

Oracle Identity Manager

Key Benefits

- **Increased Security:** Enforce internal security policies and eliminate potential security threats from rogue, expired and unauthorized accounts and privileges.
- **Enhanced Regulatory Compliance:** Cost-effectively enforce and attest to regulatory requirements (e.g. Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA) associated with identifying who has access privileges to sensitive data
- **Streamlined Operations:** Reduce inefficiency and improve service levels by automating repeatable user administration tasks
- **Improved Business Responsiveness:** Get users productive faster through immediate access to key applications and systems
- **Reduced Costs:** Reduce IT costs through efficient staff usage and common security infrastructure.

Oracle Identity Manager is a highly flexible and scalable enterprise identity management system that centrally administers user accounts and access privileges within enterprise IT. It manages the entire identity lifecycle to meet changing business and regulatory requirements and provides essential auditing, reporting and compliance functionalities.

Identity and Role Administration

Oracle Identity Manager (OIM) offers a comprehensive range of user identity and role lifecycle administration features.

Delegated Administration and User Configurable Proxy

OIM features a highly flexible security framework that:

- Supports delegation of most administrative functions to any group and/or user.
- Provides each user the ability to temporarily delegate approval tasks to a defined proxy, ensuring continuity of business processes, uninterrupted by user's time away from the office.

Self-Service Profile & Password Management

OIM's self-service capabilities allow users to manage their own profile data and update passwords across managed resources. Customizable challenge questions enable self-service identify verification and password reset. This self-service capability easily pays for itself many times over through reduced help desk calls.

Advanced Password Policy Management and Password Synchronization

IM supports multiple password complexity policies per resource, and provides the framework to synchronize passwords across managed resources and to enforce differences in password policies among these resources. This bi-directional password synchronization is offered out-of-the-box in most OIM directory server and mainframe connectors.

WS-SPML Interface

OIM provides an SPML 2.0 Web Service interface to key administration functions:

- Creation, modification, deletion and lookup of OIM users, groups and organizations
- Management of references (such as assignment and revocation of group memberships, group administrator and user's manager)
- Reset of user passwords, and suspension and resumption of users.

Approval And Request Management

Companies start by modeling their existing or best-practice business processes for resource request and approval, then use OIM's rich web-based Graphical Workflow Designer, with drag-and-drop functionality, which simplifies the creation and maintenance approval workflows. The approval workflows are highly configurable to allow for variations in a company's approval processes, and support features such as approver proxies and request escalations out-of-the-box.

In deployment, administrators, peers, or users themselves can initiate requests for access

Features Overview

- Self-Service Identity And Role Management
- Delegated Administration
- Workflow & Policy Management
- Password Management
- Audit & Compliance Management
- Integration Solutions Featuring Adapter Factory And Pre-Configured Connectors

Architecture Overview

- Ease of Deployment
- Flexible and Resilient
- Maximum Reuse of Incumbent Infrastructure
- Modular Architecture
- Standards-based

to resources, and track the status of their requests through web applications and email notifications.

Request Management

With OIM, users can create provisioning requests for resources with fine-grained entitlements. Business approvers can use the same web-based interface to examine and approve incoming requests. By placing the request and approval process closer to the business, enterprises realize better service levels and reduced operational costs. Request and approval activities are also audited for regulatory compliance reporting purposes.

Policy Based Entitlements Management

OIM's policy based management of entitlements across managed applications automates IT processes and enforces security and compliance requirements.

Policy Management

OIM supports policies driven by user roles or attributes. OIM supports both automated provisioning and denial policy. Denial policy explicitly denies user access to specific resources, thereby enforcing security or governance policies such as segregation of duties.

Workflow Management

OIM supports both approval workflow and provisioning workflow. Approval workflow, managed by the business process owner, enables an enterprise to model its preferred or best-practice approval processes for managing resource access. Provisioning workflow, managed by the IT process owner, enables an enterprise to orchestrate and automate IT tasks for provisioning resources with even the most complex provisioning procedures. OIM's graphical workflow designer simplifies workflow creation and maintenance.

Dynamic Error Handling and Transaction Integrity

Unavailable or offline resources no longer stop the provisioning transaction or cause it to fail. When a provisioning transaction fails or is stopped, the system is able to recover and rollback to the last successful state or reroute to a different path, in accordance with pre-defined rules.

Guaranteed De-provisioning

When a user leaves the organization or she no longer requires access, OIM revokes access on demand or automatically, as dictated by access policies. This minimizes security risks, and reduces access costs associated with certain resources.

Technology Integration and Adapter Factory®

OIM integrates with applications or resources through a highly configurable, agentless interface technology, and provides a growing library of pre-configured connectors to popular applications, user repositories, and technologies.

Adapter Factory

OIM's Adapter Factory technology eliminates the complexity associated with creating and maintaining these connections. Adapter Factory provides rapid integration to commercial or custom systems. Users can create new, or modify existing integrations using Adapter Factory's graphical user interface, without programming, or scripting.

Oracle Identity Management Products

- **Oracle Access Manager** delivers critical functionality for access control, single sign-on, and user profile management
- **Oracle Identity Manager** is a powerful and flexible enterprise identity provisioning and compliance monitoring solution.
- **Oracle Identity Federation** enables cross-domain single sign-on
- **Oracle Internet Directory** is a robust and scalable LDAP V3-compliant directory service
- **Oracle Virtual Directory** provides Internet and industry standard LDAP and XML views of existing enterprise identity information,
- **Oracle Web Services Manager** is a comprehensive solution for adding policy-driven security and management capabilities to Web services.
- **Oracle Enterprise Single Sign-On** provides users with unified sign-on and authentication across enterprise resources.
- **Oracle Adaptive Access Manager** provides web access real-time fraud detection and multifactor online authentication security.
- **Oracle Role Manager** is an authoritative source for role lifecycle management.

Pre-configured Out-of-the-Box Connectors

For the most popular commercial applications and interface technologies, OIM offers pre-configured connectors that enable out-of-the-box integration. The connectors can be modified using the Adapter Factory to accommodate an enterprise's unique integration requirements.

Generic Technology Connector

The Generic Technology Connector framework provides an alternative connector development environment that focuses on data flow instead of process flow. It is a framework with basic building blocks that allows system administrators to design custom connectors quickly and easily. It also allows administrators to create more building blocks and use them independently or in conjunction with the building blocks provided. With its focus on data migration, Generic Technology Connector communicates with any trusted or target resource by using standard protocols such as HTTP, SMTP, FTP and Web Services combined with generic message formats such as CSV, SPML and LDIF. Additionally, the WS-SPML provisioning provider supports HTTP basic and WS-Security authentication.

Audit And Compliance

Identity management is a key part of any audit and compliance solution. OIM is a fully integrated platform for identity provisioning, and audit and compliance

Identity Reconciliation and Rogue/Orphan Account Management

The OIM reconciliation engine helps to detect and map existing accounts in target resources, enabling the creation of an enterprise-wide identity and access profile for each user. In addition, OIM can provide continuous monitoring of rogue and orphan accounts, as well as special service accounts, also known as administrator accounts.

OIM provides out of box reports for rogue accounts and rogue entitlements. These reports provide additional attestation details to analyze whether certain rogue activity was accepted as reasonable risk in one of the previous attestation runs.

Comprehensive Reporting and Auditing

OIM provides 35+ out of box reports on both the history and the current state of the provisioning environment. The system captures all necessary data to answer the question "Who has access to What, When, How, and Why?" Some of the identity data captured includes user identity profile history, user group membership history, user resource access and fine-grained entitlement history. OIM's reporting and auditing capabilities enable an enterprise to cost effectively cope with ever increasingly stringent regulatory requirements, such as Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA, and HSPD-12.

Attestation / Recertification Automation

Attestation, also referred to as recertification, is a key part of Sarbanes-Oxley compliance and a highly recommended security best practice. OIM offers a best-in-class attestation feature that can be deployed quickly to enable an enterprise-wide entitlements review and certification process.

OIM allows the user- and resource- scope definition to be based on a rich set of rules-based expressions. Attestation reviewers can review fine-grained entitlements within an

interactive user interface that supports fine-grained certify, reject, decline, and delegate actions. It also allows configuration of a grace period for attestation. Beyond the grace period, the system automatically delegates the attestation request to a specific user in the attestation process owner group based on a priority-based algorithm.

All report data and reviewers' actions are captured for future auditing needs and can optionally trigger corrective actions by configuring OIM's workflow engine.

For more information, visit www.oracle.com/identity

Copyright 2007, Oracle. All Rights Reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor is it subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.