Oracle® Identity Manager

Connector Concepts

Release 9.1.0

E11217-02

July 2009

Oracle Identity Manager Connector Concepts, Release 9.1.0

E11217-02

Primary Author: Alankrita Prakash

Contributing Authors: Debapriya Datta, Lyju Vadassery

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

3 Reconciliation and Provisioning Processes

4 Performing Connector Operations

Index

List of Figures

Preface

This guide provides conceptual information about the predefined Oracle Identity Manager Connectors. Each of these connectors can be used to integrate Oracle Identity Manager with a specific target system.

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

To access the Oracle Identity Manager documents mentioned as references in this guide, visit Oracle Technology Network.

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

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.

1

Introduction to Oracle Identity Manager Connectors

Oracle Identity Manager can be used as the single point of management for the IT resources in your organization. Oracle Identity Manager offers various solutions for integration with various kinds of resources. Oracle Identity Manager Connectors are the recommended integration solution.

An integration of a target system with Oracle Identity Manager is composed of two parts:

- **Target account management**

  The functionality of target account management is further divided into two parts:

  - Target resource reconciliation: This is the process in which any action to create, modify, or delete a target system account for an existing OIM User is communicated to and replicated in Oracle Identity Manager.
  - Provisioning: This is the process in which any action to create, modify, or delete a target system identity on Oracle Identity Manager is communicated to and replicated on the target system.

- **Trusted source reconciliation**

  This is the process in which any action to create, modify, or delete identity information about users from authoritative sources is communicated to and replicated in Oracle Identity Manager

Together, reconciliation and provisioning are aimed at enabling Oracle Identity Manager to build an accurate picture of managed identities in all the target systems in the organization.

In data flow terms, provisioning provides the outward flow from Oracle Identity Manager. Provisioning is based on a “push” model, using which Oracle Identity Manager communicates changes to the target system. Reconciliation provides the inward flow into Oracle Identity Manager. Reconciliation is based on either a “push” or a “pull” model, using which Oracle Identity Manager finds out about any identity-related activity on the target system. Target systems that support the push model have features that enable them to send information about identity-related changes to third-party systems like Oracle Identity Manager. The pull model is used for target systems that do not support the push model. The pull model is implemented through periodic polling of the target system for identity-related changes.

This chapter contains the following sections:

- Provisioning
- Target System Configurations Enabled by a Connector

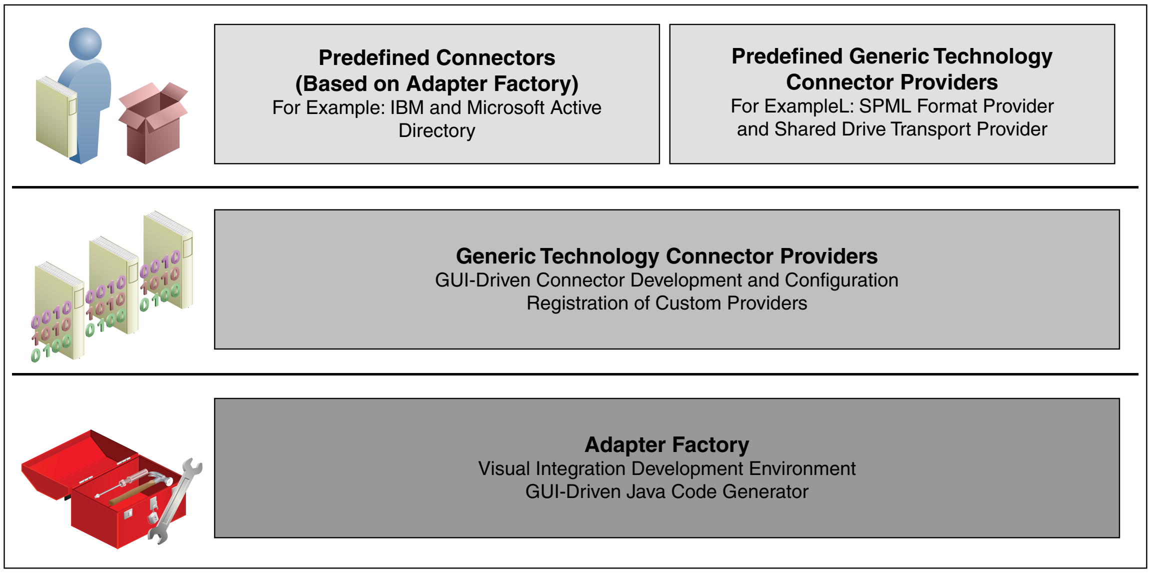
1.1 Integration Solutions

Oracle Identity Manager provides a three-tier integration solutions strategy for integration with heterogeneous identity-aware IT systems. This three-tier strategy is designed to minimize custom development, maximize the reuse of code, and reduce deployment time. The three tiers are:

- Out-of-the box integration using predefined connectors and predefined generic technology connector providers
- Connectors created using custom generic technology connector providers
- Custom connectors created using the Adapter Factory

Figure 1–1 illustrates the three-tier integration solutions strategy of Oracle Identity Manager.

Figure 1–1 Three-Tier Integration Solutions Strategy of Oracle Identity Manager


Predefined Connectors
(Based on Adapter Factory)
For Example: IBM and Microsoft Active Directory
Predefined Generic Technology Connector Providers
For ExampleL: SPML Format Provider and Shared Drive Transport Provider
Generic Technology Connector Providers
GUI-Driven Connector Development and Configuration
Registration of Custom Providers
Adapter Factory
Visual Integration Development Environment
GUI-Driven Java Code Generator

This section discusses the following topics:

- Predefined Connectors
- Generic Technology Connectors
- Custom Connectors

1.1.1 Predefined Connectors

When a predefined connector is available for a target resource, it is the recommended integration method. Because a predefined connector is designed specifically for the target application, it offers the quickest integration method. Predefined connectors support popular business applications such as Oracle eBusiness Suite, PeopleSoft, Siebel, JD Edward and SAP, as well as technology applications such as Microsoft Active Directory, Java Directory Server, UNIX, databases, and RSA ClearTrust.

Predefined connectors use target system recommended integration technologies and are preconfigured with target system-specific attributes.

1.1.2 Generic Technology Connectors

To integrate Oracle Identity Manager with a target system that has no corresponding predefined connector, you can create a custom connector to link the target system and Oracle Identity Manager. If you do not want to use the customization features of the Adapter Factory, then you can create the connector by using the Generic Technology Connector feature of Oracle Identity Manager.

> **See Also:** Part II, "Integration Solutions Features" of *Oracle Identity Manager Administrative and User Console Guide* for more information about generic technology connectors

1.1.3 Custom Connectors

If there is no technology interface or accessible user repository in the target system, then you can develop a custom connector for the target system. The Adapter Factory tool in the Design Console provides a definitional user interface that facilitates such custom development efforts without coding or scripting.

> **See Also:** The "Adapter Factory" section in *Oracle Identity Manager Concepts* and *Oracle Identity Manager Design Console Guide* for information about the Adapter Factory

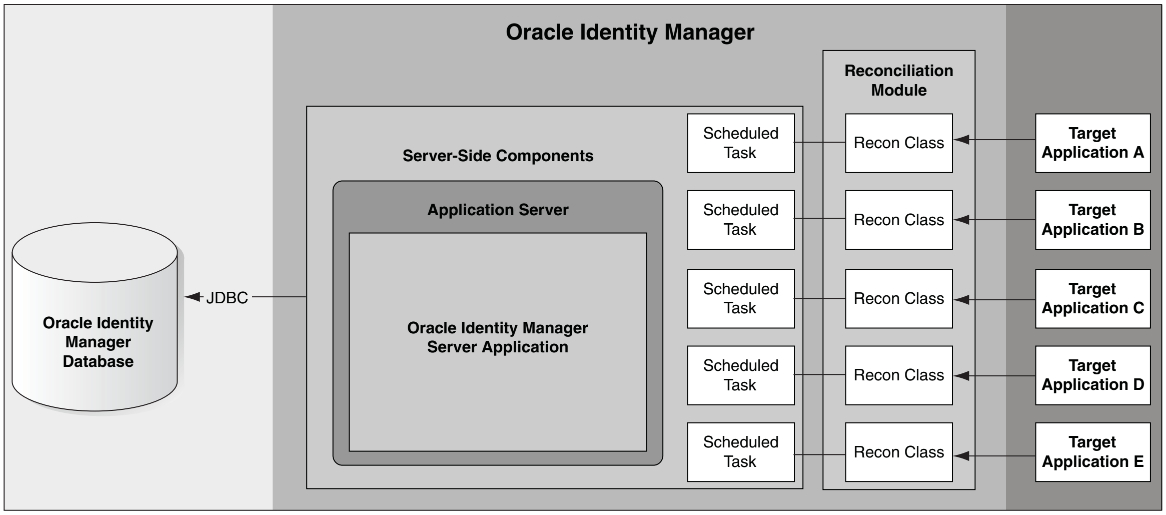
1.2 Reconciliation

Oracle Identity Manager provides a centralized control mechanism to manage users and entitlements and to control user access to resources. However, you can choose not to use Oracle Identity Manager as the primary repository or the front-end entry point of your user accounts. Instead, you can use Oracle Identity Manager to periodically poll your target systems for maintaining an up-to-date profile of all accounts that exist on those systems. This is the reconciliation configuration of Oracle Identity Manager.

> **Note:** For some target systems, the reconciliation of updates to user data takes place in real time and does not require periodic polling of the target system by Oracle Identity Manager.

Figure 1–2 illustrates reconciliation.

Figure 1–2 Reconciliation Configuration



As shown in this figure, in the reconciliation configuration, Oracle Identity Manager is used only as a single updated store for all users and user groups data of the target system. Users are created, deleted, and maintained by local resource-specific administrators.

Reconciliation involves using the user discovery and account discovery features of Oracle Identity Manager.

The following sections provide more information about reconciliation:

- Reconciliation Configuration Options
- Regular Reconciliation Events vs. Delete Reconciliation Events

1.2.1 Reconciliation Configuration Options

Configuring reconciliation involves selecting a combination of options from the following reconciliation parameters:

- Reconciliation Type: Target Resource or Trusted Source
- Reconciliation Mode: Full or Incremental
- Batched Reconciliation
- Limited Reconciliation
- Periodic, On-Demand, or Real-Time Reconciliation

See "Sample Reconciliation Configurations" on page 1-8 for examples of reconciliation configurations.

1.2.1.1 Reconciliation Type: Target Resource or Trusted Source

This section describes the reconciliation types, target resource and trusted source.

1.2.1.1.1 Target Resource Reconciliation

While configuring reconciliation, you can designate a target system as a **target resource**. In a target resource reconciliation run, resources assigned to OIM Users are synchronized with target system accounts of the same users.

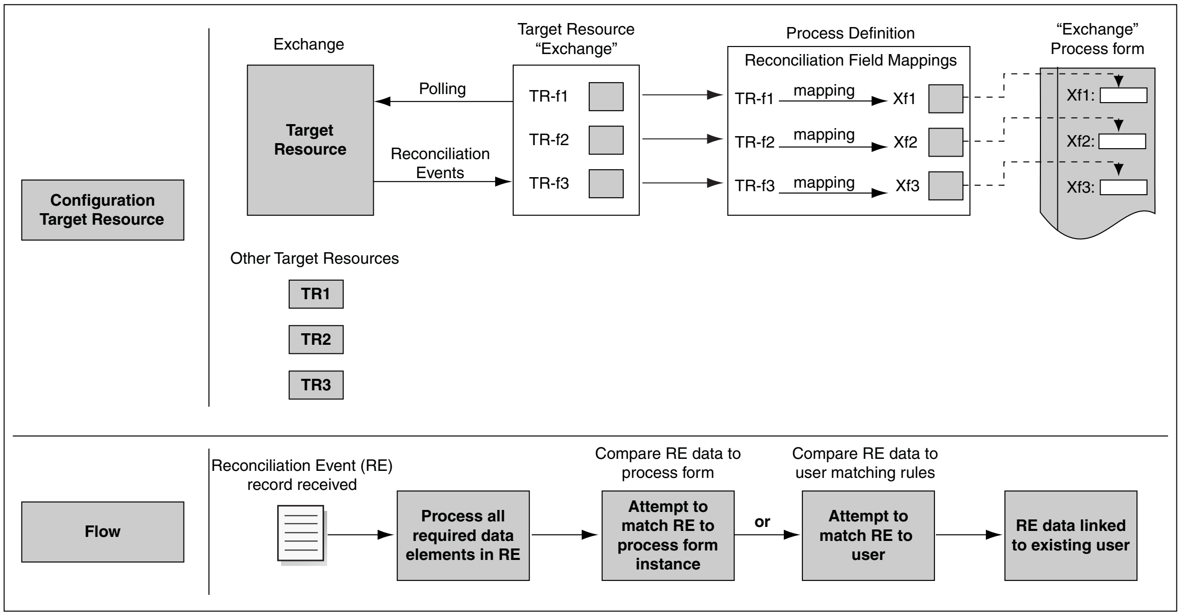
The following example illustrates how target resource reconciliation works:

Suppose an account is created for user John Doe on Microsoft Active Directory. After the next target resource reconciliation run, the Microsoft Active Directory resource is allocated to the OIM User identity of John Doe. The attributes of the resource allocated to the OIM User have the same values as the attributes of the account created in Microsoft Active Directory.

If changes are made to the account in Microsoft Active Directory, then the same changes are made to the resource allocated to the OIM User during subsequent reconciliation runs.

Figure 1–3 illustrates the steps involved in target resource reconciliation.

Figure 1–3 Target Resource Reconciliation


Configuration Target Resource
Exchange
Target Resource
Polling
Reconciliation Events
Target Resource "Exchange"
TR-f1
TR-f2
TR-f3
Process Definition
Reconciliation Field Mappings
TR-f1 mapping Xf1
TR-f2 mapping Xf2
TR-f3 mapping Xf3
"Exchange" Process form
Xf1:
Xf2:
Xf3:
Other Target Resources
TR1
TR2
TR3
Flow
Reconciliation Event (RE) record received
Process all required data elements in RE
Compare RE data to process form
Attempt to match RE to process form instance
or
Compare RE data to user matching rules
Attempt to match RE to user
RE data linked to existing user

1.2.1.1.2 Trusted Source Reconciliation

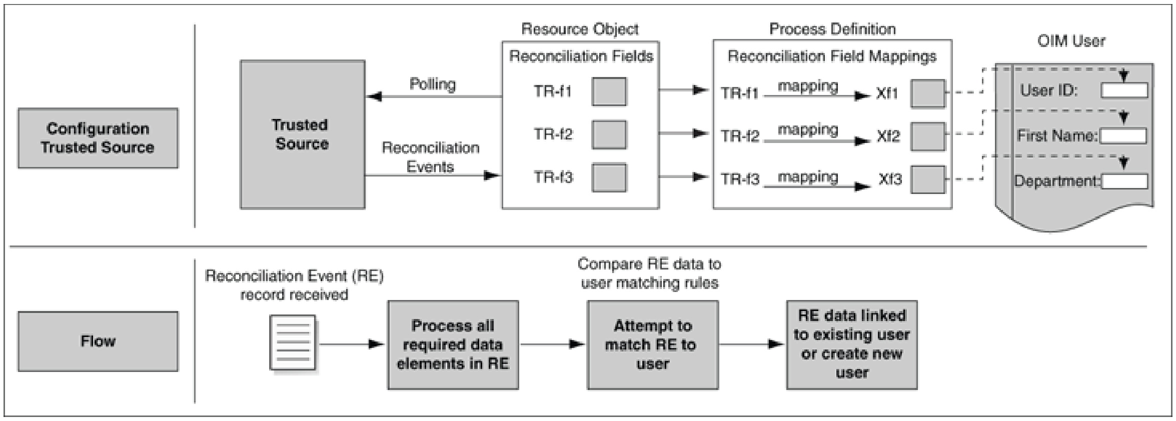
While configuring reconciliation, you can designate a target system as a **trusted source**. The following example illustrates how trusted source reconciliation works.

Suppose an account is created for user John Doe on Microsoft Active Directory. After the next trusted source reconciliation run, an OIM User identity is created for John Doe. The attributes of the OIM User have the same values as the attributes of the account created in Microsoft Active Directory.

If changes are made to the account in Microsoft Active Directory, then the same changes are made to the OIM User during subsequent reconciliation runs.

Figure 1–4 illustrates the steps involved in trusted source reconciliation.

Figure 1–4 Trusted Source Reconciliation


Configuration Trusted Source
Trusted Source
Polling
Reconciliation Events
Resource Object
Reconciliation Fields
TR-f1
TR-f2
TR-f3
Process Definition
Reconciliation Field Mappings
TR-f1 mapping Xf1
TR-f2 mapping Xf2
TR-f3 mapping Xf3
OIM User
User ID:
First Name:
Department:
Flow
Reconciliation Event (RE) record received
Process all required data elements in RE
Compare RE data to user matching rules
Attempt to match RE to user
RE data linked to existing user or create new user

In the operating environment of your organization, multiple target systems might act as trusted sources for the various attributes that constitute the user account. For example, employees' first names and last names might come from the HR system, and employees' e-mail addresses might come from Microsoft Active Directory. In such a scenario, you can configure each target system as a trusted source for a specific attribute or set of attributes of the user accounts. By doing this, you configure multiple trusted source reconciliation, which is a special implementation of trusted source reconciliation.

In another form of multiple trusted source reconciliation, you designate multiple target systems as trusted sources for user accounts belonging to specific user types. This is illustrated by the following example.

In the operating environment of your organization, Siebel is used to track transactions with customers. User accounts created for customers are grouped under the Customer user type. Sun Java System Directory is used to store information about employees in the form of user accounts that are grouped under the Employee user type. When you configure multiple trusted source reconciliation, you designate Siebel as the trusted source for all accounts of the Customer user type and you designate Sun Java System Directory as the trusted source for all accounts of the Employee user type.

In summary, multiple trusted source reconciliation can be implemented in one of the following forms:

- Each target system is designated as the trusted source for a specific attribute or a set of attributes of the user account.
- Each target system is designated as the trusted source for a particular user type.

1.2.1.2 Reconciliation Mode: Full or Incremental

You can use Oracle Identity Manager to perform **full reconciliation** with a target system. The purpose of this mode of reconciliation is to fetch all target system accounts for processing during reconciliation. Full reconciliation is performed by default during the first reconciliation run performed on a target system. The timestamp at which this reconciliation run begins is recorded in Oracle Identity Manager. For the next reconciliation run, accounts that have been added, modified, or deleted after the recorded time stamp are fetched for reconciliation. In other words, from the second reconciliation run onward, **incremental reconciliation** becomes the default reconciliation mode.

You can manually switch from incremental reconciliation to full reconciliation or from full reconciliation to incremental reconciliation.

1.2.1.3 Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager by default. Depending on the number of records to be reconciled, this process might take a long time to complete. In addition, if the connection breaks during reconciliation, then the process might take even more time. You can configure **batched reconciliation** to avoid such problems.

In batched reconciliation, the total set of records to be reconciled is divided into batches containing the number of records that you specify as the batch size.

There may be minute variations from connector to connector in the actual implementation of this feature. The following example illustrates how batched reconciliation works.

Suppose that Sun Java System Directory is configured as a target system in the operating environment of your organization. To configure batched reconciliation for this target system, you specify values for the following scheduled task attributes:

- StartRecord: Use this attribute to specify the record number from which batched reconciliation must begin. Suppose you specify `120` as the value of this attribute.
- BatchSize: Use this attribute to specify the number of records that must be included in each batch. Suppose you specify `50` as the value of this attribute.
- NumberOfBatches: Use this attribute to specify the total number of batches that must be reconciled. Suppose you specify `6` as the value of this attribute.

At the start of the next reconciliation run, if there are 136 records to be reconciled, then these records will be divided into three batches of 50, 50, and 36 records and then each batch is reconciled into Oracle Identity Manager.

If you do not want to configure batched reconciliation, then do not specify a batch size. In this case, a **nonbatched** reconciliation will occur.

1.2.1.4 Limited Reconciliation

By default, all target system records that are added or modified after the previous reconciliation run are reconciled during the current reconciliation run. You can filter records for reconciliation by specifying the subset of newly added or modified records that must be reconciled. You implement this form of **limited reconciliation** by creating **customized queries** for reconciliation. The following example illustrates how limited reconciliation works:

For Sun Java System Directory, you implement limited reconciliation by specifying a customized query as the value of the CustomizedReconQuery IT resource parameter. The following are sample customized queries:

- `givenname=John&sn=Doe`

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

- `givenname=John&sn=Doe|departmentnumber=033`

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

  – The user's first name is `John` and last name is `Doe`.

  – The user belongs to the department whose number is `033`.

If you do not want to configure limited reconciliation, then do not specify a customized query, then a **regular reconciliation** takes place.

1.2.1.5 Periodic, On-Demand, or Real-Time Reconciliation

You can use Oracle Identity Manager for periodic, on-demand, or real-time reconciliation.

> **Note:** All connectors do not support all of these reconciliations.

Periodic reconciliation is reconciliation that is run at regular intervals. Typically, periodic reconciliation is scheduled using a scheduled task. For example, for a particular connector, you can schedule reconciliation to run on a daily, weekly, or monthly basis.

On-demand reconciliation refers to a reconciliation run that you start when required. Consider the following example:

Suppose you have scheduled reconciliation to run at 1:00 a.m. everyday. On a particular Saturday, major changes occurs are made in the target system, and these changes must be reconciled into Oracle Identity Manager immediately. In this situation, you can manually start the reconciliation run to copy the changes into Oracle Identity Manager.

Real-time reconciliation involves an immediate transfer of created or modified data from the target system to Oracle Identity Manager. Usually, this transfer of data is performed through a listener. Whenever data is created or modified on the target system, the target system sends the modified data to the listener. The listener parses this data and forwards it to Oracle Identity Manager.

1.2.1.6 Sample Reconciliation Configurations

As mentioned earlier, you configure reconciliation by selecting specific options from the reconciliation parameters discussed in the preceding sections. The following sample reconciliation configurations are supported in Oracle Identity Manager release 9.1.0:

> **Note:** Oracle Identity Manager Connectors release 9.1.0 can be deployed only on Oracle Identity Manager release 9.1.0..

- Trusted source, full, batched, and regular reconciliation for a single target system. For example, Oracle e-Business Employee Reconciliation for all Oracle Identity Manager users.
- Trusted source, incremental, and regular reconciliation for a single target system. For example, Oracle e-Business Employee Reconciliation for all Oracle Identity Manager users.
- Target resource, full, and regular reconciliation. For example, IBM RACF for all user accounts.
- Target resource, incremental, and batched reconciliation. For example, Lotus Notes for all user accounts.

In a multiple trusted source environment, the combination of the following reconciliation runs provides the complete user identity population of a single Oracle Identity Manager deployment.

- Multiple trusted source, full, nonbatched, and limited (`userType=Employee`) reconciliation. For example, Oracle e-Business Employee Reconciliation used as a trusted source for only the Employee OIM User type.

- Multiple trusted source, full, batched, and regular reconciliation. For example, Microsoft Active Directory used as a trusted source for only Contractor OIM User type.

1.2.2 Regular Reconciliation Events vs. Delete Reconciliation Events

Reconciliation events can be divided into two types depending on their expected behavior within Oracle Identity Manager. If the incoming data relates to an account that must be either created (because Oracle Identity Manager was not aware of it before) or updated (because Oracle Identity Manager has a record of it), then the reconciliation event is a **regular reconciliation event**.

If the input data relates to an account that must be marked as having been deleted (revoked), then the reconciliation event is a **delete reconciliation event**. There are two types of delete reconciliation events:

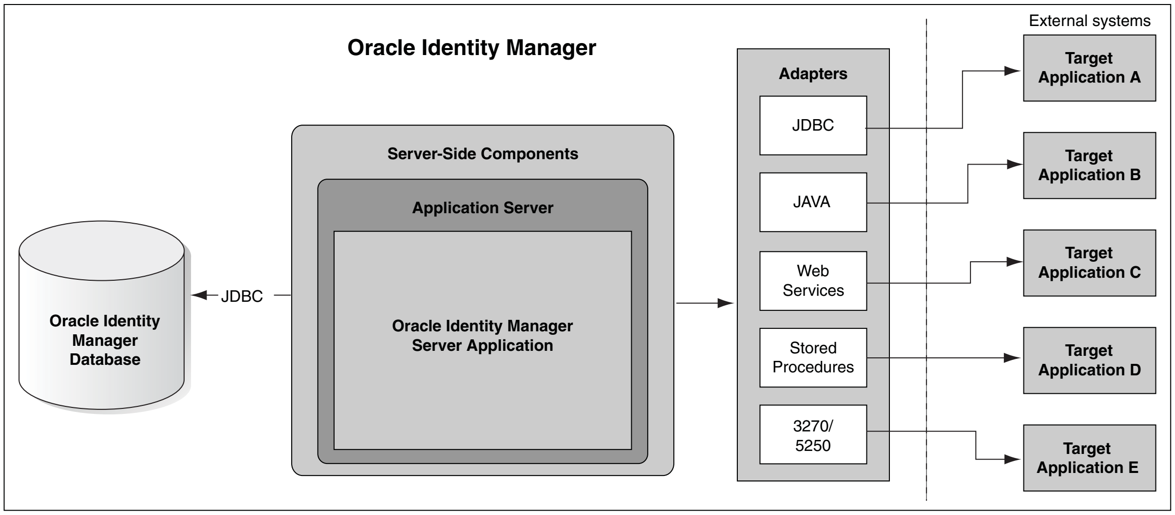
- The data for deleting an account is provided and the Oracle Identity Manager locates the matching account based on existing rules.
- The matching account record in Oracle Identity Manager is provided as the data for deleting an account.

The latter happens when the delete detection mechanism of reconciliation is employed. In both cases, if the accounts are matched, then the resource instance in Oracle Identity Manager is marked as revoked.

1.3 Provisioning

You can use Oracle Identity Manager to create, maintain, and delete users on target systems. In this configuration, Oracle Identity Manager acts as the front-end entry point for managing user data on the target systems. After accounts are provisioned, the users for whom the accounts have been provisioned can access the target systems without any interaction with Oracle Identity Manager. This is the provisioning configuration of Oracle Identity Manager. Figure 1–5 illustrates the provisioning configuration of Oracle Identity Manager.

Figure 1–5 Provisioning



A provisioning operation can be started through any of the following ways:

- **Request-based provisioning**

In request-based provisioning, an individual creates a request for a target system account. The provisioning process is completed when an OIM User with the required privileges approves the request and provisions the target system account to the requester.

- **Policy-based provisioning**

  This type of provisioning refers to resources being granted to users automatically through access policies. Access policies are used to define the association between user groups (or roles) and target resources. User groups are collections of users to whom you grant access to common functionality, such as access rights, roles, or permissions. You use user groups to create and collectively manage records of group members.

  You can also assign or remove membership rules to and from these groups. These rules define which users can be assigned to a particular user group. By default, each member of these user groups gets a predefined account in the target system. In addition, you can also use Oracle Identity Manager to create approval processes that can be run as part of the policy-based provisioning cycle.

  Sometimes, the introduction of or change to an access policy may entail changes in privileges assigned to users who meet the criteria specified in the policy. For example, suppose the following policy is introduced:

  All project managers working from the London office must have access to the SAP system.

  When this policy is introduced in Oracle Identity Manager, SAP user accounts are automatically provisioned to all project managers.

- **Direct provisioning**

  This type of provisioning is a special administrator-only function in which an Oracle Identity Manager administrator provisions a resource to an OIM User. The workflow for this form of provisioning does not include the request and approval steps. You perform direct provisioning by using the Oracle Identity Manager Administrative and User Console.

1.4 Target System Configurations Enabled by a Connector

The type of operations that can be performed by using a connector depends on how you configure the target system:

- Target System Configured As a Target Resource
- Target System Configured As a Trusted Source

1.4.1 Target System Configured As a Target Resource

When configured as a managed or target resource, you can provision target system accounts to OIM Users. In the Oracle Identity Manager context, these target system accounts are called resources that are assigned to OIM Users.

This section discusses connector operations that can be performed when the target system is configured as a target resource.

Lookup field synchronization involves copying data about additions or changes made to lookup field data on the target system into Oracle Identity Manager lookup fields. Lookup field synchronization is started using a scheduled task. For each lookup field in a particular target system, a lookup definition is created in Oracle Identity Manager. Oracle Identity Manager lookup fields are used during provisioning. During a lookup field synchronization run, additions or modifications to existing data in the target system lookup fields are replicated in the lookup definitions in Oracle Identity Manager.

The other actions that can be performed on a target resource are target resource reconciliation and provisioning. For target resource reconciliation, changes made to accounts on the target system itself can be reconciled into Oracle Identity Manager. In other words, resources in Oracle Identity Manager can be synchronized with changes made to the corresponding accounts on the target system. These activities constitute reconciliation.

During target resource reconciliation:

- For a newly created target system identity that is fetched from the target system, a target resource account (resource object) is granted (provisioned) to the corresponding OIM User. This takes place only if an OIM User already exists for the target system identity.
- For a modified target system identity that is fetched from the target system, the same modifications are made to its corresponding resource object provisioned to an entity in Oracle Identity Manager.

Typically, target systems like e-mail servers are designated as target resources.

Note: A target resource can have a provisioning flow associated with it.

You can also create and manage resources on the target system through Oracle Identity Manager. These activities constitute provisioning. The purpose of provisioning is to automate the creation and maintenance of users on target systems. Provisioning is also used to accommodate any requirement for workflow approvals and auditing that can be a component of that provisioning life cycle.

See "Provisioning" on page 1-9 for information about provisioning and the different types of provisioning operations that can be performed.

1.4.2 Target System Configured As a Trusted Source

A target system is known as a trusted source if it is used as the authoritative source for identity information about entities (both individuals and resources) in the organization. Each identity on a trusted source must correspond to a single OIM User on Oracle Identity Manager. An entity can have an account on other systems in the organization only if it has an account on the trusted source.

Note: In the Oracle Identity Manager context, the term “OIM User” is used as a synonym for an Oracle Identity Manager identity created for a person.

During trusted source reconciliation:

- For a newly created target system identity that is fetched from the target system, a corresponding OIM User is created in Oracle Identity Manager.
- For a modified target system identity that is fetched from the target system, the same modifications are made to its corresponding OIM User.

- If you specify certain attributes of a target system as trusted sources, then Oracle Identity Manager must be disabled from provisioning the same set of attributes in the target system.

Typically, target systems like HR systems and corporate directories are designated as trusted sources.

2

Components Used for Connector Operations

A connector is an abstraction for a collection of components that are used to perform reconciliation and provisioning operations on a target system. Each component plays a specific role during reconciliation, provisioning, or both. When you build a custom connector, you create these components by using the Oracle Identity Manager Design Console. In a predefined connector, the definitions of these components are included in the connector XML files. When you import the connector XML files during connector deployment, these components are automatically created in Oracle Identity Manager. Along with connector components, this chapter also discusses certain Oracle Identity Manager components that are essential during connector deployment.

The Oracle Identity Manager and connector components are described in the following sections:

- Oracle Identity Manager Components
- Connector Components

2.1 Oracle Identity Manager Components

The following components of Oracle Identity Manager are used during connector operations:

- Reconciliation APIs
- Reconciliation Engine
- Reconciliation Manager
- Remote Manager

2.1.1 Reconciliation APIs

The published set of Oracle Identity Manager APIs includes a set related to reconciliation. Oracle Identity Manager uses these APIs to create reconciliation events. These APIs provide for the mechanisms by which the appropriate data is provided for the events.

> **See Also:** Chapter 2, "What's New" of *Oracle Identity Manager API Usage Guide* for information about the APIs related to reconciliation

2.1.2 Reconciliation Engine

The reconciliation engine uses all components, data processors, and rule evaluators that use these components to convert input data into a list of action items. It also includes the components that determine whether or not the actions can be automated based on the rule context. When an action is performed, either automatically or manually, the reconciliation engine performs the appropriate updates and provisioning actions.

2.1.3 Reconciliation Manager

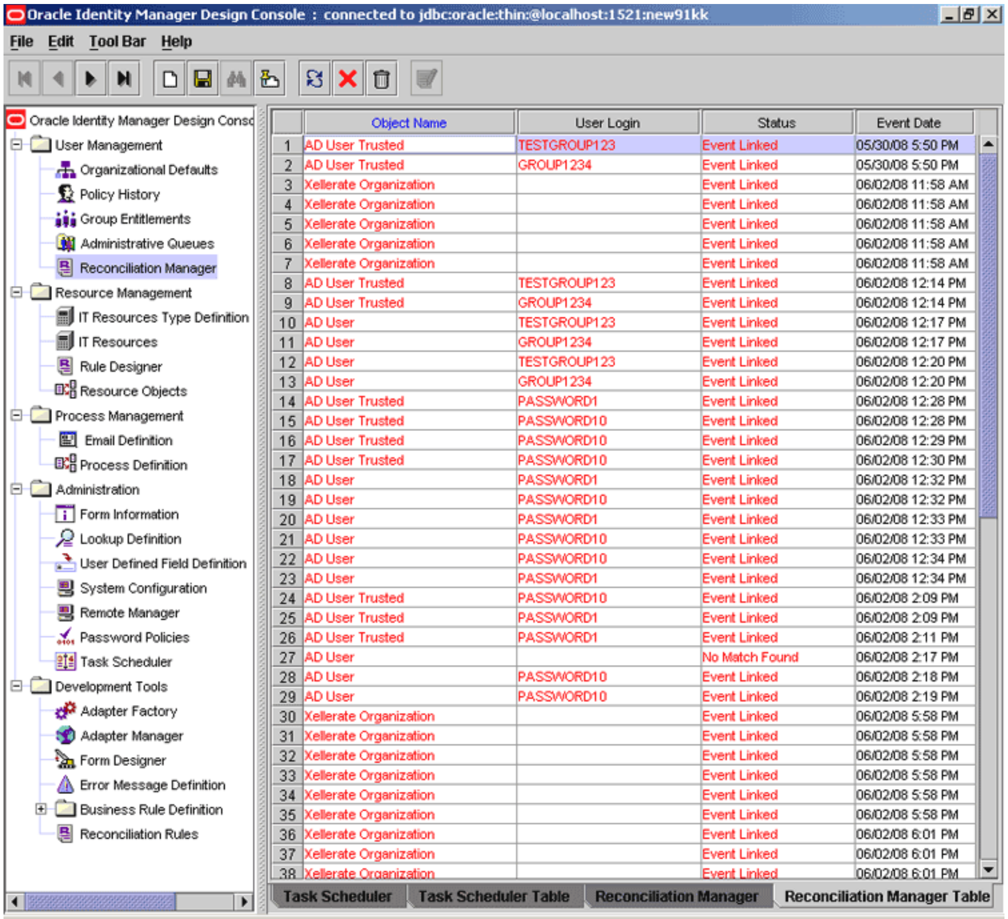
The Reconciliation Manager is a form in the Oracle Identity Manager Design Console. You can use this form to examine a reconciliation event and perform the actions based on the status of the event. The Reconciliation Manager displays the data received, results of rule evaluation, actions that you can perform, and results of the actions.

The main section of the form displays the event information, including the resource object with which it is associated, the date the event occurred, its current status, and the entity to which it is linked. The following are action buttons in the form for the actions that you can perform:

- Close Event: Closes an event without any resolution.
- Re-apply Matching Rules: Takes the processed data and reapplies all reconciliation rules by deleting the results from previous applications of the rule. This action must be performed when the rule is modified.
- Create User: Enables the creation of an OIM User based on the data provided.
- Create Organization: Enables the creation of an OIM Organization based on the data provided.

To view the Reconciliation Manager, you must click Reconciliation Manager under User Management on the left pane of the Oracle Identity Manager Design Console. The status of the events are displayed on the right pane. Figure 2–1 shows the Reconciliation Manager form of Microsoft Active Directory.

Figure 2–1 Reconciliation Manager



	Object Name	User Login	Status	Event Date
1	AD User Trusted	TESTGROUP123	Event Linked	05/30/08 5:50 PM
2	AD User Trusted	GROUP1234	Event Linked	05/30/08 5:50 PM
3	Xellerate Organization		Event Linked	06/02/08 11:58 AM
4	Xellerate Organization		Event Linked	06/02/08 11:58 AM
5	Xellerate Organization		Event Linked	06/02/08 11:58 AM
6	Xellerate Organization		Event Linked	06/02/08 11:58 AM
7	Xellerate Organization		Event Linked	06/02/08 11:58 AM
8	AD User Trusted	TESTGROUP123	Event Linked	06/02/08 12:14 PM
9	AD User Trusted	GROUP1234	Event Linked	06/02/08 12:14 PM
10	AD User	TESTGROUP123	Event Linked	06/02/08 12:17 PM
11	AD User	GROUP1234	Event Linked	06/02/08 12:17 PM
12	AD User	TESTGROUP123	Event Linked	06/02/08 12:20 PM
13	AD User	GROUP1234	Event Linked	06/02/08 12:20 PM
14	AD User Trusted	PASSWORD1	Event Linked	06/02/08 12:28 PM
15	AD User Trusted	PASSWORD10	Event Linked	06/02/08 12:28 PM
16	AD User Trusted	PASSWORD10	Event Linked	06/02/08 12:29 PM
17	AD User Trusted	PASSWORD10	Event Linked	06/02/08 12:30 PM
18	AD User	PASSWORD1	Event Linked	06/02/08 12:32 PM
19	AD User	PASSWORD10	Event Linked	06/02/08 12:32 PM
20	AD User	PASSWORD1	Event Linked	06/02/08 12:33 PM
21	AD User	PASSWORD10	Event Linked	06/02/08 12:33 PM
22	AD User	PASSWORD10	Event Linked	06/02/08 12:34 PM
23	AD User	PASSWORD1	Event Linked	06/02/08 12:34 PM
24	AD User Trusted	PASSWORD10	Event Linked	06/02/08 2:09 PM
25	AD User Trusted	PASSWORD1	Event Linked	06/02/08 2:09 PM
26	AD User Trusted	PASSWORD1	Event Linked	06/02/08 2:11 PM
27	AD User		No Match Found	06/02/08 2:17 PM
28	AD User	PASSWORD10	Event Linked	06/02/08 2:18 PM
29	AD User	PASSWORD10	Event Linked	06/02/08 2:19 PM
30	Xellerate Organization		Event Linked	06/02/08 5:58 PM
31	Xellerate Organization		Event Linked	06/02/08 5:58 PM
32	Xellerate Organization		Event Linked	06/02/08 5:58 PM
33	Xellerate Organization		Event Linked	06/02/08 5:58 PM
34	Xellerate Organization		Event Linked	06/02/08 5:58 PM
35	Xellerate Organization		Event Linked	06/02/08 5:58 PM
36	Xellerate Organization		Event Linked	06/02/08 6:01 PM
37	Xellerate Organization		Event Linked	06/02/08 6:01 PM
38	Xellerate Organization		Event Linked	06/02/08 6:01 PM

2.1.4 Remote Manager

A Remote Manager is an application that enables Oracle Identity Manager to interact with local commands on the target system. You may use a Remote Manager in one of the following situations:

- The target system is not network aware. In other words, the target system does not provide features that can be used to communicate with it over a network.
- Fields of the target system are not in a format that is compatible with the format of fields in Oracle Identity Manager.
- The network APIs do not provide all the required functionality.

A Remote Manager is deployed on the target system host computer.

2.2 Connector Components

The following components are created when you deploy a connector:

- Reconciliation Field Definitions
- Reconciliation Field Mappings
- Reconciliation Rules
- Reconciliation Action Rules

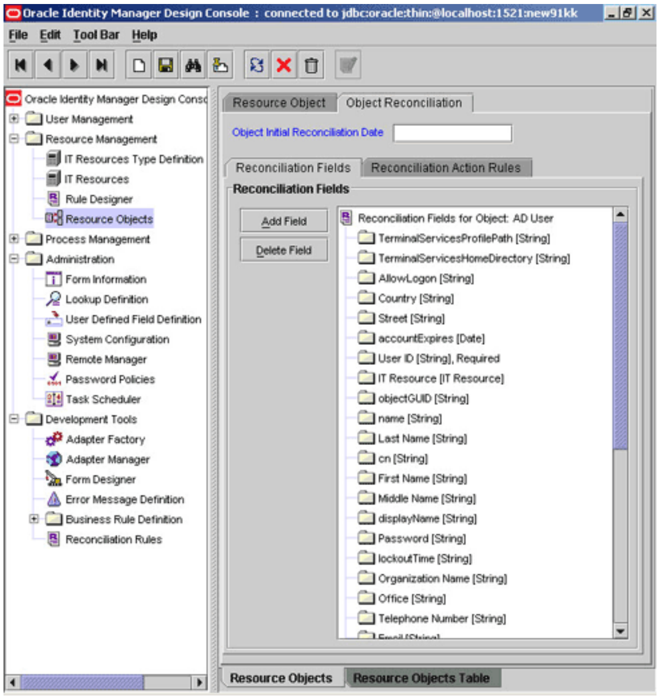
- Reconciliation Provisioning Tasks
- IT Resource
- IT Resource Type
- Lookup Definitions
- Scheduled Tasks
- Resource Object
- Process Form
- Provisioning Process, Process Tasks, and Adapters

2.2.1 Reconciliation Field Definitions

When you define a target system as a resource object in Oracle Identity Manager, reconciliation fields represent the actual fields of the target system.

To view the reconciliation fields, you click Resource Objects under Resource Management on the left pane of the Oracle Identity Manager Design Console, and then click the Object Reconciliation tab. Figure 2–2 shows the screenshot of the reconciliation fields of Microsoft Active Directory.

Figure 2–2 Reconciliation Fields



Reconciliation Fields for Object: AD User
- TerminalServicesProfilePath [String]
- TerminalServicesHomeDirectory [String]
- AllowLogon [String]
- Country [String]
- Street [String]
- accountExpires [Date]
- User ID [String], Required
- IT Resource [IT Resource]
- objectGUID [String]
- name [String]
- Last Name [String]
- cn [String]
- First Name [String]
- Middle Name [String]
- displayName [String]
- Password [String]
- lockoutTime [String]
- Organization Name [String]
- Office [String]
- Telephone Number [String]
- Email [String]

2.2.2 Reconciliation Field Mappings

After you define the reconciliation fields, you must map them to the fields that are defined on a process form. Reconciliation field mappings define how the data received from the target system is used to update the fields on a process form. Each reconciliation field of a target system is mapped to a process form field in Oracle Identity Manager.

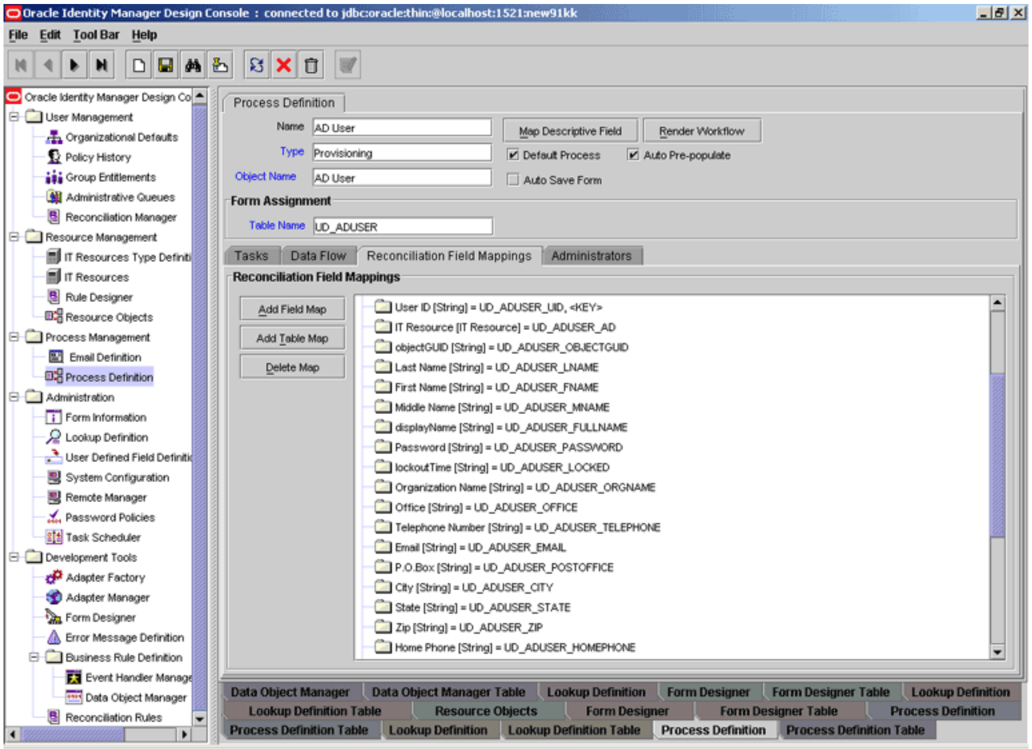
See Also:

- The "Process Definition Form" section in *Oracle Identity Manager Design Console Guide*

- The "Reconciliation Field Mappings Tab" section in *Oracle Identity Manager Design Console Guide* for information about status reconciliation

To view the reconciliation field mappings, you click Process Definition under Process Manager on the left pane of the Oracle Identity Manager Design Console, and then click the Reconciliation Field Mappings tab. Figure 2–3 shows the screenshot of the reconciliation field mappings for Microsoft Active Directory.

Figure 2–3 Reconciliation Field Mappings



Name: AD User

Type: Provisioning

Object Name: AD User

☑ Default Process ☑ Auto Pre-populate

☐ Auto Save Form

Table Name: UD_ADUSER

- User ID [String] = UD_ADUSER_UID, <KEY>
- IT Resource [IT Resource] = UD_ADUSER_AD
- objectGUID [String] = UD_ADUSER_OBJECTGUID
- Last Name [String] = UD_ADUSER_LNAME
- First Name [String] = UD_ADUSER_FNAME
- Middle Name [String] = UD_ADUSER_MNAME
- displayName [String] = UD_ADUSER_FULLNAME
- Password [String] = UD_ADUSER_PASSWORD
- lockoutTime [String] = UD_ADUSER_LOCKED
- Organization Name [String] = UD_ADUSER_ORGNAME
- Office [String] = UD_ADUSER_OFFICE
- Telephone Number [String] = UD_ADUSER_TELEPHONE
- Email [String] = UD_ADUSER_EMAIL
- P.O.Box [String] = UD_ADUSER_POSTOFFICE
- City [String] = UD_ADUSER_CITY
- State [String] = UD_ADUSER_STATE
- Zip [String] = UD_ADUSER_ZIP
- Home Phone [String] = UD_ADUSER_HOMEPHONE

2.2.3 Reconciliation Rules

During reconciliation, when a target system record is brought to Oracle Identity Manager, the reconciliation engine tries to match the record with an existing record in Oracle Identity Manager. The rules that the reconciliation engine applies to look for a match are called reconciliation rules.

The reconciliation rules are used by the reconciliation engine to determine the identity to which Oracle Identity Manager must assign a newly discovered account on the target system. The reconciliation engine can locate the user of the newly discovered account based on well-known patterns established for the target system. Consider the following example:

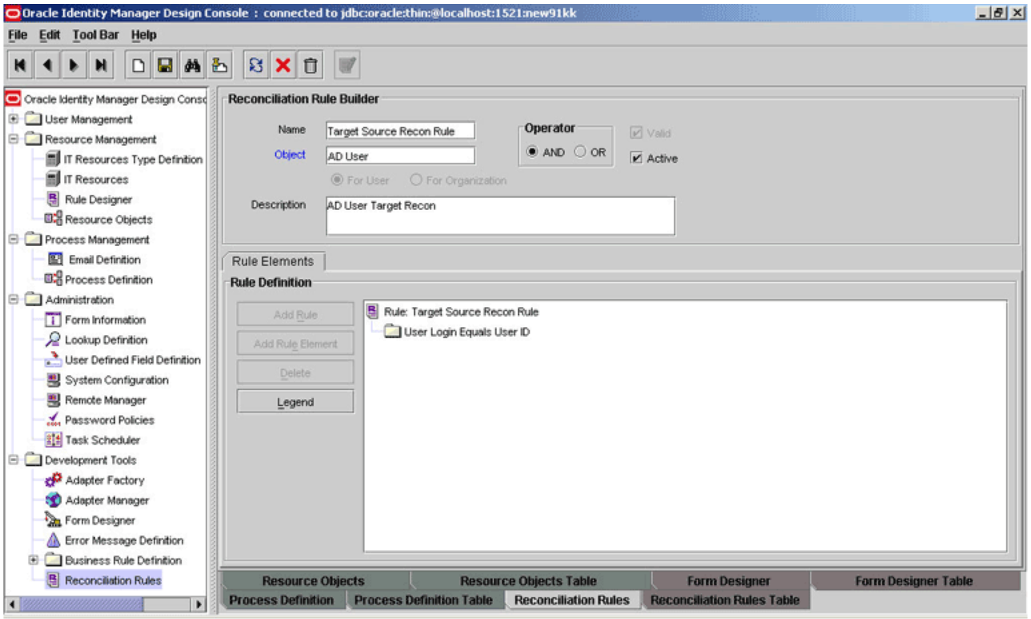
Suppose that all login IDs on the target system are created from the user’s initial and last name. You could then set up a rule that accepts the login ID received from the target system and searches for any user whose first name starts with the first character of the login ID, and the last name is the same as the remainder of the login ID.

> **See Also:** "The Reconciliation Manager Form" in *Oracle Identity Manager Design Console Guide* for more information about reconciliation rules

The manner and sequence in which the rules and action rules are applied is described in "Target Resource Reconciliation" on page 3-1 and "Trusted Source Reconciliation" on page 3-3.

To view a reconciliation rule, you click Reconciliation Rules under Development Tools on the left pane of the Oracle Identity Manager Design Console. The rule is displayed on the Rule Elements tab. Figure 2–4 shows the screenshot of the target resource reconciliation rule for the Microsoft Active Directory connector.

Figure 2–4 Target Resource Reconciliation Rule



Name: Target Source Recon Rule

Object: AD User

Operator: ● AND ○ OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: AD User Target Recon

Rule: Target Source Recon Rule
- User Login Equals User ID

2.2.4 Key Field for Reconciliation Matching

The key field for reconciliation matching is used for process matching, just like the reconciliation rule is used for entity matching. The reconciliation field mappings include the key field for reconciliation matching. The key field is marked in a special way, and it can be highlighted in the list of reconciliation field mappings. During a target resource reconciliation run, process matching is performed first. If no match is found, then entity matching is performed.

2.2.5 Reconciliation Action Rules

Reconciliation action rules define the actions that must be performed based on the reconciliation rules. These action rules are created during connector deployment. Using the reconciliation action rules, the following actions can be defined that the reconciliation engine must automatically perform based on the reconciliation rule evaluations:

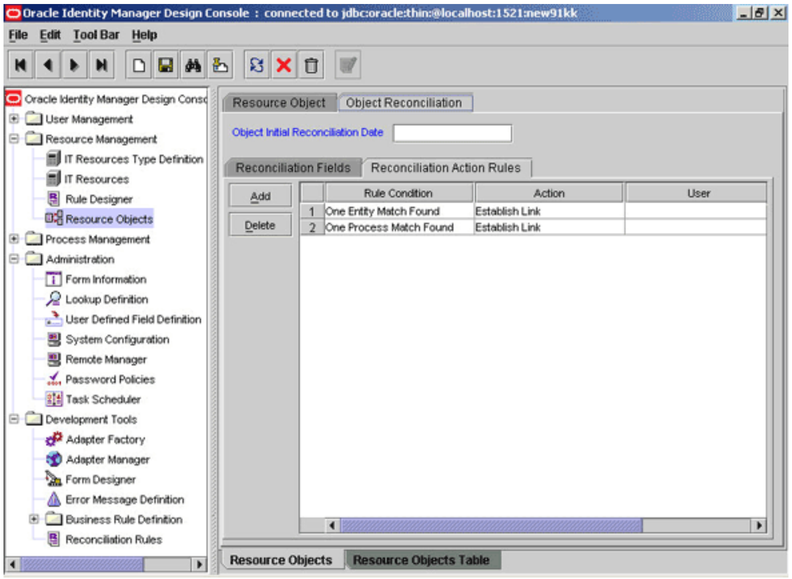
- Assign an event to an administrator.

- Create a new provisioned resource in Oracle Identity Manager and associate it with the corresponding owner identity.
- Update the matched provisioned resource in Oracle Identity Manager.
- Delete the matched provisioned resource in Oracle Identity Manager.
- Create a new user in Oracle Identity Manager.
- Update an existing user in Oracle Identity Manager.
- Delete an existing user in Oracle Identity Manager.

> **See Also:** "The Resource Objects Form" in *Oracle Identity Manager Design Console Guide* for more information about reconciliation action rules

To view the reconciliation action rules, you click Resource Objects under Resource Management on the left pane of the Oracle Identity Manager Design Console, and then click the Reconciliation Action Rules tab. Figure 2–5 shows the screenshot of the target resource reconciliation action rules for the Microsoft Active Directory connector.

Figure 2–5 Reconciliation Action Rules



	Rule Condition	Action	User
1	One Entity Match Found	Establish Link	
2	One Process Match Found	Establish Link	

2.2.6 Reconciliation Provisioning Tasks

In target resource reconciliation, if an event is linked to an existing instance of a provisioned resource, then the process form for that resource instance is updated.

> **Note:** In trusted source reconciliation, the user record is updated instead.

If the account did not exist in Oracle Identity Manager before the reconciliation run, then the default provisioning process is started, adapters are suppressed, and all nonconditional tasks are completed automatically.

In both cases, a marker task is added to the provisioning process for the provisioned resource (or user). The marker task can be either Reconciliation Insert Received or

Reconciliation Update Received. These tasks might have adapters attached to them to begin provisioning. If no adapters are attached to the task, then a response code of "Event Processed" is assigned to that task. Additional provisioning process tasks could be generated based on this response code to start a provisioning flow due to the reconciliation event. This mechanism can be leveraged to start multitarget synchronization processes.

2.2.7 IT Resource

An IT resource is composed of parameters that store connection and other generic information about a target system. Oracle Identity Manager uses this information to connect to a specific installation or instance of the target system. The information stored by these IT resource parameters includes the following:

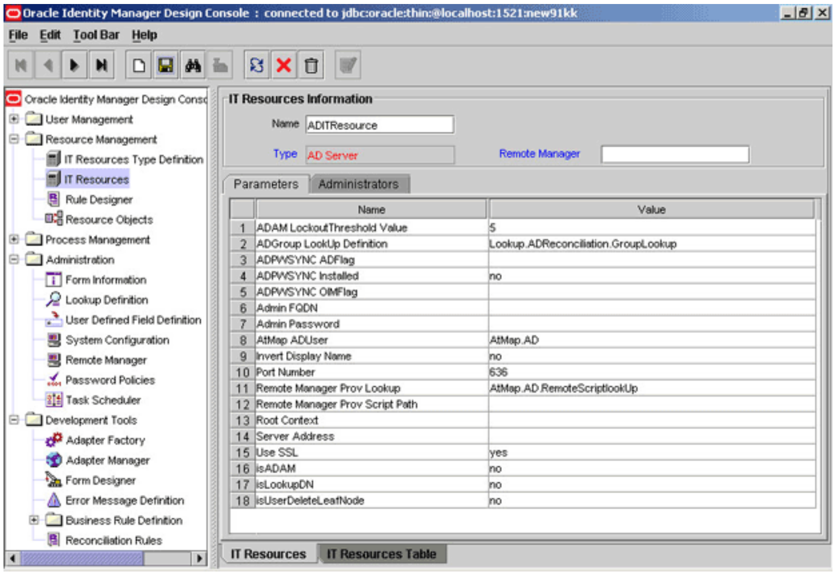
- Host name or IP address of the computer that hosts the target system
- User name and password of the target system account that Oracle Identity Manager uses to connect to the target system
- Whether or not SSL communication is enabled between the target system and Oracle Identity Manager

There must be one IT resource for each installation or instance of the target system. For example, a Microsoft Active Directory installation in the Tokyo office of an organization will have its own IT resource, which will be different from the IT resource used for the Microsoft Active Directory installation in the London office of the organization.

While deploying a connector, you provide the connection information as the values of parameters of the IT resource.

To view the parameters of an IT resource, you click IT Resources under Resource Management on the left pane of the Oracle Identity Manager Design Console, and then enter the name of an IT resource or search for an IT resource. The parameters are displayed on the Parameters tab. Figure 2–6 shows the screenshot of the parameters of one Microsoft Active Directory IT resource.

Figure 2–6 IT Resource Parameters



IT Resources Information

Name ADITResource

Type AD Server

Remote Manager

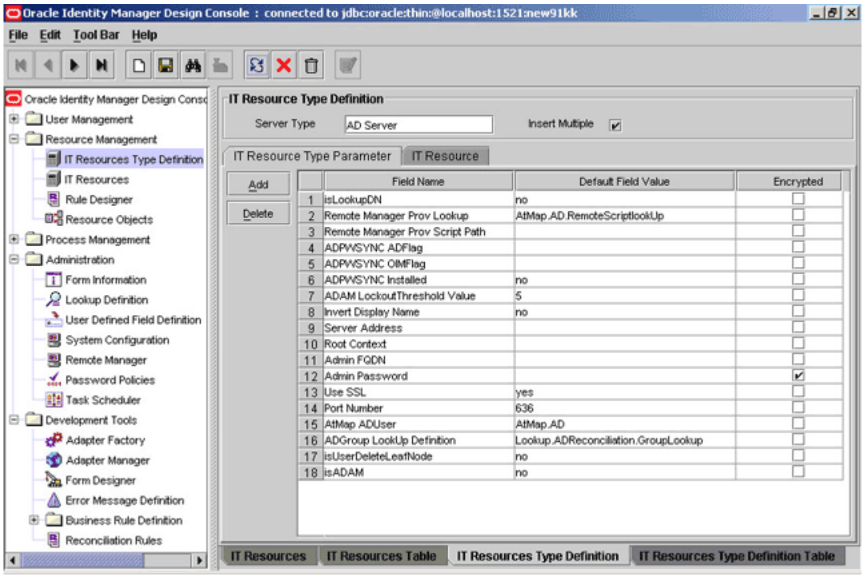
	Name	Value
1	ADAM LockoutThreshold Value	5
2	ADGroup LookUp Definition	Lookup.ADReconciliation.GroupLookup
3	ADPWSYNC ADFlag	
4	ADPWSYNC Installed	no
5	ADPWSYNC OIMFlag	
6	Admin FQDN	
7	Admin Password	
8	AtMap ADUser	AtMap.AD
9	Invert Display Name	no
10	Port Number	636
11	Remote Manager Prov Lookup	AtMap.AD.RemoteScriptlookUp
12	Remote Manager Prov Script Path	
13	Root Context	
14	Server Address	
15	Use SSL	yes
16	isADAM	no
17	isLookupDN	no
18	isUserDeleteLeafNode	no

2.2.8 IT Resource Type

The number and type of parameters that constitute target system connection information may vary from one target system to another. An IT resource type stores the definitions of the connection parameters for a particular target system. An IT resource is an instance of an IT resource type. In other words, IT resources for multiple installations or instances of a particular target system belong to the same IT resource type. For example, the IT resources for the London and Tokyo offices of an organization are created from the same IT resource type.

The IT resource type is linked with the process form. To view the parameters of an IT resource type, you click IT Resources Type Definition under Resource Management on the left pane of the Oracle Identity Manager Design Console. The parameters are displayed under the IT Resource Type Parameter tab. Figure 2–7 shows the screenshot of the IT resource type of Microsoft Active Directory.

Figure 2–7 IT Resource Type



Server Type: AD Server

Insert Multiple ☑

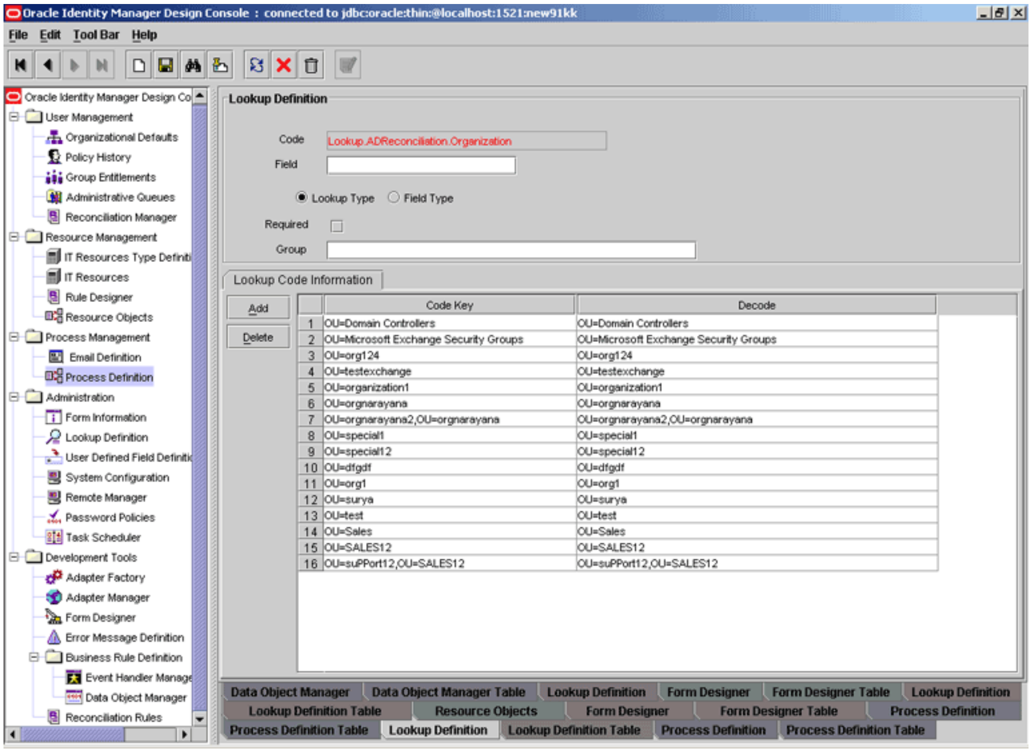
	Field Name	Default Field Value	Encrypted
1	isLookupDN	no	☐
2	Remote Manager Prov Lookup	AtMap.AD.RemoteScriptlookUp	☐
3	Remote Manager Prov Script Path		☐
4	ADPWSYNC ADFlag		☐
5	ADPWSYNC OIMFlag		☐
6	ADPWSYNC Installed	no	☐
7	ADAM LockoutThreshold Value	5	☐
8	Invert Display Name	no	☐
9	Server Address		☐
10	Root Context		☐
11	Admin FQDN		☐
12	Admin Password		☑
13	Use SSL	yes	☐
14	Port Number	636	☐
15	AtMap ADUser	AtMap.AD	☐
16	ADGroup LookUp Definition	Lookup.ADReconciliation.GroupLookup	☐
17	isUserDeleteLeafNode	no	☐
18	isADAM	no	☐

2.2.9 Lookup Definitions

A lookup definition is a repository for a list of values that you can select from while performing a provisioning operation. When a connector is deployed, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. During a provisioning operation, these values are fetched from the definitions and displayed in lookup fields. Country, Currency Code, and Language Code are examples of lookup fields.

To view the lookup definitions, you click Process Definition under Process Management on the left pane of the Oracle Identity Manager Design Console. The lookup definitions are displayed on the Lookup Code Information tab. Figure 2–8 shows the screenshot of the lookup definitions for Microsoft Active Directory.

Figure 2–8 Lookup Definitions



Lookup Definition

Code: Lookup.ADReconciliation.Organization

Field:

● Lookup Type ○ Field Type

Required □

Group:

Lookup Code Information

	Code Key	Decode
1	OU=Domain Controllers	OU=Domain Controllers
2	OU=Microsoft Exchange Security Groups	OU=Microsoft Exchange Security Groups
3	OU=org124	OU=org124
4	OU=testexchange	OU=testexchange
5	OU=organization1	OU=organization1
6	OU=orgnarayana	OU=orgnarayana
7	OU=orgnarayana2,OU=orgnarayana	OU=orgnarayana2,OU=orgnarayana
8	OU=special1	OU=special1
9	OU=special12	OU=special12
10	OU=dfgdf	OU=dfgdf
11	OU=org1	OU=org1
12	OU=surya	OU=surya
13	OU=test	OU=test
14	OU=Sales	OU=Sales
15	OU=SALES12	OU=SALES12
16	OU=suPPort12,OU=SALES12	OU=suPPort12,OU=SALES12

2.2.10 Scheduled Tasks

A scheduled task is used to start a specific action at a specified time. For example, the Password Warning Task scheduled task of Oracle Identity Manager sends e-mail to users for whom the password warning date has passed at the time when the task is run.

A lookup field synchronization scheduled task is used to synchronize the values of lookup fields that are used during provisioning operations.

A reconciliation scheduled task is used to fetch data from the target system for reconciliation with Oracle Identity Manager.

Most predefined connectors contain scheduled tasks for lookup field synchronization and reconciliation of user data. In addition to user data, some target systems require scheduled tasks for reconciliation of group data.

While configuring a scheduled task, you specify values for the attributes of the task in addition to configuring the time at which the task must run.

The following are some of the information that you specify as values of scheduled task attributes for lookup field synchronization:

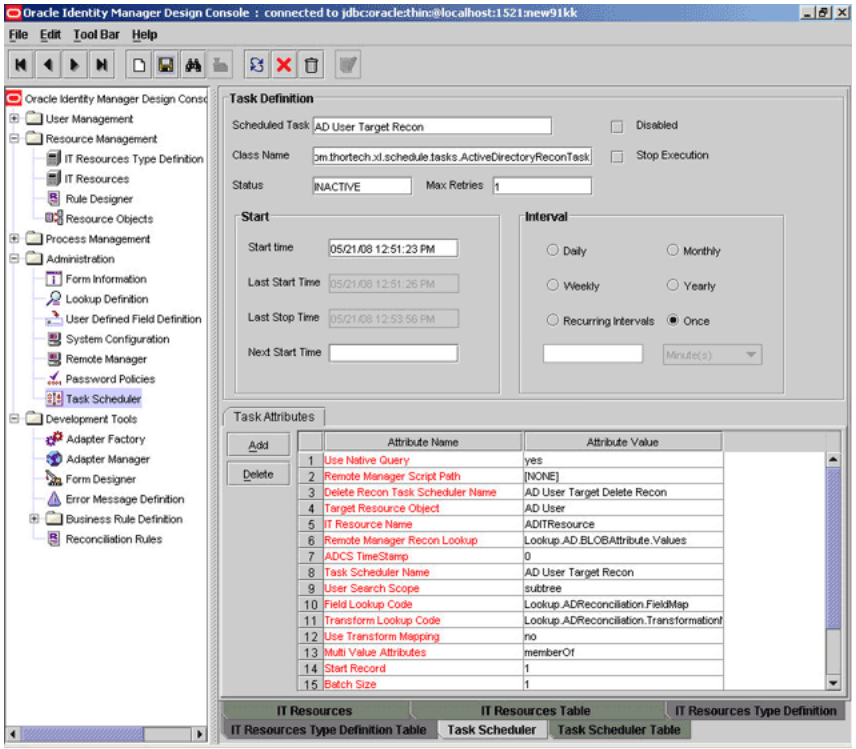
- Name of the IT resource
- Type of data that is searched for in the target system
- Path of the file in which the lookup data to be reconciled is stored
- Whether you want the existing values of the Oracle Identity Manager lookup definition to be deleted or whether these should be updated with the changes made to the target system lookup fields

The following are some of the information that you specify as values of scheduled task attributes for reconciliation:

- Name of the IT resource
- Name of the resource object
- Whether or not you want to run reconciliation
- Whether you want to perform full reconciliation or incremental reconciliation

To view the attributes of a scheduled task, you click Task Scheduler under Administration on the left pane of the Oracle Identity Manager Design Console. The scheduled task attributes are displayed on the Task Attributes tab. Figure 2–9 shows the screenshot of the attributes of the AD User Target Recon scheduled task of Microsoft Active Directory.

Figure 2–9 Scheduled Task Attributes



Task Definition

Scheduled Task: AD User Target Recon

□ Disabled

Class Name: om.thortech.xl.schedule.tasks.ActiveDirectoryReconTask

□ Stop Execution

Status: INACTIVE

Max Retries: 1

Start

Start time: 05/21/08 12:51:23 PM

Last Start Time: 05/21/08 12:51:26 PM

Last Stop Time: 05/21/08 12:53:56 PM

Next Start Time:

Interval

○ Daily ○ Monthly

○ Weekly ○ Yearly

○ Recurring Intervals ● Once

Minute(s)

Task Attributes

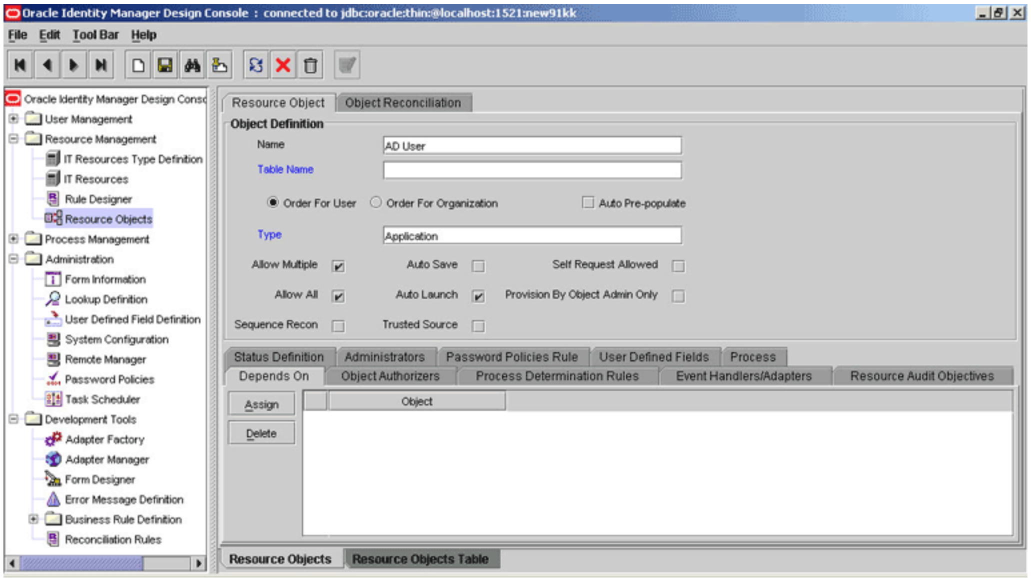
	Attribute Name	Attribute Value
1	Use Native Query	yes
2	Remote Manager Script Path	[NONE]
3	Delete Recon Task Scheduler Name	AD User Target Delete Recon
4	Target Resource Object	AD User
5	IT Resource Name	ADITResource
6	Remote Manager Recon Lookup	Lookup.AD.BLOBAttribute.Values
7	ADCS TimeStamp	0
8	Task Scheduler Name	AD User Target Recon
9	User Search Scope	subtree
10	Field Lookup Code	Lookup.ADReconciliation.FieldMap
11	Transform Lookup Code	Lookup.ADReconciliation.Transformationl
12	Use Transform Mapping	no
13	Multi Value Attributes	memberOf
14	Start Record	1
15	Batch Size	1

2.2.11 Resource Object

A resource object is a virtual representation of a target system. It contains details of the target system attributes (reconciliation fields) whose values are fetched during reconciliation. In addition, configuration information that is specific to a target system is stored in the resource object. A connector can have only one resource object.

To view the details of a resource object, you click Resource Objects under Resource Management on the left pane of the Oracle Identity Manager Design Console. The different parameters of the resource object stored in different tabs are displayed on the Resource Object tab. Figure 2–10 shows the screenshot of the Microsoft Active Directory resource object.

Figure 2–10 Resource Object



Oracle Identity Manager Design Console : connected to jdbc:oracle:thin:@localhost:1521:new91kk

Object Definition

Name: AD User

Table Name:

● Order For User ○ Order For Organization □ Auto Pre-populate

Type: Application

Allow Multiple ☑ Auto Save □ Self Request Allowed □

Allow All ☑ Auto Launch ☑ Provision By Object Admin Only □

Sequence Recon □ Trusted Source □

2.2.12 Process Form

A process form stores the details of the target system identity attributes to which Oracle Identity Manager writes data during a provisioning operation and from which Oracle Identity Manager reads data during reconciliation. The name of the IT resource is stored as an attribute on the process form. If there are multivalued target system fields, then one child form is included for each multivalued field and all the child forms are linked to the parent process form.

To view the different attributes used in a process form, you click Form Designer under Development Tools on the left pane of the Oracle Identity Manager Design Console. The details of the different attributes are displayed on the right pane. Figure 2–13 shows the screenshot of the configuration of the process form for Microsoft Active Directory.

Figure 2–11 Configuration of a Process Form

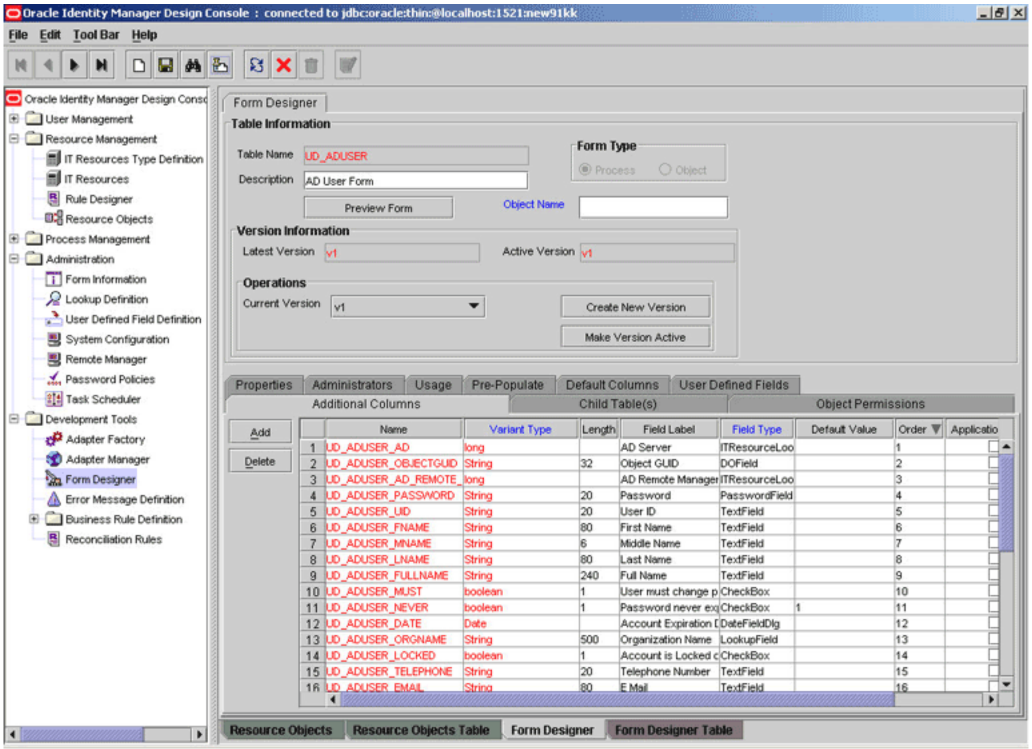


Table Information

Table Name: UD_ADUSER

Description: AD User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: v1

Active Version: v1

Operations

Current Version: v1

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Applicatio
1	UD_ADUSER_AD	long		AD Server	ITResourceLoo		1	□
2	UD_ADUSER_OBJECTGUID	String	32	Object GUID	DOField		2	□
3	UD_ADUSER_AD_REMOTE_	long		AD Remote Manager	ITResourceLoo		3	□
4	UD_ADUSER_PASSWORD	String	20	Password	PasswordField		4	□
5	UD_ADUSER_UID	String	20	User ID	TextField		5	□
6	UD_ADUSER_FNAME	String	80	First Name	TextField		6	□
7	UD_ADUSER_MNAME	String	6	Middle Name	TextField		7	□
8	UD_ADUSER_LNAME	String	80	Last Name	TextField		8	□
9	UD_ADUSER_FULLNAME	String	240	Full Name	TextField		9	□
10	UD_ADUSER_MUST	boolean	1	User must change p	CheckBox		10	□
11	UD_ADUSER_NEVER	boolean	1	Password never ex	CheckBox	1	11	□
12	UD_ADUSER_DATE	Date		Account Expiration D	DateFieldDlg		12	□
13	UD_ADUSER_ORGNAME	String	500	Organization Name	LookupField		13	□
14	UD_ADUSER_LOCKED	boolean	1	Account is Locked c	CheckBox		14	□
15	UD_ADUSER_TELEPHONE	String	20	Telephone Number	TextField		15	□
16	UD_ADUSER_EMAIL	String	80	E Mail	TextField		16	□

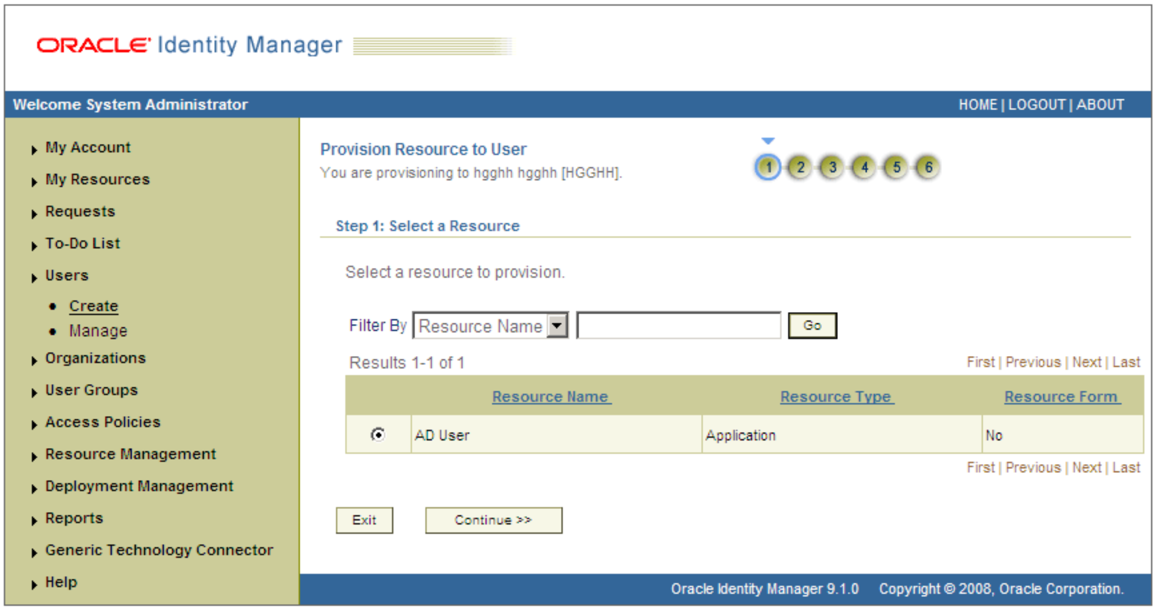
There is a one-to-one relationship between a process form and a provisioning process.

Each connector is shipped with certain default process forms. You can manually create additional/custom process forms.

Attributes defined on a process form are displayed on the Oracle Identity Manager Administrative and User Console page that is used to provision the target system resource to an entity in Oracle Identity Manager. To access this page, you click Manager under Users on the left pane of the Oracle Identity Manager Administrative and User Console, and then navigate through the pages on the right pane until you reach this page.

Figure 2–12 shows the screenshot of the Oracle Identity Manager Administrative and User Console page for provisioning a Microsoft Active Directory resource to an OIM User.

Figure 2–12 Provisioning a Resource to an OIM User



Provision Resource to User

You are provisioning to hgghh hgghh [HGGHH].

Step 1: Select a Resource

Select a resource to provision.

Filter By: Resource Name

Results 1-1 of 1

	Resource Name	Resource Type	Resource Form
●	AD User	Application	No

2.2.13 Provisioning Process, Process Tasks, and Adapters

A provisioning process is a representation of the workflow for provisioning operations. It forms the link between the resource object and process form, and it is composed of process tasks. A process task performs a specific function during a provisioning operation. For example, there can be one process task for each of the following provisioning operations:

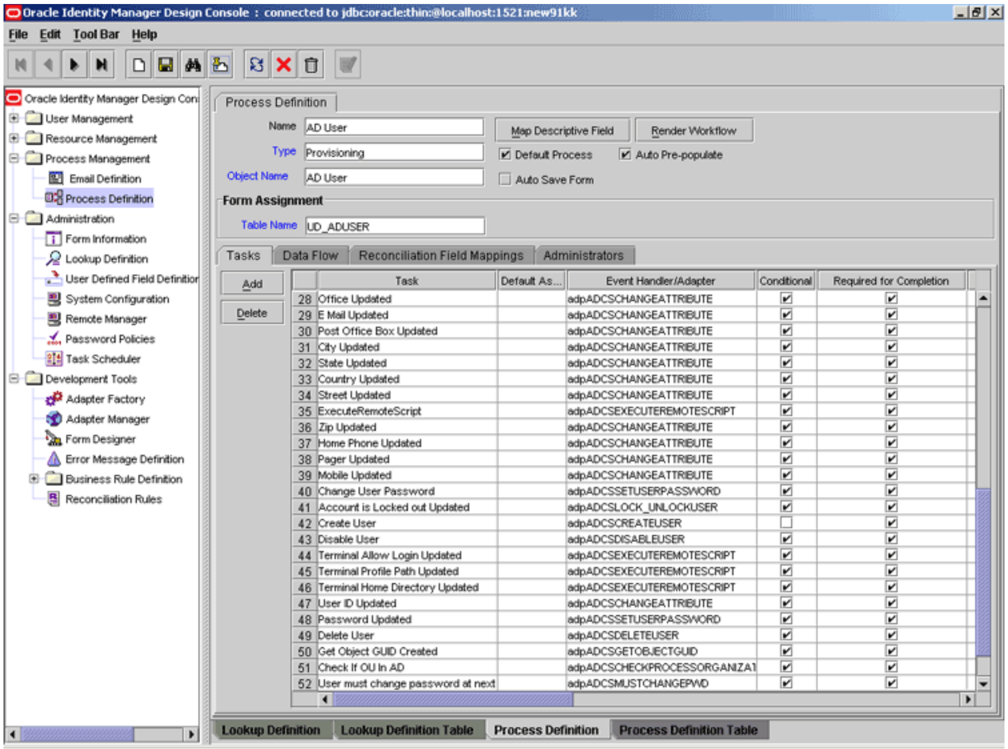
- Create User
- Modify User Attribute
- Delete User

If required, there can be a set of process tasks for a single provisioning operation. For example, the Create User provisioning operation can be performed by a combination of the Create Login for User and Assign Privileges to User process tasks.

An adapter calls the code for performing a specific provisioning operation on the target system. The adapter, in turn, is called by a process task. There is a one-to-one relationship between an adapter and a process task. The code called by the adapter is custom-built for compatibility with the features that the target system provides for performing provisioning operations initiated on other systems. For example, the adapters in an SAP connector interact with the application programming interfaces (APIs) of SAP.

To view the mappings between process tasks and adapters, you click Process Definition under Process Management on the left pane of the Oracle Identity Manager Design Console. The details of the process tasks are displayed on the Tasks tab. Figure 2–13 shows the screenshot of the provisioning process for the Microsoft Active Directory connector. Mappings between process tasks and adapters are shown on the Tasks tab.

Figure 2–13 Provisioning Process



Process Definition

Name: AD User

Type: Provisioning

Object Name: AD User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_ADUSER

	Task	Default As...	Event Handler/Adapter	Conditional	Required for Completion
28	Office Updated		adpADCSCHANGEATTRIBUTE	☑	☑
29	E Mail Updated		adpADCSCHANGEATTRIBUTE	☑	☑
30	Post Office Box Updated		adpADCSCHANGEATTRIBUTE	☑	☑
31	City Updated		adpADCSCHANGEATTRIBUTE	☑	☑
32	State Updated		adpADCSCHANGEATTRIBUTE	☑	☑
33	Country Updated		adpADCSCHANGEATTRIBUTE	☑	☑
34	Street Updated		adpADCSCHANGEATTRIBUTE	☑	☑
35	ExecuteRemoteScript		adpADCSEXECUTEREMOTESCRIPT	☑	☑
36	Zip Updated		adpADCSCHANGEATTRIBUTE	☑	☑
37	Home Phone Updated		adpADCSCHANGEATTRIBUTE	☑	☑
38	Pager Updated		adpADCSCHANGEATTRIBUTE	☑	☑
39	Mobile Updated		adpADCSCHANGEATTRIBUTE	☑	☑
40	Change User Password		adpADCSSETUSERPASSWORD	☑	☑
41	Account is Locked out Updated		adpADCSLOCK_UNLOCKUSER	☑	☑
42	Create User		adpADCSCREATEUSER	□	☑
43	Disable User		adpADCSDISABLEUSER	☑	☑
44	Terminal Allow Login Updated		adpADCSEXECUTEREMOTESCRIPT	☑	☑
45	Terminal Profile Path Updated		adpADCSEXECUTEREMOTESCRIPT	☑	☑
46	Terminal Home Directory Updated		adpADCSEXECUTEREMOTESCRIPT	☑	☑
47	User ID Updated		adpADCSCHANGEATTRIBUTE	☑	☑
48	Password Updated		adpADCSSETUSERPASSWORD	☑	☑
49	Delete User		adpADCSDELETEUSER	☑	☑
50	Get Object GUID Created		adpADCSGETOBJECTGUID	☑	☑
51	Check If OU In AD		adpADCSCHECKPROCESSORGANIZAT	☑	☑
52	User must change password at next		adpADCSMUSTCHANGEPWD	☑	☑

The provisioning process also contains mappings between the reconciliation fields defined in the resource object and the attributes defined on the process form. These mappings are shown in Figure 2–3.

3 Reconciliation and Provisioning Processes

This chapter discusses the processes that are involved during target resource reconciliation and provisioning, and trusted source reconciliation.

If you want to configure target resource reconciliation and provisioning, then see the following sections for the respective processes involved:

- Target Resource Reconciliation
- Provisioning

If you want to configure trusted source reconciliation, then see the following section for the process involved:

- Trusted Source Reconciliation

3.1 Target Resource Reconciliation

The target resource reconciliation process involves the following steps:

1. A change is made on the target system.

   A change on the target system can be the creation, modification, or deletion of an account on the target system. This event is called a reconciliation event.

2. The change on the target system is detected and communicated to Oracle Identity Manager by the reconciliation APIs.

   The manner in which the change is communicated to Oracle Identity Manager depends on whether reconciliation is configured according to the push model or the pull model.

3. A reconciliation event record is created for each target system record that is communicated to Oracle Identity Manager.

4. Events for which matches with existing OIM Users are found are forwarded for further processing.

   Events for which matches cannot be found can be further processed by an administrator. The administrator can manually map these events to their corresponding OIM Users, and these events are then forwarded for further processing.

5. The reconciliation engine checks if there are values in each event for the attributes that are designated as mandatory attributes in Oracle Identity Manager. Events in which there are values for all the mandatory attributes are forwarded for further processing. Events in which there is no value for a mandatory attribute are sent to an administrator. The administrator can manually enter values for these attributes, and these events are then forwarded for further processing.

6. For each event, the process matching rules (defined by the key field for reconciliation matching) are evaluated to find the provisioned resource that matches the event.
7. If a match is found, then the match is added to the list of provisioned resource matches that have been found up to this point.

   If no match is found, then the reconciliation owner matching rule (that is, the reconciliation rule) is evaluated to determine the owner (OIM User) of the event in Oracle Identity Manager. If a match is found, then the match is added to the list of owner matches that have been found up to this point.
8. After rule evaluation, each event is in one of the following states:
   - Match found with a provisioned resource in Oracle Identity Manager.
   - No match found with a provisioned resource in Oracle Identity Manager, but match found with an OIM User .
   - Match found with neither provisioned resource nor OIM owner.

   Depending on the state of each event, reconciliation action rules are applied to it. If the action rule specifies assignment, then the event is assigned to an administrator or administrator group. If the action rule specifies linking, then the event is forwarded for linking.
9. If the event is a Delete event, then:
   a. The provisioning process for the resource instance is canceled.
   b. The status of the resource is set to “Revoked.”
   c. The “Reconciliation Delete Received” task is inserted.

   If the event is not a Delete event and if a match was found with a provisioned resource, then:
   a. The data of the process form of the provisioned resource is updated.
   b. The “Reconciliation Update Received” task is inserted.

   If the event is not a Delete event, and if no match was found with a provisioned resource but an owner match was found, then:
   a. A new instance of the resource is created for the owner.
   b. The process form for the provisioned resource is populated with the data from the event.
   c. The “Reconciliation Insert Received” task is inserted.

3.2 Provisioning

> **Note:** Direct provisioning has been used to illustrate the provisioning process. Some of these steps are actions that an Oracle Identity Manager administrator performs on the Oracle Identity Manager Administrative and User Console. The remaining steps are provisioning-driven and take place automatically.

To provision a resource to an OIM User, you log in to the Oracle Identity Manager Administrative and User Console and follow the procedure to provision a resource.

When you enter values in the page that contains the process form details and click continue, the provisioning process is started.

"Provisioning Resources" on page 4-3 contains the procedure to perform direct provisioning for an OIM User.

The following is the sequence of steps for the direct provisioning process in Microsoft Active Directory:

1. The IT resource for the target system is linked with the resource object that you select for the provisioning operation. When you submit the provisioning data, this data and the parameter values of the IT resource are passed on to the process task. For example, information from the AD Server IT resource and the UD_ADUSER process form is passed on to the Create User process task.
2. The process task passes the information to the adapter with which it is associated. For the example described in the preceding step, the Create User process task passes the information to the adpADCSCREATEUSER adapter.
3. The adapter passes the request to the Microsoft Active Directory API.
4. The target system API creates the user account on the target system and returns a response code to the adapter, which carries the code back to the process task. Depending on the response code it receives, the process task displays the outcome of the provisioning operation on the Oracle Identity Manager Administrative and User Console. The message is also recorded in the application server log file.

3.3 Trusted Source Reconciliation

The trusted source reconciliation process involves the following steps:

1. A change is made on the target system.

   A change on the target system can be the creation, modification, or deletion of an account on the target system. This event is called a reconciliation event.
2. The change on the target system is detected and communicated to Oracle Identity Manager by the reconciliation APIs.

   The manner in which the change is communicated to Oracle Identity Manager depends on whether reconciliation is configured according to the push model or the pull model.
3. A reconciliation event record is created for each target system record that is communicated to Oracle Identity Manager.
4. Events for which matches with existing OIM Users are found are forwarded for further processing.

   Events for which matches cannot be found can be further processed by an administrator. The administrator can manually map these events to their corresponding OIM Users, and these events are then forwarded for further processing.
5. The reconciliation engine checks if there are values in each event for the attributes that are designated as mandatory attributes in Oracle Identity Manager. Events in which there are values for all the mandatory attributes are forwarded for further processing. Events in which there are no values for even one mandatory attribute are sent to an administrator. The administrator can manually enter values for these attributes, and these events are then forwarded for further processing.

6. For each event, the reconciliation rules are evaluated to find the matching OIM User for the event.
7. If a match is found, then the match is added to the list of matches that have been found up to this point.
8. After rule evaluation, each event is in one of the following states:
   - Match found with an OIM User.
   - No match found with a provisioned resource in Oracle Identity Manager, but match found with an OIM User.
   - Match found with neither provisioned resource nor OIM owner.

   Depending on the state of each event, reconciliation action rules are applied to it. If the action rule specifies assignment, then the event is assigned to an administrator or administrator group. If the action rule specifies linking, then the event is forwarded for linking.
9. If the event is a Delete event, then:
   a. The OIM User is deleted.
   b. All related deprovisioning activities are carried out.

      This depends on the target systems and their settings for data integrity. For example, if a user is deleted, then the connector must ensure that the user's group memberships at the target system are deleted as well.
   c. The “Reconciliation Delete Received” task is inserted.

   If the event is not a Delete event and if a match was found with an OIM User, then:
   a. The data of the OIM User is updated.
   b. The “Reconciliation Update Received” task is inserted.

   If the event is not a Delete event if no match was found with an owner entity, then:
   a. A new instance of the entity (OIM User) is created.
   b. The attribute fields for the entity is populated with the data from the event.
   c. All related provisioning activities are carried out.
   d. The “Reconciliation Insert Received” task is inserted.
10. If the task is automated, then the response code of the task is set to “Event Processed” and any related provisioning actions are initiated.

4

Performing Connector Operations

This chapter discusses guidelines on performing connector operations. This chapter contains the following sections:

4.1 Guidelines on Running Reconciliation

The following are guidelines on running reconciliation:

- After you deploy a connector, perform full reconciliation to ensure that all the data on the target system is imported into Oracle Identity Manager. Thereafter, you can run incremental reconciliation, which can be periodic, on-demand or real-time.
- Before you perform user reconciliation, ensure that the lookup definitions are 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 and before provisioning operations.
- Leave the value of the StartRecord scheduled task attribute as `1`. All the connectors contain this scheduled task attribute for reconciliation. This attribute specifies the first record in a batch during reconciliation.

  The time stamp attribute is updated after an event is created for each user record. If the reconciliation fails, then the reconciliation is resumed from the updated time stamp. Therefore, it is recommended that you leave the value of the StartRecord attribute as `1`.

  After you configure reconciliation, if reconciliation fails during a reconciliation run, then you rerun the scheduled task without changing the values of the task attributes.
- The scheduled task for reconciliation of user data must be run before the scheduled task for reconciliation of deleted user data.

4.2 Managing Scheduled Tasks

To make changes to the reconciliations that are performed, you must modify the scheduled tasks accordingly. You can make the following changes to a scheduled task:

- You can change the schedule of the reconciliation runs. For example, you can change a daily schedule to a weekly or a monthly one.
- You can change the criteria for limited reconciliation in a scheduled task. For example, you have scheduled a reconciliation only for users who belong to a particular group. You can change the criteria to include managers of the users who belong to that group.
- At any time, you can disable a scheduled task for a certain period of time. When required, the same scheduled task can be enabled also.
- You can delete a scheduled task.
- You can configure a scheduled task to run full or incremental reconciliation. To do so, use the scheduled task attribute that specifies whether the reconciliation run must be full or incremental.
- You can configure a scheduled task for reconciliation. To do so, you must specify the batch size, the record that is the first in a batch, and the number of batches to be reconciled in the scheduled task.
- You can also stop a reconciliation run by using the Stop Execution option, which is available in the Task Scheduler form of the Oracle Identity Manager Design Console.

For all the actions mentioned in the preceding list, you must modify the reconciliation scheduled task. To refer to the procedure to modify a scheduled task, see the "Managing Scheduled Tasks" section in *Oracle Identity Manager Administrative and User Console Guide*.

4.3 Guidelines on Performing Provisioning Operations

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

- Passwords for user accounts provisioned from Oracle Identity Manager must adhere to the password policy set in the target system.

  On some target systems, password policies may be controlled through password complexity rules. Complexity requirements are enforced when passwords are changed or created. While changing the password of an 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.
- Specifying multibyte values for fields

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

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

  If you come across a situation similar to the preceding example, then you may create a newer version of the form in which the length of the fields are appropriate for language settings selected.

- The character length of target system fields must be taken into account when specifying values for the corresponding Oracle Identity Manager fields

  During a provisioning operation, you must keep the lengths of target system fields in mind while entering values for Oracle Identity Manager process form fields. The character limit specified for some process form fields may be more than that of the corresponding target system field.

4.4 Provisioning Resources

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

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 target system account to the user.
   - Select **Manage** if you want to provision a target system 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**.
4. If you select Manage, then search for the OIM User and select the link for the user from 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.
6. On the Resource Profile page, click **Provision New Resource**.
7. On the Step 1: Select a Resource page, select the resource object from the list and then click **Continue**.
8. On the Step 2: Verify Resource Selection page, click **Continue**.
9. On the Step 5: Provide Process Data page, enter the details of the account that you want to create on the target system and then click **Continue**.
10. On the Step 6: Verify Process Data page, verify that you entered and then click **Continue**.

    The account is created on the target system and provisioned as a resource to the OIM User. The page that is displayed provides options to disable or revoke the resource from the OIM User.

Index