ORACLE IDENTITY MANAGER 11g

KEY FEATURES

- Feature-rich user interface that supports durable customizations
- Self-service identity management with personalized, business user friendly experience
- Accelerated application on-boarding
- Advanced delegated administration and password management
- Requests with approval workflows and policy-driven provisioning
- Integration solutions featuring Adapter Factory and pre-configured connectors for enterprise applications, LDAP & DB repositories.
- Comprehensive auditing and reporting

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 self service and common security infrastructure

Oracle Identity Manager is a highly flexible and scalable enterprise identity administration system that provides operational and business efficiency by providing centralized administration & complete automation of identity and user provisioning events across enterprise as well as extranet applications. It manages the entire identity and role lifecycle to meet changing business and regulatory requirements and provides essential reporting and compliance functionalities. Its seamless integration with Oracle Identity Analytics (OIA) and Oracle Privileged Access Manager (OPAM) ensures consistent enforcement of identity-based controls, reducing ongoing operational and compliance costs.

Extensible User Interfaces (UI)

Oracle Identity Manager (OIM) supports simple and complex web-browser based customizations to its user interface. These customizations can be staged in a sandbox environment that enables administrators to perform, test, commit or rollback all such customizations without impacting other users. OIM remembers user preferences like changes to home page layout, saving repeated queries, specifying sort and search preferences. All such customizations are stored in a specialized and reserved namespace in OIM's metadata repository to ensure that they are durable and that they survive patching and upgrades thereby reducing upgrade costs.

Intuitive Self Service

Registration & Profile Management

Using OIM's self-service interface, users can create self-registration requests that can require a configurable approval process before being granted an account. Users can easily manage their own mutable profile/contact data or set a proxy/delegate user to act on their behalf for a specified time period.

Password Management

OIM's self-service interface enables users to change their enterprise password that can then get propagated to all target resources provisioned to the user. Users can easily reset their forgotten password using the security challenge questions they set during their first login or captured during self-registration. Additionally, OIM's password management features are integrated with all login and password-related flows in Oracle Access Manager (OAM) and Oracle Adaptive Access Manager (OAAM) serving as a platform for advanced user authentication for scenarios requiring stronger authentication.

Simplified Request Management

Request Catalog

OIM provides a unified catalog of access rights, including enterprise and application roles,

ARCHITECTURE OVERVIEW

- **Ease of Deployment:** Integrations and configurations can easily be moved between environments.
- **Flexible and Resilient:** Oracle Identity Manager can be deployed in single or multiple server instances. Multiple server instances provide optimal configuration options, fault tolerance, redundancy, fail-over and system load balancing
- **Maximum Reuse of Incumbent Infrastructure:** Oracle Identity Manager is built on an open architecture to integrate with and leverage existing software and middleware already implemented within an organization's IT infrastructure
- **Modular Architecture:** Oracle Identity Manager is made up of abstraction layers, which allows the execution logic to be changed and refined without affecting logic or definitions that still apply
- **Standards-based:** Oracle Identity Manager incorporates leading industry standards, such as Java EE, BPEL and OASIS

AVAILABLE CONNECTORS

- **Business Applications:** Oracle Fusion Applications, Oracle E-Business, PeopleSoft, JD Edwards, Siebel and SAP
- **LDAP stores**: Oracle Internet Directory, Oracle DSEE, Oracle Unified Directory, Active Directory and e-Directory
- **Security systems**: RSA, RACF, Top Secret and ACF2
- **Operating systems**: Unix, AS/400 and Windows
- **Ticket Management systems**: BMC Remedy
- **Cloud Connectors**: Oracle CRM On-demand, Google Apps

application accounts, and entitlements. Privileges are harvested into the catalog allowing catalog administrators to then provide user friendly metadata like specifying risks, audit levels, search tags, specify users or roles that will be involved in approval, certification or manual provisioning fulfillment activities related to the corresponding roles, accounts or entitlements etc. Once configured, users can use OIM's "shopping-cart" like interface to request for access for self or for other users. OIM also enables users to bundle frequently requested privileges and model them as a saved carts that can also be shared with other users. Users and helpdesk administrators can easily and visually track the progress of their requests through the tracking interface thereby ensuring their requests are handled in a timely fashion.

Approval Orchestration

OIM uses Oracle BPEL Process Manager, an integral component of Oracle SOA Suite, for its approval workflow and routing engine. Developers can use Oracle JDeveloper as their Integrated Development Environment (IDE) that offers a rich visual design paradigm for creating and deploying BPEL based processes. Additionally policy owners can change the approval routing logic using a web interface without relying on developers. This not only results into significantly faster deployment time, but also provides the architecture agility to adjust workflows quickly when business processes and enterprise policies change for the approval needs.

Advanced Identity Lifecycle & User Provisioning

OIM enables policy-based automated provisioning of resources with fine-grained entitlements. For any set of users, administrators may specify access levels for each resource to be provisioned, granting each user only the exact level of access required to perform his job, no more and no less. These policies can be driven by user roles or attributes, enabling implementation of role based access control (RBAC), as well as attribute based access control. OIM ensures that any entitlements granted to a user based on policy get revoked when that policy no longer applies to that user (due to role or context changing).

OIM employs a sophisticated delegated administration system that uses logical organizations to control the visibility of data to the delegated administrators and a fine-grained authorization service based on Oracle Entitlement Server (OES) to control what each of these delegated administrators can perform within their realm of control.

OIM enables an accelerated application on-boarding functionality that enables administrators to onboard-disconnected applications without writing any code. As and when needed, such disconnected systems can then be easily converted to a connected provisioning solution using any of the available OIM connectors.

OIM also provides out of box integration with OIA to provide end-to-end role lifecycle management, integrated role engineering and closed loop remediation services.

Comprehensive Audit and Compliance Management

Identity Certifications

With advanced, risk-based analytics and easy to navigate dashboards, OIM offers a robust set of identity certification features that streamline the review and approval processes to effectively manage risk on an ongoing basis. Beyond understanding "who has access to what", in depth analytics can provide detailed graphical and actionable business context, as well as 360-degree views on how such access was granted and highlights outliers for individuals versus their roles. In addition, Identity Certifications promote business user friendliness via innovative capabilities such as the ability for reviewers to complete certifications offline. In addition, workflow capabilities that allow both Business and IT teams to collaborate on a single Identity Certification campaign are also included. Finally, the

solution offers closed loop remediation, which provides an automated way for reviewers to revoking improper access across target systems and includes alerts should remediation fail.

Account Reconciliation

OIM allows administrators to detect changes in access privileges originating outside the identity management system. These account changes are potentially rogue activities, and therefore trigger various remediation activities through OIM including exception approvals, certification cycles, and de-provisioning of entitlements or disabling accounts. Accounts can be linked in OIM either manually or by defining correlation rules. By combining denial access policies, workflows and reconciliation, an enterprise can execute the requisite corrective actions when such orphan accounts are discovered, in accordance with security and governance policies.

Policy Enforcement & Compliant Provisioning

OIM ensures that all provisioning triggered from it is compliant to various enterprise-IT Audit policies defined in OIA. It also integrates with ERP IT audit policy engines such as Oracle Application Access Controls Governor and SAP BusinessObjects GRC Access Control for ERP-level IT audit policy enforcement. This ensures that policy violations are caught while provisioning rather than "after the fact" in the detective controls.

Reporting

OIM 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?" and make this data available in reports through 30+ out-of-the-box reports. Oracle Identity Manager'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.

Contact Us

For more information about Oracle Identity Management, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2011, Oracle and/or its affiliates. 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 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 1010

Hardware and Software, Engineered to Work Together

ORACLE