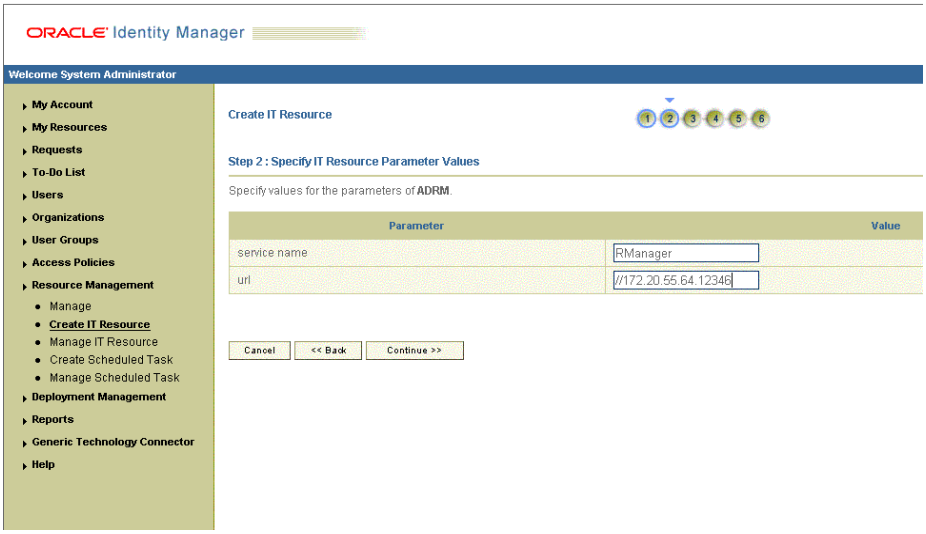


Table 2–6 provides information about the parameters of the IT resource.

Table 2–6 Parameters of the IT Resource for the Remote Manager

Parameter	Description
service name	Enter a name for the Remote Manager. Sample value: `RManager`
url	Enter the IP address of the target system host computer and the port number at which the Remote Manager is listening. Sample value: `rmi://10.0.0.1:12346`

7. On the Step 3: Set Access Permission to IT Resource page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

   Note: This step is optional.

   If you want to assign groups to the IT resource and set access permissions for the groups, then:

   a. Click **Assign Group**.

   b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

   c. Click **Assign**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

   Note:

   - This step is optional.
   - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

   a. Click **Update Permissions**.

   b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

   c. Click **Update**.

9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

   Note:

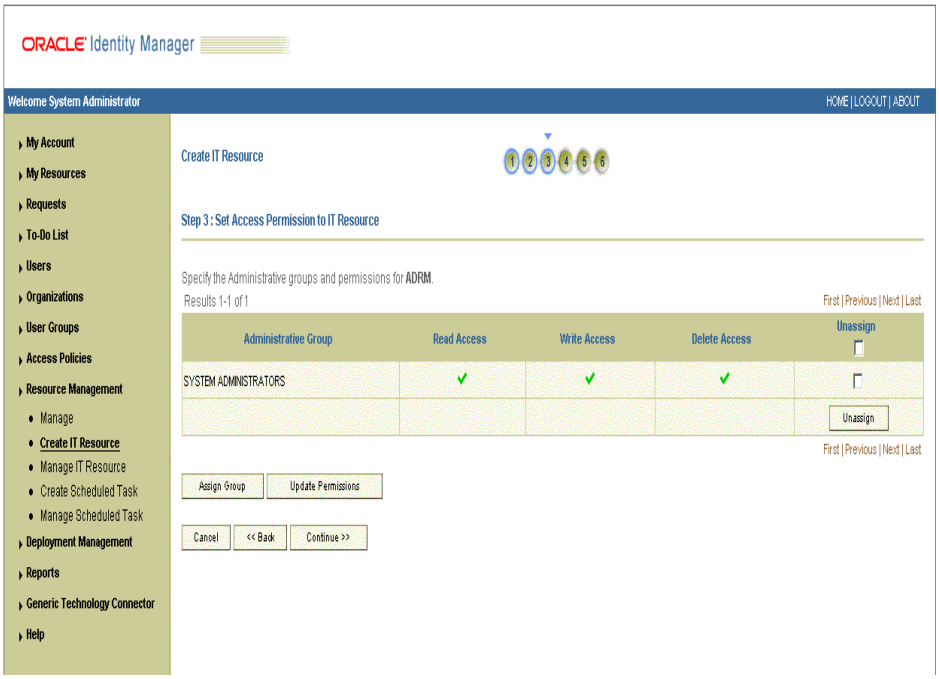
   - This step is optional.
   - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

a. Select the **Unassign** check box for the group that you want to unassign.

b. Click **Unassign**.

10. Click **Continue**. Figure 2–5 shows the Step 3: Set Access Permission to IT Resource page.

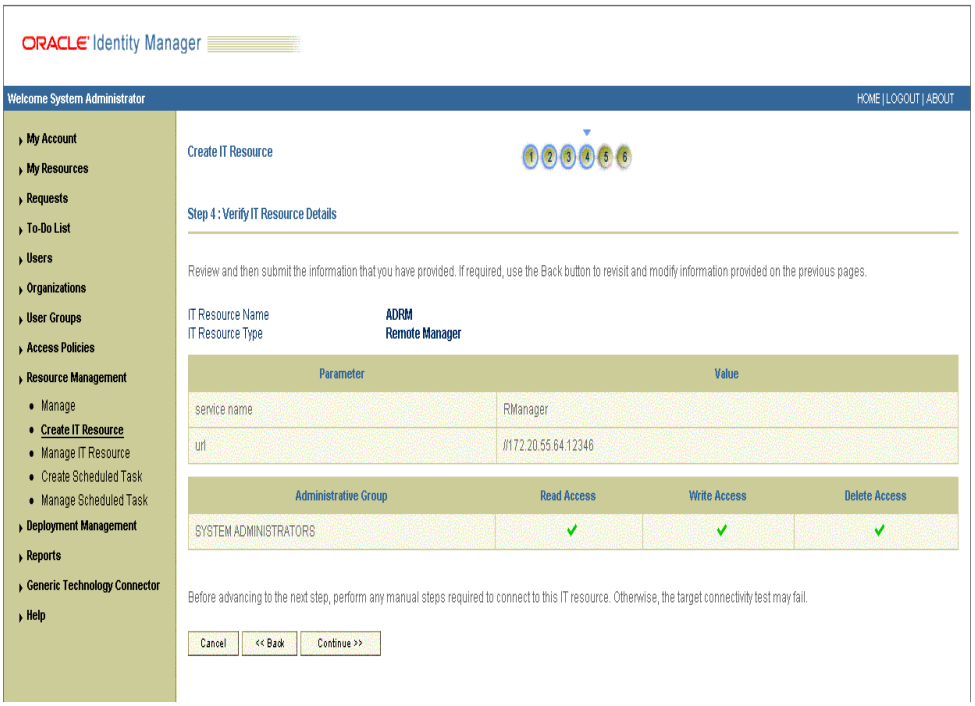
Figure 2–5 Step 3: Set Access Permission to IT Resource



11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.

12. To proceed with the creation of the IT resource, click **Continue**. Figure 2–6 shows Step 4: Verify IT Resource Details page.

Figure 2–6 Step 4: Verify IT Resource Details



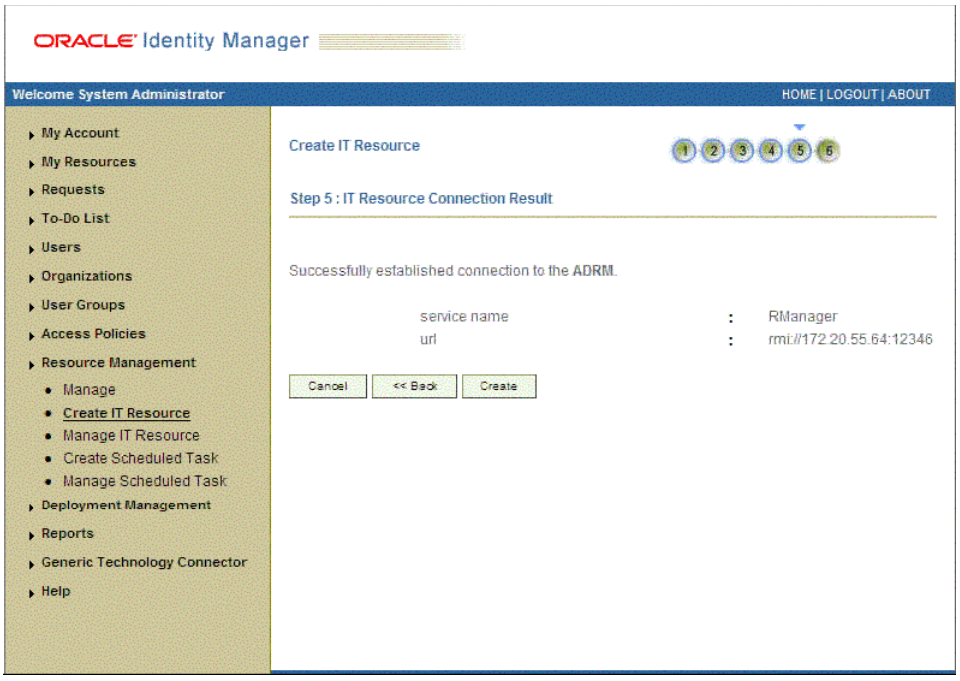
13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Create**. If the test fails, then you can perform one of the following steps:

    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.
    - Proceed with the creation process by clicking **Create**. You can fix the problem later, and then rerun the connectivity test by using the Diagnostic Dashboard.

    Note: If no errors are encountered, then the label of the button is **Create**, not **Continue**.

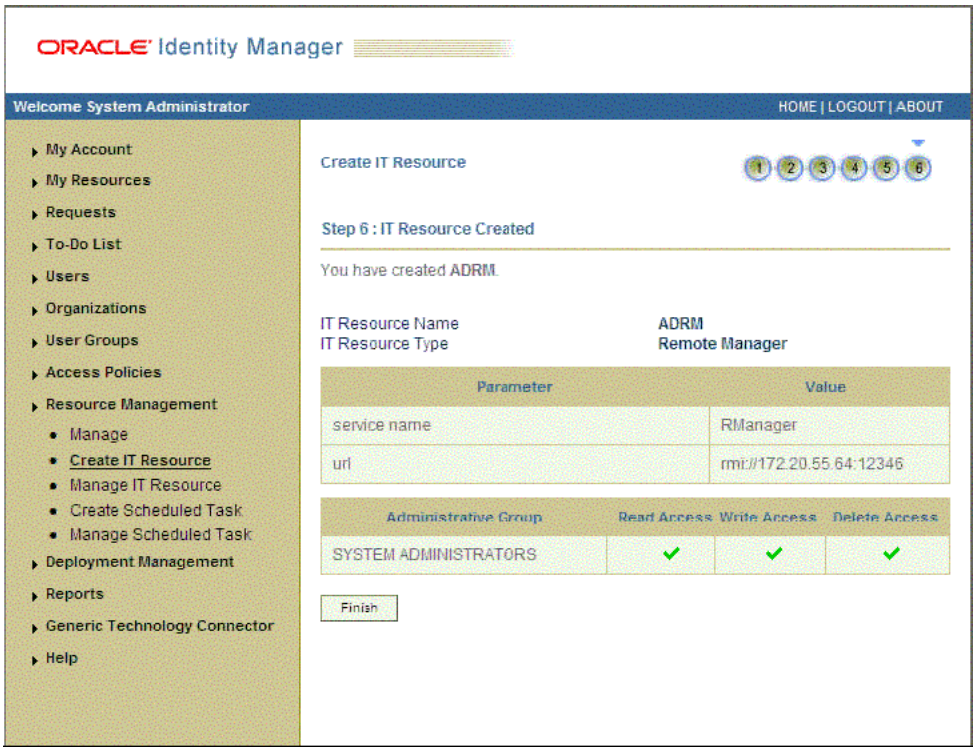
    Figure 2–7 shows the Step 5: Resource Connection Result page.

Figure 2–7 Step 5: IT Resource Connection Result



14. Click **Finish**. Figure 2–8 shows the IT Resource Created Page

Figure 2–8 Step 6: IT Resource Created



2.3.3.2 Configuring Oracle Identity Manager to Trust the Remote Manager

To configure Oracle Identity Manager to trust the Remote Manager:

1. From the computer hosting the Remote Manager, copy the *RM_HOME*/xlremote/config/xlserver.cert file to a temporary directory on the Oracle Identity Manager host computer.

   Note: The server certificate in the *OIM_HOME* directory is also named xlserver.cert. Ensure that you do not overwrite that certificate.

2. To import the certificate by using the keytool utility, run the following command:

   ```
   JAVA_HOME/jre/bin/keytool -import -alias ALIAS -file
   RM_CERT_LOCATION/xlserver.cert -keystore OIM_HOME/xellerate/config/.xlkeystore
   -storepass PASSWORD
   ```

   In the preceding command, replace:

   - *JAVA_HOME* with the location of the Java directory for your application server.
   - *ALIAS* with an alias for the certificate in the store.
   - *RM_CERT_LOCATION* with the full path of the temporary directory where you copied the certificate.
   - *PASSWORD* with the password of the keystore.

3. Copy the *OIM_HOME*/xellerate/config/xlserver.cert file to a temporary directory on the Remote Manager host computer.

4. To import the certificate by using the keytool utility on the Remote Manager host computer, run the following command:

   ```
   JAVA_HOME/jre/bin/keytool -import -alias ALIAS -file
   OIM_CERT_LOCATION/xlserver.cert -keystore RM_HOME/xlremote/config/.xlkeystore
   -storepass PASSWORD
   ```

   In the preceding command, replace:

   - *JAVA_HOME* with the location of the Java directory for your application server.
   - *ALIAS* with an alias for the certificate in the store.
   - *OIM_CERT_LOCATION* with the full path of the temporary directory where you copied the certificate.
   - *PASSWORD* with the password of the keystore.

   Note: It is recommended that you follow security best practices and change the default passwords used for the Remote Manager keystore. To change the Remote Manager keystore password, follow the instructions given in *Oracle Identity Manager Installation and Configuration Guide* for your application server.

2.3.3.3 Verifying That the Remote Manager Is Running

To verify that the Remote Manager is running:

1. Use the following script to start the Remote Manager:

   RM_HOME\xlremote\remotemanager.bat

2. Log in to the Design Console.

3. Expand **Administration**, and double-click **Remote Manager**.

4. Search for and open the Remote Manager that you have created.
5. Click the Refresh icon. The screen displays details of the Remote Manager that you have configured. The "running" check box should be selected for the Remote Manager. This implies that the status of the Remote Manager is active.

2.3.4 Configuring SSL for Microsoft Active Directory

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

- Installing Certificate Services
- Enabling LDAPS
- Setting Up the Target System Certificate As a Trusted Certificate

2.3.4.1 Installing Certificate Services

To install Certificate Services on the target system host computer:

Note: Before you begin installing Certificate Services, you must ensure that Internet Information Services (IIS) is installed on the target system host computer.

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. In the Windows Components Wizard, follow the instructions to start Certificate Services.

Note: While providing input to the wizard, select **Enterprise root CA** as the CA type. This is required for adding a policy with the Domain Controller template, which is a step that you perform in the next procedure.

2.3.4.2 Enabling LDAPS

The target system host computer must have LDAP over SSL (LDAPS) enabled. To enable LDAPS:

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 LDAPS is enabled on port 636. You can use an LDAP browser utility to verify that LDAPS is working.

> **Note:** While performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7, you specify the port number as the value of the Port Number parameter.

2.3.4.3 Setting Up the Target System Certificate As a Trusted Certificate

If the Microsoft Active Directory certificate is not issued or certified by a 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 host computer as a trusted CA 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.

To import the target system certificate into the certificate store of the Oracle Identity Manager host computer:

> **Note:** All application server releases supported by Oracle Identity Manager release 9.1.0 are supported.
>
> In a clustered environment, you must perform this procedure on all the nodes of the cluster.

1. Copy the target system certificate to the Oracle Identity Manager host computer.
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.

     Table 2–7 shows the location of the certificate store for each of the supported application servers.

Table 2–7 Certificate Store Locations

Application Server	Certificate Store Location
Oracle WebLogic Server	■ If you are using BEA jrockit_R27.3.1-jdk, then copy the certificate into the following directory: *JROCKIT_HOME*/jre/lib/security ■ If you are using the default Oracle WebLogic Server JDK, then copy the certificate into the following directory: *WEBLOGIC_HOME*/java/jre/lib/security/cacerts
IBM WebSphere Application Server	■ For a nonclustered configuration of any supported IBM WebSphere Application Server release, import the certificate into the following certificate store: *WEBSPHERE_HOME*/java/jre/lib/security/cacerts ■ For IBM WebSphere Application Server 6.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/AppServer/profiles/*SERVER_NAME*/config/cells/*CELL_NAME*/nodes/*NODE_NAME*/trust.p12 For example: C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02\config\cells\wkslaurel3224Node02Cell\nodes\wkslaurel3224Node02\trust.p12 ■ For IBM WebSphere Application Server 5.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/etc/DummyServerTrustFile.jks
JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts

3. To confirm whether or not the certificate has been imported successfully, enter a command similar to the following:

   ```
   keytool -list -alias ALIAS -keystore MY_CACERTS -storepass PASSWORD
   ```

   For example:

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

4. For a nonclustered configuration of IBM WebSphere Application Server, download the jsse.jar file from the Sun Web site and copy this file into the *WEBSPHERE_HOME*/java/jre/lib/ext directory.
5. For a clustered configuration of IBM WebSphere Application Server, download the jnet.jar, jsse.jar, and jcert.jar files from the Sun Web site and copy these files into the *WEBSPHERE_HOME*/java/jre/lib/ext directory.

2.3.5 Configuring SSL for Microsoft ADAM

To configure SSL communication between Oracle Identity Manager and Microsoft ADAM, you must perform the following tasks:

- Generating the Certificate in Microsoft ADAM
- Setting Up the Target System Certificate As a Trusted Certificate

2.3.5.1 Generating the Certificate in Microsoft ADAM

Note: Before you begin generating the certificate, you must ensure that Internet Information Services (IIS) is installed on the target system host computer.

To generate the certificate in Microsoft ADAM, perform the following procedures:

- Submitting a Request for the Certificate
- Issuing the Certificate
- Adding the Certificate to the Personal Store of the Microsoft ADAM Service
- Assigning Permissions to the Certificate Key
- Restarting the Microsoft ADAM Instance
- Testing the Certificate

2.3.5.1.1 Submitting a Request for the Certificate To submit a request for the certificate:

1. On the target system host computer, open Internet Information Services (IIS) Manager.

   You can use one of the following methods to open Internet Information Services (IIS) Manager:

   - Use the following URL:

     `http://localhost/certsrv`

   - Open Control Panel, double-click **Administrative Tools**, and then double-click **IIS Service**.
2. Expand **Web Sites**, and then expand **Default Web Site**.
3. Right-click **CertSrv**, and then select **Browse**.
4. Click **Request a certificate**.
5. Click **Advanced certificate request**.
6. Click **Create and submit a request to this CA**.
7. On the Advanced Certificate Request page, perform the following actions:

   Note: There are instructions for only some of the fields on this page. For the remaining fields, you can enter values according to your requirements.

   – In the Name field, enter the fully qualified domain name (FQDN) of the target system host computer. For example, enter `hk128.corp.example.com`.

   Note: On your target system installation, if a value is already selected in this field, then you need not change it.

   You need not enter values in the remaining fields of the Identifying Information region.

- Select **Store certificate in local computer certificate store**.
- Select **PCKS10** as the format.
- In the **Friendly name** field, enter the FQDN of the target system host computer. For example, enter `hk128.corp.example.com`.

8. Click **Submit**.
9. When a message asking you to confirm that you want to request a certificate is displayed, click **Yes**.

2.3.5.1.2 Issuing the Certificate

To issue the certificate:

1. On the target system host computer, open Control Panel.
2. Double-click **Administrative Tools**, and then double-click **Certification Authority**.
3. In the Certification Authority window, expand **Administrator** and then open **Pending Requests**.

   The request that you created earlier is displayed on the right pane.
4. Right-click the request, select **All Tasks**, and then select **Issue**.
5. Open the **Issued Certificates** folder.

   The certificate is displayed on the right pane.
6. Open Internet Information Services (IIS) Manager.
7. Expand **Web Sites**, and then expand **Default Web Site**.
8. Right-click **CertSrv**, and then select **Browse**.
9. Click **View the status of pending certificate request**.
10. Click the link for the certificate request.
11. Click **Install this certificate**.
12. When a message asking you to confirm that you want to add the certificate is displayed, click **Yes**.

    A message saying that the certificate has been successfully installed is displayed.

2.3.5.1.3 Adding the Certificate to the Personal Store of the Microsoft ADAM Service

To add the certificate to the personal store of the Microsoft ADAM service:

1. On the target system host computer, use the Run dialog box to run the command for opening the Microsoft Management Console:

   ```
   mmc
   ```
2. On the Microsoft Management Console, click **File** and then select **Add/Remove Snap-in**.
3. On the Standalone tab of the Add/Remove Snap-in dialog box, click **Add**.
4. From the list of snap-ins, select **Certificates** and then click **Add**.
5. In the Certificates snap-in dialog box, select **Service account**.
6. In the Select Computer dialog box, select **Local computer** and then click **Next**.
7. From the Service account list in the Certificates snap-in dialog box, select the Microsoft ADAM service instance and then click **Finish**.

8. In the Certificates snap-in dialog box, select **My user account** and then click **Finish**.
9. In the Certificates snap-in dialog box, select **Computer account** and then click **Next**.
10. In the Select Computer dialog box, select **Local computer** and then click **Finish**.
11. Click **Close**, and then click **OK**.
12. In the Microsoft Management Console window, expand **Certificates - Local Computer**, expand **Personal**, and then open **Certificates**.
13. Right-click the certificate that you have added and copy it.

    The name of this certificate is the FQDN of the host computer.
14. Paste the certificate into the following folders:
    - **Personal** folder under the Certificates - Service (*ADAM_INSTANCE_NAME)* on Local Computer folder
    - **Personal** folder under the Certificates - Current User folder
15. To save the changes that you have made to the Microsoft Management Console, click **File** and then select **Save**.

2.3.5.1.4 Assigning Permissions to the Certificate Key To assign the required permissions to the folder containing the certificate key:

1. In Microsoft Windows Explorer, navigate to the **MachineKeys** folder. The path to this folder is similar to the following:

   C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys
2. Right-click the **MachineKeys** folder, and then select **Properties**.
3. Use the **Add** button to add the following groups and users:
   - Administrators
   - Everyone
   - NETWORK SERVICE
   - The user name of the account used to install Microsoft ADAM
   - SYSTEM
4. From the Permissions list, select **Full Control**.
5. Click **Apply**, and then click **OK**.
6. In Microsoft Windows Explorer, expand the **MachineKeys** folder and select the certificate key. The time stamp for this certificate key is the date and time at which you created the certificate.

   Note: Refresh the folder if the certificate key that you created is not displayed.
7. Right-click the key, and select **Properties**.
8. Use the **Add** button to add the following groups and users:
   - Administrators

- Everyone
- NETWORK SERVICE
- The user name of the account used to install Microsoft ADAM
- SYSTEM

9. From the Permissions list, select **Full Control**.
10. Click **Apply**, and then click **OK**.

2.3.5.1.5 Restarting the Microsoft ADAM Instance To restart the Microsoft ADAM instance:

1. Open Control Panel.
2. Double-click **Administrative Tools**, and then select **Services**.
3. In the Services window, right-click the Microsoft ADAM instance and then select **Restart**.

2.3.5.1.6 Testing the Certificate To test the certificate:

1. To open the ADAM Tools Command Prompt window on the target system host computer, click **Start**, **Programs**, **ADAM**, and **ADAM Tools Command Prompt**.
2. In the ADAM Tools Command Prompt window, enter `ldp` and then press **Enter**.
3. From the Connection menu of the LDAPS dialog box, select **Connect**.
4. In the Connect dialog box:
   - In the **Server** field, enter the FQDN of the target system host computer.
   - In the **Port** field, enter the SSL port number.
   - Select **SSL**.
5. Click **OK**.
6. If SSL has been successfully configured, then status messages about the connection are displayed on the right pane of the LDAPS window.

2.3.5.2 Setting Up the Target System Certificate As a Trusted Certificate

If the Microsoft ADAM certificate is not issued or certified by a 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 host computer as a trusted CA certificate.

To export the Microsoft ADAM certificate:

1. Open the Microsoft Management Console.
2. In the Microsoft Management Console window, expand **Certificates - Local Computer**, expand **Personal**, and then open **Certificates**.
3. Right-click the certificate, select **All Tasks**, and then select **Export**.
4. Use the wizard to create a certificate (.cer) file using base-64 encoding.

To import the target system certificate into the certificate store of the Oracle Identity Manager host computer:

> **Note:** All application server releases supported by Oracle Identity Manager release 9.1.0 are supported.
>
> In a clustered environment, you must perform this procedure on all the nodes of the cluster.

1. Copy the target system certificate to the Oracle Identity Manager host computer.
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.

     Table 2–8 shows the location of the certificate store for each of the supported application servers.

Table 2–8 Certificate Store Locations

Application Server	Certificate Store Location
Oracle WebLogic Server	▪ If you are using BEA jrockit_R27.3.1-jdk, then copy the certificate into the following directory: *JROCKIT_HOME*/jre/lib/security ▪ If you are using the default Oracle WebLogic Server JDK, then copy the certificate into the following directory: *WEBLOGIC_HOME*/java/jre/lib/security/cacerts
IBM WebSphere Application Server	▪ For a nonclustered configuration of any supported IBM WebSphere Application Server release, import the certificate into the following certificate store: *WEBSPHERE_HOME*/java/jre/lib/security/cacerts ▪ For IBM WebSphere Application Server 6.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/AppServer/profiles/*SERVER_NAME*/config/cells/*CELL_NAME*/nodes/*NODE_NAME*/trust.p12 For example: C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02\config\cells\wkslaurel3224Node02Cell\nodes\wkslaurel3224Node02\trust.p12 ▪ For IBM WebSphere Application Server 5.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/etc/DummyServerTrustFile.jks
JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts

3. To confirm whether or not the certificate has been imported successfully, enter a command similar to the following:

   ```
   keytool -list -alias ALIAS -keystore MY_CACERTS -storepass PASSWORD
   ```

   For example:

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

4. For a nonclustered configuration of IBM WebSphere Application Server, download the jsse.jar file from the Sun Web site and copy this file into the *WEBSPHERE_HOME*/java/jre/lib/ext directory.
5. For a clustered configuration of IBM WebSphere Application Server, download the jnet.jar, jsse.jar, and jcert.jar files from the Sun Web site and copy these files into the *WEBSPHERE_HOME*/java/jre/lib/ext directory.

3

Using the Connector

This chapter is divided into the following sections:

3.1 Guidelines on Using the Connector

This section discusses the following topics:

3.1.1 Guidelines on Configuring Reconciliation

The following are guidelines that you must apply while configuring reconciliation:

- Before a target resource reconciliation run is performed, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before user reconciliation runs.
- The scheduled task for user reconciliation must be run before the scheduled task for reconciliation of deleted user data.
- In the identity reconciliation mode, if you want to configure group reconciliation, then note that group reconciliation does not cover reconciliation of updates to existing groups on the target system. If you modify the name of a group on the target system, then it is reconciled as a new group in Oracle Identity Manager.
- In the identity reconciliation mode, if you want to configure organization reconciliation, then note that:
  - Organization reconciliation does not cover reconciliation of updates to existing organizations on the target system. If you modify the name of an organization

on the target system, then it is reconciled as a new organization in Oracle Identity Manager.

- Organization reconciliation events created by the scheduled task for organization reconciliation (AD Organization Recon) must be successfully processed before the scheduled task for trusted source reconciliation (AD User Trusted Recon) is run. In other words, organization reconciliation must be run and the organization records reconciled from the target system must be successfully linked in Oracle Identity Manager.
- On the target system, users are created in specific organizations. During trusted source reconciliation of user data, if you want OIM Users to be created in the same organizations on Oracle Identity Manager, then you must set the MaintainHierarchy attribute of the trusted source reconciliation scheduled task to `yes`. In addition, you must configure organization reconciliation to run before trusted source reconciliation.
- In Oracle Identity Manager, the organization namespace is a flat namespace although it allows parent-child hierarchical relationships between organizations. Therefore, two Microsoft Active Directory OUs with the same name cannot be created in Oracle Identity Manager, even if they have different parent OUs on the target system.
- The name of an organization in Oracle Identity Manager cannot contain special characters, such as the equal sign (=) and comma (,). However, these special characters can be used in the name of an organization on the target system.
- During reconciliation, child organization records cannot be created in Oracle Identity Manager before the corresponding parent organization records are created.

  Suppose you create an organization on the target system and then create child organizations under the organization. During the next organization reconciliation run, you would expect to see the parent and child organizations created in Oracle Identity Manager. This might not happen if the reconciliation engine receives the child organization records before the parent organization record. However, the parent organizations are created in Oracle Identity Manager because they do not have any dependency.

  This would be automatically resolved during the next reconciliation run. At that time, parent organizations already exist in Oracle Identity Manager and child organizations can be created and linked to the parent.

  Note: The alternative is to manually link child organization records with parent organization records after the reconciliation run.

- The synchronization of organization lookup fields is independent of whether or not you configure organization reconciliation.

- While configuring batched reconciliation, leave the value of the Start Record attribute as 1.

  During a reconciliation run, the time stamp attribute (ADCS TimeStamp) of the scheduled task is updated each time a reconciliation event is created for a target system user record. If the reconciliation run fails, then reconciliation resumes from the time stamp captured at the end of the previous reconciliation run. If you set the value of the Start Record attribute to an integer other than 1, then some

reconciliation-ready records on the target system might not be fetched to Oracle Identity Manager. Therefore, it is recommended that you leave the value of the Start Record attribute as 1.

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then you only need to rerun the scheduled task without changing the values of the task attributes.

- If a user in Microsoft Active Directory has not been assigned values for the First Name or Last Name fields, then these fields in Oracle Identity Manager are updated with the cn field value at the end of the reconciliation run. This is because First Name and Last Name are mandatory fields in Oracle Identity Manager.
- If you are going to configure Microsoft ADAM as the trusted source, then you must ensure that a value (either `true` or `false`) is set for the msDS-UserAccountDisabled field of each user record on the target system. In Microsoft ADAM, the msDS-UserAccountDisabled field does not have a default value.
- The value of the isLookupDN parameter of the IT resource for the target system is used during lookup field synchronization, provisioning, and reconciliation. After a lookup field synchronization run, you must not change the value of this parameter.
- You must configure batched reconciliation if you want to reconcile Terminal Services Profile fields.

3.1.2 Guidelines on Performing Provisioning Operations

The following are guidelines that you must apply while performing provisioning operations:

- Before you perform provisioning operations, lookup definitions must be synchronized with the lookup fields of the target system. In other words, scheduled tasks for lookup field synchronization must be run before provisioning operations.
- If you want to use the E-mail Redirection feature, then note that:

  Note: The E-Mail Redirection feature is not supported in Microsoft ADAM.

  – E mail and Redirection Mail ID are two of the fields on the process form. During a provisioning operation, if you enter an e-mail address in the Redirection Mail ID field, then e-mail is sent to that account. This is regardless of whether or not you enter an address in the E mail field. At the end of the provisioning operation, the address in the Redirection Mail ID field becomes the primary SMTP address of the user.

    During the next reconciliation run, the E mail field is updated with the primary SMTP address. In other words, the E mail and Redirection Mail ID fields hold the same address at the end of the reconciliation run.

  – The E-mail Redirection feature involves the use of Microsoft Exchange. Therefore, the target Microsoft Active Directory installation must have Microsoft Exchange configured. However, a user for whom you set a redirection e-mail address need not have a Microsoft Exchange mailbox. In

other words, you need not provision a Microsoft Exchange mailbox for the user.

- During a provisioning operation, if you do not specify an organization for the user, then the user is provisioned to the cn=Users organization.
- Passwords for user accounts provisioned from Oracle Identity Manager must adhere to the password policy set in Microsoft Active Directory.

Note: If you install Microsoft ADAM in a domain controller then it acquires all the policies of Microsoft Active Directory installed in the same domain controller. If you install Microsoft ADAM in a workgroup, then the local system policies are applied.

In Microsoft Active Directory, password policies are controlled through password complexity rules. These complexity rules are enforced when passwords are changed or created. While changing the password of a Microsoft Active Directory account by performing a provisioning operation on Oracle Identity Manager, you must ensure that the new password adheres to the password policies on the target system.

If the password specified during a provisioning operation on Oracle Identity Manager is not accepted by the target system, then a message stating that the password could not be set is displayed on the Administrative and User Console.

See Also: For more information about password guidelines applicable on the target system, visit the Microsoft TechNet Web site at

`http://technet2.microsoft.com`

- Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.
- The character length of target system fields must be taken into account when specifying values for the corresponding Oracle Identity Manager fields.
- On the target system, the Manager Name field accepts only DN values. Therefore, when you set or modify the Manager Name field on Oracle Identity Manager, you must enter the DN value.

  For example:

  `cn=abc,ou=lmn,dc=corp,dc=com`
- By default, the cn field of the target system is mapped to the UD_ADUSER_COMMONNAME field of Oracle Identity Manager. This mapping information is stored in the AtMap.AD (and AtMap.ADAM) lookup definition, and it can be modified by renaming the code key value for the cn field.

  For example, the code key for the cn field can be changed to UD_ADUSER_UID. This is the User ID field on the process form.

- During a provisioning operation, the ExecuteRemoteScript process task is run even when you do not select the Remote Manager IT resource on the Administrative and User Console.

  The following response is displayed at the end of the provisioning operation:

  ```
  Task completed
  Response: Remote Manager Not Selected during provisioning
  Response Description: Remote Manager is not selected while provisioning the
  user
  ```

- The value of the isLookupDN parameter of the IT resource for the target system is used during lookup field synchronization, provisioning, and reconciliation. After a lookup field synchronization run, you must not change the value of this parameter.

3.2 Setting Up Lookup Definitions in Oracle Identity Manager

The following sections discuss lookup definitions that you must manually configure in Oracle Identity Manager:

- Configuring the Lookup.AD.Configuration Lookup Definition
- Configuring the Lookup.AD.Country Lookup Definition

3.2.1 Configuring the Lookup.AD.Configuration Lookup Definition

When you deploy the connector, the Lookup.AD.Configuration lookup definition is created in Oracle Identity Manager. The entries in this lookup definition are used during both reconciliation and provisioning.

To configure the Lookup.AD.Configuration lookup definition:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the **Lookup.AD.Configuration** lookup definition.
4. Enter decode values for each of the parameters listed in Table 3–1.

Table 3–1 Entries in the Lookup.AD.Configuration Lookup Definition

Code Key	Description	Default Decode Value
LdapUserObjectClass	Enter the name of the object class to which newly created users on the target system are assigned. By default, newly created users on the target system are assigned to the user object class. If you want to assign new users to additional object classes, then enter the list of object classes in the Decode column. The character that you use to separate the names of object classes in the list must be entered as the value of the UserObjectClassDelimiter entry, which is described later in this table. 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.	`user`
UserObjectClassDelimiter	Enter the delimiter character that you have used to separate the list of object classes entered as the value of the LdapUserObjectClass property. This parameter is used only during provisioning.	`|` **Note:** This is the vertical bar character. You can use any character, such as the semicolon (;), as the delimiter.
LdapUserDNPrefix	Enter the LDAP attribute for forming the relative DN or user account DN. This value forms the logon attribute for creating the user. This parameter is used only during provisioning. **Note:** It is recommended that you do not change the default value of this code key.	`cn`
LdapGroupMember	Target system field that stores the names of users who belong to a particular group This parameter is used only during provisioning. **Note:** You must not change the value of this parameter.	`member`

Table 3–1 (Cont.) Entries in the Lookup.AD.Configuration Lookup Definition

Code Key	Description	Default Decode Value
Pagesize	Enter the page size of records fetched in each call to the target system during a reconciliation run. This page size is used only if you do not configure batched reconciliation, which is described in "Batched Reconciliation" on page 3-11. This parameter is used only during reconciliation. **Note:** If you do not want to configure batched reconciliation, then it is recommended that you set a page size between 100 and 1000.	`100`
MultiValueAttributes	Specify all the multivalued attributes that are to be reconciled. The character that you use as a delimiter for the list of multivalued attributes must be entered as the value of the MultiValueAttributesDelimiter entry, which is described later in this table. This parameter is used only during reconciliation. Sample value: `memberOf,carLicense` There are two multivalued attributes in this sample value.	`memberOf`
MultiValueAttributesDelimiter	Enter the delimiter character that you have used in the list of multivalued attributes specified as the value of the MultiValueAttributes entry. This parameter is used only during reconciliation.	, **Note**: This is the comma character. You can use any character, such as the semicolon (;), as the delimiter.
ROUserID	If you create a copy of the process form, then specify the name of the attribute (column) in the new process form that holds the user ID value.	UD_ADUSER_UID
ROUserManager	If you create a copy of the process form, then specify the name of the attribute (column) in the new process form that holds the manager ID value.	UD_ADUSER_MANAGER
ROFormName	If you create a copy of the process form, then specify the name of the new process form.	UD_ADUSER
ROUserGUID	If you create a copy of the process form, then specify the name of the attribute (column) in the new process form that holds the objectGUID value.	UD_ADUSER_OBJECTGUID
TargetDateFormat	Enter the target system date format.	yyyyMMddHHmmss.0Z
AppendValueToDate	Enter the extension that you want add as a suffix to the date value in the TargetDateFormat parameter.	.0Z

5. Click **Save**.

3.2.2 Configuring the Lookup.AD.Country Lookup Definition

The Lookup.AD.Country lookup definition is one of the lookup definitions that is created in Oracle Identity Manager when you deploy the connector. The values in this lookup definition are used to populate the Country lookup field on the process form.

The following are the default entries in the AD.Country lookup definition:

- Brazil

- Canada
- China
- France
- Germany
- India
- Italy
- Japan
- Korea
- Spain
- United Kingdom
- United States

Depending on your requirements, add or delete entries in the AD.Country lookup definition. See "Configuring the Lookup.AD.Configuration Lookup Definition" on page 3-5 for information about modifying lookup definitions. Note that for each entry in the lookup definition, the Code Key value is the country code and the Decode value is the country name. For example, the Code Key value for Australia is `AU` and the Decode value is `Australia`.

Information about country codes is available at

`http://www.iso.org/iso/home.htm`

> **See Also:** The known issue tracked through Bug 7136085 documented in the "Known Issues" chapter

3.3 Scheduled Tasks for Lookup Field Synchronization

The following are the scheduled tasks for lookup field synchronization:

> **Note:** The procedure to configure these scheduled tasks is described later in the guide.

- AD Group Lookup Recon

  This scheduled task is used to synchronize group lookup fields in Oracle Identity Manager with group-related data in the target system.

- AD Organization Lookup Recon

  This scheduled task is used to synchronize organization lookup fields in Oracle Identity Manager with organization-related data in the target system.

Table 3–2 describes the attributes of both scheduled tasks.

Table 3–2 Attributes of the Scheduled Tasks for Lookup Field Synchronization

Attribute	Description

Lookup Search Filter	This attribute holds the filter or query condition for lookup synchronization.
	■ Value of this attribute for group lookup synchronization:
	`(objectclass=group)`
	■ Value of this attribute for organization lookup synchronization:
	`(objectclass=OrganizationalUnit)`
	Note: You must not change the value of this attribute.

Search Base	Enter the DN of the organization in which the search for the lookup field (group or organization) values must be performed during reconciliation. Sample values: ■ `ou=abc,dc=corp,dc=com` ■ `dc=corp,dc=com`
Recon Type	Enter `Refresh` as the value of this attribute if you want the following events to occur during lookup field synchronization: ■ 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 `Update` as the value of this attribute if you want the following events to occur during lookup field synchronization: ■ 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: `Refresh`
IT Resource Name	Enter the name of the IT resource that you configure by performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7. Sample value: `ADITResource`
AttrName For Decode Value In Lookup	This attribute holds the name of the target system field that is used to populate the Decode column of the lookup definition. ■ Value of this attribute for group lookup synchronization: `distinguishedName` ■ Value of this attribute for organization lookup synchronization: `distinguishedName` **Note:** You must not change the value of this attribute.

Table 3–2 (Cont.) Attributes of the Scheduled Tasks for Lookup Field Synchronization

Attribute	Description
AttrName For Code Value In Lookup	This attribute holds the name of the target system field that is used to populate the Code Key column of the lookup definition. ▪ Value of this attribute for group lookup synchronization: `distinguishedName` ▪ Value of this attribute for organization lookup synchronization: `distinguishedName` **Note:** You must not change the value of this attribute.

Lookup Code Name	This attribute holds the name of the lookup definition that contains mappings between the lookup fields of the target system and corresponding lookup definitions created in Oracle Identity Manager.
	▪ In the lookup definition for groups, the following is the default value:
	`Lookup.ADReconciliation.GroupLookup`
	▪ In the lookup definition for organizations, the following is the default value:
	`Lookup.ADReconciliation.Organization`

Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.AD.Configuration` **Note:** You must not change the value of this attribute. However, if you create a copy of this lookup definition, then you can enter the unique name of the new lookup definition as the value of the Configuration Lookup attribute.

3.4 Configuring Reconciliation

When you run the Connector Installer, scheduled tasks for user reconciliation are automatically created in Oracle Identity Manager. Configuring reconciliation involves providing values for the attributes of these scheduled tasks.

The following sections provide information about the attributes of the scheduled tasks:

> **See Also:** The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for detailed information about these configuration options

- Limited Reconciliation vs. Regular Reconciliation
- Batched Reconciliation
- Full Reconciliation vs. Incremental Reconciliation
- Reconciliation Scheduled Tasks

3.4.1 Limited Reconciliation vs. Regular Reconciliation

This section discusses the Search Filter attribute of the scheduled tasks for target resource reconciliation and trusted source 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 specify the subset of newly added or modified target system records that must be reconciled. You do this by creating a query condition that is used as a filter during reconciliation runs.

To create a query condition, use a combination of target system fields and the following logical operators:

> **Note:** You can use any target system fields, even the ones that are not supported (by default) for reconciliation and provisioning. The default target system fields for reconciliation and provisioning are listed in "Features of the Connector" on page 1-2.

- The AND operator represented by the ampersand (&)
- The OR operator represented by the vertical bar (|)
- The EQUAL operator represented by the equal sign (=)

You must apply the following guidelines while creating the query condition:

- The Search Filter attribute for each scheduled task has a default value. For example, the default value for user reconciliation is `(objectClass=user)`. When you create query, it is recommended that you retain the default value as one of the query conditions. For example:

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

- You must independently verify that the query returns the objects that you want it to return. The scheduled task does not validate your query.
- For the target system fields, you must use the same case (uppercase or lowercase) as given in "Features of the Connector" on page 1-2. This is because the field names are case-sensitive.
- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

The following are sample query conditions:

- `(&(objectClass=user)(sAMAccountName=John12))`
- `(&(objectClass=user)(sn=Doe))`
- `(&(objectClass=user)(givenName=John))`
- `(& (&(givenName=John)(sn=Doe)) (objectClass=user))`
- `(|(|(sn=Doe)(givenName=John))(objectClass=user))`

While performing the procedure described in the "Scheduled Tasks for Target Resource Reconciliation" or "Scheduled Tasks for Trusted Source Reconciliation" section, set the value of the Search Filter attribute to the query condition that you create.

3.4.2 Batched Reconciliation

This section discusses the Start Record, Batch Size, and Number of Batches attributes of the scheduled tasks for target resource reconciliation (AD User Target Recon) and trusted source reconciliation (AD User Trusted Recon).

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. 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.

Note: You must configure batched reconciliation if you want to reconcile Terminal Services Profile fields.

To configure batched reconciliation, specify values for the following attributes while performing the procedure described in the "Scheduled Tasks for Target Resource Reconciliation" or "Scheduled Tasks for Trusted Source Reconciliation" section:

- Start Record: Use this attribute to specify the record number from which batched reconciliation must begin. The default value of this attribute is 1. To ensure that all newly created and modified records are reconciled, it is recommended that you accept the default value.
- Batch Size: Use this attribute to specify the number of records that must be included in each batch. The default value of this attribute is 1.
- Number of Batches: Use this attribute to specify the total number of batches that must be reconciled. The default value of this attribute is `All Available`. If you do not want to implement batched reconciliation, then accept the default value. When you accept the default value, the values of the Start Record and Batch Size attributes are ignored.

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then you only need to rerun the scheduled task without changing the values of the task attributes.

3.4.3 Full Reconciliation vs. Incremental Reconciliation

This section discusses the Will Submit All Records attribute of the scheduled tasks for target resource reconciliation (AD User Target Recon) and trusted source reconciliation (AD User Trusted Recon).

After you deploy the connector, you first reconcile all the existing target system records into Oracle Identity Manager. This is a full reconciliation run. During the reconciliation run, the time stamp attribute (ADCS TimeStamp) of the scheduled task is updated each time a reconciliation event is created for a target system user record.

During the next reconciliation run, the value of the ADCS TimeStamp attribute is used to determine the time stamp at which the last run ended. User records added or modified after the time stamp are selected for reconciliation during the current run. This is incremental reconciliation.

Some user records may never be reconciled into Oracle Identity Manager during subsequent reconciliation runs. For example, user records that are added or modified around the time that the ADCS TimeStamp attribute is updated may not meet the time-stamp criterion for reconciliation during the next reconciliation run. To ensure that such records are reconciled into Oracle Identity Manager, you must run full reconciliation at periodic intervals.

While configuring the AD User Target Recon and AD User Trusted Recon scheduled tasks by performing the procedure described in "Reconciliation Scheduled Tasks" on page 3-13:

- If you want to run full reconciliation, set the value of the Will Submit All Records attribute to `yes`.
- If you want to continue with incremental reconciliation, accept the default value of `no` for the attribute.

3.4.4 Reconciliation Scheduled Tasks

When you run the Connector Installer, the following reconciliation scheduled tasks are automatically created in Oracle Identity Manager:

- Scheduled Tasks for Target Resource Reconciliation
- Scheduled Tasks for Trusted Source Reconciliation

3.4.4.1 Scheduled Tasks for Target Resource Reconciliation

The following are the scheduled tasks for target resource reconciliation:

> **Note:** The procedure to configure these scheduled tasks is described later in the guide.

- AD User Target Recon
- AD User Target Delete Recon
- AD Group Recon

AD User Target Recon

The AD User Target Recon scheduled task is used to reconcile user data in the target resource (account management) mode of the connector. Table 3–3 describes the attributes of this scheduled task.

Table 3–3 Attributes of the Scheduled Task for Reconciliation of User Data from a Target Resource

Attribute	Description
Remote Manager Script Path	Enter the full path and name of the Remote Manager script for reconciliation (ReconTerminalServiceAttr.vbs) on the target system host computer. You copy this file to the target system host computer while performing the procedure described in "Installing the Remote Manager" on page 2-12. Enter `[NONE]` if you do not want to enable the reconciliation of Terminal Services Profile fields from the target system. Sample value: `c:\ReconTerminalServiceAttr.vbs` Default value: `[NONE]` **Note:** For Microsoft ADAM, accept the default value.
Delete Recon Task Scheduler Name	This attribute holds the name of the scheduled task for reconciliation of deleted user data from the target system. Value: `AD User Target Delete Recon` **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task and the scheduled task for reconciliation of deleted user data, then you must enter the unique name of that new Delete reconciliation scheduled task as the value of the Delete Recon Task Scheduler Name attribute in the copy of this scheduled task.
Target Resource Object	This attribute holds the name of the resource object against which target resource reconciliation runs must be performed. Value: `AD User` **Note:** For the resource object shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the resource object, then you must enter the unique name of that resource object as the value of this attribute.
IT Resource Name	Enter the name of the IT resource that you configure by performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7. Sample value: `ADITResource`

Table 3–3 (Cont.) Attributes of the Scheduled Task for Reconciliation of User Data from a Target Resource

Attribute	Description
Lookup For BLOB Attributes	This attribute holds the name of the lookup definition that contains mappings for the Terminal Services Lookup fields. Value: `Lookup.AD.BLOBAttribute.Values` **Note:** You must not change the value of this attribute. The "Adding New Fields for Target Resource Reconciliation" on page 4-3 provides information about adding entries in the Lookup.AD.BLOBAttribute.Values lookup definition.
ADCS TimeStamp	This attribute holds the date and time at which the last user reconciliation run ended. The reconciliation engine automatically enters a value in this attribute. Default value: `0` **Note:** You must not change the value of this attribute.
Task Scheduler Name	This attribute holds the name of the scheduled task. Value: `AD User Target Recon` **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that scheduled task as the value of the attribute in that scheduled task.
Search Scope	Enter `subtree` if you want the scope of the search for records to be reconciled to include the container specified by the Search Base attribute *and* all of its child containers. For example, if the search base is set to `OU=abc,DC=corp,DC=com`, then the search would cover the `abc` OU and all of its child OUs. Enter `onelevel` if you want the scope of the search for records to be restricted to only the container specified by the Search Base attribute. Child containers of the specified container are not included in the search. For example if the search base is set to `OU=abc,DC=corp,DC=com`, then the search would cover only the `abc` OU. **Note:** If you want to enter `onelevel`, then remember that you must not include a space between "one" and "level." Default value: `subtree`

Field Lookup Code	This attribute holds the name of the lookup definition that contains mappings between the target system fields and the corresponding Oracle Identity Manager fields.
	▪ If the target system is Microsoft Active Directory, then enter the following value:
	`Lookup.ADReconciliation.FieldMap`
	▪ If the target system is Microsoft ADAM, then enter the following value:
	`Lookup.ADAMReconciliation.FieldMap`

Transform Lookup Code	Enter the name of the lookup definition that you have created to link Microsoft Active Directory fields with the JAR files that must be run to transform each field. This attribute is valid only when the Use Transform Mapping attribute is set to `yes`. Value: `Lookup.ADReconciliation.TransformationMap` **Note:** You must not change the value of this attribute. See "Transforming Data Reconciled Into Oracle Identity Manager" on page 4-34 for detailed information about using the Transform Lookup Code attribute.
Use Transform Mapping	Enter `yes` to specify that you want the transformations referenced by the Transform Lookup Code attribute to be applied. Otherwise, enter `no`. Default value: `no` See "Transforming Data Reconciled Into Oracle Identity Manager" on page 4-34 for detailed information about using the Use Transform Mapping attribute.

Table 3–3 (Cont.) Attributes of the Scheduled Task for Reconciliation of User Data from a Target Resource

Attribute	Description
Start Record	Enter the number of the target system record from which a batched reconciliation run must begin. Default value: `1` This attribute is used in conjunction with the Batch Size and Number of Batches attributes. All three attributes are discussed in "Batched Reconciliation" on page 3-11. As mentioned in that section, it is recommended that you accept the default value of the Start Record attribute.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system. Default value: `1` This attribute is used in conjunction with the Number of Batches and Start Record attributes. All three attributes are discussed in "Batched Reconciliation" on page 3-11.
Number of Batches	Enter the number of batches that must be reconciled. Default value: `All Available` Sample value: `25` This attribute is used in conjunction with the Batch Size and Start Record attributes. All three attributes are discussed in detail in "Batched Reconciliation" on page 3-11. If you accept the default value (`All Available`), then batched reconciliation is not performed. In addition, the reconciliation of Terminal Services Profile fields is disabled.
Will Submit All Records	Enter `yes` to configure full reconciliation. Enter `no` to configure incremental reconciliation. Default value: `no` See "Full Reconciliation vs. Incremental Reconciliation" on page 3-12 for detailed information about this attribute.
Search Base	Enter the DN of the organization in which the search for user records must be performed during reconciliation. Sample value: `ou=abc,dc=corp,dc=com`
Search Filter	Enter the query condition that is to be used during reconciliation for locating target system user accounts that meet certain criteria. Default value: `(objectClass=user)` Sample value: `(&(objectClass=user)(givenName=first))` See "Limited Reconciliation vs. Regular Reconciliation" on page 3-10 for detailed information about this attribute.
Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.AD.Configuration` **Note:** You must not change the value of this attribute. However, if you create a copy of this lookup definition, then you can enter the unique name of the new lookup definition as the value of the Configuration Lookup attribute.

AD User Target Delete Recon

The AD User Target Delete Recon scheduled task is used to reconcile data about deleted users in the target resource (account management) mode of the connector. During a reconciliation run, for each deleted user account on the target system, the AD User resource is revoked for the corresponding OIM User. Table 3–8 describes the attributes of this scheduled task.

Table 3–4 Attributes of the Scheduled Task for Reconciliation of Deleted User Data from a Target Resource

Attribute	Description
Target Resource Object	This attribute holds the name of the resource object against which the reconciliation run is performed. Value: `AD User` **Note:** For the resource object shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the resource object, then you can enter the unique name of that resource object as the value of this attribute.
ADCS TimeStamp	This attribute holds the time stamp at which the last Delete User reconciliation run ended. In addition, the value of this attribute is updated when the scheduled task for target resource reconciliation of user accounts (AD User Target Recon) is run with its ADCS TimeStamp attribute set to 0. The reconciliation engine automatically enters a value in this attribute. Default value: 0 **Note:** You must not change the value of this attribute.
IT Resource Name	Enter the name of the IT resource that you configure by performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7. Sample value: `ADITResource`
Search Filter	This attribute holds the LDAP search filter that is used to locate deleted user accounts on the target system. Value: `(objectclass=user)` **Note:** You must not change the value of this attribute.
Task Scheduler Name	This attribute holds the name of the scheduled task. Value: `AD User Target Delete Recon` **Note:** You must not change the value of this attribute.
Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.AD.Configuration` **Note:** You must not change the value of this attribute. However, if you create a copy of this lookup definition, then you can enter the unique name of the new lookup definition as the value of the Configuration Lookup attribute.

AD Group Recon

The AD Group Recon scheduled task is used to reconcile group data from the target system. Table 3–5 describes the attributes of this scheduled task.

Table 3–5 Attributes of the Scheduled Task for Reconciliation of Group Data from a Target Resource

Attribute	Description
MultiValued Attributes	Enter a comma-separated list of multivalued group attributes that you want to reconcile. Sample value: `member`
Search Base	Enter the DN of the organization in which the search for group records must be performed during reconciliation. Sample value: `ou=abc,dc=corp,dc=com`
Search Scope	Enter `subtree` if you want the scope of the search for group records to be reconciled to include the container specified by the Search Base attribute *and* all of its child containers. For example, if the search base is set to `OU=abc,DC=corp,DC=com`, then the search would cover the `abc` OU and all of its child OUs. Enter `onelevel` if you want the scope of the search for group records to be restricted to only the container specified by the Search Base attribute. Child containers of the specified container are not included in the search. For example if the search base is set to `OU=abc,DC=corp,DC=com`, then the search would cover only the `abc` OU. **Note:** If you want to enter `onelevel`, then remember that you must not include a space between "one" and "level." Default value: `subtree`
Search Filter	Enter the query condition that is to be used during reconciliation for locating target system user accounts that meet certain criteria. Default value: `(objectClass=group)` Sample value: `(&(objectClass=group)(sAMAccountName=first))` See "Limited Reconciliation vs. Regular Reconciliation" on page 3-10 for detailed information about this attribute.
Organization Name	Enter one of the following values: ▪ 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> *GROUP_NAME* (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.
Use Organization Name	Enter yes as the value of this attribute if you want all target system groups to be reconciled into a single organization. Enter no as the value of this attribute if you want each target system group to be reconciled into an organization of its own.
IT Resource Name	Enter the name of the IT resource that you configure by performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7. Sample value: `ADITResource`

Table 3–5 (Cont.) Attributes of the Scheduled Task for Reconciliation of Group Data from a Target

Attribute	Description
Resource Object	This attribute holds the name of the resource object against which group reconciliation runs must be performed. Value: `AD Group` **Note:** For the resource object shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the resource object, then you must enter the unique name of that resource object as the value of this attribute.
ADCS TimeStamp	This attribute holds the date and time at which the last group reconciliation run ended. The reconciliation engine automatically enters a value in this attribute. Default value: `0` **Note:** You must not change the value of this attribute.
Task Scheduler Name	This attribute holds the name of the scheduled task for reconciliation of group data from the target system. Value: `AD Group Recon` **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that scheduled task as the value of this attribute.
Field Lookup Code	Enter one of the following values: ■ For Microsoft Active Directory, enter `Lookup.ADGroupReconciliation.FieldMap`. ■ For Microsoft ADAM, enter `Lookup.ADAMGroupReconciliation.FieldMap`.
Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.AD.Configuration` **Note:** You must not change the value of this attribute. However, if you create a copy of this lookup definition, then you can enter the unique name of the new lookup definition as the value of the Configuration Lookup attribute.

3.4.4.2 Scheduled Tasks for Trusted Source Reconciliation

The following are the scheduled tasks for trusted source reconciliation:

Note: The procedure to configure these scheduled tasks is described later in the guide.

- AD Organization Recon
- AD User Trusted Recon
- AD User Trusted Delete Recon

AD Organization Recon

The AD Organization Recon scheduled task is used to reconcile data about organizations. Table 3–6 describes the attributes of this scheduled task.

Table 3–6 Attributes of the Scheduled Task for Reconciliation of Organization Data from a Trusted Source

Attribute	Description
Search Base	Enter the DN of the organization in which the search for organization records must be performed during reconciliation. Sample values: ▪ `ou=abc,dc=corp,dc=com` ▪ `dc=corp,dc=com`
Resource Object	This attribute holds the name of the resource object against which the reconciliation run must be performed. Value: `Xellerate Organization` **Note:** You must not change the value of this attribute.
Search Filter	This attribute holds the LDAP search filter that is used to locate organization accounts. Sample value: `(objectclass=organizationalUnit)` **Note:** If you want data about target system containers to be used to create OIM organizations, then set the value of this attribute to the following: `(|(objectclass=organizationalUnit)(objectclass=container))`
IT Resource Name	Enter the name of the IT resource that you configure by performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7. Sample value: `ADITResource`
Search Scope	Enter `subtree` if you want the scope of the search for organization records to be reconciled to include the container specified by the Search Base attribute *and* all of its child containers. For example, if the search base is set to `OU=abc,DC=corp,DC=com`, then the search would cover the `abc` OU and all of its child OUs. Enter `onelevel` if you want the scope of the search for organization records to be restricted to only the container specified by the Search Base attribute. Child containers of the specified container are not included in the search. For example if the search base is set to `OU=abc,DC=corp,DC=com`, then the search would cover only the `abc` OU. **Note:** If you want to enter `onelevel`, then remember that you must not include a space between "one" and "level." Default value: `subtree`
ADCS TimeStamp	This attribute holds the date and time at which the last reconciliation run ended. The reconciliation engine automatically enters a value in this attribute. Default value: `0` **Note:** You must not change the value of this attribute.
Task Scheduler Name	This attribute holds the name of the scheduled task. Value: `AD Organization Recon` **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that scheduled task as the value of the attribute in that scheduled task.
Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.AD.Configuration` **Note:** You must not change the value of this attribute. However, if you create a copy of this lookup definition, then you can enter the unique name of the new lookup definition as the value of the Configuration Lookup attribute.

AD User Trusted Recon

The AD User Trusted Recon scheduled task is used to reconcile user data. Table 3–7 describes the attributes of this scheduled task.

Table 3–7 Attributes of the Scheduled Task for Reconciliation of User Data from a Trusted Source

Attribute	Description
OIM Employee Type	Enter the employee type that must be set for OIM Users created through reconciliation. You must select one of the following values: ▪ Full-Time Employee ▪ `Part-Time Employee` ▪ `Temp` ▪ `Intern` ▪ `Consultant` Default value: `Consultant`
OIM User Type	Enter the role that must be set for OIM Users created through reconciliation. You must select one of the following values: ▪ `End-User` ▪ `End-User Administrator` Default value: `End-User`
OIM Organization	Enter the name of the Oracle Identity Manager organization in which reconciled users must be created. The OIM Organization attribute is taken into account only if you set the MaintainHierarchy attribute to `no`. If you set the MaintainHierarchy attribute to `yes`, then the value of the OIM Organization attribute is ignored. The MaintainHierarchy attribute is described later in this table. Default value: `Xellerate Users`
Trusted Resource Object	Enter the name of the resource object against which the trusted reconciliation run must be performed. Default value: `AD User Trusted` **Note:** For this resource object, you must not change the value of this attribute. However, if you create a copy of the resource object, then you must enter the unique name of that resource object as the value of the attribute.
Delete Recon Task Scheduler Name	This attribute holds the name of the scheduled task for reconciliation of deleted user data from the target system. Value: `AD User Trusted Delete Recon` **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task and the scheduled task for reconciliation of deleted user data, then you must enter the unique name of that new Delete reconciliation scheduled task as the value of the Delete Recon Task Scheduler Name attribute in the copy of this scheduled task.
IT Resource Name	Enter the name of the IT resource that you configure by performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7. Sample value: `ADITResource`
ADCS TimeStamp	This attribute holds the date and time at which the last user reconciliation run ended. The reconciliation engine automatically enters a value in this attribute. Default value: `0` **Note:** You must not change the value of this attribute.

Table 3–7 (Cont.) Attributes of the Scheduled Task for Reconciliation of User Data from a Trusted Source

Attribute	Description
Task Scheduler Name	This attribute holds the name of the scheduled task. Value: AD User Trusted Recon **Note:** For this scheduled task, you must not change the value of this attribute. However, if you create a copy of this scheduled task, then you must enter the unique name of that scheduled task as the value of the attribute in that scheduled task.
Search Scope	Enter `subtree` if you want the scope of the search for records to be reconciled to include the container specified by the Search Base attribute *and* all of its child containers. For example, if the search base is set to `OU=abc,DC=corp,DC=com`, then the search would cover the `abc` OU and all of its child OUs. Enter `onelevel` if you want the scope of the search for records to be restricted to only the container specified by the Search Base attribute. Child containers of the specified container are not included in the search. For example if the search base is set to `OU=abc,DC=corp,DC=com`, then the search would cover only the `abc` OU. **Note:** If you want to enter `onelevel`, then remember that you must not include a space between "one" and "level." Default value: `subtree`

Field Lookup Code	This attribute holds the name of the lookup definition that contains mappings between the target system fields and the corresponding Oracle Identity Manager fields.
	■ If the target system is Microsoft Active Directory, then enter the following value:
	`Lookup.ADReconciliation.FieldMap`
	■ If the target system is Microsoft ADAM, then enter the following value:
	`Lookup.ADAMReconciliation.FieldMap`

MaintainHierarchy	Enter `yes` to specify that you want to maintain in Oracle Identity Manager the same organization hierarchy that is maintained on the target system. Otherwise, enter `no`. If the MaintainHierarchy attribute is set to `yes`, then the value specified for the Search Base attribute must begin with `ou`. This attribute is described later in this table. If the value of the Search Base attribute began with `dc`, then organization hierarchy might not be maintained during reconciliation. Default value: `no` **Note:** If you set this attribute to `yes`, then you must schedule the task for organization reconciliation (AD Organization Recon) to run before this scheduled task.
Transform Lookup Code	Enter the name of the lookup definition that you have created to link Microsoft Active Directory fields with the JAR files that must be run to transform each field. This attribute is valid only when the Use Transform Mapping attribute is set to yes. Value: `Lookup.ADReconciliation.TransformationMap` **Note:** You must not change the value of this attribute. See "Transforming Data Reconciled Into Oracle Identity Manager" on page 4-34 for detailed information about using the Transform Lookup Code attribute.
Use Transform Mapping	Enter `yes` to specify that you want the transformations referenced by the Transform Lookup Code attribute to be applied. Otherwise, enter `no`. Default value: `no` See "Transforming Data Reconciled Into Oracle Identity Manager" on page 4-34 for detailed information about using the Use Transform Mapping attribute.

Table 3–7 (Cont.) Attributes of the Scheduled Task for Reconciliation of User Data from a Trusted Source

Attribute	Description
Start Record	Enter the number of the target system record from which a batched reconciliation run must begin. Default value: `1` This attribute is used in conjunction with the Batch Size and Number of Batches attributes. All three attributes are discussed in "Batched Reconciliation" on page 3-11. As mentioned in that section, it is recommended that you accept the default value of the Start Record attribute.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system. Default value: `1` This attribute is used in conjunction with the Number of Batches and Start Record attributes. All three attributes are discussed in "Batched Reconciliation" on page 3-11.
Number of Batches	Enter the number of batches that must be reconciled. Default value: `All Available` Sample value: `25` This attribute is used in conjunction with the Batch Size and Start Record attributes. All three attributes are discussed in detail in "Batched Reconciliation" on page 3-11. If you accept the default value (`All Available`), then batched reconciliation is not performed. In addition, the reconciliation of Terminal Services Profile fields is disabled.
Will Submit All Records	Enter `yes` to configure full reconciliation. Enter `no` to configure incremental reconciliation. Default value: `no` See "Full Reconciliation vs. Incremental Reconciliation" on page 3-12 for detailed information about this attribute.
Search Base	Enter the DN of the organization in which the search for user records must be performed during reconciliation. Sample value: `ou=abc,dc=corp,dc=com`
Ignored Chars Username	Enter the list of characters that must be removed from user ID values reconciled from the target system. Use this attribute to prevent the reconciliation of characters that may cause errors in other target systems. The list that you enter must be a string of characters, without any delimiters. If you do not want to use this feature, then enter `[NONE]`. Sample value: # This sample value will remove the number sign (#) character from all user ID values that are reconciled from the target system. Default value: `[NONE]`
Search Filter	Enter the query condition that is to be used during reconciliation for locating target system user accounts that meet certain criteria. Default value: `(objectClass=user)` Sample value: `(&(objectClass=user)(givenName=first))` See "Limited Reconciliation vs. Regular Reconciliation" on page 3-10 for detailed information about this attribute.
Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.AD.Configuration` **Note:** You must not change the value of this attribute.

AD User Trusted Delete Recon

The AD User Trusted Delete Recon scheduled task is used to reconcile data about deleted users. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted. Table 3–8 describes the attributes of this scheduled task.

Table 3–8 Attributes of the Scheduled Task for Reconciliation of Deleted User Data from a Trusted Source

Attribute	Description
IT Resource Name	Enter the name of the IT resource that you configure by performing the procedure described in "Configuring the IT Resource for the Target System" on page 2-7. Sample value: `ADITResource`
Search Filter	This attribute holds the LDAP search filter that is used to locate deleted user accounts on the target system. Value: `(objectclass=user)` **Note:** You must not change the value of this attribute.
ADCS Timestamp	This attribute holds the time stamp at which the last Delete User reconciliation run ended. In addition, the value of this attribute is updated when the scheduled task for trusted source reconciliation of user accounts (AD User Trusted Recon) is run with its ADCS TimeStamp attribute set to 0. The reconciliation engine automatically enters a value in this attribute. Default value: `0` **Note:** You must not change the value of this attribute.
Trusted Resource Object	This attribute holds the name of the resource object against which the reconciliation run is performed. Value: `AD User Trusted`
Task Scheduler Name	This attribute holds the name of the scheduled task. Value: `AD User Trusted Delete Recon` **Note:** You must not change the value of this attribute.
Configuration Lookup	This attribute holds the name of the lookup definition containing values that are used during both reconciliation and provisioning: Value: `Lookup.AD.Configuration` **Note:** You must not change the value of this attribute. However, if you create a copy of this lookup definition, then you can enter the unique name of the new lookup definition as the value of the Configuration Lookup attribute.

3.5 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–9 lists the scheduled tasks that you must configure.

Table 3–9 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

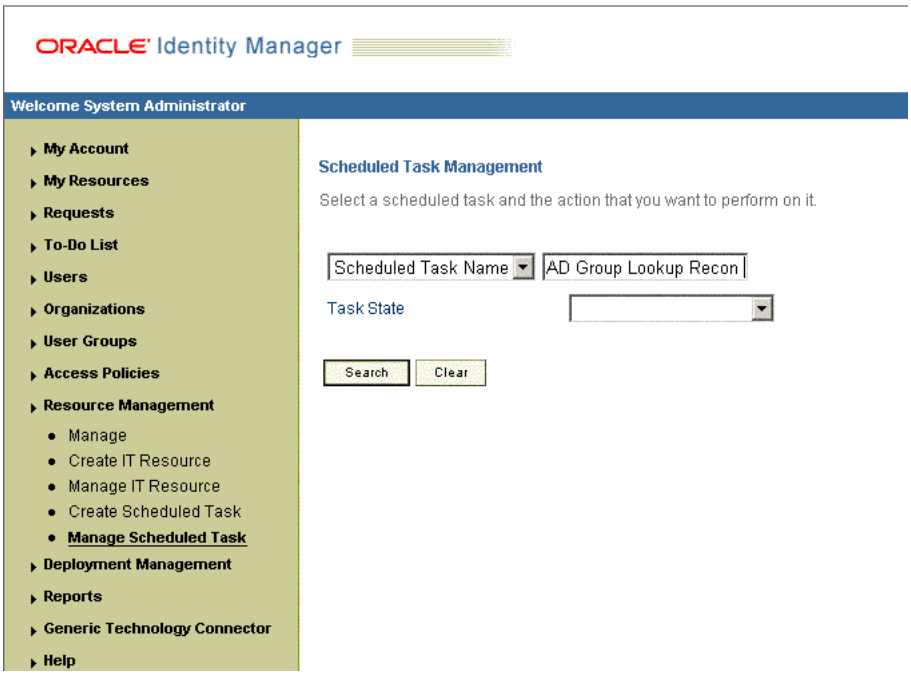
Scheduled Task	Description
AD Group Lookup Recon	This scheduled task is used to synchronize the values of group lookup fields between Oracle Identity Manager and the target system. For information about this scheduled task and its attributes, see "Scheduled Tasks for Lookup Field Synchronization" on page 3-8.
AD Organization Lookup Recon	This scheduled task is used to synchronize the values of organization lookup fields between Oracle Identity Manager and the target system. For information about this scheduled task and its attributes, see "Scheduled Tasks for Lookup Field Synchronization" on page 3-8.
AD User Target Recon	This scheduled task is used to fetch user data during target resource reconciliation. For information about this scheduled task and its attributes, see "Scheduled Tasks for Target Resource Reconciliation" on page 3-13.
AD User Target Delete Recon	This scheduled task is used to fetch data about deleted users during target resource reconciliation. During a reconciliation run, for each deleted user account on the target system, the AD User resource is revoked for the corresponding OIM User. For information about this scheduled task and its attributes, see "Scheduled Tasks for Target Resource Reconciliation" on page 3-13.
AD Organization Recon	This scheduled task is used to reconcile data about organizations. For information about this scheduled task and its attributes, see "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18.
AD User Trusted Recon	This scheduled task is used to fetch user data during trusted source reconciliation. For information about this scheduled task and its attributes, see "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18.
AD User Trusted Delete Recon	This scheduled task is used to fetch data about deleted users during trusted source reconciliation. During a reconciliation run, for each deleted target system account, the corresponding OIM User is deleted. For information about this scheduled task and its attributes, see "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18.
AD Group Recon	This scheduled task is used to fetch data about groups during target resource reconciliation. For information about this scheduled task and its attributes, see "Scheduled Tasks for Target Resource Reconciliation" on page 3-13.

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage Scheduled Task**.
4. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

   Figure 3–1 shows the Scheduled Task Management page.

Figure 3–1 Scheduled Task Management Page



5. In the search results table, click the edit icon in the Edit column for the scheduled task. Figure 3–2 shows the Scheduled Task Details page.

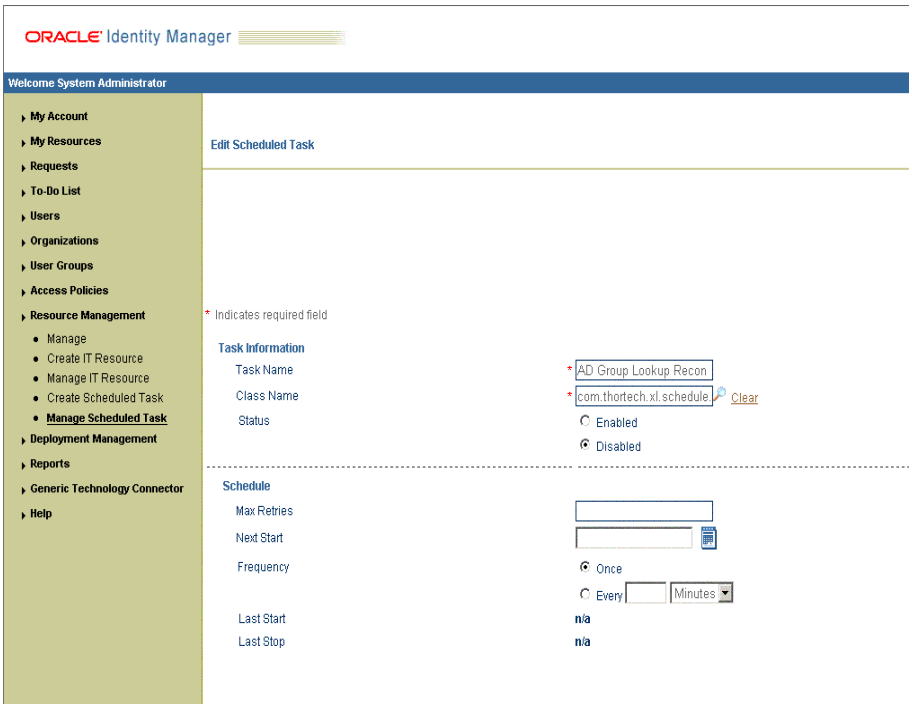
Figure 3–2 Scheduled Task Details Page

6. On the Edit Scheduled Task Details page, you can modify the following details of the scheduled task by clicking **Edit**:

- **Status:** Specify whether or not you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
- **Max Retries:** Enter an integer value in this 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. The default value is 1.
- **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
- **Frequency:** Specify the frequency at which you want the task to run.

When you click Edit, the Edit Scheduled Task page is displayed. Figure 3–3 shows this page.

Figure 3–3 Edit Scheduled Task Page



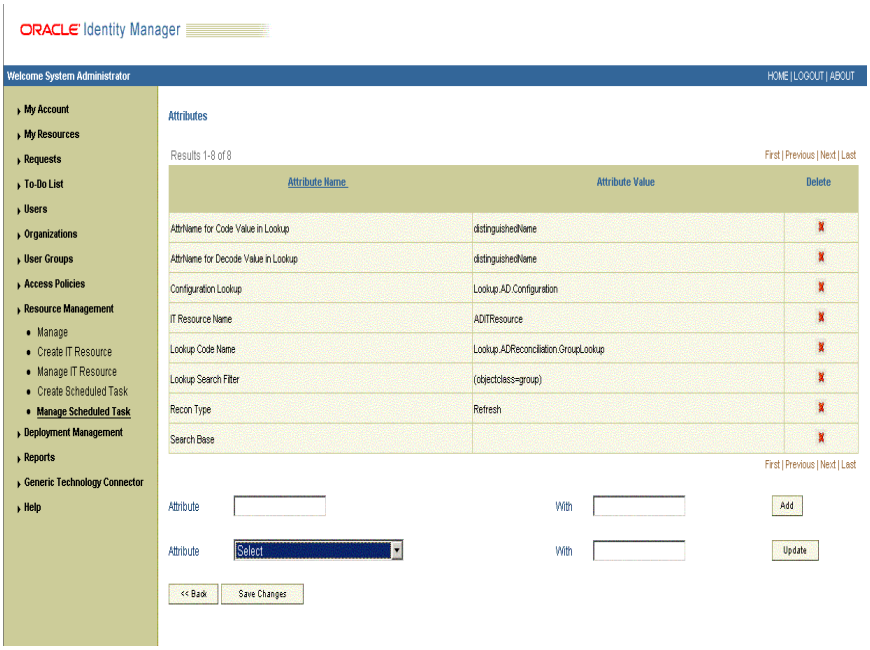
7. After modifying the values for the scheduled task details listed in the previous step, click **Continue**.
8. Specify values for the attributes of the scheduled task. To do so, select each attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for the 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 is left empty, then reconciliation is not performed.

Figure 3–4 shows the Attributes page. The attributes of the scheduled task that you select for modification are displayed on this page.

Figure 3–4 Attributes Page



9. Click **Save Changes** to commit all the changes to the database.

> **Note:** If you want to stop a scheduled task while it is running, then use the Stop Execution feature of the Design Console. See the "The Task Scheduler Form" section in *Oracle Identity Manager Design Console Guide* for information about this feature.

3.6 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.

3.6.1 Specifying the Object Class for User Provisioning

By default, newly created users on the target system are assigned to the user object class. While performing the Create User provisioning operation on Oracle Identity Manager, you may want to assign the user to other object classes, in addition to the user object class. The connector implements this feature through the Lookup.AD.Configuration lookup definition. See "Configuring the Lookup.AD.Configuration Lookup Definition" on page 3-5 for more information.

3.7 Performing Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a Microsoft Active Directory account for the user. The following are types of provisioning operations:

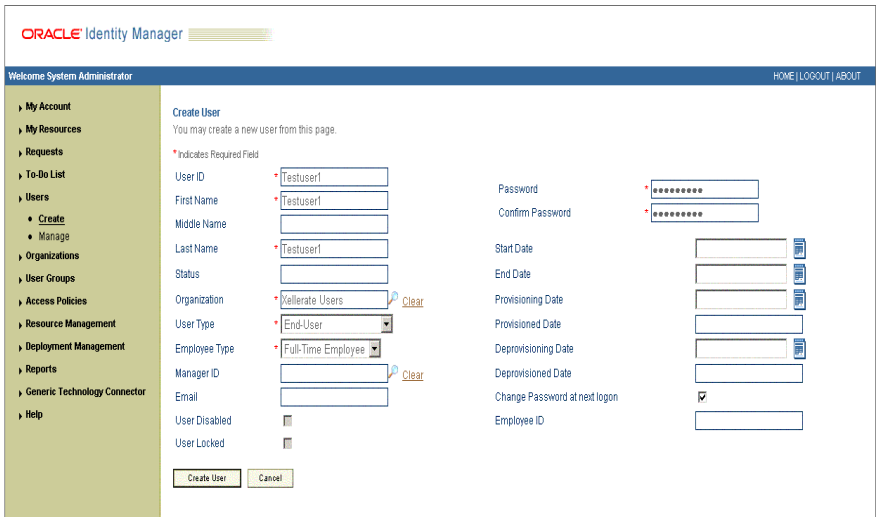
- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

> **See Also:** *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

To provision a resource by using the direct provisioning approach:

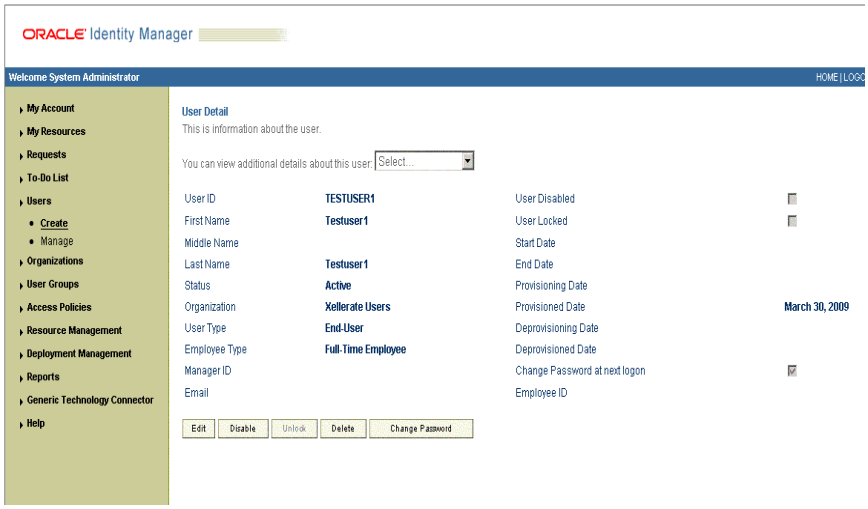
1. Log in to the Administrative and User Console.
2. From the Users menu:
   - Select **Create** if you want to first create the OIM User and then provision a Microsoft Active Directory account to the user.
   - Select **Manage** if you want to provision a Microsoft Active Directory account to an existing OIM User.
3. If you select Create, on the Create User page, enter values for the OIM User fields and then click **Create User**. Figure 3–5 shows the Create User page.

Figure 3–5 Create User Page



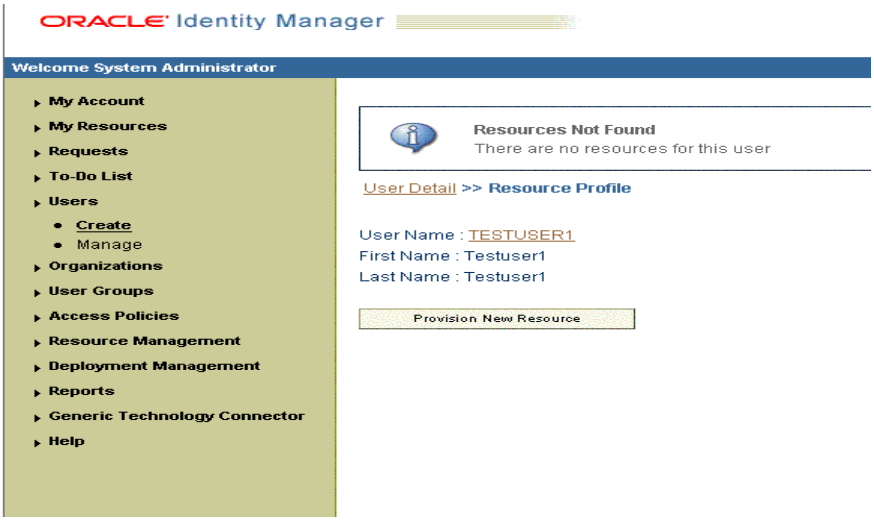
4. If you select Manage, then search for the OIM User and select the link for the user from the list of users displayed in the search results.
5. On the User Detail page, select **Resource Profile** from the list at the top of the page. Figure 3–6 shows the User Detail page.

Figure 3–6 User Detail Page



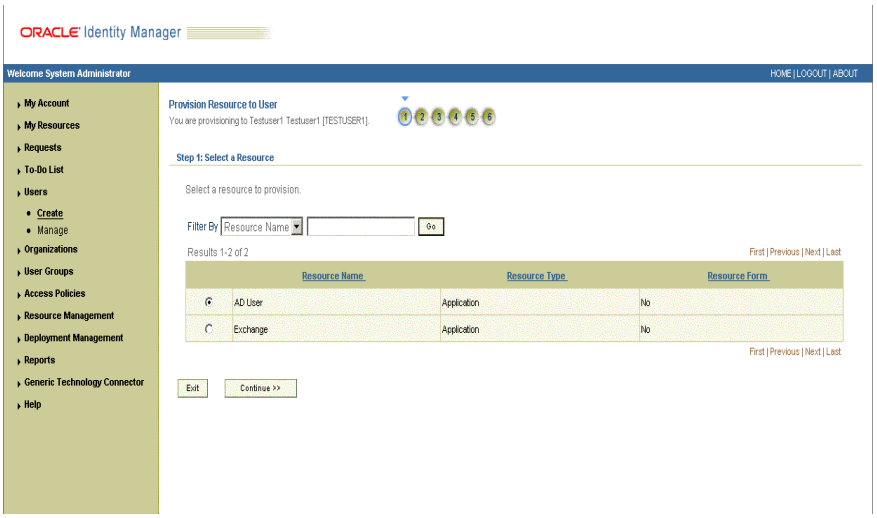
6. On the Resource Profile page, click **Provision New Resource**. Figure 3–7 shows the Resource Profile page.

Figure 3–7 Resource Profile Page



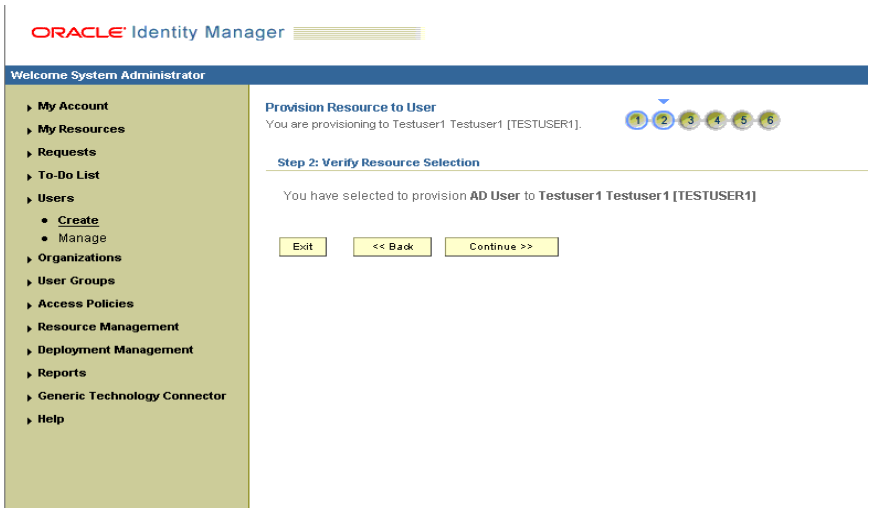
7. On the Step 1: Select a Resource page, select **AD User** from the list and then click **Continue**. Figure 3–8 shows the Step 1: Select a Resource page.

Figure 3–8 Step 1: Select a Resource Page



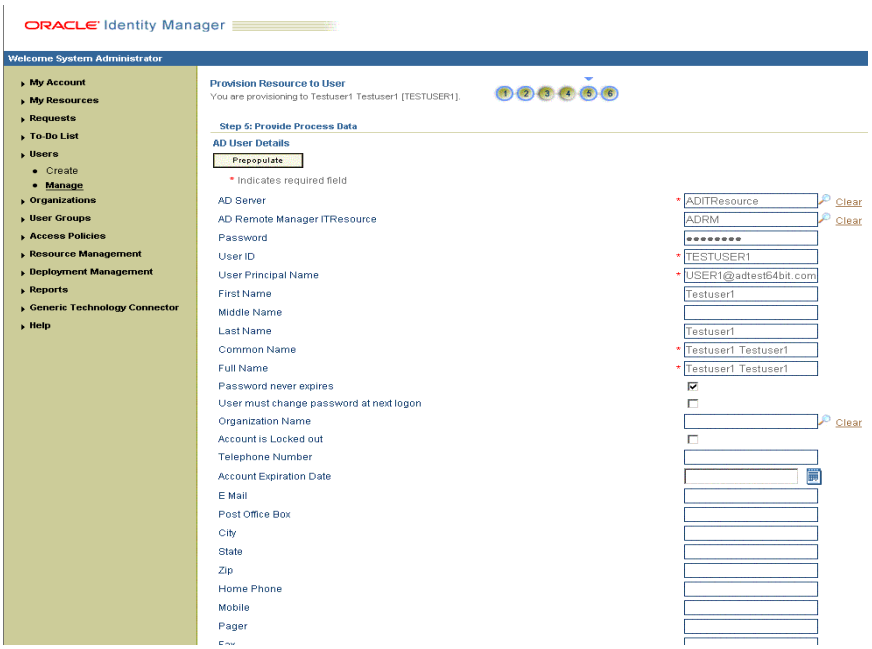
8. On the Step 2: Verify Resource Selection page, click **Continue**. Figure 3–9 shows the Step 2: Verify Resource Selection page.

Figure 3–9 Step 2: Verify Resource Selection Page



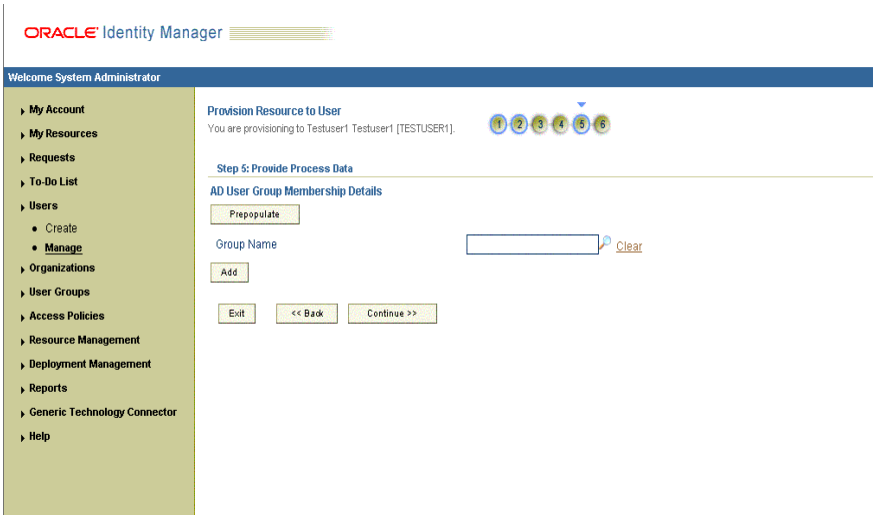
9. On the Step 5: Provide Process Data for AD User Details page, enter the details of the account that you want to create on the target system and then click **Continue**. If you are setting values for the Terminal Services Profile fields, then you must select the Remote Manager IT resource. Figure 3–10 shows the user details added.

Figure 3–10 Step 5: Provide Process Data for AD User Details Page



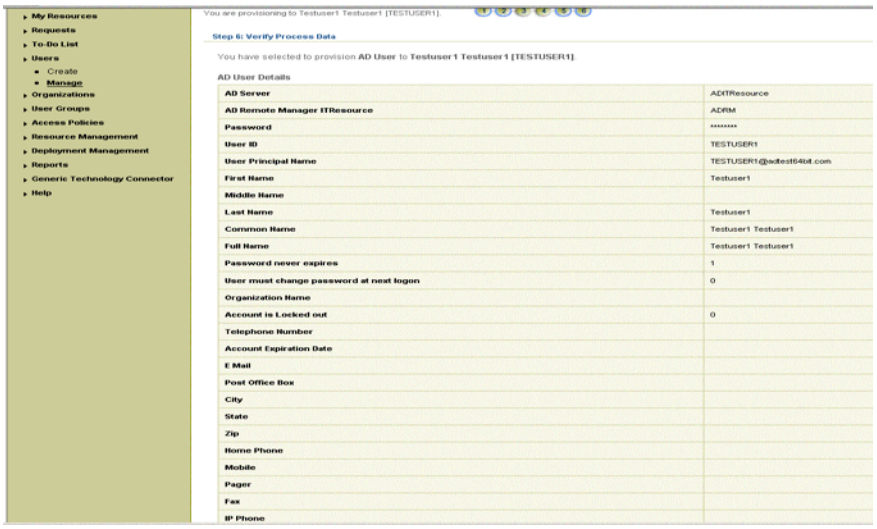
10. On the Step 5: Provide Process Data for AD User Group Membership Details page, search for and select a group for the user on the target system and then click **Continue**. Figure 3–11 shows this page.

Figure 3–11 Step 5: Provide Process Data for AD User Group Membership Details Page



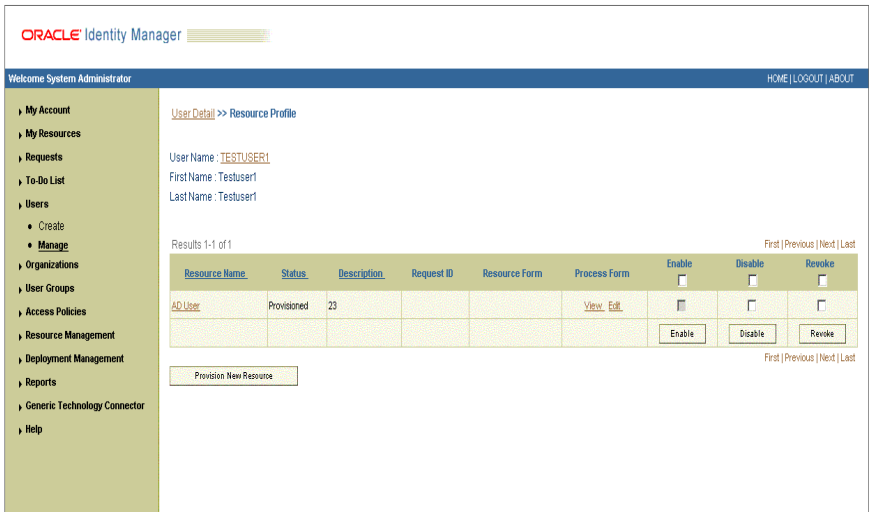
11. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**. Figure 3–12 shows Step 6: Verify Process Data page.

Figure 3–12 Step 6: Verify Process Data Page



The Resource Profile page is displayed. Figure 3–13 shows this page. The resource that you provisioned is displayed on this page.

Figure 3–13 Resource Profile Page



4

Extending the Functionality of the Connector

This chapter describes procedures that you can perform to extend the functionality of the connector for addressing your specific business requirements.

This chapter discusses the following optional procedures:

- See "Modifying Existing Field Mappings" if you want to modify the default field mappings between Oracle Identity Manager and the target system.
- The following sections describe procedures that are aimed at extending the target resource reconciliation functionality of the connector:
  - The "Adding New Fields for Target Resource Reconciliation" section describes the procedure to add mappings between fields of the target system and Oracle Identity Manager.
  - The "Adding New Multivalued Fields for Target Resource Reconciliation" section describes the procedure to add mappings between multivalued fields of the target system and Oracle Identity Manager.
- The following sections describe procedures that are aimed at extending the provisioning functionality of the connector:
  - The "Adding New Fields for Provisioning" section describes the procedure to add mappings between fields of the target system and Oracle Identity Manager.
  - The "Adding New Multivalued Fields for Provisioning" section describes the procedure to add mappings between multivalued fields of the target system and Oracle Identity Manager.
  - The "Adding Mappings for New Object Classes" section describes the procedure to add mappings for object classes that you create on the target system.
  - The "Enabling the Auto Pre-populate and Auto Save Options" section describes the procedure to enable the Auto Pre-populate and Auto Save options of the resource object.
  - The "Using Your Own Provisioning Script" section provides instructions on extending or changing the functionality of the default provisioning script.
  - The "Removing the ExecuteRemoteScripts Process Task" section describes the procedure to disable the ADCS Execute Remote Script adapter. This adapter is run by default at the end of a successful Create User provisioning operation.
- The "Adding New Fields for Trusted Source Reconciliation" section describes the procedure to add mappings between fields of the target system and Oracle Identity Manager.

- The "Transforming Data Reconciled Into Oracle Identity Manager" section describes the procedure to modify data that is fetched into Oracle Identity Manager for reconciliation.
- The "Configuring the Connector for Multiple Trusted Source Reconciliation" section describes the procedure for using the target system as one of the trusted sources of identity data in your organization.
- The "Configuring the Connector for Multiple Installations of the Target System" section describes the procedure to configure the connector for multiple installations of the target system.

4.1 Modifying Existing Field Mappings

Default mappings between fields of the target system and Oracle Identity Manager are listed in the following sections:

- "User Fields for Target Resource Reconciliation" on page 1-8
- "User Fields for Provisioning" on page 1-16
- "User Fields for Trusted Source Reconciliation" on page 1-25

If you want to modify these mappings, then:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the lookup definition that you want to modify.

   Table 4–1 describes the contents of the lookup definitions that store field mapping information for reconciliation and provisioning.

Table 4–1 Lookup Definitions That Store Field Mapping Information

Lookup Definition	Contents of the Code Key Column	Contents of the Decode Column
Lookup.ADReconciliation.FieldMap This is used during reconciliation.	Names of user fields in Microsoft Active Directory	Names of process form fields for Microsoft Active Directory users
Lookup.ADGroupReconciliation.FieldMap This is used during reconciliation.	Names of group fields in Microsoft Active Directory	Names of process form fields for Microsoft Active Directory groups
Lookup.ADAMReconciliation.FieldMap This is used during reconciliation.	Names of user fields in Microsoft ADAM	Names of process form fields for Microsoft ADAM users
Lookup.ADAMGroupReconciliation.FieldMap This is used during reconciliation.	Names of group fields in Microsoft ADAM	Names of process form fields for Microsoft ADAM groups
Lookup.AD.BLOBAttribute.Values This is used during reconciliation.	Names of Terminal Services Profile fields in Microsoft Active Directory	Names of process form fields corresponding to the Terminal Services Profile fields in Microsoft Active Directory

Table 4–1 (Cont.) Lookup Definitions That Store Field Mapping Information

Lookup Definition	Contents of the Code Key Column	Contents of the Decode Column
AtMap.AD This is used during provisioning.	Names of process form fields for Microsoft Active Directory users	Names of user fields in Microsoft Active Directory
AtMap.ADGroup This is used during provisioning.	Names of process form fields for Microsoft Active Directory groups	Names of group fields in Microsoft Active Directory
AtMap.ADAM This is used during provisioning.	Names of process form fields for Microsoft ADAM users	Names of user fields in Microsoft ADAM
AtMap.ADAMGroup This is used during provisioning.	Names of process form fields for Microsoft ADAM groups	Names of group fields in Microsoft ADAM
AtMap.AD.RemoteScriptlookUp This is used during provisioning.	Names of process form fields corresponding to the Terminal Services Profile fields in Microsoft Active Directory	Names of Terminal Services Profile fields in Microsoft Active Directory

4. Make the required change in the field mappings by modifying the Code Key and Decode values.
5. Click **Save**.

4.2 Adding New Fields for Target Resource Reconciliation

Note:

- This procedure can be applied to add either user or group fields.
- 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 you want to add a multivalued field for target resource reconciliation, then see "Adding New Multivalued Fields for Target Resource Reconciliation" on page 4-8.

By default, the fields listed in Table 1–4 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new fields for target resource reconciliation.

By default, the connector provides mappings for the Terminal Services Profile fields of the target system. You can add mappings for fields of the Environment, Remote Control, and Sessions categories.

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

Note: Do not perform the procedure to determine the target system name of the field if it belongs to one of the following user data categories:

- Remote Control
- Sessions
- Environment

Instead, refer to Appendix C, "Terminal Services Profile Field Names for Reconciliation and Provisioning" for information about a replacement for the target system field name.

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:

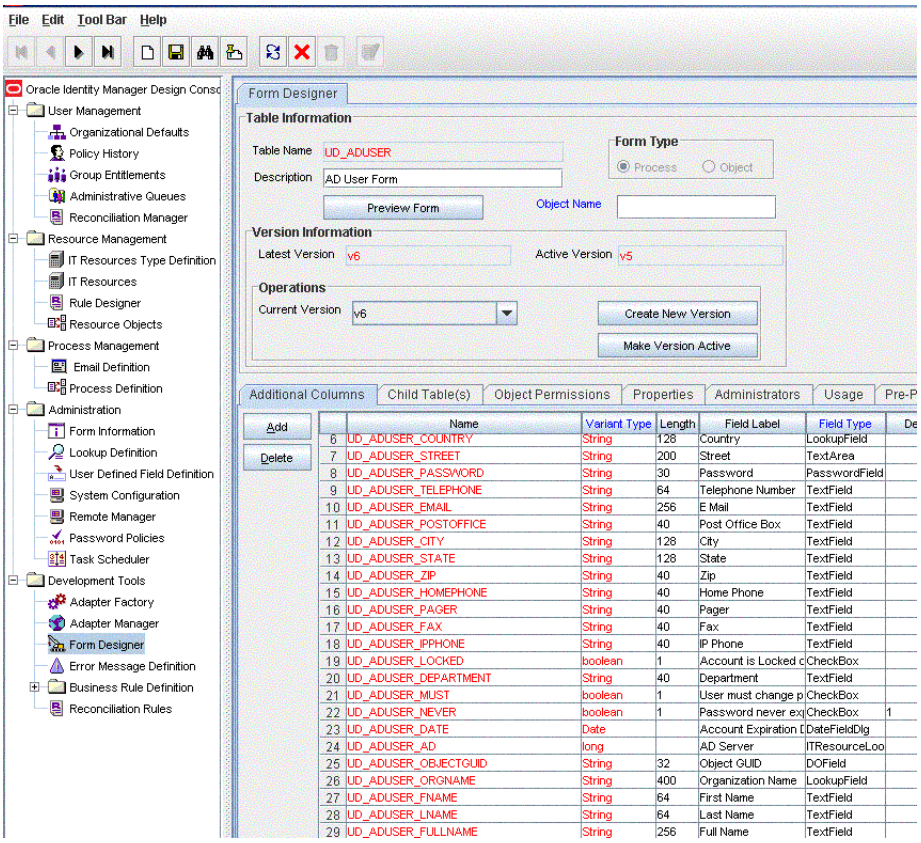
See Also: *Oracle Identity Manager Design Console Guide* for detailed information about these steps

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. For groups, search for **UD_ADGRP** 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.** Figure 4–1 shows the new field added to the process form.

Figure 4–1 New Field Added to the Process Form



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. For groups, search for and open the **AD Group** resource object

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

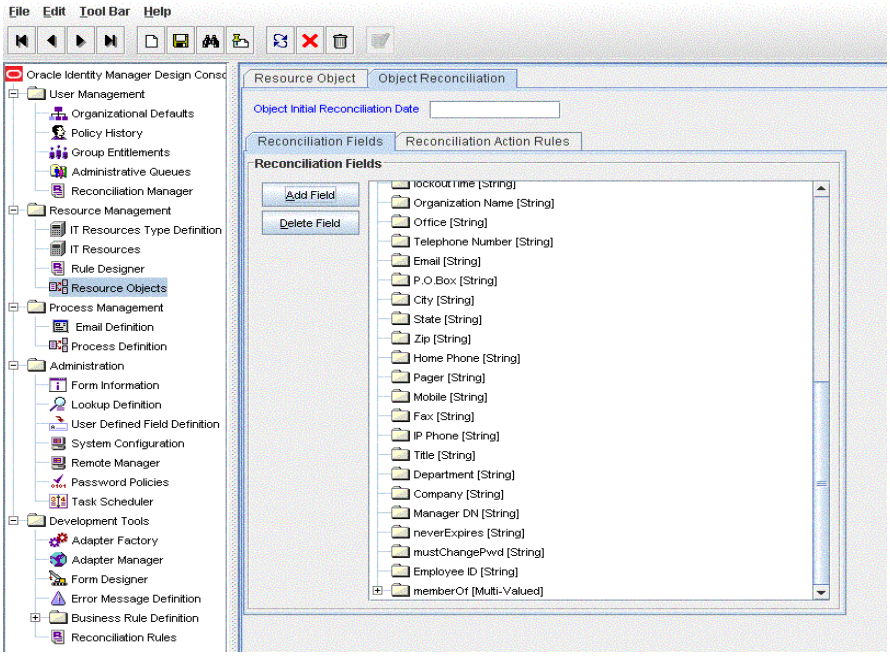
   e. Enter the details of the field.

      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**. Figure 4–2 shows the new reconciliation field added to the resource object.

Figure 4–2 New Reconciliation Field Added in the Resource Object



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

   a. Expand **Process Management**.

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

   c. Search for and open the **AD User** process definition. For groups, search for and open the **AD Group** process definition.

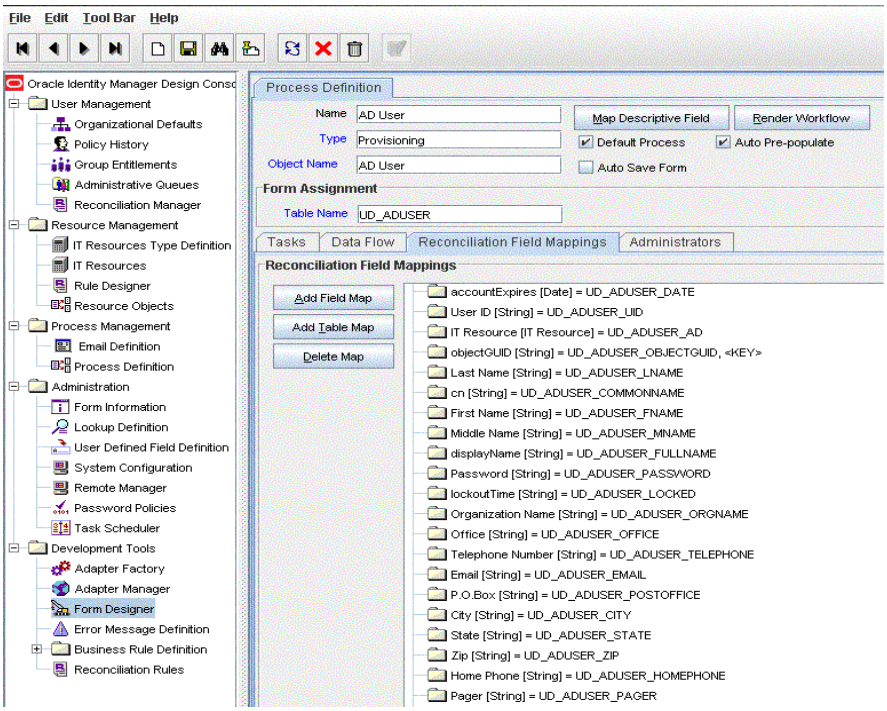
   d. On the **Reconciliation Field Mappings** tab of the **AD User** (or AD Group) process definition, click **Add Field Map**.

   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**. Figure 4–3 shows the new reconciliation field mapped to a process data field in the process definition.

Figure 4–3 New Reconciliation Field Mapped to the Process Data Field



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

   Note: For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

   – For a user field on Microsoft Active Directory, open **Lookup.ADReconciliation.FieldMap**.

   – For a user field on Microsoft ADAM, open **Lookup.ADAMReconciliation.FieldMap**.

   – For a group field on Microsoft Active Directory, open **Lookup.ADGroupReconciliation.FieldMap**.

   – For a group field on Microsoft ADAM, open **Lookup.ADAMGroupReconciliation.FieldMap**.

   d. For a user field, if the field that you want to add is an Environment, Remote Control, or Sessions field, then search for and open the **Lookup.AD.BLOBAttribute.Values** lookup definition.

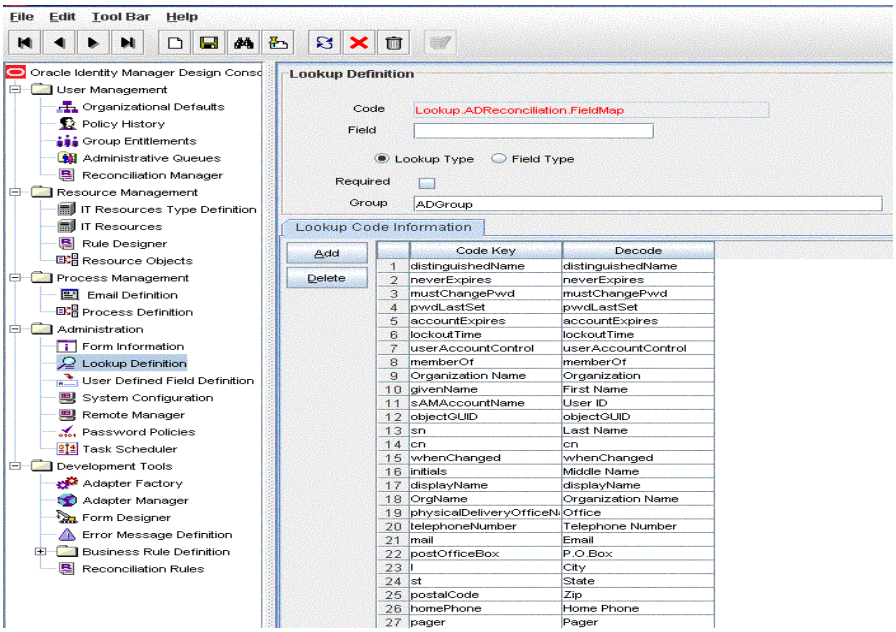
   Note: You need not make any change in the VBScript file run by the Remote Manager during provisioning operations.

e. 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.

f. Click **Save**. Figure 4–4 shows the lookup code added to the lookup definition.

Figure 4–4 Entry Added in the Lookup Definition



4.3 Adding New Multivalued Fields for Target Resource Reconciliation

Note:

This procedure can be applied to add either user or group fields.

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.

By default, the multivalued fields listed in Table 1–4 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued fields for target resource reconciliation.

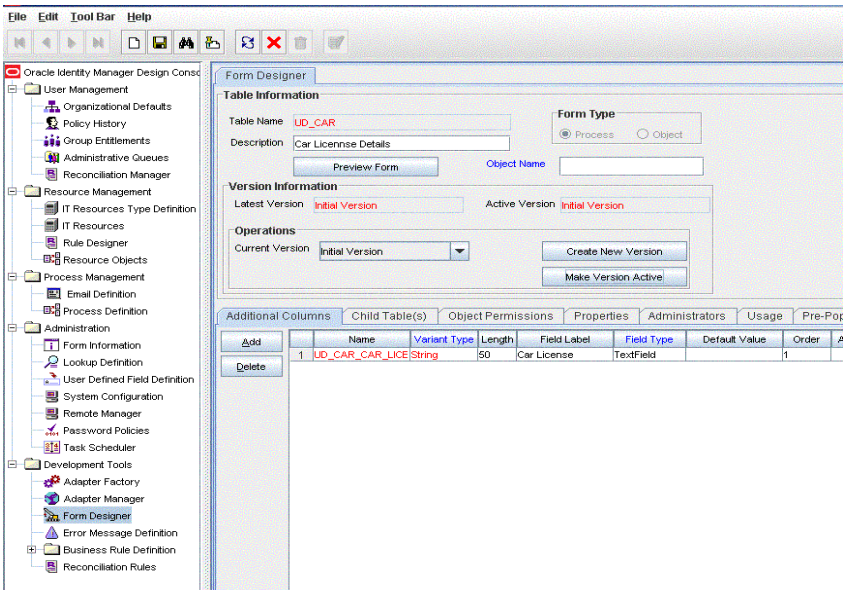
To add a new multivalued field for target resource reconciliation:

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.** Figure 4–5 shows the multivalued field added on a new form.

Figure 4–5 Multivalued Field Added on a New Form



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** process form. For groups, search for and open the **UD_ADGRP** process form.

b. Click **Create New Version**.

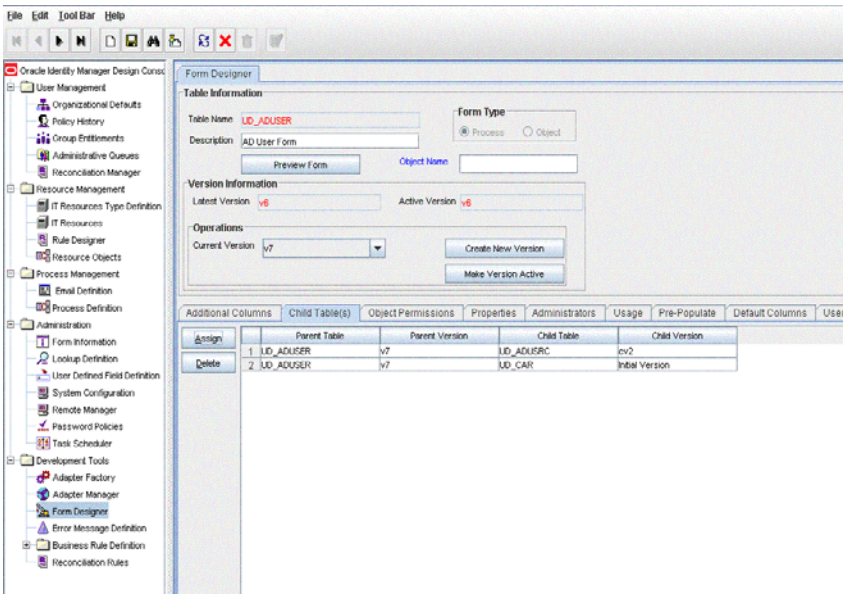
c. Click the **Child Table(s)** tab.

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.** Figure 4–6 shows the child form added to the process form.

Figure 4–6 Child Form Added to the Process Form



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** resource object. For groups, search for and open the **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.

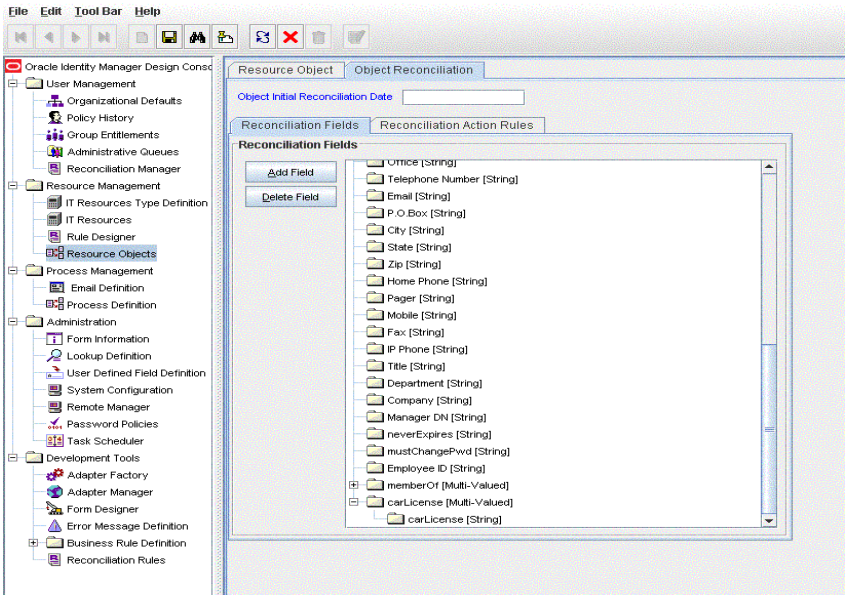
   h. Select **Define Property Fields**.

   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. Figure 4–7 shows the new reconciliation field added in the resource object.

Figure 4–7 New Reconciliation Field Added in the Resource Object



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** process definition. For groups, search for and open the **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.

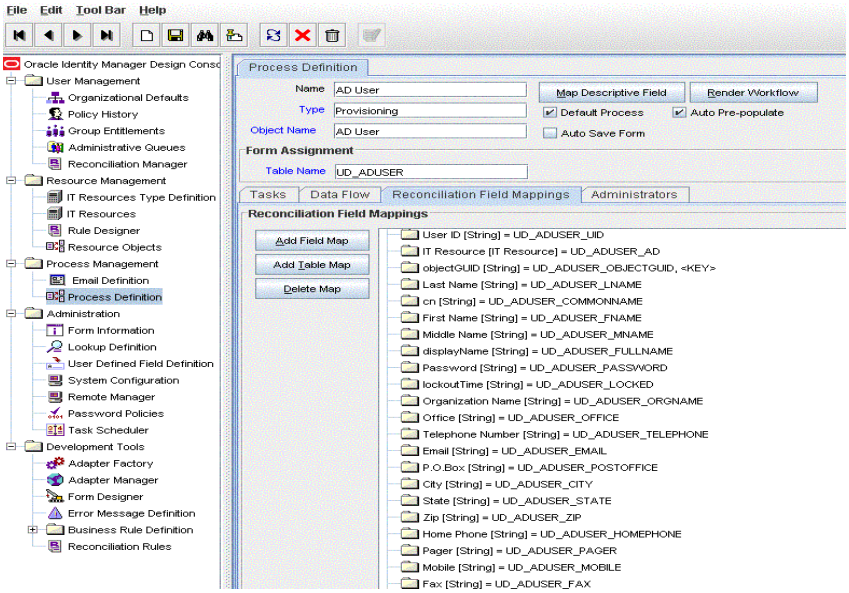
   f. Right-click the newly created field, and select **Define Property Field Map**.

   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 UD_CAR_LICENSE.

   i. Select **Key Field for Reconciliation Field Matching** and click **Save**. Figure 4–8 shows the new reconciliation field mapped to a process data field in the process definition.

Figure 4–8 New Reconciliation Field Mapped to a Process Data Field



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** (or Lookup.ADGroupReconciliation.FieldMap) lookup definition if the target system is Microsoft Active Directory.

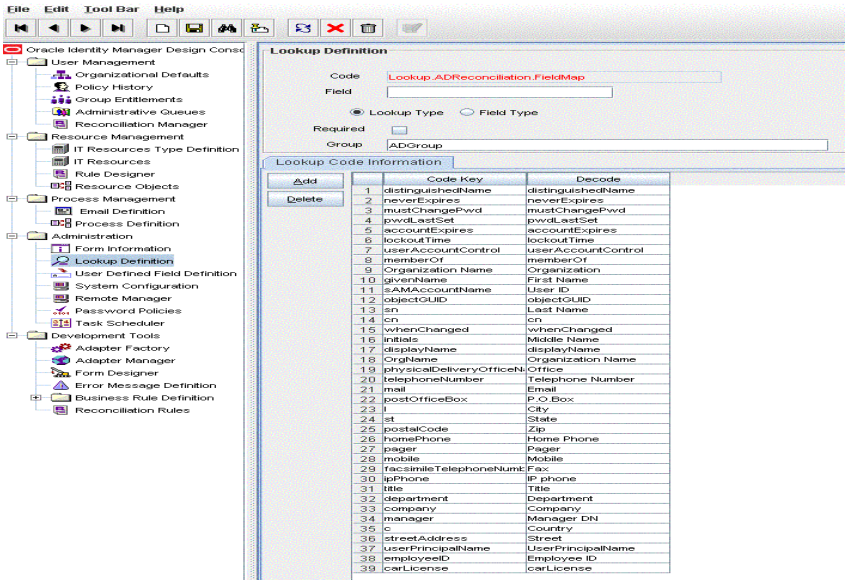
   Note: For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

   Search for and open the **Lookup.ADAMReconciliation.FieldMap** (or Lookup.ADAMGroupReconciliation.FieldMap) lookup definition if the target system is Microsoft ADAM.

   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. Figure 4–9 shows the lookup code added to the lookup definition.

Figure 4–9 Entry Added in the Lookup Definition



7. For a user field, add the multivalued field to the Lookup.AD.Configuration lookup definition as follows:

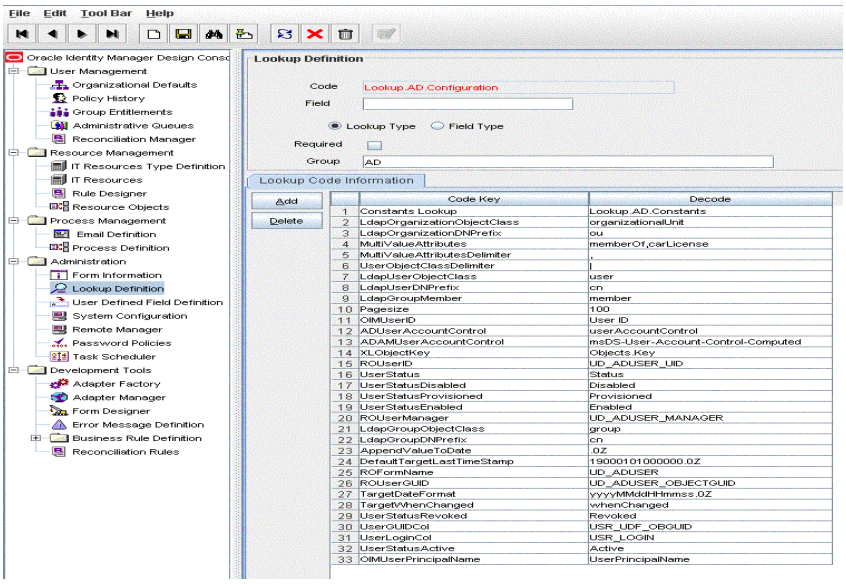
   a. Double-click **Lookup Definition**.

   b. Search for and open the **Lookup.AD.Configuration** lookup definition.

   c. Add multivalued attributes that are to be reconciled in the Decode field and click **Save**. The attributes must be separated by the Decode value entered in the MultiValueAttributesDelimiter field.

      For example, if MultiValueAttributesDelimiter contains the semicolon (;) as the Decode value, then the Decode value of MultiValueAttributes must be `memberOf;carLicense`. In this value, the semicolon has been used as the delimiter character. Figure 4–10 shows the multivalued field added to the Lookup.AD.Configuration lookup definition.

Figure 4–10 Multivalued Field Added to the Lookup Definition



4.4 Adding New Fields for Provisioning

By default, the fields listed in Table 1–8 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional fields for provisioning.

By default, the connector provides mappings for the Terminal Services Profile fields of the target system. You can add mappings for fields of the Environment, Remote Control, and Sessions categories.

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

Note: Do not perform the procedure to determine the target system name of the field if it belongs to one of the following user data categories:

- Remote Control
- Sessions
- Environment

Instead, refer to Appendix C, "Terminal Services Profile Field Names for Reconciliation and Provisioning" for information about a replacement for the target system field name.

---

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

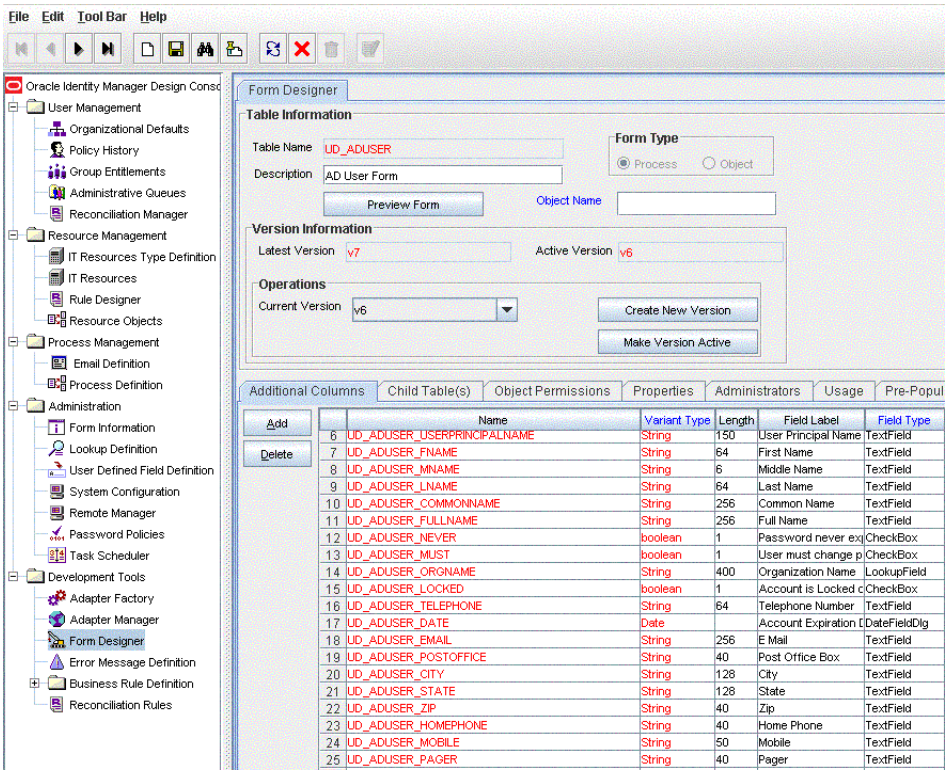
1. Log in to the Oracle Identity Manager Design Console.
2. Add the new field on the process form.

   If you have added the field on the process form by performing Step 2 of "Adding New Fields for Target Resource Reconciliation" on page 4-3, then you need not add the field again. If you have not added the field, then:

   a. Expand **Development Tools**.
   b. Double-click **Form Designer.**
   c. Search for and open the **UD_ADUSER** process form. For groups, search for and open the **UD_ADGRP** 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.** Figure 4–11 shows the new field added to the process form.

Figure 4–11 New Field Added to the Process Form



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 one of the lookup definitions:

      – For a user field on Microsoft Active Directory, open **AtMap.AD**.

      – For a user field on Microsoft ADAM, open **AtMap.ADAM**.

      – For a group field on Microsoft Active Directory, open **AtMap.ADGroup**.

      – For a group field on Microsoft ADAM, open **AtMap.ADAMGroup**.

   d. If the field that you want to add is an Environment, Remote Control, or Sessions field, then search for and open the **AtMap.AD.RemoteScriptlookUp** lookup definition.

      Note: You need not make any change in the VBScript file run by the Remote Manager during provisioning operations.

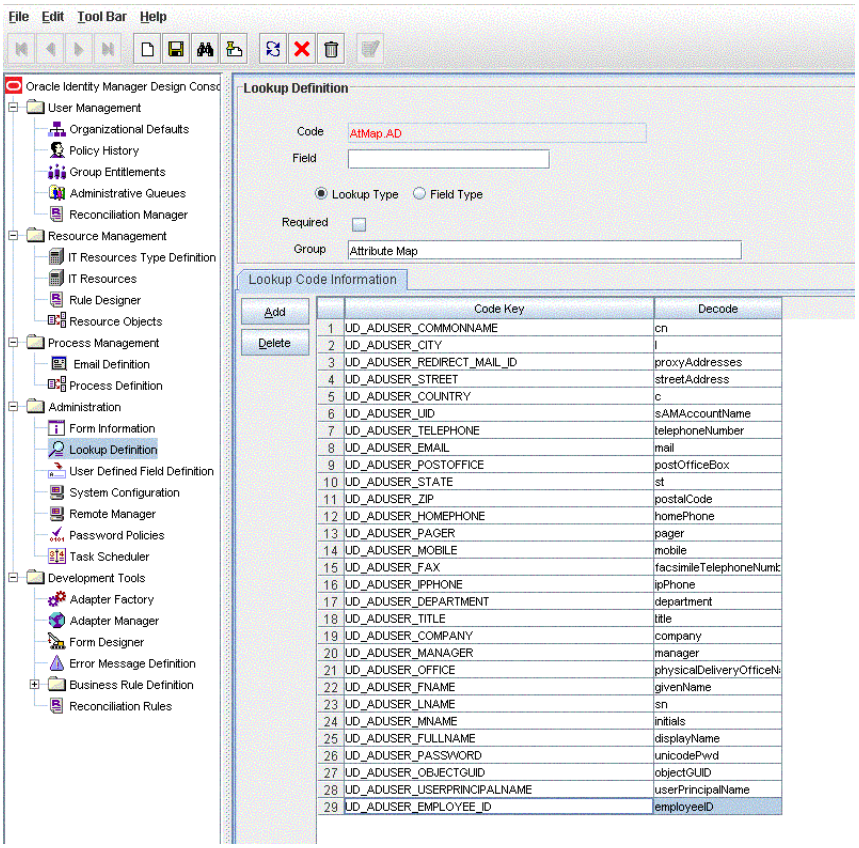
      ---

   e. 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.

Note: For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

For example, enter `UD_ADUSER_EMPLOYEE_ID` in the **Code Key** field and then enter `employeeID` in the **Decode** field. Figure 4–12 shows the entry added to the lookup definition.

Figure 4–12 Entry Added to the Lookup Definition



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 process definition, add a new task for updating the field as follows:
   a. Expand **Process Management**.

b. Double-click **Process Definition**, and then open the **AD User** process definition for a user attribute or the **AD Group** process definition for a group attribute.

c. Click **Add** and enter the task name and the task description.

d. In the Task Properties section, select the following fields:

   – Conditional

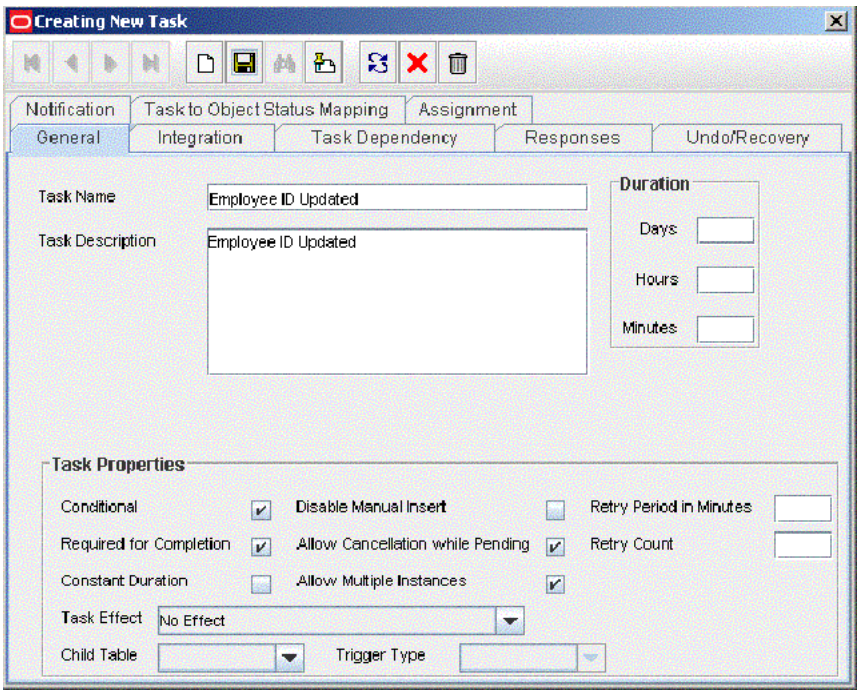
   – Required for Completion

   – Allow Cancellation while Pending

   – Allow Multiple Instances

e. Click **Save**. Figure 4–13 shows the new task added to the process definition.

Figure 4–13 New Task Added to the Provisioning Process



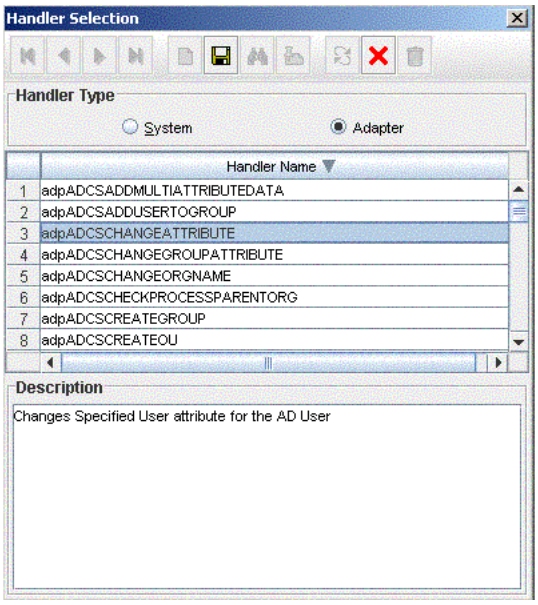
3. In the AD User process definition, select the adapter name in the Handler Type section as follows:

   a. Go to the Integration tab, click **Add** and select **Adapter**.

   b. In the Handler Type section, select **adpADCSCHANGEATTRIBUTE** for a user attribute or **adpADCSGROUPCHANGEATTRIBUTE** for a group attribute.

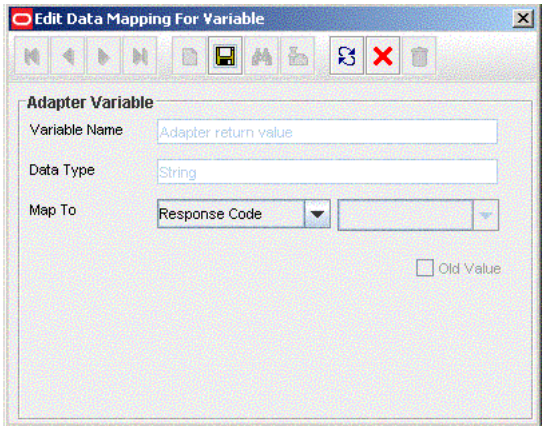
   c. Click **Save**. Figure 4–14 shows the adapter added to the handler.

Figure 4–14 Adapter Added to the Handler



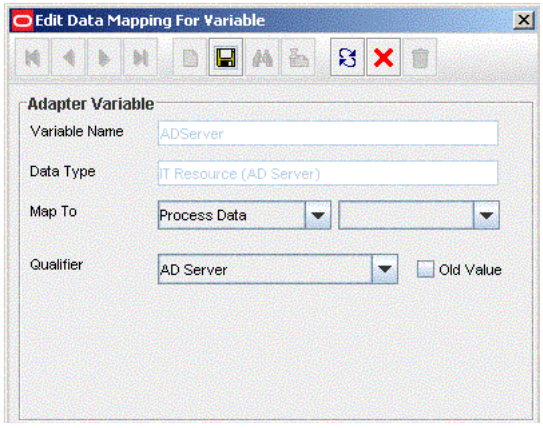
4. Double-click the **Variable Name** field to get the value and map the adapter variable to **Response Code** Figure 4–15 shows the variable name mapped to **Response Code**.

Figure 4–15 Adapter Return Value Mapped to Response Code



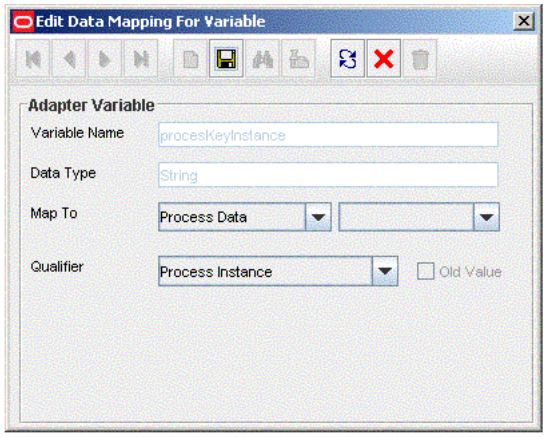
5. Double-click the **Variable Name** field to get the value and map the adapter variable to a process data field. Figure 4–16 shows the variable name mapped to a process data field.

Figure 4–16 Adapter Variable Mapped to a Process Data Field



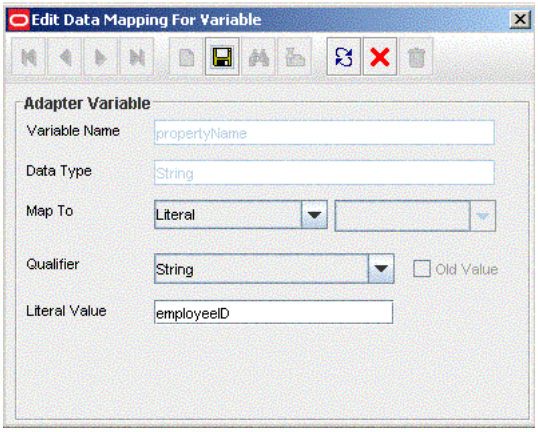
6. Double-click the **Variable Name** field to get the value and map the adapter variable to a process data field. Figure 4–17 shows the adapter variable mapped to a process data field.

Figure 4–17 Adapter Variable Mapped 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, which you determined in the "Adding New Fields for Provisioning" on page 4-14. For example, enter employeeID for updating Employee ID. Figure 4–18 shows the adapter variable mapped to a target system field.

Figure 4–18 Adapter Variable Mapped to a Target System Field



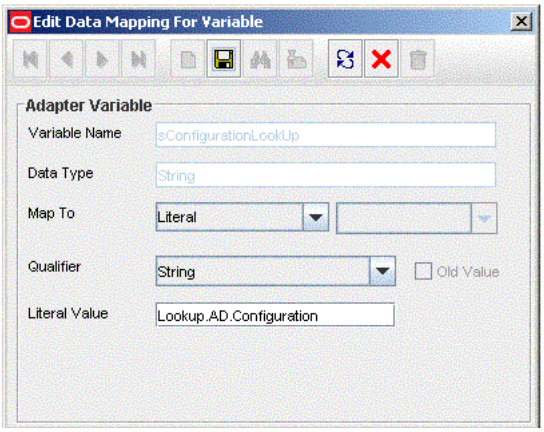
8. If you create a copy of the Lookup.AD.Configuration lookup definition, then:

   a. Double-click the **Variable Name** field and select the **sConfigurationLookUp** variable.

   b. Map the variable to the literal value `Lookup.AD.Configuration`.

   Figure 4–18 shows the adapter variable mapped to the literal.

Figure 4–19 Adapter Variable Mapped to a Literal



9. Click **Save**.

4.5 Adding New Multivalued Fields for Provisioning

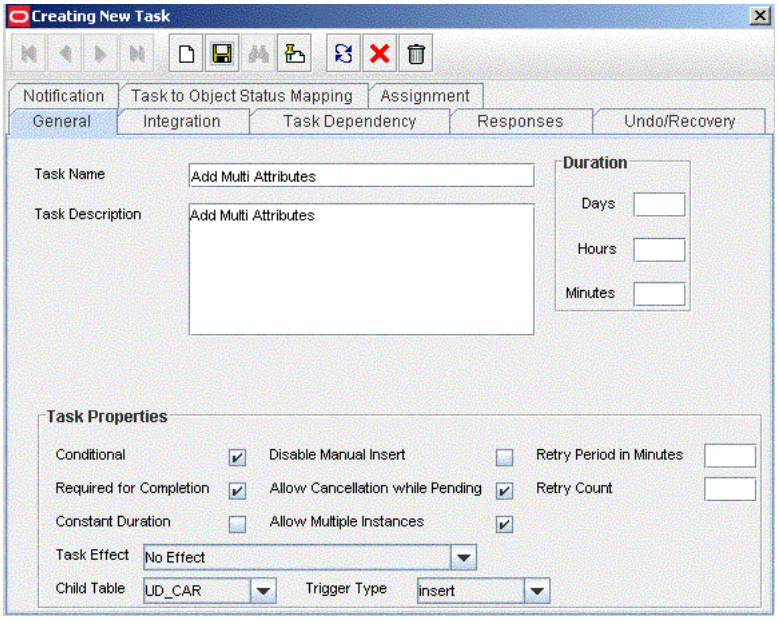
To add new multivalued fields for provisioning:

> **Note:** Before starting the following procedure, perform Steps 1 through 3 as described in the section "Adding New Multivalued Fields for Target Resource Reconciliation" on page 4-8. 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** process definition. For groups, open the **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**. Figure 4–20 shows the multivalued task added to the process.

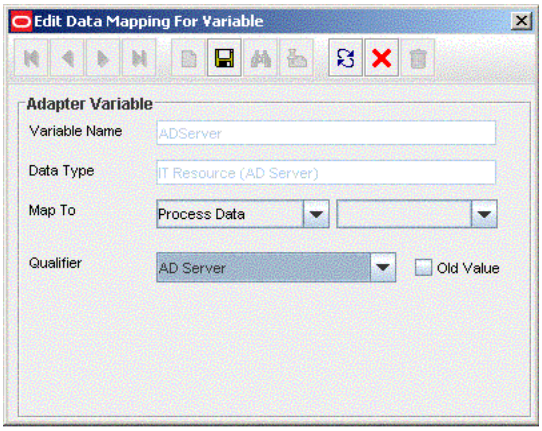
Figure 4–20 Multivalued Field Added to the AD User Provisioning Process



4. Select the adapter as follows:
   a. On the Integration tab in the AD User 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**.

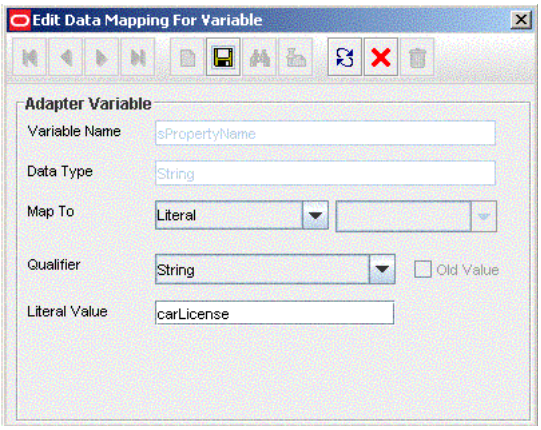
5. Double-click and map the adapter variable to a process data field and click **Save**. Figure 4–21 shows the adapter variable name mapped to a process data field.

Figure 4–21 Adapter Variable Mapped to a Process Data Field



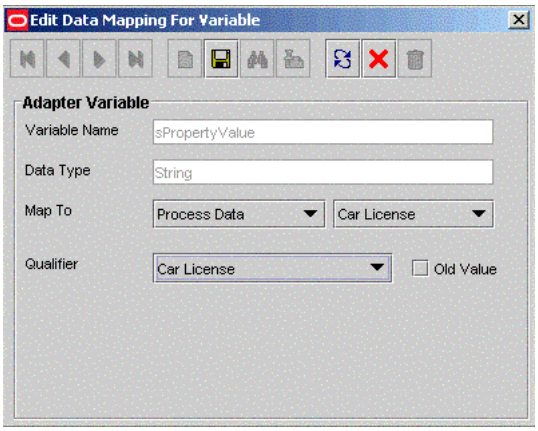
6. Double-click and map the adapter variable to a literal and specify the name of the attribute to be updated in the Literal Value field, and then click **Save**. Figure 4–22 shows the adapter variable mapped to a literal.

Figure 4–22 Adapter Variable Mapped to a Literal



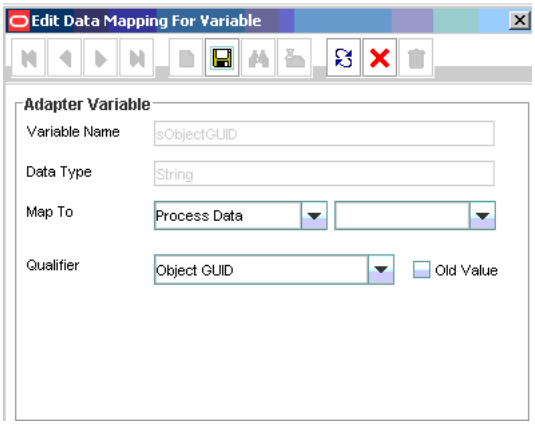
7. Double-click and map the adapter variable to a process data field of the newly created form. If you are removing the attribute, then select **Old Value** and click **Save**. Figure 4–23 shows the adapter variable mapped to a process data field.

Figure 4–23 Adapter Variable Mapped to a Process Data Field



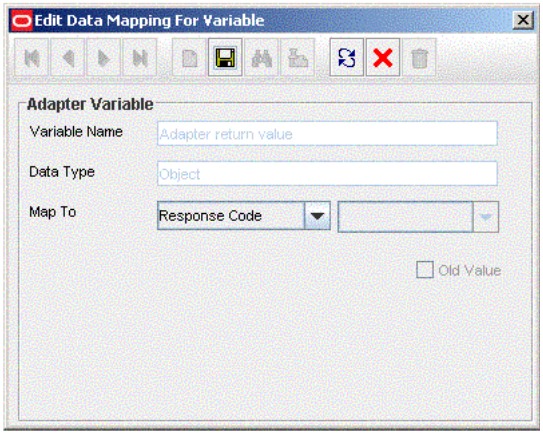
8. Double-click and map the adapter variable to a process data field and click **Save**. Figure 4–24 shows the adapter variable name mapped to a process data field.

Figure 4–24 Adapter Variable Mapped to a Process Data Field



9. Double-click and map the adapter variable to a response code field and click **Save**. Figure 4–25 shows the adapter variable name mapped to a response code field.

Figure 4–25 Adapter Variable Mapped to a Response Code Field



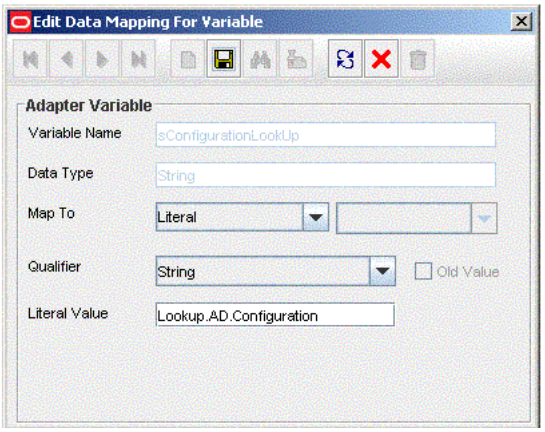
10. If you create a copy of the Lookup.AD.Configuration lookup definition, then:

a. Double-click the **Variable Name** field and select the **sConfigurationLookUp** variable.

b. Map the variable to the literal value `Lookup.AD.Configuration`.

Figure 4–18 shows the adapter variable mapped to the literal.

Figure 4–26 Adapter Variable Mapped to a Literal



11. 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.

4.6 Adding Mappings for New Object Classes

To create an object class and add fields of the object class for provisioning:

1. Create the object class and assign mandatory and optional attributes to the object class.

   Refer to Microsoft documentation for information about creating the object class.

   > **Note:** Assign the user object class as the parent of the object class that you create.

2. Refresh the schema.
3. To add the mandatory and optional attributes of the object class for provisioning, perform the procedure described in "Adding New Fields for Provisioning" on page 4-14.
4. Open the Lookup.AD.Configuration lookup definition and change the decode value of the LdapUserObjectClass code key value to include the new object class name.

   Refer to "Configuring the Lookup.AD.Configuration Lookup Definition" on page 3-5 for detailed information about performing this step.

4.7 Enabling the Auto Pre-populate and Auto Save Options

Auto Pre-populate and Auto Save are two of the options available in the resource object. You use the Auto Pre-populate option to specify whether a custom form will be populated by Oracle Identity Manager or a user. You use the Auto Save option to specify that Oracle Identity Manager must save the data, without user intervention, in any resource-specific form that was created using the Form Designer form.

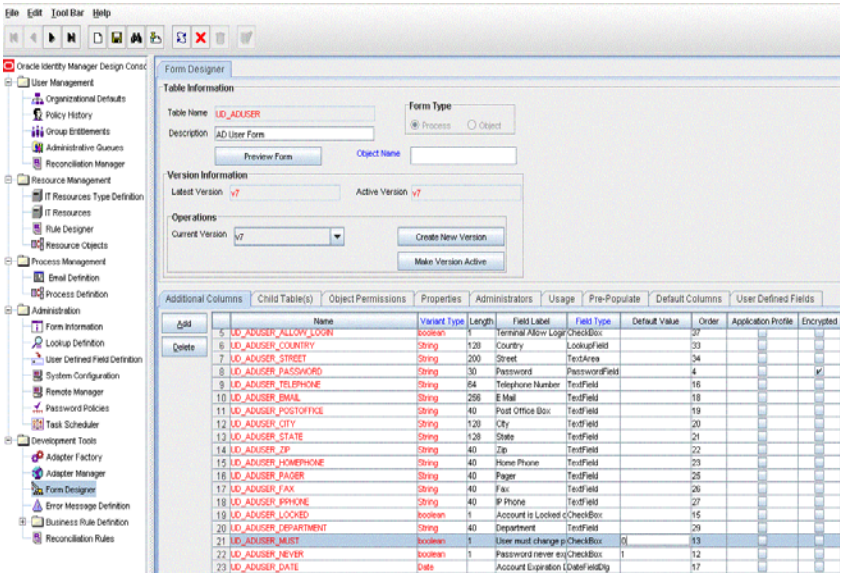
> **See Also:** *Oracle Identity Manager Design Console Guide* for more information about both options

If you want to use either of these options, then specify default values for mandatory check boxes of the process definition as follows:

1. Log in to the Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **AD User** process definition.
4. On the Additional Columns tab:
   - For the UD_ADUSER_MUST field, enter a value (`0` or `1`) in the **Default** column.
   - For the UD_ADUSER_NEVER field, enter a value (`0` or `1`) in the **Default** column.
5. Click **Save**.

   Figure 4–27 shows the default values specified for the Checkbox field types on the process form.

Figure 4–27 Default Values Specified for the Checkbox Field Types on the Process Form



4.8 Using Your Own Provisioning Script

Note: The information in this section does not apply to Microsoft ADAM.

The default provisioning script, ProvTerminalServiceAttr.vbs, is described in "Connector Architecture" on page 1-3. As mentioned in that section, this script is used to work with the Terminal Services Profile fields of the target system. During a Create User provisioning operation, the Remote Manager calls the provisioning script regardless of whether or not you enter a value for any of the Terminal Services Profile fields of the process form. During an Update User provisioning operation, the Remote Manager calls the provisioning script only if any of the Terminal Services Profile fields is updated.

If you want to extend or change the functionality of the default provisioning script, then you can replace it with your own script. For example, you can create a script that manipulates the Terminal Services Profile fields and the Remote Control fields.

To use your own provisioning script:

1. Create the script.
2. Place the script in any directory on the target system computer.

   Note: Ensure that the directory into which you copy the scripts has the required read and write permissions for the target system user account that you create by performing the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-3.

3. Edit the ADITResource IT resource, and enter the full path and name of the script as the value of the Remote Manager Prov Script Path parameter.

   See Also: The "Managing IT Resources" section of *Oracle Identity Manager Administrative and User Console Guide*

While creating the script, you can apply the following information about parameters in the default provisioning script:

- **UserID**

  During a provisioning operation, this parameter accepts the user ID in the following format:

  `LDAP://cn=`*`CN_VALUE`*`,ou=`*`OU_VLAUE`*`,dc=`*`DC_VALUE`*`,dc=`*`DC_VALUE`*

  The following is a sample value for the UserID parameter:

  `LDAP://cn=john,ou=sales,dc=globalv,dc=com`

- **UserLookupdecodeValues**

  Note: Although this parameter is defined in the script, the script does not use this parameter in the current release of the connector.

During a provisioning operation, this parameter accepts a list of the following key-value pairs:

- The key is the field name from the Decode column of the AtMap.AD lookup definition.
- The value is the value of the field entered on the process form.

The vertical bar (|) is used as the delimiting character in this list.

The following is a sample value for the UserLookupdecodeValues parameter:

```
givenName=John|depart=accounts|homePhone=123456 . . .
```

- **TerminalLookupDecodeValues**

  During a provisioning operation, this parameter accepts a list of the following key-value pairs:

  - The key is the field name from the Decode column of the AtMap.AD.RemoteScriptlookUp lookup definition.
  - The value is the value of the field entered on the process form.

  The vertical bar (|) is used as the delimiting character in this list.

  The following is a sample value for the TerminalLookupDecodeValues parameter:

```
TerminalServicesProfilePath
=C:\test|TerminalServicesHomeDirectory=C:\test1|AllowLogon=0
```

- **BlobAttrName**

  During a provisioning operation, this parameter accepts one of the following values:

  - `ALL`

    This value is passed to the parameter during a Create User provisioning operation. The ALL value indicates that values for all of the Terminal Services Profile fields must be updated by the script.

  - The name of a specific field that must be updated by the script.

    Note: If more than one Terminal Services Profile field is updated during a provisioning operation, then each field is passed to the Remote Manager one call at a time.

  The following is a sample value for the BlobAttrName parameter:

```
TerminalServicesProfilePath
```

- Click **Save**.

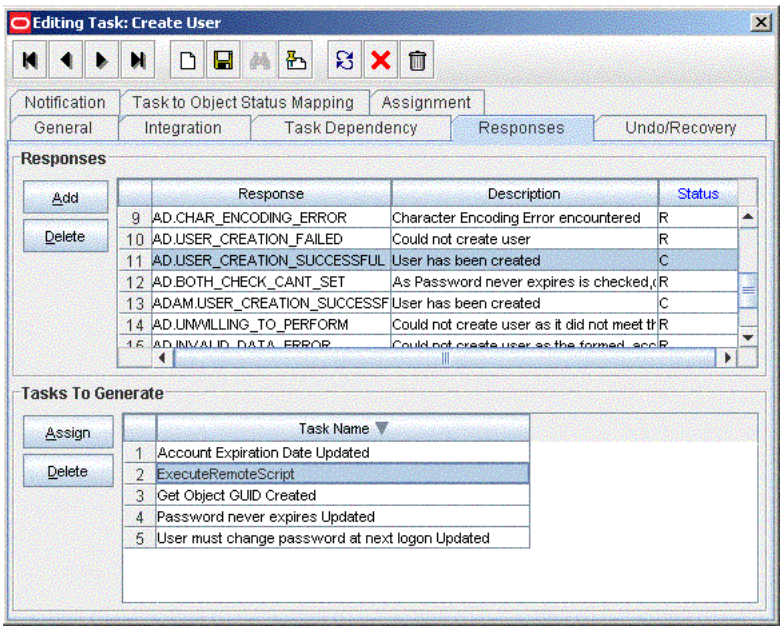
4.9 Removing the ExecuteRemoteScripts Process Task

During a provisioning operation, the ExecuteRemoteScripts process task is used to set values for the Terminal Services Profile fields of the target system. This process task is triggered after successful completion of the Create User process task, even if values are not entered for the Terminal Services Profile fields on the process form. If you do not want the ExecuteRemoteScripts process task to be triggered, then:

1. Log in to the Oracle Identity Manager Design Console.

2. Expand **Process Management**.
3. Double-click **Process Definition**.
4. Search and open the **AD User** process definition.
5. Search for and open the **Create User** process task.
6. On the Responses tab, select **AD.USER_CREATION_SUCCESSFUL**.
7. From the Task Name list, select **ExecuteRemoteScript** and then click **Delete**.
8. Click **Save**. Figure 4–28 shows ExecuteRemoteScript deleted from the process form.

Figure 4–28 ExecuteRemoteScript Deleted from the Process Form



4.10 Adding New Fields for Trusted Source Reconciliation

Note: 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.

By default, the attributes listed in Table 1–11 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new fields for trusted source reconciliation.

Before you add a new field for trusted source 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`.

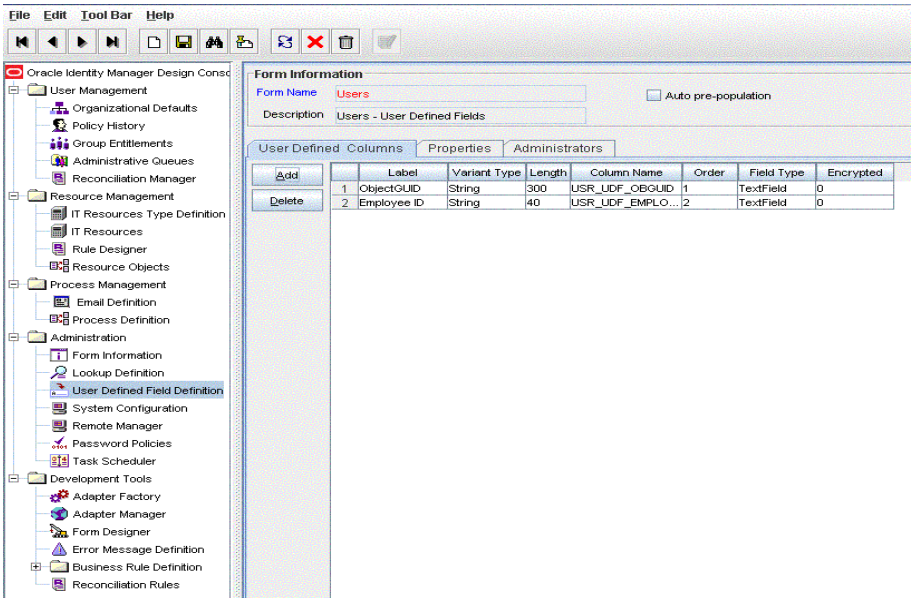
To add a new field for trusted source reconciliation:

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 OIM User process form as follows:
   a. Expand **Administration**.
   b. Double-click **User Defined Field Definition**.
   c. Search for and open the **Users** form.
   d. Click **Add** and enter the details of the field.

      For example, if you are adding the Employee ID field, then enter `Employee ID` in the **Name** field, set the data type to **String**, enter `USR_UDF_EMPLOYEE_ID` as the column name, and enter a field size value.
   e. Click **Save**. Figure 4–29 shows the new field added on the User Defined Columns tab of the Users form.

Figure 4–29 New Field Added to the Users Form



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

   a. Expand the **Resource Management** folder.

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

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

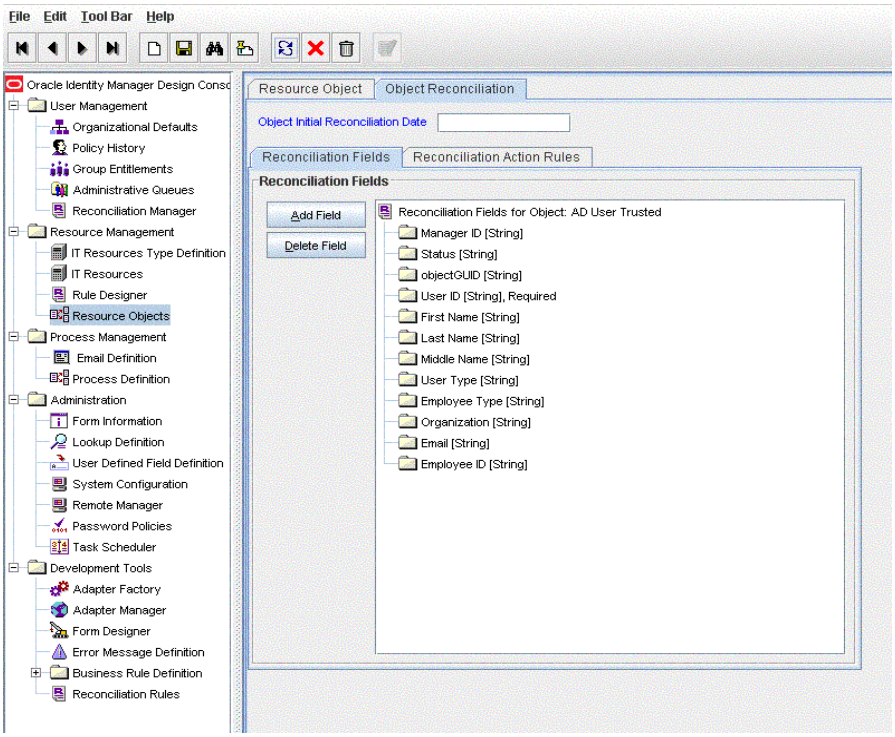
   d. On the Object Reconciliation tab, click **Add Field**.

   e. Enter the details of the field and click **Save**.

      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. Figure 4–30 shows the new field added to the process data field in the process form.

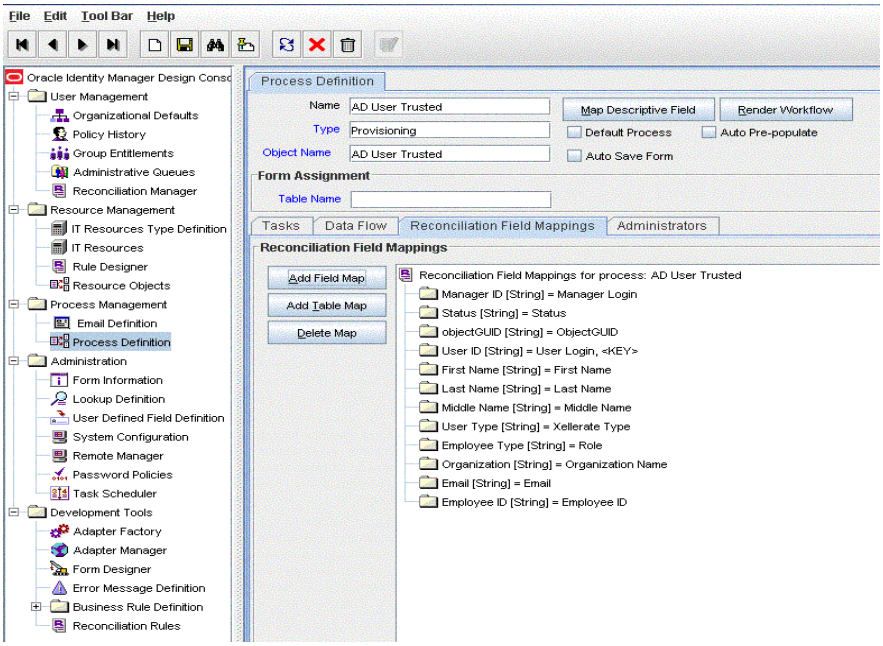
Figure 4–30 New Field Added to the Resource Object



4. 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 Trusted** process definition.
   d. On the Reconciliation Field Mappings tab, click **Add Field Map**.
   e. In the **Field Name** field, select the value for the field that you want to add.

      For example, select **Employee ID = Employee ID**.
   f. Click **Save**. Figure 4–31 shows the new reconciliation field mapped to a process data field in the process definition.

Figure 4–31 New Reconciliation Field Mapped to a Process Data Field



5. 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.

      Search for and open the **Lookup.ADAMReconciliation.FieldMap** lookup definition if you are using Microsoft ADAM.

   d. Cick **Add** and then 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.

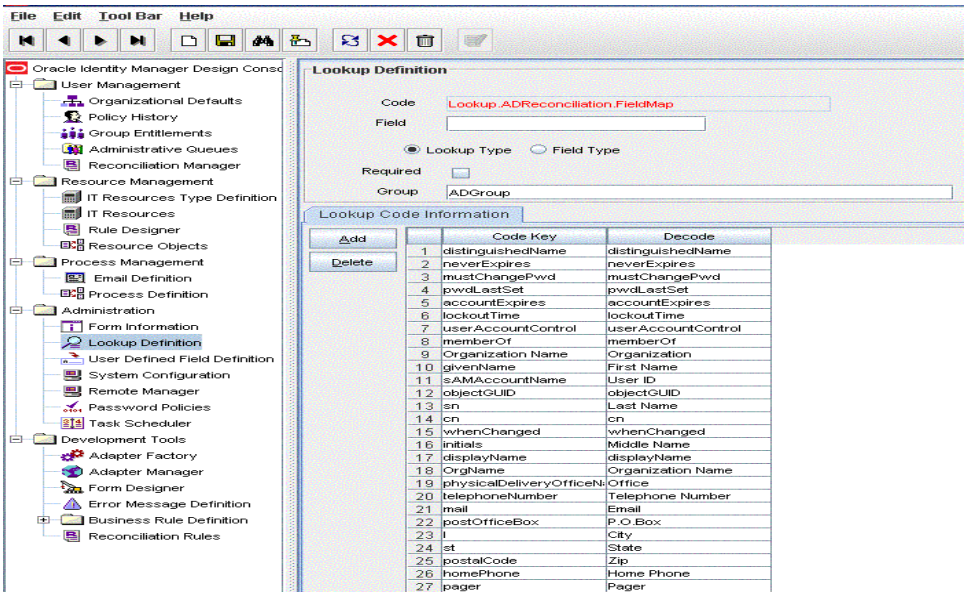
      Note: For the target system fields, you must use the same case (uppercase or lowercase) as given on the target system. This is because the field names are case-sensitive.

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

   e. Click **Save**.

6. Select **Field Type** and click **Save**. Figure 4–32 shows the entry added to the lookup definition.

Figure 4–32 Entry Added to the Lookup Definition



4.11 Transforming Data Reconciled Into Oracle Identity Manager

This section discusses the Transform Lookup Code and Use Transform Mapping attributes of the scheduled tasks for target resource and trusted source reconciliation, AD User Target Recon and AD User Trusted Recon.

During reconciliation, you may want to transform the values of some target system fields before they are stored in Oracle Identity Manager. Appending a number at the end of the user ID is an example of a data transformation.

The Transform Lookup Code and Use Transform Mapping attributes provide a method for implementing such transformations. To use these attributes:

1. Identify the fields that you want to transform.
2. Create the Java file containing the code implementation of the transformation that must be performed during reconciliation.

   See Also: Appendix D, "Sample Transformation Class"

3. Compile the Java file. While compiling the file, you must reference the xliADRecon.jar in the *OIM_HOME*/xellerate/ScheduleTask directory.
4. Create JAR files containing the code to implement the required transformations on the fields.
5. Copy the JAR files into the following directory:

   OIM_HOME/xellerate/ScheduleTask

6. In the Lookup.ADReconciliation.TransformationMap lookup definition, add an entry for the transformation. In the Code Key column, enter the name of the reconciliation field (in the resource object) on which you want the transformation to be performed. In the Decode column, enter the name of the class file. For example:

Note: You can use this lookup definition for both Microsoft Active Directory and Microsoft ADAM.

Code Key: `First Name`

Decode: `AppendNumber`

See Also: *Oracle Identity Manager Design Console Guide* for information about creating lookup definitions

7. While configuring the AD User Target Recon scheduled task by performing the procedure described in "Scheduled Tasks for Target Resource Reconciliation" on page 3-13 and AD User Trusted Recon scheduled task by performing the procedure described in "Scheduled Tasks for Trusted Source Reconciliation" on page 3-18:
   - Enter the name of the lookup definition as the value of the Transform Lookup Code attribute.
   - Enter `yes` as the value of the Use Transform Mapping attribute to specify that you want transformations to be applied. If you enter `no` as the value, then the transformations are not applied.

4.12 Configuring the Connector for Multiple Trusted Source Reconciliation

The following are examples of scenarios in which there is more than one trusted source for user data in an organization:

- One of the target systems is a trusted source for data about employees. The second target system is a trusted source for data about contractors. The third target system is a trusted source for data about interns.
- One target system holds the data of some of the identity fields that constitute an OIM User. Two other systems hold data for the remaining identity fields. In other words, to create an OIM User, data from all three systems would need to be reconciled.

If the operating environment of your organization is similar to that described in either one of these scenarios, then this connector enables you to use the target system as one of the trusted sources of user data in your organization.

Refer to *Oracle Identity Manager Design Console Guide* for detailed information about multiple trusted source reconciliation.

4.13 Configuring the Connector for Multiple Installations of the Target System

Note: The information in this section also applies to Microsoft ADAM.

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 Example 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:

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

1. Create IT resources of the AD Server IT resource type so that there is one IT resource for each installation of the target system.

   Refer to "Configuring the IT Resource for the Target System" on page 2-7 for information about the values to be specified for the IT resource parameters.

2. Create copies of the reconciliation scheduled tasks for each installation of the target system. While creating a scheduled task, specify attribute values corresponding to the target system installation for which you are creating the scheduled task.

   Refer to "Reconciliation Scheduled Tasks" on page 3-13 for information about the values to be specified for the scheduled task attributes.

3. Manually synchronize the lookup definitions in Oracle Identity Manager with the lookup field values on the target system.

4. If you are using Oracle Identity Manager release 9.1.0, then you can configure the target system installations as attribute-level trusted sources. To achieve this:

   > **See Also:** The "Multiple Trusted Source Reconciliation" section in *Oracle Identity Manager Design Console Guide*

   a. Create a trusted resource object for each target system installation.

   b. Create a reconciliation rule for each resource object.

Before you perform provisioning operations:

The User Principal Name field on the process form is pre-populated with values from the User ID field and the UPN Domain IT resource parameter. Before you switch to a different IT resource during a provisioning operation, you must change the IT resource to which the User Principal Name field is mapped.

1. Expand **Development Tools**, and double-click **Form designer**.
2. Search for and open the **AD User** form.
3. On the Pre-Populate tab, double-click the **User Principal Name** row.
4. In the Pre-Population adapter dialog box, double-click the IT resource that you are currently using (for example, ADITResource).
5. From the **Qualifier** list in the Map Adapter Variables dialog box, select the IT resource that you want to use. For example, select `ADITResource2`. Then, click the Save icon and close the dialog box.
6. In the Pre-Population adapter dialog box, click the Save icon and close the dialog box.
7. Click the Save icon on the Form Designer form.

When you perform provisioning operations:

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.

4.13.1 Creating Copies of the Connector

To create a copy of the connector:

1. Create copies of the IT resource, resource object, process form, provisioning process, scheduled tasks, and lookup definitions that hold attribute mappings.
2. Create a copy of the Lookup.AD.Configuration lookup definition. In the copy that you create, change the values of the following entries to match the details of the process form copy that you create.
   - ROUserID
   - ROUserManager
   - ROFormName
   - ROUserGUID

   See "Configuring the Lookup.AD.Configuration Lookup Definition" for information about these entries.
3. Map the new process tasks to the copy of the Lookup.AD.Configuration lookup definition.

5

Testing the Connector

You must test the connector to ensure that it functions as expected. You can use one of the following options to test the connector:

- Using the Testing Utility
- Using the Diagnostic Dashboard

5.1 Using the Testing Utility

You can use the testing utility to conduct provisioning tests on the connector. This type of test involves using Oracle Identity Manager to provision a target system account for an OIM User.

To use the testing utility:

1. Ensure that all the steps to deploy the connector have been performed.
2. If Oracle Identity Manager is running on IBM WebSphere Application Server, then perform the following steps:
   a. Copy the xlapiclient.ear file from the *OIM_HOME*/XLIntegrations/ADUM/test/lib directory into the *OIM_HOME*/client/xlclient directory.
   b. Copy the wsapiclient.cmd file from the *OIM_HOME*/XLIntegrations/ADUM/test/scripts directory into the *OIM_HOME*/client/xlclient directory.
   c. In the *WEBSPHERE_CLIENT_HOME*/properties/sas.client.props file, specify values for the following:

      Note: *WEBSPHERE_CLIENT_HOME* is the directory in which you install the IBM WebSphere Application Server client.

      ```
      com.ibm.CORBA.securityServerHost=OIM_HOST_NAME_OR_IP_ADDRESS
      com.ibm.CORBA.securityServerPort=PORT_AT_WHICH_OIM_IS_LISTENING
      com.ibm.CORBA.loginSource=properties
      com.ibm.CORBA.loginUserid=xelsysadm
      com.ibm.CORBA.loginPassword=xelsysadm
      ```

3. Ensure that Oracle Identity Manager is running.
4. If Oracle Identity Manager is running on Oracle WebLogic Server, JBoss Application Server, or Oracle Application Server, then update the following entries in the *OIM_HOME*/XLIntegrations/ADUM/test/scripts/runADTest.bat script:

```
set OIM_JARS = OIM_HOME\xellerate
```

In the preceding line, change *OIM_HOME* to the full path of the xellerate directory.

```
set APPSERVER_HOME = APPSERVER_HOME
```

In the preceding line:

- For JBoss Application Server, replace *APPSERVER_HOME* with the full path of the *JBOSS_HOME*/client directory.
- For Oracle WebLogic Server, replace *APPSERVER_HOME* with the full path of the *WEBLOGIC_HOME*/weblogic81/server/lib directory.
- For Oracle Application Server, replace *APPSERVER_HOME* with the full path of the *ORACLE_HOME*/j2ee/home directory.

5. In the *OIM_HOME*/XLIntegrations/ADUM/test/config/config.properties file, specify values for the identity fields of the user that will be created on the target system during the provisioning test. In addition, specify the name of the IT resource for the target system. See "Configuring the IT Resource for the Target System" on page 2-7 for information about this IT resource.
6. In the *OIM_HOME*/XLIntegrations/ADUM/test/config/log.properties file, specify log messages that must be displayed on the console when you run the connector testing utility.
7. If Oracle Identity Manager is installed on Oracle WebLogic Server, JBoss Application Server, or Oracle Application Server, then run the *OIM_HOME*/XLIntegrations/ADUM/test/scripts/runADTest script as follows:

   ```
   runADTest.bat ARGUMENT_TO_INDICATE_APPLICATION_SERVER
   ```

   In this command, replace *ARGUMENT_TO_INDICATE_APPLICATION_SERVER* with one of the following:

   - `1` for JBoss Application Server
   - `2` for Oracle WebLogic Server
   - `3` for Oracle Application Server

   For example, if Oracle Identity Manager is installed on Oracle WebLogic Server, then run the command as follows:

   ```
   runADTest.sh 2
   ```

8. If Oracle Identity Manager is running on IBM WebSphere Application Server, run wsapiclient.cmd from the *OIM_HOME*/client/xlclient directory.

If the script runs without any error, then the "User created true" message is displayed in the command window. Verify that the user has been created in Microsoft Active Directory.

5.2 Using the Diagnostic Dashboard

The Diagnostic Dashboard is a utility shipped with Oracle Identity Manager. In addition to tests that can be run on the Oracle Identity Manager installation, this utility offers the following connector-related tests:

- Test Basic Connectivity
- Test Provisioning

- Test Reconciliation

For information about these tests, refer to the "Working with the Diagnostic Dashboard" chapter in *Oracle Identity Manager Administrative and User Console Guide*.

6

Known Issues

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

- **Bug 5526185**

  On the target system, you can use one of the following methods to change the group membership details of a user account:

  – Edit the user account and directly change the group membership details.

  – Edit the group and add or modify the user's membership details.

  During both operations, only the group object is time stamped. Incremental reconciliation from the target system is based on the time stamp of the user object. Therefore, group membership changes made to a user account are not reconciled into Oracle Identity Manager.

  Note: This known issue affects only reconciliation of *updates* to group membership details. Reconciliation of new group membership details is not affected.

- **Bug 7225753 and 7232276**

  Through provisioning, you cannot move a target system user from one domain controller to another. This is because the IT resource enables you to specify only a single domain controller as the target system.

- **Bug 7003816**

  Microsoft ADAM does not support the "User must change password at next logon" attribute. In order for provisioning to be successful, this attribute (check box) must not be checked when the target system in ADAM.

- **Bug 7136085**

  The Country lookup field displays country names in English, regardless of the locale you select.

- **Bug 7212391**

  The ADITResource IT resource is created by default when you install the connector. If you want to use the Invert Display Name parameter of the IT resource, then you must use the ADITResource IT resource. If you create and use a new IT resource with a different name, then the Invert Display Name parameter is not used.

- **Bug 7296381**

If Oracle Identity Manager is using Microsoft SQL Server, then a limit is imposed on the total character length of all the fields on the process form. During the connector installation process, this check is implemented when the Deployment Manager imports the connector XML files. If the combined length of the process form fields is determined to be more than 8060 characters, then the XML file is not imported.

To work around this requirement, the character lengths of some process form fields are kept less than their target system counterparts. For example, although the length of the Department field on the target system is 64 characters, the length of this field on the process form is 40 characters.

After you deploy the connector, you can modify the lengths of the process form fields. See Appendix A, "Character Lengths of Target System Fields and Process Form Fields" for a listing of the fields whose lengths are different on the target system and the process form. This appendix also describes the procedure to use the Design Console for modifying the lengths of the process form fields.

- **Bug 7207232**

  Some Asian languages use multibyte character sets. If the character limit for fields on the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this point:

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

- **Bug 7126712**

  After you revoke the Microsoft Active Directory resource of an OIM User, if you run the AD User Target Delete Recon scheduled task, then the button to provision new Active Directory resources for the user is disabled.

- **Bug 8346302**

  During first-time reconciliation of a resource, the status of the resource is set to Enabled or Disabled instead of Provisioned.

- **Bug 6736667**

  Critical extensions in an SSL certificate are not supported.

- **Bug 8262055**

  The following issue is observed when the Remote Manager is not running (that is, not in use):

  If you perform an Update User provisioning operation on a resource created through target resource reconciliation, then the Terminal Allow Login Updated process task is triggered. The status of the task is shown as Rejected on the Administrative and User Console. However, the Update User operation gives the expected results, and it is not affected by rejection of the Terminal Allow Login Updated process task.

A

Character Lengths of Target System Fields and Process Form Fields

Table A–1 lists the fields whose lengths are different on the target system and on the process form.

Table A–1 Fields with Different Lengths on the Target System and the Process Form

Process Form Field, Process Form Database Column, and Field Length	Microsoft Active Directory Field and Field Length	Microsoft ADAM Field and Field Length
Department, UD_ADUSER_DEPARTMENT, 40	department, 64	department, 64
Fax, UD_ADUSER_FAX, 40	facsimileTelephoneNumber, 64	facsimileTelephoneNumber, 64
Home Phone, UD_ADUSER_HOMEPHONE, 40	homePhone, 64	homePhone, 64
IP Phone, UD_ADUSER_IPPHONE, 40	ipPhone, 64	ipPhone, 64
Manager Name, UD_ADUSER_MANAGER, 200	manager, *Not Specified*	manager, *Not Specified*
Mobile, UD_ADUSER_MOBILE, 50	mobile, 64	mobile, 64
Office, UD_ADUSER_OFFICE, 80	physicalDeliveryOfficeName, 128	physicalDeliveryOfficeName, 128
Organization Name, UD_ADUSER_ORGNAME, 400	Distinguished name of the organization, *Not Specified*	Distinguished name of the organization, *Not Specified*
Pager, UD_ADUSER_PAGER, 40	pager, 64	pager, 64
Street, UD_ADUSER_STREET, 200	StreetAddress, 1024	StreetAddress, 1024
Terminal Home Directory, UD_ADUSER_TERMINAL_HDIRECTORY, 60	Part of the data stored in the userParameters field, 100	NA
Terminal Profile Path, UD_ADUSER_TERMINAL_PPATH, 60	Part of the data stored in the userParameters field, 100	NA

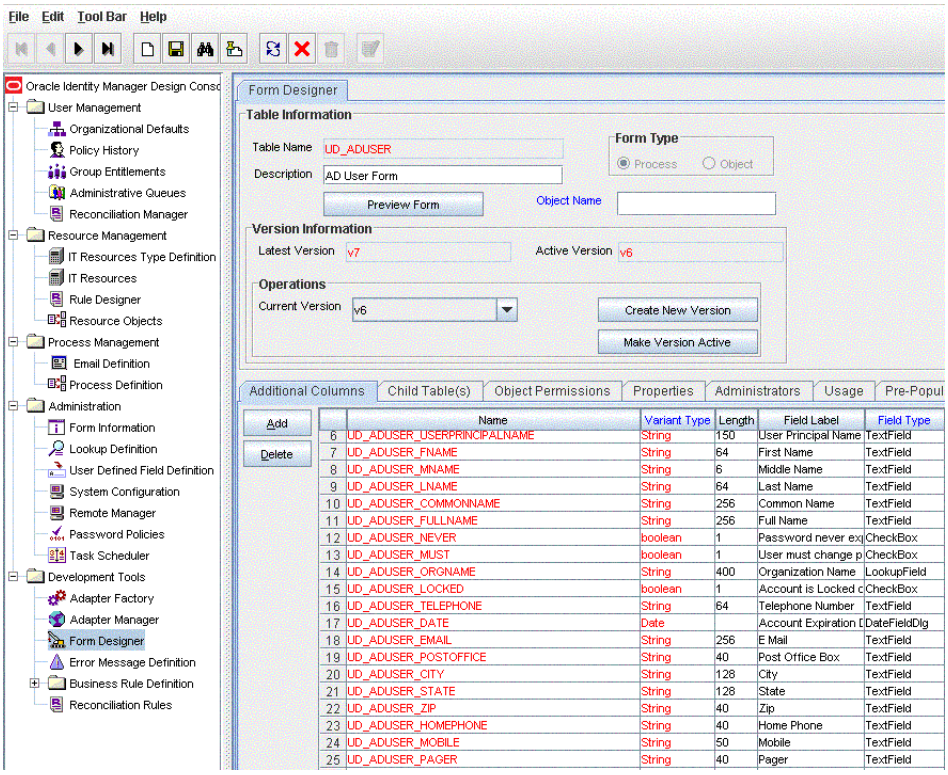
If you want to change the length of a process form field, then:

1. Expand **Development Tools**.
2. Double-click **Form Designer**.
3. Search for and open the **UD_ADUSER** process form.
4. Click **Create New Version**.

5. On the Additional Columns tab, change the length of the field in the **Length** column.
6. Click **Save**, and then click **Make Version Active**.

Figure A–1 shows the field length changed on the Additional Columns tab of the UD_ADUSER process form.

Figure A–1 Process Form Field Lengths Displayed on the Additional Columns Tab of the Process Form



B

Special Characters Supported for Passwords

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

Table B–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	-
underscore	_

C

Terminal Services Profile Field Names for Reconciliation and Provisioning

Note: The information in this appendix is applicable only to the Microsoft Active Directory target system and only if you are going to use the target system as a target resource.

Microsoft Active Directory stores the following user information in BLOB format:

- Environment
- Remote Control
- Sessions
- Terminal Services Profile

As mentioned earlier in this guide, reconciliation and provisioning scripts are used to work with the Terminal Services Profile fields of the target system. Although only the Terminal Services Profile fields are supported by default, the scripts contain code that can handle fields of the remaining three categories.

Table 1–4 lists the fields that are supported for target resource reconciliation, and Table 1–8 lists the fields that are supported for provisioning. If required, you can add new fields for reconciliation and provisioning.

Chapter 4, "Extending the Functionality of the Connector" describes the procedure to add new fields. One of the steps of the procedure is to determine the target system name of the field that you want to add. However, if you want to add an Environment, Remote Control, or Sessions field, then you must use the field names defined in the reconciliation and provisioning scripts. Table C–1 lists these fields and the values that the scripts accept during provisioning and reconciliation. While performing the procedure described in Chapter 4, use the field names given in the "Name of the Field in the Scripts" column of the table.

Table C–1 Terminal Services Profile Fields Included in the Reconciliation and Provisioning Scripts

User Information Tab in Microsoft Active Directory	Name of the Field in the Scripts	Values That the Field Can Take
Remote Control	EnableRemoteControl	The value can be 0, 1, 2, 3, or 4: ■ 0: Disable Remote Control ■ 1: Remote Control Enabled, User's Permission Required, Interact ■ 2: Remote Control Enabled, User's Permission Not Required, Interact ■ 3: Remote Control Enabled, User's Permission Required, View only ■ 4: Remote Control Enabled, User's Permission Not Required, View only
Sessions	MaxDisconnectionTime	Integer value specifying the number of minutes
	MaxConnectionTime	Integer value specifying the number of minutes
	MaxIdleTime	Integer value specifying the number of minutes
	BrokenConnectionAction	The value can be 0 or 1: ■ 0: Disconnect ■ 1: End
	ReconnectionAction	The value can be 0 or 1: ■ 0: Any ■ 1: Originating
Environment	TerminalServicesInitialProgram	Path to the executable file (string value)
	TerminalServicesWorkDirectory	Path to the working directory (string value)
	ConnectClientDrivesAtLogon	The value can be 0 or 1: ■ 0: Disabled ■ 1: Enabled
	ConnectClientPrintersAtLogon	The value can be 0 or 1: ■ 0: Disabled ■ 1: Enabled
	DefaultToMainPrinter	The value can be 0 or 1: ■ 0: Disabled ■ 1: Enabled

D

Sample Transformation Class

When you use this connector, you can transform reconciled data according to your requirements. This feature has been described in "Transforming Data Reconciled Into Oracle Identity Manager" on page 4-34, along with the discussion on the Transform Lookup Code and Use Transform Mapping attributes.

If you want to transform the value of a target system field that is fetched during reconciliation, then the first step is to implement the required transformation logic in a Java class. This transformation class must implement the com.thortech.xl.schedule.tasks.AttributeTransformer interface and the transform method.

The following is a sample transformation class:

```
import com.thortech.xl.schedule.tasks.AttributeTransformer;
public class AppendNumber implements AttributeTransformer {
/**
* @param value: This is the input string to be transformed.
* @return String: This is the string that is returned.
*/
public String transform(String value) {
value=value+"123";
return value;
}
}
```

The method defined in this class accepts the value of the field to be transformed, appends the string `123` to it, and returns the transformed string value.

Index

M

N

O

P

R

S

T

W