Oracle® Identity Manager

Connector Framework Guide

Release 9.0.4

E10449-01

July 2007

ORACLE®

Oracle Identity Manager Connector Framework Guide, Release 9.0.4

E10449-01

Primary Author: Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Framework Guide provides information about integrating Oracle Identity Manager with various third-party applications.

Note: Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for any supported third-party application.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

1

Introduction to Oracle Identity Manager

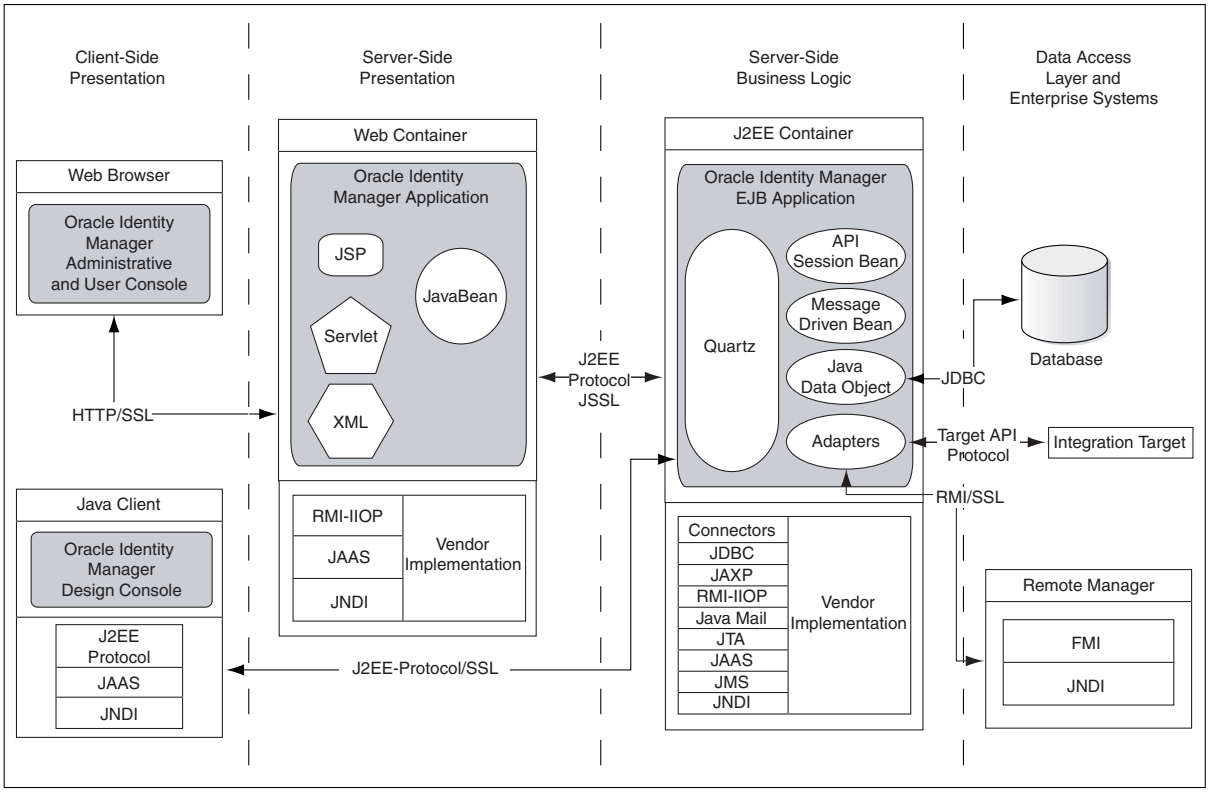
Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. This chapter provides an overview of Oracle Identity Manager.

This chapter is divided into the following sections:

Architecture of Oracle Identity Manager

Oracle Identity Manager is based on the n-tier J2EE application architecture. Figure 1–1 illustrates the architecture of Oracle Identity Manager.

Figure 1–1 Architecture of Oracle Identity Manager



This section discusses the following tiers of the Oracle Identity Manager architecture:

- Presentation Layer
- Dynamic Presentation Logic Layer
- Business Logic Layer
- Data Access Layer
- Backend System Integration Layer

Presentation Layer

The Presentation layer consists of two clients: the Oracle Identity Manager Administrative and User Console and the Oracle Identity Manager Design Console. The Administrative and User Console is a Web-based thin client that can be accessed from any Web browser. This console provides user self-service and delegated administration features that serve most of the provisioning requirements.

The Design Console provides the full range of the Oracle Identity Manager system configuration and development capabilities including Form Designer, Workflow Designer, and the Adapter Factory. You can access the Design Console by using a desktop Java client.

Dynamic Presentation Logic Layer

Because both the Administrative and User Console and the Design Console are highly dynamic, the Dynamic Presentation Logic layer guides the content displayed on these interfaces. In the case of the Administrative and User Console, there is a clear

separation between the Presentation and Presentation Logic Layer. No such boundary exists in the Design Console.

Business Logic Layer

The Business Logic layer is implemented as an EJB application. Oracle Identity Manager runs on leading J2EE-compliant application server platforms, leveraging the J2EE services provided by these application servers to deliver a high-performance, fault-tolerant enterprise application.

The following are components of the Business Logic layer:

- Application Server
- Client Interfaces and Business Logic Implementation

Application Server

The application server on which Oracle Identity Manager runs provides life-cycle management, security, deployment, and run-time services to the logical components that make up Oracle Identity Manager. These services include:

- Scalable management of resources (clustering and failover)
- Transaction management
- Security management
- Client access
- Technology resources (such as database connection pooling and messaging)

Client Interfaces and Business Logic Implementation

The core functionality of the Oracle Identity Manager platform is implemented in Java using a highly modular, object-oriented methodology. This includes the various engines that comprise the Oracle Identity Manager platform: Workflow Engine, Request Engine, User Management Engine, Rule Engine, and Reconciliation Engine. It also includes the integration layer based on the Adapter Factory, which dynamically generates integration code based on the metadata definition of the adapters.

Access to the functionality of the platform is through a set of EJB Beans. These session beans can be divided into two types:

- **Nonpublished APIs:** These are session beans that expose functionality used only by the Design Console.
- **Published Public APIs:** These are session beans that expose the public functionality of Oracle Identity Manager.

The API layer provides access to high-level functionality in Oracle Identity Manager. It is the basis for the functionality implemented in the Oracle Identity Manager Administrative and User Console. It is also the interface that custom clients can use to access Oracle Identity Manager functionality.

Data Access Layer

J2EE contains several technologies for manipulating and interacting with transactional resources (such as databases) that are based on JDBC, JTA, and JTS. The Oracle Identity Manager architecture leverages the following J2EE services:

- Database connection pooling

- Integration with JNDI (lookup of DataSources in the JNDI namespace)
- XA compliance
- Batch updates

The system administrator can manage data sources in the same manner in which all standard J2EE applications in the enterprise are managed. Oracle Identity Manager can use these data sources to communicate with the database tier.

Backend System Integration Layer

The Backend System Integration layer can be divided into the following:

- Database
- Remote Manager

Database

The Database tier consists of the Oracle Identity Manager repository, which manages and stores Oracle Identity Manager metadata in an ANSI SQL 92-compliant relational database. All the data resides in the Oracle Identity Manager repository.

Remote Manager

The remote manager is an Oracle Identity Manager server component that runs on a target system computer. It provides the network and security layer required to integrate with applications that do not have network-aware APIs or do not provide security. It is built as a lightweight RMI server. The communication protocol is RMI tunneled over HTTP/S.

The J2EE RMI framework enables the creation of virtually transparent, distributed services and applications. RMI-based applications consist of Java objects making method calls to one another, regardless of their location. This enables one Java object to call methods on another Java object residing on another virtual computer in the same manner in which methods are called on a Java object residing on the same virtual computer.

Deployment Configurations of Oracle Identity Manager

This section discusses the following deployment configurations of Oracle Identity Manager:

- Provisioning
- Reconciliation
- Provisioning and Reconciliation

Provisioning

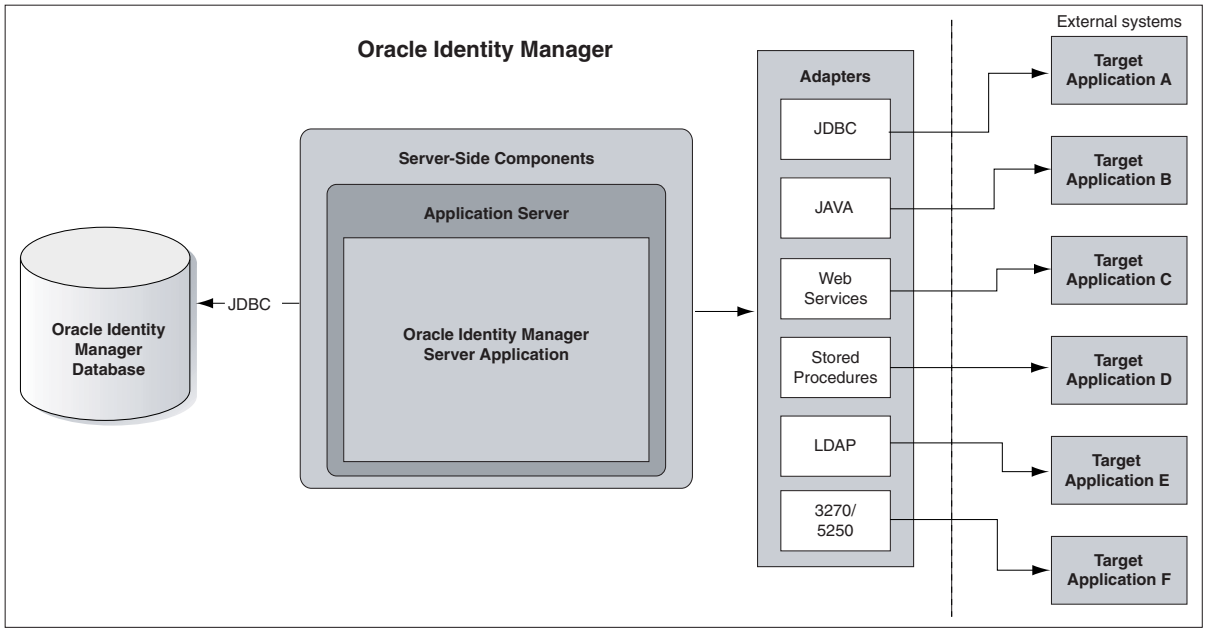
You can use Oracle Identity Manager to create, maintain, and delete accounts on target systems. Oracle Identity Manager becomes the front-end entry point for managing all the accounts on these systems. After the accounts are provisioned, the users for whom accounts have been provisioned are able to access the target systems without any interaction with Oracle Identity Manager. This is the **provisioning** configuration of Oracle Identity Manager.

The purpose of provisioning is to automate the creation and maintenance of user accounts on target systems. Provisioning is also used to accommodate any

requirement for workflow approvals and auditing that may be a component of that provisioning lifecycle.

Figure 1–2 illustrates the provisioning configuration.

Figure 1–2 Provisioning Configuration of Oracle Identity Manager



Provisioning events are initiated either through requests or by direct provisioning.

A request can be manually created by an administrator or, in certain cases, by target users themselves. Oracle Identity Manager automatically creates requests for some events. For example, a request is automatically created when Oracle Identity Manager enforces the requirements of an access policy. You can also use Oracle Identity Manager to create approval processes that can be run as part of the request-based provisioning cycle.

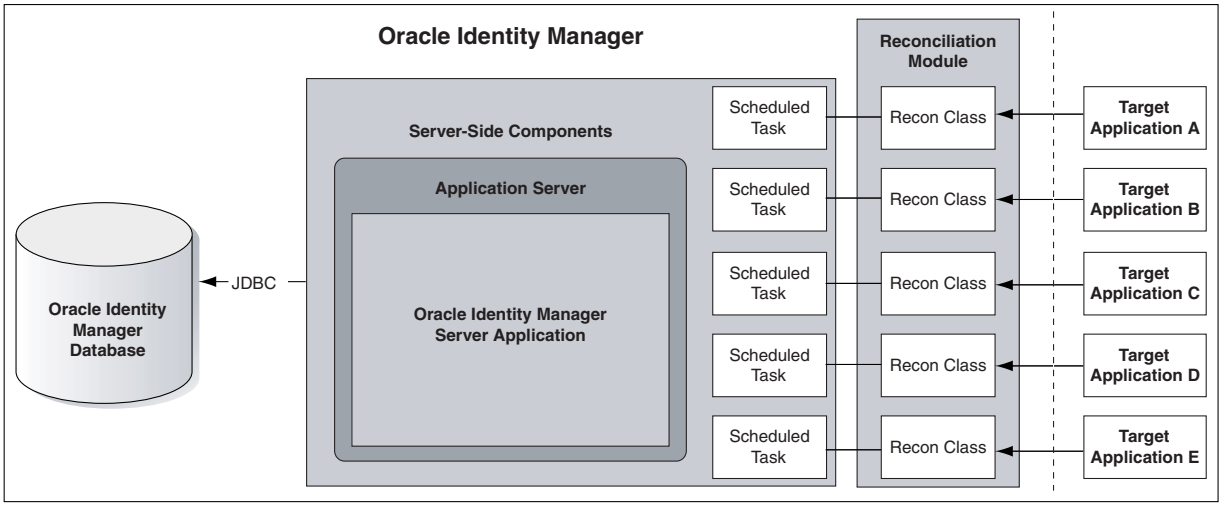
Direct provisioning is a special administrator-only function. It lets you create an account for a particular user on a target application without having to wait for any workflow or approval processes.

Reconciliation

Oracle Identity Manager provides a centralized control mechanism to manage user accounts 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 system applications to maintain an up-to-date profile of all accounts that exist on those systems. This is the **reconciliation** configuration of Oracle Identity Manager.

Figure 1–3 illustrates the reconciliation configuration.

Figure 1–3 Reconciliation Configuration of Oracle Identity Manager



In this configuration, Oracle Identity Manager is used only as an archive for all account management actions that are performed on the target system. It is assumed that user accounts are created, deleted, and maintained by the local resource-specific administrators.

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

User discovery is the process of recognizing the existence of a user account on a primary database. The primary database is the repository that is considered to contain the master list of user accounts. Within the context of user discovery and reconciliation, the primary database is also referred to as the **trusted source** or **authoritative source.** There may be more than one trusted source for each Oracle Identity Manager environment.

Account discovery is the process of recognizing changes to user-related information on resources. If the information that is changed affects the user's primary record, it is generally a change associated with a trusted source. If the information that is changed is related to a user's access to a resource, it is generally a change associated with a target resource.

The following are different forms of reconciliation:

- One-Time Reconciliation
- Target Resource Reconciliation
- Trusted Source Reconciliation

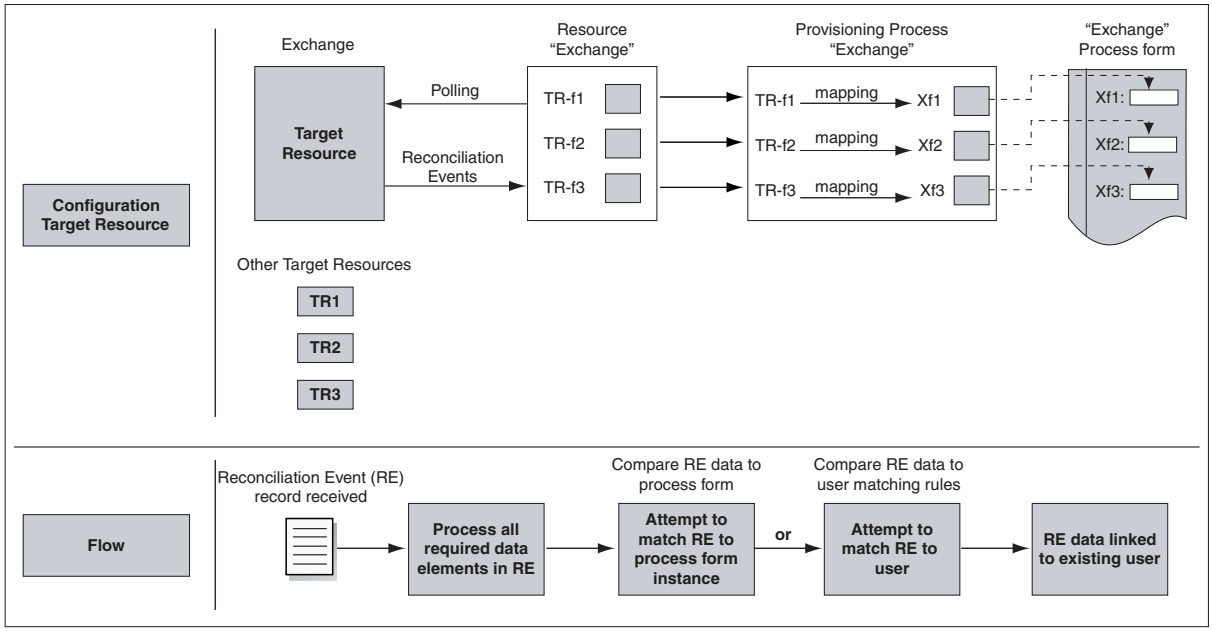
One-Time Reconciliation

You can use Oracle Identity Manager to perform a single, one-time reconciliation with a legacy target system. The purpose of this form of reconciliation is to import all accounts on that system into Oracle Identity Manager. After one-time reconciliation is performed, you can use Oracle Identity Manager to provision accounts for your users.

Target Resource Reconciliation

Figure 1–4 illustrates the steps involved in target resource reconciliation.

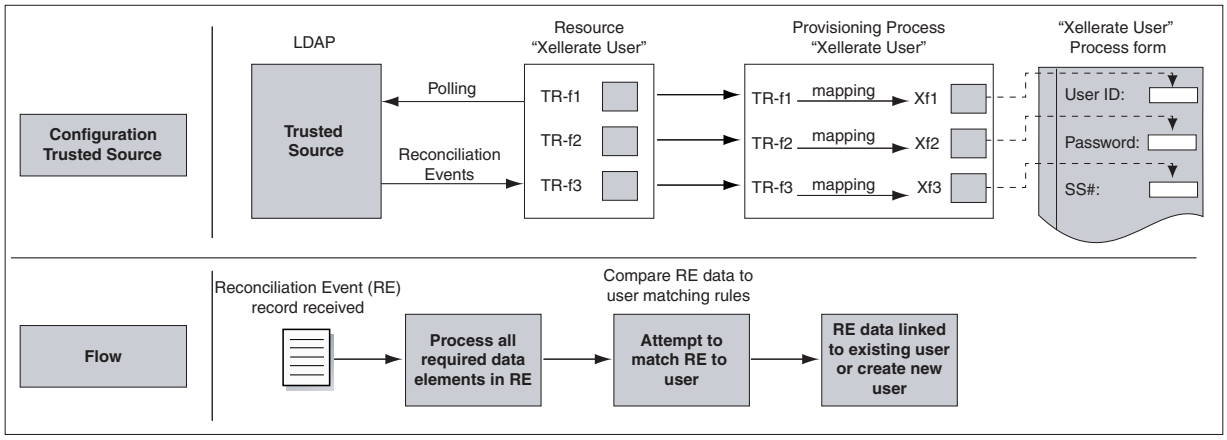
Figure 1–4 Target Resource Reconciliation



Trusted Source Reconciliation

Figure 1–5 illustrates the steps involved in trusted source reconciliation.

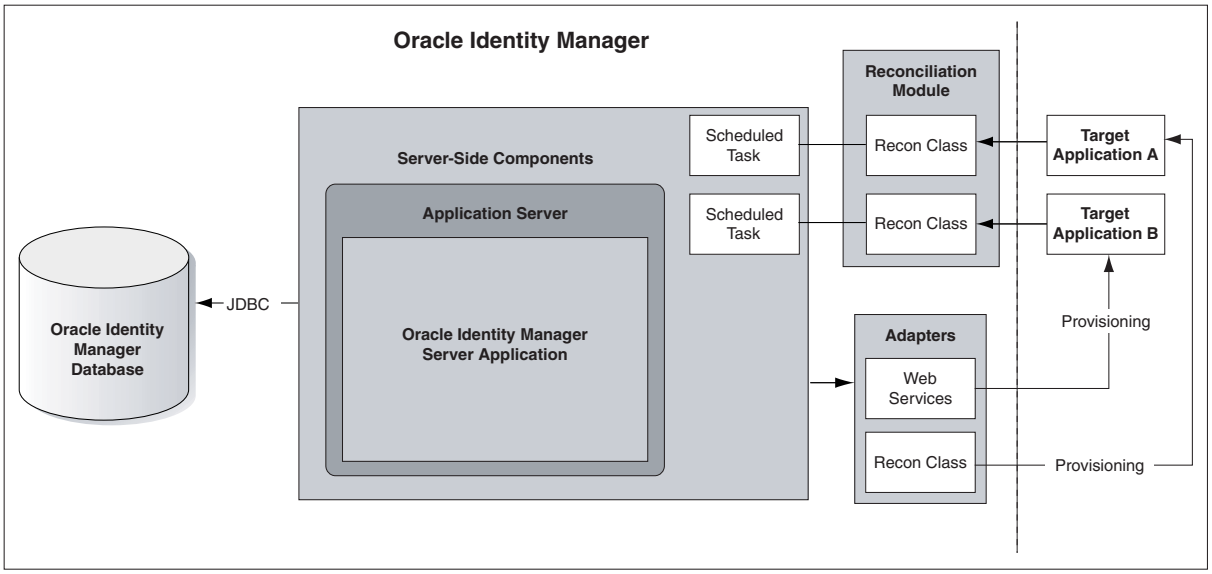
Figure 1–5 Trusted Source Reconciliation



Provisioning and Reconciliation

Figure 1–6 illustrates the **provisioning and reconciliation** configuration in which you use Oracle Identity Manager to perform both provisioning and reconciliation tasks. In this configuration, it is assumed that you allow accounts on target systems to be created and maintained by both local administrators and Oracle Identity Manager.

Figure 1–6 Provisioning and Reconciliation Configuration of Oracle Identity Manager



To achieve this configuration, you must perform all the steps associated with setting up both provisioning and reconciliation.

Features of Oracle Identity Manager

The following are the features of Oracle Identity Manager:

- **Scalable architecture**

  Oracle Identity Manager is based on open, standards-based technology. The J2EE application server model of Oracle Identity Manager offers scalability, failover, load-balancing, and built-in Web deployment features.

- **Comprehensive user management**

  Oracle Identity Manager can support unlimited user organizational hierarchies and user groups with inheritance, customizable user ID policy management, password policy management, and user access policies. It also offers the feature of delegated administration with comprehensive permission settings. You can use Oracle Identity Manager to maintain resource allocation history and to manage application parameters and entitlements.

- **Web-based user self-service**

  Oracle Identity Manager contains a user self-service portal that is customizable and Web based. This portal can be used to manage user information, change and synchronize passwords, reset passwords, request access to applications, review and edit entitlements, and work on workflow tasks.

- **Flexible process engine**

  Using Oracle Identity Manager, you can create business and provisioning process models in applications such as Microsoft Project and Microsoft Visio. Process models include support for approval workflows and escalations. You can track the progress of each provisioning event in the workflow.

  Oracle Identity Manager provides support for complex branching, self-healing processes, and nested processes with data interchange and dependencies. The process flow can be customized without making code changes.

- **Comprehensive reporting for audit-trail accounting**

  Oracle Identity Manager provides status reports on all processes with full-state information, in real time. In addition, it even offers OLAP features.

- **Automated tool for connector management**

  Oracle Identity Manager provides an automated tool for connector generation. This tool, which is known as the **Adapter Factory,** supports a wide range of interfaces, applications, and devices. The adapters generated by the Adapter Factory run on the Oracle Identity Manager server, and they do not require any agents to be installed or updated on the target systems. The use of the Adapter Factory helps speed up the process of connector development and simplifies the task of updating existing connectors.

  If the target system does not have a network-enabled interface, then you can use the Oracle Identity Manager remote manager to provide an SSL-secured network communication channel and interface to local APIs that are not running on the Oracle Identity Manager server. By using the remote manager, you can run functions on target systems having APIs that are not network aware.

- **Built-in change management**

  Oracle Identity Manager enables you to package new processes, import and export existing processes, and move packages from one system to another.

2

What Is an Oracle Identity Manager Connector?

An Oracle Identity Manager connector is used to integrate Oracle Identity Manager with a specific third-party application, such as Microsoft Exchange or Novell eDirectory. Oracle Identity Manager is packaged with a number of predefined connectors.

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

Components Common to All Connectors

In general, an XML file for a connector contains definitions of the connector components listed in the following table.

Component	Description
Resource Object	This is a virtual representation of the target application on which you want to provision accounts. It is the parent record with which the provisioning process and process form are associated.
Provisioning Process	This process definition is used to create, maintain, and delete accounts on the target system. It consists of definitions of the individual tasks that are used to perform automated functions on the target system. Each connector is packaged with a single provisioning process. You can manually create additional provisioning processes.
Process Form	This form is used to provide information about user accounts to be created, updated, or deleted on the target system. This form is also used to capture data that can be used by provisioning process tasks or to provide a mechanism for users to provide real-time data. This form is also extensively used when conducting reconciliation. The table structure associated with this form supports the archiving and auditing of user accounts on the target system. Each process form consists of field definitions required by a standard connector. If you require additional fields, then you can create another version of the form and add the required fields. Each connector is shipped with certain default process forms. You can manually create additional process forms.

Component	Description
IT Resource Type	This component is a template for all IT resource definitions associated with the connector. An IT resource type specifies the parameters that are common to all IT resource instances, such as host servers and computers, of that particular IT resource type. The parameters specified in this definition are inherited by all IT resource definitions of that type. For example, the `Solaris 8` IT resource type may have a parameter called `IP Address`. The value of that parameter for the `Target_Solaris` IT resource instance may be set to `192.168.50.25`.
Adapters	This includes all adapters that are required to perform common functions on the target application. Each adapter is predefined with certain mappings and functionality. These adapters are capable of interacting with the tasks in the provisioning process and the fields of the process form.
Scheduled Task (where applicable)	If the connector that you want to use is shipped with a predefined reconciliation module, then you are provided with a scheduled task definition. You use this component to control the frequency at which the target system is polled for changes to tracked data.

Provisioning Process Tasks

The Provisioning Process component contains the predefined tasks (or their equivalents) listed in the following table.

Provisioning Process Task	Purpose
Create User	Creates a new user account in the target application (provisions the user with an account)
Disable User	Temporarily disables a user account in the target application
Enable User	Reenables a disabled user account in the target application
Delete User	Deletes a user account in the target application (revoke the user's account)
Update User	Modifies the privileges or profile of a user account in the target application

Some of these tasks are also preconfigured with the process task adapter that automates their function on the target system. Before you complete the deployment of a connector, you must examine the default functionality and variable mappings of these adapters to ensure that they interact with your target system as required.

Reconciliation-Related Provisioning Process Tasks

In addition to the tasks listed in the earlier section, the Provisioning Process component also contains the reconciliation-related tasks listed in the following table.

Note: When Oracle Identity Manager receives a reconciliation event, all provisioning-related tasks within the provisioning process are suppressed and the relevant reconciliation-related task is inserted.

Provisioning Process Task (Reconciliation-Related)	Purpose
Reconciliation Insert Received	This task is inserted into the Provisioning Process instance associated with the user when Oracle Identity Manager determines that the reconciliation event received from the target system represents the creation of a user account. In addition, the information in the reconciliation event record is stored in the process form according to the mappings set on the provisioning process.
Reconciliation Update Received	This task is inserted into the Provisioning Process instance associated with the user when Oracle Identity Manager determines that the reconciliation event received from the target system represents the update of an existing user account. In addition, the information in the reconciliation event record is stored in the process form according to the mappings set on the provisioning process.
Reconciliation Delete Received	This task is inserted into the Provisioning Process instance associated with the user when Oracle Identity Manager determines that the reconciliation event received from the target system represents the deletion of an existing user account.

3

Deploying Connectors

This chapter provides generic information about the procedure to deploy a connector. For detailed information about the procedure to deploy a target-specific connector, refer to the deployment guide for that connector. The "Related Documents" section of the preface contains a list of all the deployment guides.

> **Note:** It is recommended that you customize and test connectors before you move them to your production environment.

This chapter discusses the following sections:

- Overview of Connector Deployment
- General Considerations

Overview of Connector Deployment

The following are the high-level steps involved in deploying a connector:

1. Import the relevant XML file into the Oracle Identity Manager environment. There may be more than one XML file associated with the connector for your target application.

   When you import the connector XML file, create at least one IT resource definition. This definition is used by Oracle Identity Manager to connect to the actual computer on which the target application is hosted. This definition is required for the provisioning process and the associated adapters to run successfully.

2. Determine whether you want to deploy Oracle Identity Manager as a provisioning, reconciliation, or provisioning and reconciliation solution. The procedure that you must follow depends on the type of solution you select.

   > **See Also:** "Deployment Configurations of Oracle Identity Manager" on page 1-4 for information about the various configurations in which Oracle Identity Manager can be deployed

3. Compile the adapters that are predefined with the connector XML file.

General Considerations

The following are general considerations that you must address:

- Some connectors require external libraries in the form of JAR files for normal functioning. You may need to purchase these JAR files from the respective vendors.

  After you obtain these JAR files, you must configure Oracle Identity Manager as required. For example, you may need to update the CLASSPATH environment variable.

- Some connectors require external software to be installed on the target system. For example, if you are using the Bourne (`sh`) shell on Solaris, then you must install and start WBEM Services on the target Solaris computer. Otherwise, you cannot use Oracle Identity Manager to provision users on Solaris.

- To make most prepackaged connectors function as required, you must configure the target systems separately. Where required, this step is explained in the connector deployment guides.

- While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, all the JAR files that you copy to the Oracle Identity Manager server during the connector deployment process must be copied to the corresponding directories on each node of the cluster. You must also copy the adapters, which you recompile while deploying the connector, to the corresponding directory on each node.

Index