

ORACLE IDENTITY MANAGER

KEY FEATURES AND BENEFITS

ORACLE IDENTITY MANAGER

- **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 controls user accounts and access privileges within enterprise IT resources. It manages the entire identity lifecycle to meet changing business and regulatory requirements and provides essential reporting and compliance functionalities. Oracle Identity Manager is a component of Oracle's Identity Management solution and Oracle Fusion Middleware.

Introduction

Oracle Identity Manager is an enterprise provisioning solution built using the latest internet architectural best practices. It provides the functionalities of identity and role administration, approval and request management, policy-based entitlement management, technology integration, and audit and compliance automation. Oracle Identity Manager delivers flexibility and scalability with product features such as a J2EE implementation, N-tier deployment architecture, browser-based user interfaces and Oracle Grid compatibility.

Identity And Role Administration

Oracle Identity Manager offers a comprehensive range of user identity and role lifecycle administration features. User identities can be managed centrally, by delegated administrators, or through user self-administration. The ability to delegate any subset of tasks to organizations and individuals makes it possible to efficiently manage large user populations across an extended organization. Self-registration and self-service of identity profiles, as well as self-service password and security question changes and password retrievals, reduces calls to the help desk.

Approval And Request Management

With Oracle Identity Manager, account request and approval processes can be automated to meet every organization's needs. Companies start by modeling their existing or best-practice business processes for resource request and approval. In deployment, administrators, peers, or users themselves can initiate requests for access to resources, and track the status of their requests through web applications and email notifications. The approval workflows are highly configurable to allow for variations in a company's approval processes based on organization, user, application and other entity attributes and supports features such as approver proxies and request escalations out-of-the-box.

Policy-Based Entitlement Management

Oracle Identity Manager's policy engine manages the fine-grained entitlements

ORACLE IDENTITY MANAGEMENT PRODUCTS

Oracle Access Manager delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment.

Oracle Identity Manager is a powerful and flexible enterprise identity provisioning and compliance monitoring solution that automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases, and ERP.

Oracle Identity Federation enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the box.

Oracle Internet Directory is a robust and scalable LDAP V3-compliant directory service that leverages the high availability capabilities of the Oracle 10g Database platform.

Oracle Virtual Directory provides Internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

Oracle Web Services Manager is a comprehensive solution for adding policy-driven security and management capabilities to existing or new Web services.

across managed applications, automating IT processes and enforcing security and compliance requirements such as segregation of duties. It can also detect rogue and orphan accounts and privileges during reconciliation activities and trigger appropriate corrective actions. Policy-based management of entitlements allows multiple request and approval processes to be implemented and refined over time in parallel, reducing the total cost of implementation.

Technology Integration and Adapter Factory®

Oracle Identity Manager integrates with any application or resource through a highly configurable, agentless interface technology. Oracle provides a growing library of pre-configured connectors to popular applications, user repositories, and technologies. In addition, Identity Manager includes the Adapter Factory®, a Java code generator with a graphical user interface which enables users without programming skills to create and modify application connectors. Identity Manager's integration architecture reduces the overall costs of deployment and maintenance of a provisioning solution.

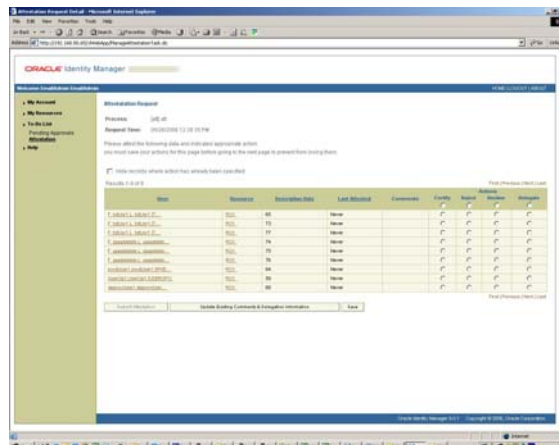


Figure 1: Oracle Identity Manager's Attestation Review Interface

Audit And Compliance

Oracle Identity Manager captures an organization's complete lifecycle data for identities, roles, resources and entitlements. An embedded reporting engine generates a growing list of pre-defined operational and historical reports. Identity Manager's attestation feature fully automates the periodic entitlement recertification process for financially significant applications, a requirement for compliance with Sarbanes-Oxley and other regulations. Identity Manager helps companies contain cost and risk associated with compliance audits by automating a highly manual process and capturing and ensuring the integrity of the attested data.

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