Oracle® Identity Manager

Concepts

Release 9.1.0.1

E14065-01

February 2009

Oracle Identity Manager Concepts, Release 9.1.0.1

E14065-01

Primary Author: Debapriya Datta

Contributing Author: Lyju Vadassery

Contents

5 Oracle Identity Manager Deployment Configurations

6 Oracle Identity Manager Interfaces

7 Oracle Identity Manager Integration Solutions

8 Context Manager

9 Oracle Identity Manager Globalization

Index

Preface

This guide provides conceptual information about the functionality, architecture, deployment configuration, and user interfaces of Oracle Identity Manager. This guide also discusses connector concepts and explains how connectors function with Oracle Identity Manager.

Audience

This guide is intended for administrators and users who want to learn about the functional aspects of Oracle Identity Manager.

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.

TTY Access to Oracle Support Services

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at `http://www.consumer.att.com/relay/tty/standard2.html`. After the AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support

Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

Related Documents

For more information, see the other documents in the Oracle Identity Manager documentation set for this release.

Documentation Updates

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

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

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), and names of files, directories, attributes, and parameters.

1 Introduction to Identity Management

Oracle Identity and Access Management is a product set that enables organizations to manage the end-to-end life cycle of user identities and to secure access to enterprise resources and assets. Oracle has developed products with identity and access management features that provide directory synchronization, secure directory administration, and a Web single sign-on service. Oracle enhanced the product set further through strategic acquisitions and investments in areas such as identity federation, Web access management, delegated identity administration, user identity provisioning, and virtual directory management.

> **See Also:** *Oracle Identity and Access Management Introduction Guide* for more information about the Identity and Access Management product set

This chapter describes the various products available in the Oracle Identity and Access Management product set and where Oracle Identity Manager is located in the product set.

1.1 Oracle Identity and Access Management Products

The Oracle Identity and Access Management product set consists of products that can be divided into the following categories:

- Identity Management
- Directory Services
- Access Management

1.1.1 Identity Management

Identity management enables enterprises to manage the entire life cycle of user identities across all enterprise resources both within and beyond a firewall. An enterprise identity management solution can provide a mechanism for implementing the user management aspects of a corporate policy. It can also be a means to audit users and their access privileges. The identity management category consists of the following products:

- Oracle Identity Manager: Automates user identity provisioning and deprovisioning and enables organizations to manage the entire life cycle of user identities across all resources in the organization.
- Oracle Delegated Administration Services: Provides trusted proxy-based administration of directory information to users and application administrators.

The subsequent chapters of this guide will focus on Oracle Identity Manager and its various aspects.

1.1.2 Directory Services

Directory services, which are based on the Lightweight Directory Access Protocol (LDAP), are central to an identity and access management strategy. Oracle provides a scalable directory and integration technology that meets the requirements of general enterprise deployment, and is also leveraged by other Oracle products in the product set. The directory services category consists of the following products and product components:

- Oracle Internet Directory: A scalable, robust, LDAP v3-compliant directory service that leverages the scalability, availability, and the security features of Oracle database.
- Oracle Virtual Directory: Single and dynamic access point to existing user identity information. This directory service uses the LDAP or the XML protocols.
- Oracle Directory Integration Platform: A component of Oracle Internet Directory designed to perform directory synchronization and application integration across various directories and compatible Oracle products.

1.1.3 Access Management

Access management is a means to control user access to enterprise resources. Access management products provide centralized and efficient user management for heterogeneous application environments as well as out-of-the-box integration with Oracle products such as Oracle Portal, Oracle Collaboration Suite, and Oracle E-Business Suite. The access management category consists of the following products:

- Oracle Access Manager: Provides Web-based identity administration and access control to Web applications and resources running in heterogeneous environments.
- Oracle Identity Federation: Enables organizations to securely link their business partners into a corporate portal or extranet to increase their compliance with privacy and security regulations.
- Oracle Application Server Single Sign-On: Provides single sign-on access to Oracle and third-party Web applications.
- Oracle Enterprise Single Sign-On Suite: Provides single sign-on for all applications and resources in an enterprise, without modification to the applications.

2 Documentation Roadmap

Table 2–1 lists all the documentation for performing different functions in Oracle Identity Manager.

Table 2–1 Documentation Available for Oracle Identity Manager

Task	Documentation
Installing Oracle Identity Manager	*Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server* *Oracle Identity Manager Installation and Configuration Guide for BEA WebLogic Server* *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server* *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*
Administering Oracle Identity Manager	*Oracle Identity Manager Administrative and User Console Guide* *Oracle Identity Manager Design Console Guide* *Oracle Identity Manager Administrative and User Console Customization Guide* *Oracle Identity Manager Tools Reference* *Oracle Identity Manager Audit Report Developer's Guide* *Oracle Identity Manager Best Practices Guide*
Developing applications for Oracle Identity Manager	*Oracle Identity Manager Audit Report Developer's Guide* *Oracle Identity Manager API Usage Guide* *Oracle Identity Manager Tools Reference* *Oracle Identity Manager Design Console Guide*
Deploying Oracle Identity Manager in various languages	*Oracle Identity Manager Globalization Guide*
Creating Crystal Report versions of Oracle Identity Manager reports	*Oracle Identity Manager Integration Guide for Crystal Reports*
Creating and managing generic technology connectors	*Oracle Identity Manager Administrative and User Console Guide*

In addition to the guides listed in Table 2-1, you can refer to the guides for predefined Oracle Identity Manager connectors, for example, *Oracle Identity Manager Connector*

Guide for Microsoft Active Directory and *Oracle Identity Manager Connector Guide for Oracle Internet Directory*.

You can also refer to *Oracle Identity Manager Reference* for an overview of the features offered by the Design Console and the Administrative and User Console, and a glossary of terms specific to the Oracle Identity Manager context.

3

Overview of Oracle Identity Manager

Oracle Identity Manager is an identity management product that automates user provisioning, identity administration, and password management, integrated in a comprehensive workflow engine.

Automating user identity provisioning can reduce Information Technology (IT) administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Key features of Oracle Identity Manager include password management, workflow and policy management, identity reconciliation, reporting and auditing, and extensibility through adapters.

> **See Also:** The "Client Interfaces and Business Logic Implementation" section on page 4-5 for the definition of adapters

3.1 Features of Oracle Identity Manager

The features of Oracle Identity Manager can be divided into the following categories:

- Self-Service and Delegated Administration
- Workflow and Policy
- Password Management
- Audit and Compliance Management
- Integration Solutions

3.1.1 Self-Service and Delegated Administration

By deploying self-service features and delegating administrative functions, an organization can increase user productivity, user satisfaction, and operational efficiency.

Profile Management

Users can view and edit their own profiles by using the self-service interface of Oracle Identity Manager. This reduces administrative overhead and provides users with control over their identity profiles.

Request Management

The self-service interface also enables users to create provisioning requests for resources with fine-grained entitlements. Business approvers, such as team leaders, line managers, and department heads, can use the same Web-based interface to examine and approve incoming requests. This helps organizations in reducing effort and cost.

User Configurable Proxy

Oracle Identity Manager features a highly flexible security framework that supports delegation of most administrative functions to any group or user. By moving administration points as close to the user as possible, an organization can achieve tighter control and better security, increasing productivity at the same time.

3.1.2 Workflow and Policy

The use of workflow and policy to automate business and IT processes can lead to improved operational efficiency, enhanced security, and more cost-effective compliance tracking. Oracle Identity Manager provides the following features in this category:

- Policy Management
- Workflow Management
- Dynamic Error Handling
- Guaranteed Deprovisioning
- Transaction Integrity
- Real-Time Request Tracking

Policy Management

Oracle Identity Manager enables policy-based automated provisioning of resources with fine-grained entitlements. For any set of users, administrators can specify access levels for each resource to be provisioned, granting each user only the exact level of access required to complete the job.

These policies can be driven by user roles or attributes, enabling implementation of role-based access control as well as attribute-based access control. Effective blending of role-based and attribute-based policies is key to a scalable and manageable organization provisioning solution. In addition to an automated provisioning policy, Oracle Identity Manager also supports a denial policy. A *denial policy* is used to explicitly deny user access to specific resources, thereby enforcing security or governance policies such as segregation of duties.

Workflow Management

Oracle Identity Manager supports the separation of approval and provisioning workflows. An *approval workflow* enables an organization to model its preferred approval processes for managing resource access requests. A *provisioning workflow* enables an organization to automate IT tasks for provisioning resources with the most complex of provisioning procedures.

The separation of these two workflows empowers business and IT process owners to manage work efficiently with minimum cross-process interferences. It also enables an organization to leverage existing workflows already deployed in systems such as a help desk and HRMS. Oracle Identity Manager provides the Workflow Visualizer that allows business users, administrators, and auditors to visualize and edit task sequences and dependencies to understand process flow and the Workflow Designer to edit and manage the process flow.

Dynamic Error Handling

The error-handling capability of Oracle Identity Manager enables you to handle exceptions that occur during provisioning. Frequent problems, for example, absence of resources, do not stop the entire provisioning transaction or cause it to fail. Business logic defined within the provisioning workflow offers customized fail-safe capabilities within an Oracle Identity Manager implementation.

Guaranteed Deprovisioning

When the access for a user is no longer required or valid in an organization, Oracle Identity Manager revokes access on demand or automatically, as dictated by role or attribute-based access policies. This ensures that a user's access is promptly terminated where is it no longer required. This is done to minimize security risks and prevent paying for access to costly resources, such as data services.

Transaction Integrity

Based on embedded state management capabilities, Oracle Identity Manager provides the high level of transaction integrity required by other mission-critical organization systems. Oracle Identity Manager features a state engine with rollback and recovery capabilities. When a provisioning transaction fails or is stopped, the system is able to recover and roll back to the last successful state or reroute to a different path, in accordance with predefined rules.

Real-Time Request Tracking

To maintain better control and provide improved visibility into all provisioning processes, Oracle Identity Manager enables users and administrators to track request status in real time, at any point during a provisioning transaction.

3.1.3 Password Management

Password management is one of the foremost issues in organizations nowadays. Implementing a password management solution reduces cost and overhead related to raising tickets or calling help desks. The password management features of Oracle Identity Manager discussed in this section aim to help organizations in this area.

Self-Service Password Management

Users can manage their own passwords across managed resources by using the self-service capabilities of Oracle Identity Manager. In case a user forgets the password, Oracle Identity Manager can present customizable challenge questions to enable self-service identity verification and password retrieval. Research shows that the bulk of help desk calls are related to password reset and lockout. By reducing the need for help desk calls, this self-service capability lowers costs.

Advanced Password Policy Management

Most best practices are supported out of the box and are configurable through an intuitive user interface. Supported password complexity requirements include: password length, alphanumeric and special characters usage, uppercase and lowercase usage, full or partial exclusion of user name, minimum password age, and historical passwords. Oracle Identity Manager lets you define complex password policies that surpass the Microsoft Active Directory complex password requirements. In addition, Oracle Identity Manager allows the application of multiple policies for each resource. For instance, users with fewer privileges can be subjected to a more relaxed password policy, whereas privileged administrators can be subjected to a more stringent policy.

Password Synchronization

Oracle Identity Manager can synchronize or map passwords across managed resources and enforce differences in password policies among these resources. In addition, if an organization is using the desktop-based password reset feature of Microsoft Windows, the Active Directory (AD) connector of Oracle Identity Manager can intercept password changes at the AD server and subsequently propagate these changes to other managed resources in accordance with policies. Similar bidirectional password synchronization capability is offered in most Oracle Identity Manager connectors for directory servers and mainframes.

3.1.4 Audit and Compliance Management

Identity management forms a key component in any audit compliance solution of an organization. Oracle Identity Manager helps an organization to minimize risk and reduces the cost of meeting internal and external governance and security audits. This section discusses the features of Oracle Identity Manager that are listed in the audit and compliance management category.

Identity Reconciliation

Reconciliation is one of the significant capabilities of Oracle Identity Manager. The process of reconciliation is performed by the reconciliation engine. If Oracle Identity Manager detects any accounts or changes to user access privileges are affected beyond its control, then the reconciliation engine can immediately take corrective action, such as undo the change or notify you. Oracle Identity Manager also helps you to detect and map existing accounts in target resources. This helps in the creation of an organization-wide identity and access profile for each employee, partner, or customer user.

Rogue and Orphan Account Management

A *rogue account* is an account created "out of process" or beyond the control of the provisioning system. An *orphan account* is an operational account without a valid user. These accounts represent serious security risks to an organization. Oracle Identity Manager can monitor rogue and orphan accounts continuously. By combining denial access policies, workflows, and reconciliation, an organization can perform the required corrective actions when such accounts are discovered, in accordance with security and governance policies.

Oracle Identity Manager can also manage the life cycle of special *service accounts*, also known as administrator accounts. These accounts have special life cycle requirements that extend beyond the life cycle of an assigned user and across the life cycles of multiple assigned users. Proper management of service accounts can help to eliminate another source of potential orphan accounts.

Comprehensive Reporting and Auditing

Oracle Identity Manager reports on both the history and the current state of the provisioning environment. Some of the identity data captured by Oracle Identity Manager includes user identity profile history, user group membership history, user resource access, and fine-grained entitlement history. Oracle Identity Manager also captures data generated by its workflow, policy, and reconciliation engines. By combining this data along with identity data, an organization has all the required data to address any identity and access-related audit inquiry.

Attestation

Attestation, also referred to as recertification, is a key part of Sarbanes-Oxley compliance and a highly recommended security best practice. Organizations meet these attestation requirements mostly through manual processes based on spreadsheet reports and e-mails. These manual processes tend to be fragmented, are difficult and expensive to manage, and have little data integrity and auditability.

Oracle Identity Manager offers an attestation feature that can be deployed quickly to enable an organization-wide attestation process that provides automated report generation, delivery, and notification. Attestation reviewers can review fine-grained access reports within an interactive user interface that supports fine-grained *certify*, *reject*, *decline*, and *delegate* actions. All report data and reviewer actions are captured for future auditing needs. Reviewer actions can optionally trigger corrective action by configuring the workflow engine of Oracle Identity Manager.

3.1.5 Integration Solutions

A scalable and flexible integration architecture is critical for the successful deployment of organization provisioning solutions. Oracle Identity Manager offers a proven integration architecture and predefined connectors for fast and low-cost deployments.

Adapter Factory

Integrating most provisioning systems with managed resources is not easy. Connecting to proprietary systems might be difficult. The Adapter Factory eliminates the complexity associated with creating and maintaining these connections. The Adapter Factory provided by Oracle Identity Manager is a code-generation tool that enables you to create Java classes.

The Adapter Factory provides rapid integration with commercial or custom systems. Users can create or modify integrations by using the graphical user interface of the Adapter Factory, without programming or scripting. When connectors are created, the Oracle Identity Manager repository maintains their definitions, creating self-documenting views. You use these views to extend, maintain, and upgrade connectors.

Predefined Connectors

Oracle Identity Manager offers an extensive library of predefined connectors for commercial applications and other identity-aware systems that are used widely. By using these connectors, an organization can get a head start on application integration. Each connector supports a wide range of identity management functions. These connectors use the most appropriate integration technology recommended for the target resource, whether it is proprietary or based on open standards. These connectors enable out-of-the-box integration between a set of heterogeneous target systems and Oracle Identity Manager. Because the connectors provide a set of components that were originally developed by using the Adapter Factory, you can further modify them with the Adapter Factory to enable the unique integration requirements of each organization.

Generic Technology Connectors

If you do not need the customization features of the Adapter Factory to create your custom connector, you can use the Generic Technology Connector feature of Oracle Identity Manager to create the connector.

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

4

Oracle Identity Manager Architecture

The architecture of Oracle Identity Manager provides a number of compelling technical benefits for deploying a provisioning solution as part of the identity and access management architecture.

This chapter discusses consists of the following sections:

- Key Features and Benefits
- How Oracle Identity Manager Works: The Tiers of Oracle Identity Manager
- System Components

4.1 Key Features and Benefits

The Oracle Identity Manager architecture is flexible and scalable, and provides the following features:

- Ease of Deployment
- Flexibility and Resilience
- Maximum Reuse of Existing Infrastructure
- Extensive User Management
- Modular Architecture
- Built-in Audit and Compliance
- Based on Leading Software Development Standards

4.1.1 Ease of Deployment

Oracle Identity Manager provides a flexible Deployment Manager utility to assist in the migration of integration and configuration information between environments. The utility exports integration and configuration information as XML files. These files are then imported into the destination environment, which can be staging or production. You can use the XML files to archive configurations and maintain versions, as well as replicate integrations.

The Deployment Manager provides you with the flexibility to select what to import and export. It also helps you to identify data object dependencies during both import and export steps. This flexibility enables you to merge integration work done by multiple people and to ensure the integrity of any migration.

4.1.2 Flexibility and Resilience

You can deploy Oracle Identity Manager in single or multiple server instances. Multiple server instances provide optimal configuration options, supporting geographically dispersed users and resources for increased flexibility, performance, and control. The Java 2 Enterprise Edition (J2EE) application server model of Oracle Identity Manager also provides scalability, fault tolerance, redundancy, failover, and system load balancing. As deployments grow, moving from a single server to a multiserver implementation is a seamless operation.

4.1.3 Maximum Reuse of Existing Infrastructure

To lower cost, minimize complexity, and leverage existing investments, Oracle Identity Manager is built on an open architecture. This allows Oracle Identity Manager to integrate with and leverage existing software and middleware already implemented within the IT infrastructure of an organization. For example, if an implementation requires integrating with an existing customer portal, then the advanced APIs of Oracle Identity Manager offer programmatic access to a comprehensive set of system functions. This allows IT staff to customize any part of its Oracle Identity Manager provisioning implementation to meet the specific needs of the organization.

4.1.4 Extensive User Management

Oracle Identity Manager enables you to define unlimited user organizational hierarchies and user groups. It supports inheritance, customizable user ID policy management, password policy management, and user access policies that reflect customers' changing business needs. It also helps you to manage application parameters and entitlements, and to view a history of resource allocations. In addition, it provides delegated administration with comprehensive permission settings for user management.

Oracle Identity Manager contains a Web-based user self-service portal that can be customized. This portal helps you extensively in user management.

4.1.5 Modular Architecture

Oracle Identity Manager simplifies the change management required in a dynamic organization. Oracle Identity Manager supports abstraction, which separates the execution logic separate from the application of that logic. For example, if you define the logic for a task, then the abstraction layer does not combine the logic with the actual execution of that task.

The abstraction layer allows the execution logic to be changed and refined without affecting logic or definitions that still apply. This also provides an iterative provisioning approach that allows IT to implement a provisioning system to fit existing requirements and to ensure that this system can evolve to meet future business needs. As user needs and business policies evolve, outdated execution logic can be "unplugged" from the provisioning instance for replacement with new execution logic. This provides the most cost-effective mechanism for handling change management and supporting the ongoing evolution of processes and systems for the organization.

4.1.6 Built-in Audit and Compliance

Identity management is a key part of any audit and compliance solution. Therefore, auditing and compliance capabilities must be integrated into the core identity management architecture; they should not be add-on utilities for the identity provisioning platform or separate products. Oracle Identity Manager is a fully integrated platform for identity provisioning and identity audit and compliance. An integrated application means that when a resource is brought under its management, the connection can be leveraged for both provisioning and compliance use, avoiding duplication of integration cost.

The audit and compliance features need not be restricted to reporting. With these features, no additional product integration effort is required to enable corrective actions as part of an audit and compliance process. For example, when using the attestation feature of Oracle Identity Manager, a reviewer's reject action can directly trigger the workflow to send notification or deprovision a user. An integrated platform provides easy access to identity and transaction data, enabling an organization to control its auditors without lengthy reporting lag time.

4.1.7 Based on Leading Software Development Standards

Oracle Identity Manager incorporates leading industry standards. For example, Oracle Identity Manager components are fully based on a J2EE architecture, so customers can run them from within their standard application server environments. Complete J2EE support results in performance and scalability benefits while aligning with existing customer environments to leverage in-house expertise.

Oracle develops its identity management products on a foundation of current and emerging standards. For example, Oracle is a Management Board member of Liberty Alliance, and incorporates Liberty Alliance developments in its solutions. Oracle participates in the Provisioning Services Technical Committee (PSTC), which operates under the auspices of the Organization for the Advancement of Structured Information Standards (OASIS).

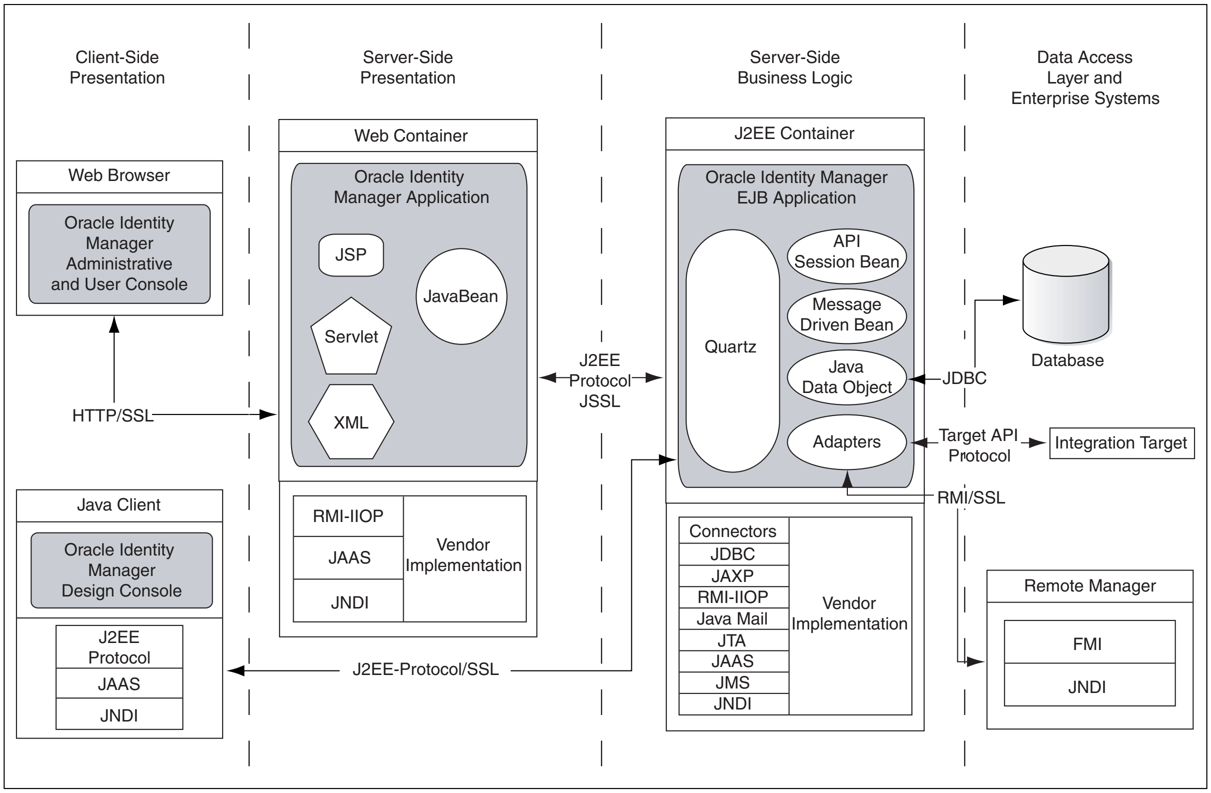
4.2 How Oracle Identity Manager Works: The Tiers of Oracle Identity Manager

Oracle Identity Manager is based on the n-tier J2EE application architecture. Oracle Identity Manager architecture contains the following tiers:

- Presentation Tier
- Dynamic Presentation Logic Tier
- Business Logic Tier
- Data Access Tier
- Back-End System Integration Tier

Figure 4–1 illustrates the Oracle Identity Manager architecture.

Figure 4–1 Oracle Identity Manager System Architecture



4.2.1 Presentation Tier

The Presentation tier 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.

4.2.2 Dynamic Presentation Logic Tier

Because both the Administrative and User Console and the Design Console are highly dynamic, the Dynamic Presentation Logic tier guides the content displayed on these interfaces. In case of the Administrative and User Console, there is a clear separation between the Presentation and Presentation Logic tier. No such boundary exists in the Design Console.

The second tier implements the business logic that resides in Java Data Objects. These objects are managed by the supported J2EE application server (JBoss Application Server, BEA WebLogic Server, IBM WebSphere Application Server, and Oracle Application Server). The Java Data Objects implement the business logic of the Oracle Identity Manager application; however, they are not exposed to any methods from the outside world. To access the business functionality of Oracle Identity Manager, you can use the API layer in the J2EE infrastructure, which provides the lookup and communication mechanism.

4.2.3 Business Logic Tier

The Business Logic tier is implemented as an Enterprise JavaBeans (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 organization application. The following are the components of the Business Logic tier.

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 constitute Oracle Identity Manager. These services include:

- Scalable management of resources
- Transaction management
- Security management
- Client access
- Technology resources

Client Interfaces and Business Logic Implementation

The core functionality of the Oracle Identity Manager platform is implemented in Java by 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, Reconciliation Engine, Audit Engine, Attestation Engine, and Reporting Engine. It also includes the integration tier based on the Adapter Factory, which dynamically generates integration code based on the metadata definition of the adapters. An adapter is the code that you can create and manage to enable Oracle Identity Manager to communicate with any IT Resource by connecting to the application programming interface (API) of that resource.

You can access the functionality of the platform through a set of EJB. 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.

4.2.4 Data Access Tier

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

- Database connection pooling

- Integration with Java Naming and Directory Interface (JNDI) that is lookup of DataSources in the JNDI namespace
- XA compliance

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

4.2.5 Back-End System Integration Tier

The Back-End System Integration tier is divided into the Oracle Identity Manager database and the 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 data is stored in the Oracle Identity Manager repository.

Remote Manager

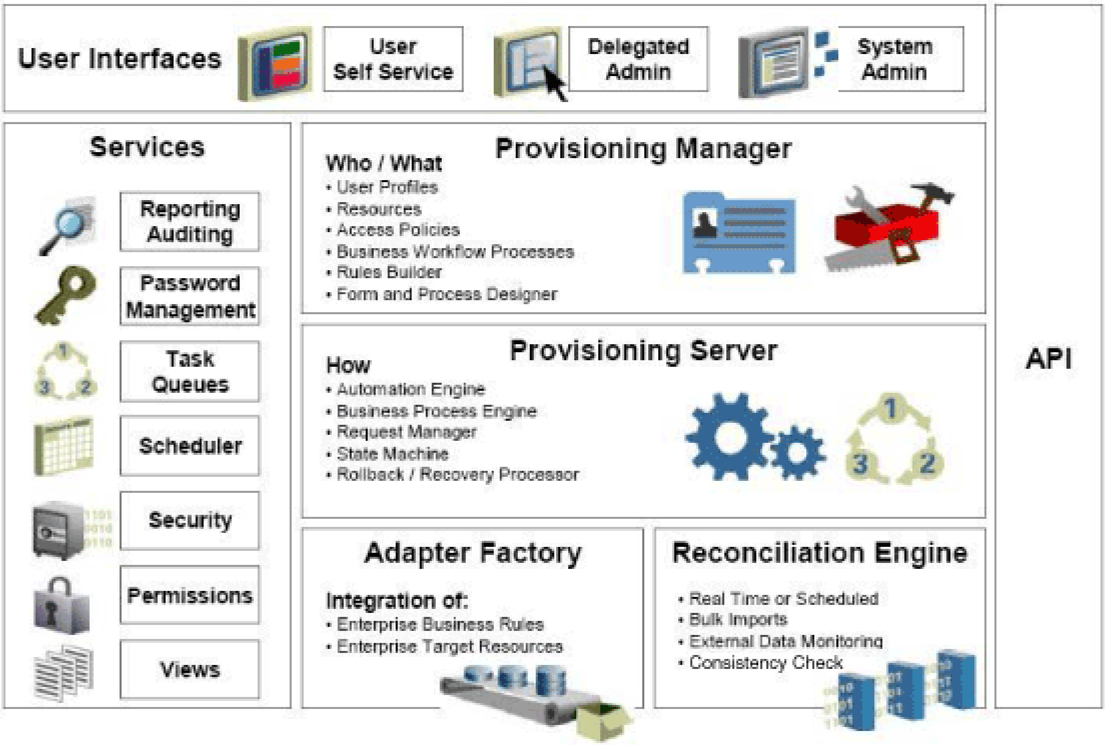
The Remote Manager is an Oracle Identity Manager server component that runs on a target system computer. It provides the network and security layer required to integrate with applications that do not have network-aware APIs or do not provide security. It is built as a lightweight Remote Method Invocation (RMI) server. The communication protocol is RMI tunneled through Hypertext Transfer Protocol/Secure (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.

4.3 System Components

Oracle Identity Manager is built on an enterprise-class, modular architecture that is both open and scalable. Each module plays a critical role in the overall functionality of the system. Figure 4–2 illustrates the system components of Oracle Identity Manager.

Figure 4–2 System Components of Oracle Identity Manager



Oracle Identity Manager user interfaces define and administer the provisioning environment. Oracle Identity Manager offers two user interfaces to satisfy both administrator and user requirements:

- Powerful Java-based Design Console for developers and system administrators
- Web-based Administration Console for identity administrators and end users

Provisioning Manager

The Provisioning Manager is where provisioning transactions are assembled and modified. The Provisioning Manager maintains the "who" and "what" of provisioning. User profiles, access policies, and resources are defined through the Provisioning Manager, as are business process workflows and business rules.

Provisioning Server

The Provisioning Server is the run-time engine for Oracle Identity Manager. It runs the provisioning process transactions as defined through the Design Console and maintained within the Provisioning Manager.

Adapter Factory

The Adapter Factory builds and maintains the integrations between Oracle Identity Manager and managed systems and applications. The Adapter Factory is designed to eliminate the need for hard-coding integrations with these systems.

For more information about the Adapter Factory, see "Integration Solutions" on page 3-5.

Reconciliation Engine

The reconciliation engine ensures consistency between the provisioning environment of Oracle Identity Manager and Oracle Identity Manager managed resources within the organization. The reconciliation engine discovers illegal accounts created outside Oracle Identity Manager. The reconciliation engine also synchronizes business rules located inside and outside the provisioning system to ensure consistency.

5

Oracle Identity Manager Deployment Configurations

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

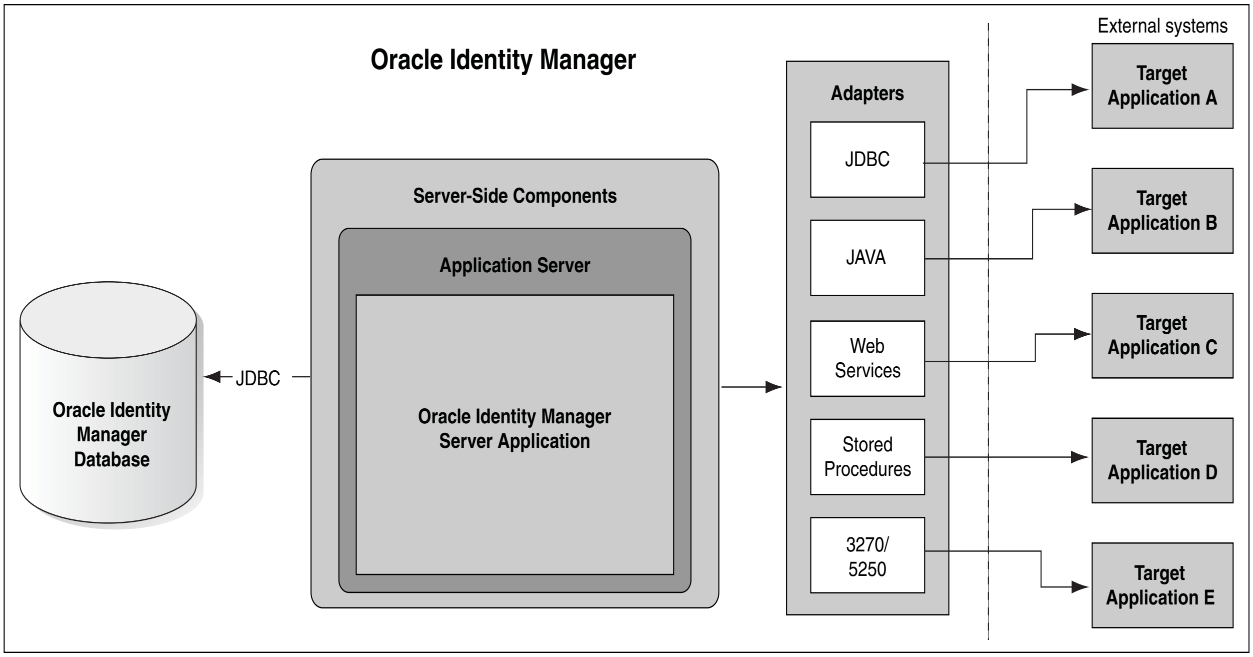
- Provisioning Configuration
- Reconciliation Configuration
- Provisioning and Reconciliation Configuration

5.1 Provisioning Configuration

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 all the 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.

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. Figure 5–1 illustrates the working of the provisioning module.

Figure 5–1 Provisioning Configuration



Provisioning events can be started through any of the following ways:

- **Request-based provisioning**

  A request can be manually created by an administrator or, in certain cases, by users themselves. Approval workflows are started after a request is submitted and provisioning of the approved account profile is started after the approval is completed.

- **Policy-based provisioning**

  This type of provisioning refers to the automation of target resources being granted to users through access policies. Access policies are used to define the association between user groups (or roles) and target resources. By default, each member of these user groups gets a predefined account in the target resource. 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.

- **Direct provisioning**

  This type of provisioning is a special administrator-only function. You can create an account for a particular user on a target system without having to wait for any approval processes.

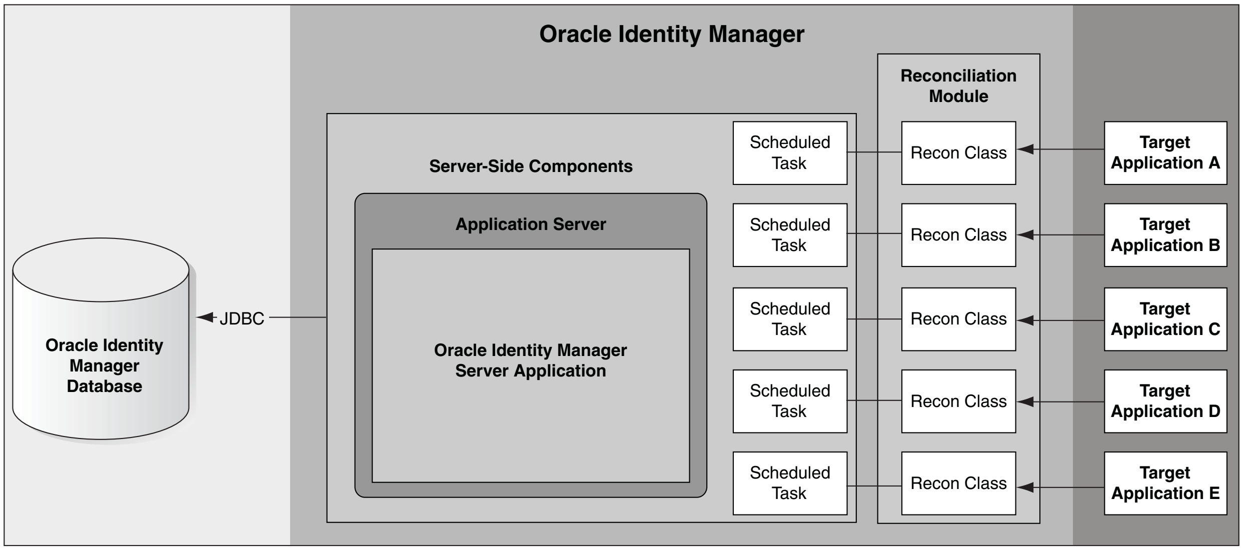
5.2 Reconciliation Configuration

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 information takes place in real time and does not require periodic polling of the target system by Oracle Identity Manager.

Figure 5–2 illustrates reconciliation.

Figure 5–2 Reconciliation Configuration



As shown in this figure, Oracle Identity Manager is used only as a single updated store for all users, user groups, and organization 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
- Components of the Reconciliation Module
- Regular Reconciliation Events Versus Delete Reconciliation Events

5.2.1 Reconciliation Configuration Options

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

- Reconciliation Type: Trusted Source or Target Resource
- Reconciliation Mode: Full or Incremental
- Batched or Nonbatched Reconciliation
- Limited or Regular Reconciliation

To create a reconciliation configuration, you must select one option from each of these parameters. See "Sample Reconciliation Configurations" on page 5-7 for examples of reconciliation configurations.

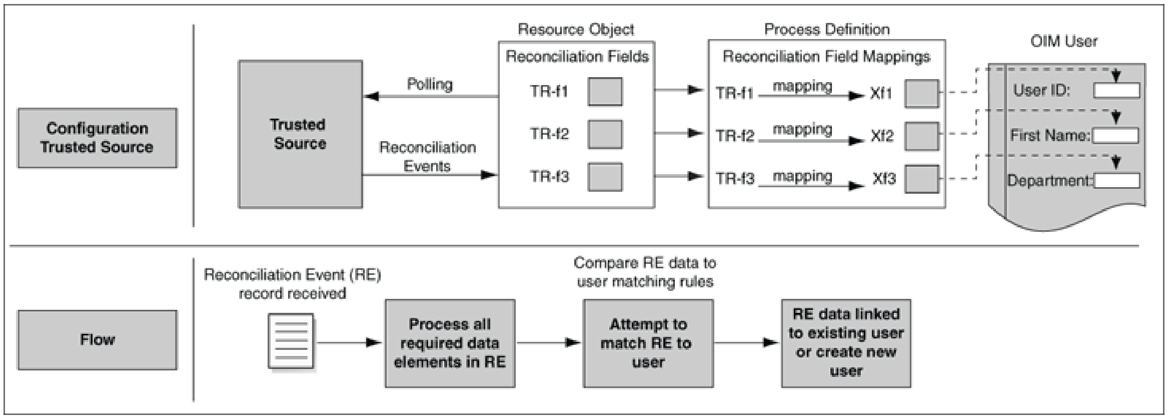
5.2.1.1 Reconciliation Type: Trusted Source or Target Resource

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

5.2.1.1.1 Trusted Source Reconciliation While configuring reconciliation, you can designate a target system as a **trusted source**. In a trusted source reconciliation run, newly created users on the target system are reconciled into Oracle Identity Manager. In other words, the target system acts as the trusted source for information about new users. Trusted source reconciliation also involves the reconciliation of changes to user records that already exist in both the target system and Oracle Identity Manager.

Figure 5–3 illustrates the steps involved in trusted source reconciliation.

Figure 5–3 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.

Note: Figure 5–3 shows the target fields mapping to Oracle Identity Manager User attributes.

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.

> **See Also:**
>
> - The "Limited or Regular Reconciliation" section on page 5-6
> - The "Resource Objects Form" section in *Oracle Identity Manager Design Console Guide* for more information about multiple trusted source reconciliation

5.2.1.1.2 Target Resource Reconciliation In the Oracle Identity Manager context, a target system that is not a trusted source is designated as a **target resource**. For an OIM User, you can create, modify, or delete target resource accounts through provisioning operations performed in Oracle Identity Manager.

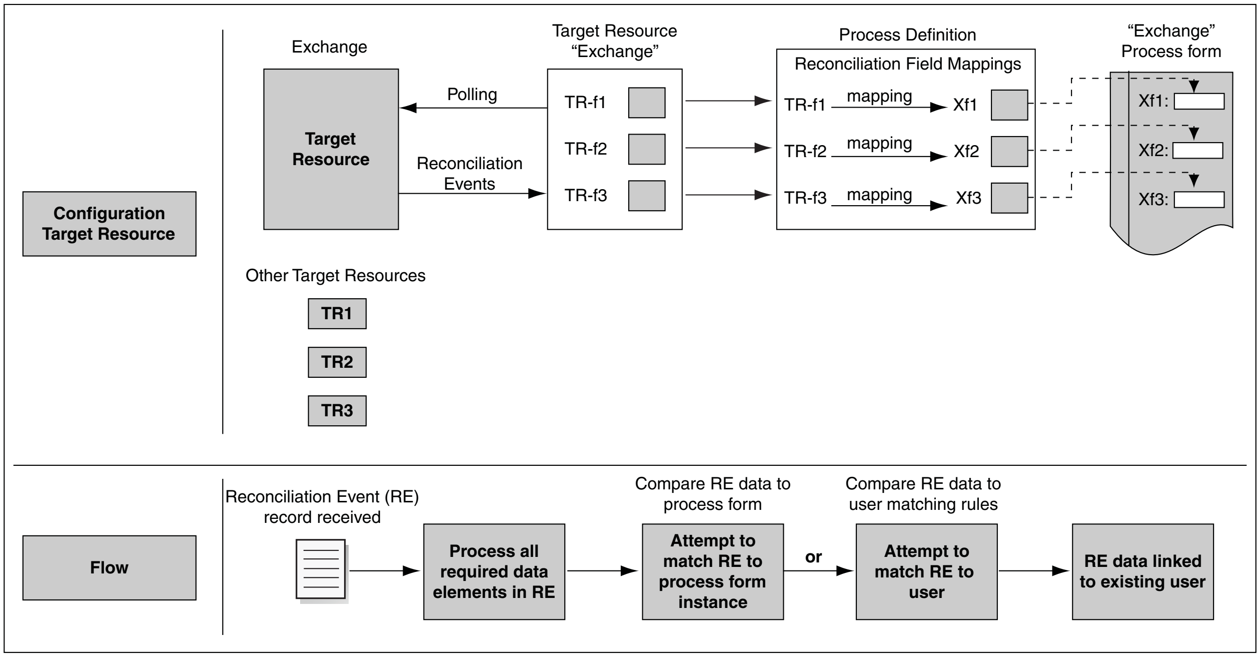
> **See Also:** The glossary of *Oracle Identity Manager Reference* for the definitions of the terms OIM User and OIM Account

Alternatively, these operations can be performed on the target resource itself. A target resource reconciliation run is aimed at reconciling into Oracle Identity Manager the creation of or changes to user accounts on a target resource.

For example, a resource representing the Microsoft Active Directory target system is provisioned to an Oracle Identity Manager user, and an attribute of the resource is modified outside of Oracle Identity Manager. The modification in the provisioned instance can be reconciled into Oracle Identity Manager through target resource reconciliation.

Figure 5–4 illustrates the steps involved in target resource reconciliation.

Figure 5–4 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

5.2.1.2 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 reconcile all accounts on the target system into Oracle Identity Manager. Full reconciliation is performed by default during the first reconciliation run performed on a target system. At the end of this reconciliation run, the value of the timestamp IT resource parameter is set to the time at which the reconciliation run ended. For the next reconciliation run, only user account records that have been added, modified, or deleted after the first reconciliation run ended 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 by setting the value of the timestamp parameter to 0. At the end of the next reconciliation run, the timestamp IT resource parameter is set to the time at which the reconciliation run ends and incremental reconciliation is performed from then onward.

> **Note:** The implementation of the timestamp parameter is different for different target systems. For example, the `Last Recon TimeStamp` parameter is used in Sun Java System Directory.

5.2.1.3 Batched or Nonbatched 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 takes longer to complete. 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.

> **See Also:** The connector pack documentation for information about the actual implementation of this feature

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. 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. You specify 50 as the value of this attribute.
- `NumberOfBatches`: Use this attribute to specify the total number of batches that must be reconciled. 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.

5.2.1.4 Limited or Regular 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`.

For any target system, if you do not specify a custom query, then a **regular reconciliation** takes place.

5.2.1.4.1 Reconciliation by User Attribute Multiple trusted source reconciliation by user type or any other user attribute is a special implementation of limited reconciliation. A customized query is used to specify the user type or attribute value, and only target system records that contain the specified value are fetched for reconciliation.

5.2.1.5 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:

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

5.2.2 Components of the Reconciliation Module

This section describes the following components of the reconciliation module:

- Reconciliation APIs
- Reconciliation Field Definitions
- Reconciliation Field Mappings
- Reconciliation Matching Rules
- Reconciliation Action Rules
- Reconciliation Engine
- Reconciliation Event Manager
- Reconciliation Provisioning Tasks

5.2.2.1 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. Because they are part of the generic API set, they can be used from any Java-based system. These APIs provide for the creation of both Regular and Delete Reconciliation events, and 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

5.2.2.2 Reconciliation Field Definitions

When you define a target system as a resource object in Oracle Identity Manager, you create reconciliation fields to represent the actual fields of the target system. This eliminates setting up the reconciliation connection to translate data from target system field names to Oracle Identity Manager field names.

When defining a reconciliation field, you must provide information in addition to the name of the field. Define a field type that indicates the type of data that the field will receive. Values for field type are *String*, *Number*, *Date*, *IT Resource*, and *Multi-Valued*.

5.2.2.3 Reconciliation Field Mappings

After you define the reconciliation fields, you must map them to the fields that are defined on a process form. These mappings serve the following purposes:

> **See Also:** "Process Definition Form" in *Oracle Identity Manager Design Console Guide*

- Define how you use the data received from the target system to update the fields on the process form.

  For example, if a reconciliation field for the `Object1` resource object is `attribute1`, and it is mapped to the process form field `field1`, then the value received for `attribute1` will be the value that is set on `field1`. For multivalued fields, the field will map to a particular child table on the process form. The interface will only show child table elements. For a trusted source, the process form fields are replaced with the fields from the entity form (user or organization form), including user-defined fields.

- Some of the mappings can be defined as key mappings. These mappings constitute the Process Matching Rule used to identify the record that must be updated. Suppose that the mapping defined in the previous example is also identified as a key mapping. In this case, when the reconciliation engine performs rule evaluation, it searches for all provisioned instances of `Object1` in which the value of `field1` is the same as the value for `attribute1` in the reconciliation data.

> **Note:** Key mappings hold true for target resource reconciliation only.

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

5.2.2.4 Reconciliation Matching Rules

The reconciliation matching 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 matching rules

5.2.2.5 Reconciliation Action Rules

Using the reconciliation action rules, you can define the following actions that the reconciliation engine must automatically perform based on the scenarios that arise from 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

5.2.2.6 Reconciliation Engine

The reconciliation engine uses all configurable components and includes the data processor and rule evaluator 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 engine performs the appropriate updates and provisioning actions.

5.2.2.7 Reconciliation Event Manager

The Reconciliation Event Manager is a form in the Design Console. You can use this form to examine a reconciliation event and perform the required actions. The Reconciliation Event 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 matching 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.

5.2.2.8 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 or organization record is updated instead.

If the account did not exist in Oracle Identity Manager before the reconciliation run, then the default provisioning process is initiated, 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/organization). 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 initiate multitarget synchronization processes.

5.2.3 Regular Reconciliation Events Versus 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**. In a regular reconciliation event, Oracle Identity Manager need not know about the existence of this account. The appropriate provisioning processes are set up and completed.

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:

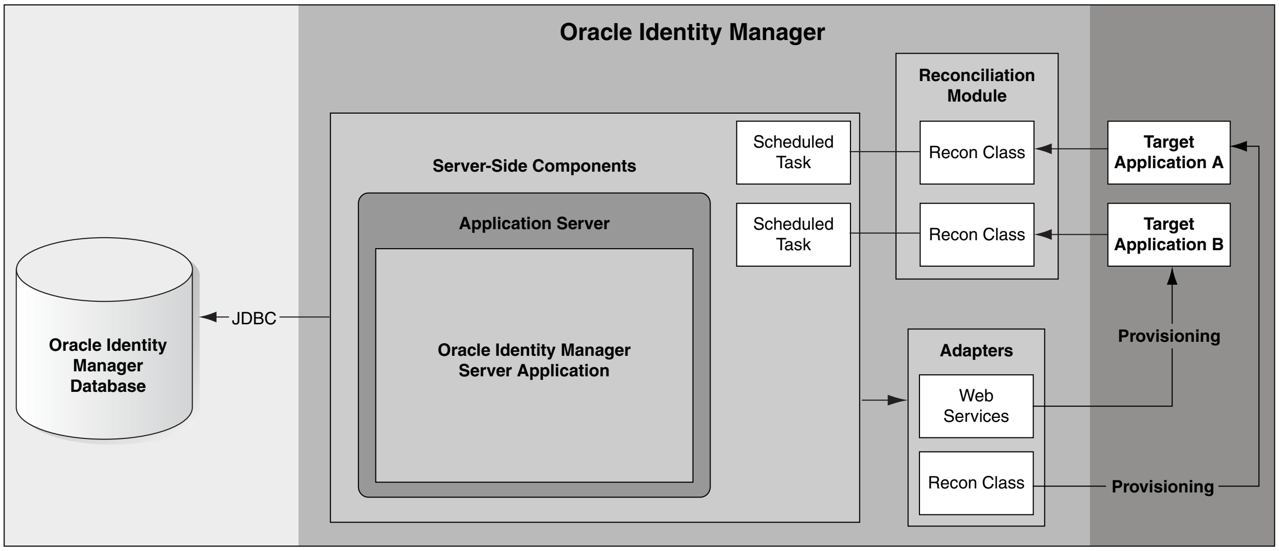
- The data for deleting an account is provided and the Oracle Identity Manager locates the matching account based on existing rules.
- The matching account record in Oracle Identity Manager is provided as the data for deleting an account.

The latter happens when the delete detection mechanism of reconciliation is employed. In both cases, if the accounts are matched, the provisioning process is canceled and the resource instance is marked as revoked.

5.3 Provisioning and Reconciliation Configuration

Figure 5–5 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 5–5 Provisioning and Reconciliation Configuration



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

6

Oracle Identity Manager Interfaces

Oracle Identity Manager provides two interfaces that you can use to perform various tasks. These are the Administrative and User Console and the Design Console. These two interfaces are located in the Presentation or Client tier of Oracle Identity Manager. Oracle Identity Manager also provides the SPML Web Service interface that supports inbound provisioning requests.

This chapter introduces the two consoles and briefly describes the functionality of each. This chapter also provides a brief introduction to the SPML Web Service. The chapter contains the following topics:

- Overview of the Administrative and User Console
- Overview of the Design Console
- SPML Web Service

6.1 Overview of the Administrative and User Console

Oracle Identity Manager is an advanced, flexible provisioning system for automatically granting and revoking access to organization applications and managed systems. The Administrative and User Console of Oracle Identity Manager can provide the staff and partners of an organization with access to the organization's resources, and enforce access policies that are associated with these resources.

The Administrative and User Console enables you to perform various functions, such as viewing user accounts, modifying profiles, viewing request status, and changing passwords. You can also customize the Administrative and User Console, as explained at the end of this section.

> **Note:** Not all functions are available to all users. The features that you can view and use in Oracle Identity Manager depend on the privileges that you are assigned.

6.1.1 Features of the Administrative and User Console

Use the Administrative and User console to perform the following functions:

- **Creating Accounts**

  If you do not have an account in Oracle Identity Manager, you must create one. Depending on how your system is configured, you might need your manager to create an account for you.

- **Locating Records**

Many fields in Oracle Identity Manager have lookup capabilities. You use them when you want to locate a record. You can locate a record by constructing a search or query and then by running it. To do so, you must enter data in one or more fields to limit the records retrieved by your search. You can also use wildcard characters in addition to the data that you enter in the fields.

> **Note:** The manner in which the search is constructed and run depends on the type of search you perform. The results retrieved are based on the context in which you are conducting the search.

- **Modifying Data Display Requirements**

  By default, the Administrative and User Console displays entire text entries, irrespective of the length of the entries. You can configure the console to truncate long text entries by using a series of three dots (…). By default, the Administrative and User Console displays any process form along with a child table that has 10 or fewer columns. You can also configure the console to display child tables with more than 10 columns.

- **Accessing and Managing Accounts**

  Using the Administrative and User Console, you can modify basic information associated with your Oracle Identity Manager user account. You can also change your password at will, or from time to time depending on system requirements. In addition, the console lets you delegate your task approval responsibilities to another user in case you are unavailable because of illness, vacation, and so on.

- **Viewing and Resourcing Requests**

  The console lets you view resources that have been provisioned to you. The console also lets you view all resource requests that you have submitted for yourself and those made by other users for you. You can also request provisioning of a new resource.

- **Creating and Tracking Requests**

  Oracle Identity Manager enables you to create and manage requests for provisioning resources to yourself, other users, and organizations. Based on the privileges granted to you by Oracle Identity Manager, you might be able to use the Administrative and User Console to view requests for resources. In addition, you might be able to edit details or approve tasks within those requests. This is known as tracking requests.

- **Managing To-Do Lists**

  A To-Do list is a list of tasks within a process. The processes for approving requests and their associated resources and making them available for provisioning consist of tasks. Before resources in a request can be provisioned to the target users, they must be approved by users assigned as approvers. If approval is required, then the approval tasks associated with the user self-registration requests also appear and require approval by an assigned approver. Using the Administrative and User Console, you can complete tasks on which your approvals are pending, retry a task if it has a Rejected status, and manage open attestation tasks that are assigned to you.

- **Creating and Managing User Records**

Using the Administrative and User Console, you can create and manage user records. Even if users are allowed to self-register, you should have the privileges to create and manage accounts on behalf of other users.

- **Creating and Managing Organization Information**

  Using the Administrative and User Console, you can create and manage organization records. You can also enable, disable, revoke, and provision resources, organizations, and suborganizations.

- **Using User Groups**

  Using the Administrative and User Console, you can define user groups to create and manage records of collections of users to whom you can assign certain common functionality, such as access rights, roles, or permissions. User groups can be organization-independent spanning across multiple organizations, or they can contain users from a single organization.

- **Creating and Managing Access Policies**

  You can create and use access policies for users, organizations, and resources in Oracle Identity Manager. The Access Policy Wizard of the Administrative and User Console helps you to define an access policy for provisioning resources to users who are members of the user groups to which the access policy is attached. The Administrative and User Console also enables you to modify information in existing access policies.

- **Managing Resources**

  You can use the Resource Management feature of the Administrative and User Console to manage resource objects for an organization or an individual user. Managing resources includes the following activities:

  - Search for a resource and view its details
  - Enable, disable, and revoke a resource from users or organizations
  - Manage Resource Administrator and Authorizer groups
  - View and edit the workflow
  - Define Resource audit objectives
  - Define and manage IT Resources
  - Define and manage scheduled tasks

- **Using the Deployment Manager**

  The Deployment Manager tool, accessed through the Administrative and User Console, helps you to export and import Oracle Identity Manager configurations. The Deployment Manager enables you to export the objects that form your Oracle Identity Manager configuration. Usually, you use the Deployment Manager to migrate a configuration from one deployment to another.

- **Generating Reports**

  Based on your needs, you can use the Administrative and User Console to generate reports that contain current operational data (Operational Reports) or historical data (Historical Reports). These reports describe resources available to users.

- **Managing Attestation Tasks**

A menu item in the Administrative and User Console provides access to attestation that creates reports for reviewers that they must review, which describes the provisioned resources that certain users have.

See Also:

- *Oracle Identity Manager Administrative and User Console Guide* for more information about the functions that you can perform by using the Administrative and User Console
- *Oracle Identity Manager Administrative and User Console Customization Guide* for information about how to customize the Administrative and User Console

6.1.2 Customizing the Administrative and User Console

You can customize the following components of the Oracle Identity Manager Administrative and User Console:

- General page layout
- Text, labels, and error messages
- Colors, font, and alignment
- Logos
- Self-registration, user profiles, and service accounts
- Field behavior and functionality
- Menus
- Search pages

See Also: *Oracle Identity Manager Administrative and User Console Customization Guide* for more information about the different components of the Administrative and User Console that can be customized

During installation, Oracle Identity Manager is deployed to your application server as an Enterprise Archive (EAR). This archive file contains some of the files for customizing your Administrative and User Console. The name of the EAR file varies depending on your application server.

To access the files for customizing your console, you unpack a Web Archive (WAR) file, make the required edits, repack the WAR file, and run a script that regenerates the EAR file and deploys it to your application server.

6.2 Overview of the Design Console

The Design Console is mainly used to configure the system settings. These settings control the systemwide behavior of Oracle Identity Manager and affect its users. This section describes the basic features of the Design Console.

6.2.1 Features of the Design Console

The following features of the Design Console let you perform different tasks:

- **Field Types**

The behavior of the basic features of Design Console is standard for all forms to enable ease of use. You can view records that are displayed in the data fields. You can also search for values by using the lookup fields. For example, the Date & Time window enables you to select a date, month, year, and time.

In addition, you can enter supplemental information about a record in the notes window. The Design Console also lets you select and assign available entities to a record.

- **Search Functions**

  Using the Design Console, you can perform searches for records in a database, also known as queries. Every form in the Design Console provides a search function. You can filter the search criteria in a form field. This limits the results that are returned to only the records that match the criteria you entered.

  You can also use a wildcard in a search. The asterisk (*) wildcard character represents unspecified portions of the search criteria. For example, if you enter B* in the Location field of a Design Console form and execute a search, you retrieve all records with locations that begin with the letter B, for example, Burbank, Boston, Bristol, and so on.

  > **Note:** If multiple records in the database match your search criteria, then you can view details of each record.

- **User Management**

  The Design Console lets you perform the following user management functions:

  – Define default values for certain process form parameters at the organizational level

  – Display resources that are allowed or disallowed by policies for each user

  – Define what forms and folders on the Design Console are allowed for which user groups

  – Create administrative queues that can be assigned to requests

  It also enables you to view, analyze, correct, link, and manage information in reconciliation events received from target resources and the trusted source.

- **Resource Management**

  You can manage resources in Oracle Identity Manager by using the Design Console. The different tasks that you can perform in resource management are:

  – Create resource types that appear as lookup values on IT resources from.

  – Define and manage IT resources.

  – Create rules that can be applied to password policy selection, auto-group membership, provisioning process selection, task assignment, and prepopulating adapters.

  – Create and manage resource objects.

- **Process Management**

  Process management includes creating and managing Oracle Identity Manager processes and templates for e-mail notifications.

An Oracle Identity Manager process is the mechanism for representing a logical workflow for approvals or provisioning. Process definitions consist of tasks that you must perform to complete a process. Using the Design Console, you can create and manage the approval and provisioning processes that are associated with the resource objects.

You can also create templates for e-mail notifications by using the Design Console. These notifications can be set to be sent to the user:

- When a task is assigned to the user
- When the task achieves a particular status
- When a request is approved
- On various attestation activities
- During self-registration and self profile modification

- **Oracle Identity Manager Administration**

  The Design Console also provides you with tools to manage the Oracle Identity Manager administrative features. You can perform various administrative tasks for Oracle Identity Manager by using these tools.

  You can associate class names, form labels, form types, menu items, graphics, icons, and online Help topics with an existing Oracle Identity Manager form. You can also modify folders that appear in the Design Console. The Design Console lets you create and manage lookup fields and their values, and user-defined fields.

  You can specify the value of properties that control the behavior of the client and server. You can also display information about servers that Oracle Identity Manager uses to communicate with third-party programs. In addition, you can set up schedules for when tasks should be run.

- **Development Tools**

  The Design Console contains a suite of development tools that enable you or developers to customize Oracle Identity Manager.

  You can create and manage the code that enables Oracle Identity Manager to communicate with any IT Resource by connecting to that resource's API. This code is known as an adapter. You can also compile multiple adapters simultaneously.

  The Design Console lets you create error messages that are displayed when certain problems occur. In addition, you can create and manage event handlers, data objects, and reconciliation rules that are used in Oracle Identity Manager.

  > **See Also:** *Oracle Identity Manager Design Console Guide* for more information about the features and functions of the Design Console

6.3 SPML Web Service

The SPML Web Service is an interface for inbound SPML-based provisioning requests. It supports the creation, modification, deletion, and lookup of Oracle Identity Manager users, user groups, and organizations. It also provides features for managing references (such as assignment and revocation of group memberships), resetting user passwords, and disabling and reenabling user accounts.

For details about the SPML Web Service, see Chapter 12, "SPML Web Service" of *Oracle Identity Manager Tools Reference*.

7

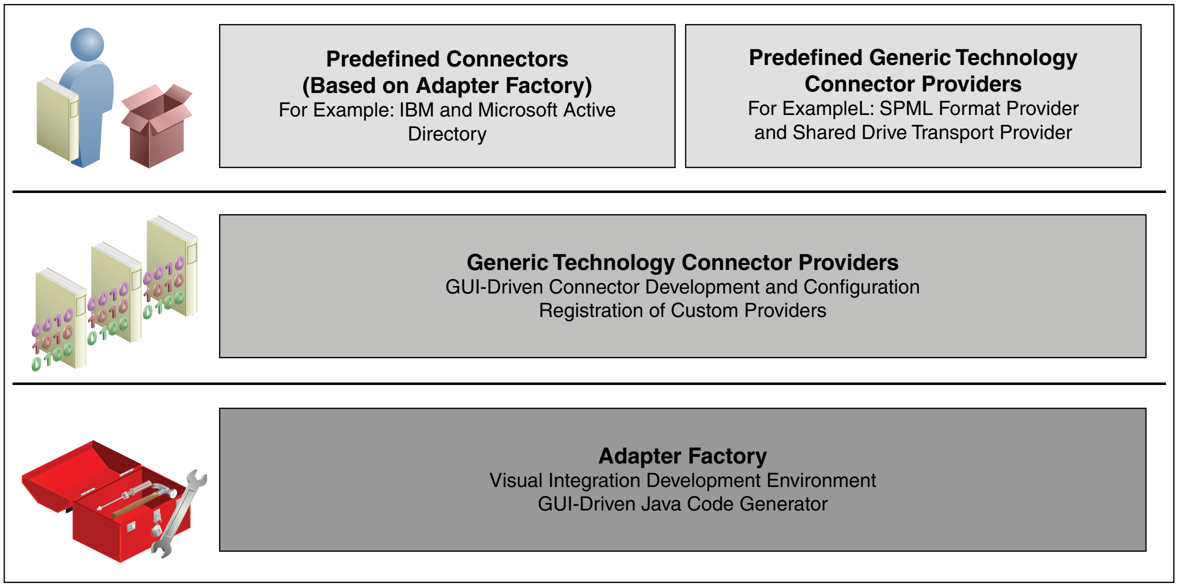
Oracle Identity Manager Integration Solutions

Oracle Identity Manager has a three-tier integration solutions strategy to provide connectors to various 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 based on custom generic technology connector providers
- Custom connectors using the Adapter Factory

Figure 7–1 illustrates the three-tier integration solutions strategy of Oracle Identity Manager.

Figure 7–1 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 chapter discusses the following topics:

- Predefined Connectors
- Generic Technology Connectors
- Custom Connectors

- Components Common to All Connectors
- Connector Installation

7.1 Predefined Connectors

When a predefined connector is available for the target resource, this is the preferred integration method. Because a predefined connector is designed specifically for the target application, it offers the quickest integration method. These connectors support popular business applications such as Oracle eBusiness Suite, PeopleSoft, Siebel, JD Edward and SAP, as well as technology applications such as Active Directory, Java Directory Server, UNIX, databases, and RSA ClearTrust. Predefined connectors offer the quickest integration alternative because they are designed specifically for the target application. They use target recommended integration technologies and are preconfigured with application specific attributes.

7.2 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 need 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 Part II, "Integration Solutions Features" of *Oracle Identity Manager Administrative and User Console* for more information about generic technology connectors.

7.3 Custom Connectors

If the target resource has no technology interface or accessible user repository, then the customer can develop a custom connector. 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 and *Oracle Identity Manager Design Console Guide* for details about the Adapter Factory

7.4 Components Common to All Connectors

Table 7–1 lists the definitions of connector components contained in the connector XML file. These components are common to all connectors.

Table 7–1 Connector Components

Components	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. Note: For more information about provisioning process, see Table 7–2 and Table 7–3.

Table 7–1 (Cont.) Connector Components

Components	Description
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 used extensively 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.
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 can have a parameter called `IP Address.` The value of that parameter for the `Target_Solaris` IT resource instance can 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. **Note**: For more information about adapters, see *Oracle Identity Manager Tools Reference*.
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.

7.4.1 Provisioning Process Tasks

Table 7–2 lists the predefined tasks (or their equivalents) that the Provisioning Process component contains.

Table 7–2 Provisioning Process Tasks

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 (revokes the user's account)
Update User	Modifies the privileges or profile of a user account in the target application

7.4.2 Reconciliation-Related Provisioning Process Tasks

In addition to the tasks listed in the previous section, the Provisioning Process component also contains the reconciliation-related tasks. Table 7–3 lists these tasks.

> **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.

Table 7–3 Reconciliation-Related Provisioning Process Tasks

Provisioning Process Task (Reconciliation-Related)	Purpose
Reconciliation Insert Received	This task is inserted into the Provisioning Process instance associated with the user or organization when Oracle Identity Manager determines that the reconciliation event received from the target system represents the creation of a user or organization 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 or organization when Oracle Identity Manager determines that the reconciliation event received from the target system represents the update of an existing user or organization 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 or organization when Oracle Identity Manager determines that the reconciliation event received from the target system represents the deletion of an existing user or organization account.

7.5 Connector Installation

The Administrator and User Console provides features to install connectors. The following are general considerations that you must address before installing connectors:

- Some connectors require external libraries in the form of JAR files for normal functioning. You can 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 can 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.
- For optimal performance of the prepackaged connectors, 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.

8 Context Manager

This chapter describes a context and its creation. It contains the following topics:

8.1 What is a Context?

A context is the environment in which an Oracle Identity Manager operation is performed. For example, a user creation operation performed on the Admin console is carried out in the Web context. The following information constitutes the context or environment in which this operation is performed:

- User performing the operation
- IP address of the computer from which the user creation request originated
- Date and time at which the request is submitted
- Proxy that is used to reach the application server

At the same time, if the user is created by running the bulk load utility, then the context includes the user who started the bulk load utility, the computer from which the operation is being performed, and so on.

A context acts like a memory-based repository in which names and values of the context variables are stored. Each functional component involved in an operation can add variables into the context. Context values can only be set, they cannot be modified. The context values act as a means of communication across components involved in an operation.

Since, context values might be used in taking decisions during the operation, the context manager supports the concept of signed (verified) context values. In other words, context values placed in the context can be signed using a digital certificate. From that point onward, the context manager validates the value of a context variable whenever the value is loaded into the context. This validation includes a check, whether the value has been altered during either storage or communication, and if the system can trust the signer. However the context manager does not perform the validation as to if the signer can set that specific name and value. If such validations are to be performed, it will be the responsibility of the functional component that uses the name and value.

Context variable values are loaded into memory only when they are required. This enhances performance. A context also acts as a cache of the typical values required by event handlers. This helps reduce the need to fetch values from the repository each time the values are needed.

Each Context sits in a ThreadLocal variable so that multiple threads in the application server have their own Identity Management execution context.

8.1.1 What is a Child Context?

A child context is a subcontext that is initiated while an operation is in progress. For example, if the Create User operation involves running a specific event handler, then the event handler is run in an environment that is a child of the one in which the user is being created. This means that contexts can be nested, and there can be a stack of contexts. New contexts can be created by functional components and further processing starts using the newly created context.

8.1.2 Storing Context Data

The context data is stored in the database. The format of the data is conducive to perform Extract, Transform, and Load (ETL) in the database so that it can be moved into reporting tables as required. The data model archives the data after its use.

A context can store values of different types, ranging from simple string, integer, and date types to complex types. The complex type is stored either as an XML value or a Binary value. Binary values are faster to retrieve, but XML values offer greater usability in terms of reporting.

When the context values are transferred to remote services or used in BPEL or other XML formats, the following schema is applicable:

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
   xmlns:tns="http://www.example.org/context/"
   targetNamespace="http://www.example.org/context/">
   <complexType name="context-type">
       <sequence>
          <element name="context-value" type="tns:context-value-type">
          </element>
          <element name="parent-context" type="tns:context-type"></element>
       </sequence>
   </complexType>
   <complexType name="context-value-type">
      <sequence>
         <element name="string-value" type="string"></element>
         <element name="numaric-value" type="int"></element>
         <element name="date-value" type="dateTime"></element>
         <element name="large-string-value" type="any"></element>
         <element name="binary-value" type="hexBinary"></element>
      </sequence>
      <attribute name="type" type="string"></attribute>
      <attribute name="class" type="string"></attribute>
   </complexType>
</schema>
```

8.2 Context Manager

The Context Manager creates an environment in which Oracle Identity Manager operations are performed. This environment/context is preserved in the database to allow Oracle Identity Manager operations to be executed asynchronously, and to enable auditing.

The Context Manager allows variables, objects, and run-time information to be stored in the context for the purposes of inter-component communication. The implication of having this intelligent context mechanism is far reaching. The Context Manager creates a place where the environment in which a specific operation is being performed is preserved.

8.2.1 Working of a Context Manager

The following sequence of steps outlines the working of a Context Manager.

1. Establish a new context.
2. Clear the context from the Thread.
3. Add a value to the context. While adding a value, assign a certificate to sign the value.

   > **Note:** It is not possible to delete or modify a value once it is added to the context.

4. Save the context into the database.
5. Load the context from the database.
6. Wrap the context into XML, so that the context can be passed while invoking remote methods.
7. Unwrap the XML context once it is retrieved in the remote API to re-establish the context.

9 Oracle Identity Manager Globalization

Globalization support in Oracle Identity Manager enables you to deploy Oracle Identity Manager by using supported languages and country locales from around the world. Globalization of software applications consists of two aspects, internationalization and localization, as described in the following topics:

- Internationalization
- Localizing Oracle Identity Manager
- Globalization Properties

See Also: *Oracle Identity Manager Globalization Guide*

9.1 Internationalization

Internationalization is the process of adapting products for use with other languages, nations, and cultures. The internationalization of software applications includes the following tasks:

- Separating resources, such as strings, images, and so on, from application code
- Selecting the appropriate code page (the character set) and defining the code page conversions
- Modifying all text manipulation algorithms to be aware of the selected code page
- Modifying the logic for algorithms that handle dates, times, currency, numerics, and so on
- Modifying the logic used in collation and sorting algorithms
- Isolating the text strings in images

9.2 Localizing Oracle Identity Manager

Localization is the process of preparing an internationalized software application for a specific market, and includes the following tasks:

- Translating resource strings into the target languages, taking into consideration characteristics of the locale where the target language is used
- Identifying potentially nonlocalizable resources and removing them, if necessary

Oracle Identity Manager has been localized into the following languages:

- Chinese (Simplified)
- Chinese (Traditional)

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

In this release of Oracle Identity Manager, application components can only understand and support one language. During installation, you select the language that you want from a list of supported languages.

9.3 Globalization Properties

The following system properties support globalization for a single language in the current release:

- **user.language**

  Oracle Identity Manager uses this property for back end activities, for example, for automatic e-mail generation when sending e-mail to users. You set this property when you select a language during installation.

  For displaying data in a browser, Oracle Identity Manager localizes the data based on the value of the accept-language parameter in the HTTP header sent by the browser. The Oracle Identity Manager application localizes all responses into this language.

- **user.region**

  As with the user.language property, Oracle Identity Manager uses this setting for back-end processes, for example, sending e-mail to users.

Index