

Oracle Identity Manager

An Oracle White Paper
December 2008

Introduction	3
Key Benefits	4
Features.....	5
Self-Service And Delegated Administration	5
Workflow And Policy.....	5
Password Management	7
Audit And Compliance Management	7
Integration Solutions	9
Oracle Identity Manager Architecture	10
SYSTEM COMPONENTS.....	12
Conclusion.....	13

Oracle Identity Manager manages user-access rights and privileges throughout the provisioning lifecycle and across heterogeneous IT environments.

INTRODUCTION

Today's enterprises are under ever greater pressure to shore up security, and meet regulatory and governance requirements, resulting in greater urgency to deploy identity management solutions based on the latest identity management technologies. Oracle Identity Manager, formerly named Oracle Xellerate Identity Provisioning, is a highly flexible and scalable enterprise identity management system that manages users' access privileges within enterprise IT resources. It helps to answer the critical compliance questions of "Who has access to What, When, How, and Why?"

Oracle Identity Manager's flexible architecture can handle the most complex IT and business requirements without requiring changes to existing infrastructure, policies or procedures. This hallmark flexibility also enables Oracle Identity Manager to excel at handling the constant flow of business changes that impact real-world identity management deployments. This flexibility is derived from the product's architecture, which elegantly abstracts core provisioning functions into discrete layers. Changes to workflow, policy, data flow, or integration technology are isolated within the respective functional layers, thus minimizing application-wide impact. In addition, Oracle Identity Manager is flexible because all configurations are done via its powerful user interface. The product does not rely on any scripting language for setup, configuration, or process modeling. These are some of the many reasons why Oracle Identity Manager is considered the most advanced enterprise identity management solution available. For detail on Oracle Identity Manager's architecture, please see *Oracle Identity Manager Architecture White Paper*, available from www.oracle.com.

Oracle Identity Manager's market-leading flexibility and scalability has been well documented in competitive shootouts such as the one featured in InfoWorld's October 10, 2005 issue. Oracle Identity Manager is managing one of the industry's largest provisioning implementations today, an implementation with more than 650 enterprise resources under management. This award winning deployment has received recognition by ComputerWorld, Digital ID World, Gartner, InfoWorld, NetworkWorld, and SC Magazine.

These factors, coupled with the unique advantages detailed in this paper make Oracle Identity Manager an ideal platform for any large-scale enterprise.

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 utilization of a common security infrastructure

Deploying self service features can help an enterprise increase user productivity, user satisfaction and operational efficiency.

FEATURES

Self-Service And Delegated Administration

Profile Management

Using Oracle Identity Manager's self-service interface, end users can view, manage and update their own profile data. This reduces administrative overhead and provides users with control over their identity profiles.

Request Management

Oracle Identity Manager's self-service interface allows end users to create provisioning requests for resources with fine-grained entitlements. Business approvers (e.g. team leaders, line managers, department heads, etc.) 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 costs.

Delegated Administration

Oracle Identity Manager features a highly flexible security framework that supports delegation of most administrative functions to any group and/or user. By moving administration points as close to the user as possible, an enterprise can achieve tighter control and better security, all the while increasing productivity. Delegated administration plays an increasingly important role as the already extended enterprise becomes more virtual and the service provider delivery model becomes more prevalent.

User Configurable Proxy

In addition to administrator defined delegation, Oracle Identity Manager also provides each user the ability to temporarily delegate approval tasks to a defined proxy. This user-defined proxy capability reduces the need for system reconfiguration and ensures continuity of business processes, uninterrupted by user's time away from the office.

Workflow And Policy

Policy Management

Oracle Identity Manager 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. Effective blending of role and attribute based policies is key to a scalable and manageable enterprise provisioning solution. In addition to an automated provisioning policy, Oracle

Use of workflow & policy to automate business and IT processes can lead to improved operational efficiency, enhanced security and more cost effective compliance tracking.

Identity Manager also supports a denial policy. 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 separation of approval and provisioning workflows. Approval workflow enables an enterprise to model its preferred or best-practice approval processes for managing resource access requests. Provisioning workflow enables an enterprise to orchestrate and automate IT tasks for provisioning resources with even the most complex provisioning procedures. Separation of the two types of workflow empowers business and IT process owners to manage most efficiently with minimum cross-process interferences. It also enables an enterprise to leverage existing workflows already deployed in systems such as help desk and HRMS. Oracle Identity Manager provides a workflow visualizer that offers a graphical representation of even the most complex workflow processes. This allows business users, administrators, and auditors to visualize task sequences, dependencies, etc. to understand the process flow.

Dynamic Error Handling

Oracle Identity Manager's error-handling capability provides IT staff with the ability to handle any exceptions that occur during the provisioning process. Everyday problems such as unavailable or offline resources no longer need to stop the entire provisioning transaction or cause it to fail. Business logic defined within the provisioning workflow offers customized failsafe capabilities within an Oracle Identity Manager implementation.

Guaranteed De-provisioning

When a user leaves the organization or her access is no longer required or valid due to a job change, 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 across all no-longer-required resources to minimize security risks, as well as to prevent paying for access to costly resources, such as data services.

Transaction Integrity

Provisioning automates a very important part of an enterprise's daily business. Based on embedded state management capabilities, Oracle Identity Manager provides the same level of transaction integrity required by other mission-critical enterprise 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 rollback to the last successful state or reroute to a different path, in accordance with pre-defined rules.

Real Time Request Tracking

In order to maintain better control over and provide improved visibility into all provisioning processes, end users and administrators can track request status in real time, at any point during a provisioning transaction.

Password Management

Research show over 80% of calls to IT help desk are password management related issue. Implementing a password management solution can result in quick and very quantifiable return on investment.

Self-Service Password Management

Oracle Identity Manager's self-service capabilities allow users to manage their own passwords across managed resources. In case a user forgets his password, Oracle Identity Manager can present customizable challenge questions to enable self-service identity verification and password retrieval. Research shows the bulk of help desk calls are related to password reset and lockout. This self-service capability easily pays for itself many times over through reduced help desk calls.

Advanced Password Policy Management

Oracle Identity Manager features very rich password policy management capabilities. Most best-practice password policies are supported out-of-the-box and are configurable via an intuitive user interface. Supported password complexity requirements include: password length, alphanumeric and special characters usage, upper and lower case usage, full or partial exclusion of username and historical passwords. Furthermore, Oracle Identity Manager allows the application of multiple policies per resource. For instance, less-privileged users may be subjected to a more relaxed password policy, whereas privileged administrators may be subject 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 enterprise is using Microsoft Windows' desktop-based password reset feature, Oracle Identity Manager's Active Directory (AD) Connector can intercept password changes at the AD server and subsequently propagate it to other managed resources in accordance with policies. Similar bi-directional password synchronization capability is offered in most Oracle Identity Manager Connectors for directory servers and mainframes.

Identity management is a key component of any enterprise wide audit & compliance solution. Oracle Identity Manager helps an enterprise to minimize risk and reduces the cost of meeting internal and external governance and security audits.

Audit And Compliance Management

Identity Reconciliation

One of Oracle Identity Manager's most powerful capabilities is the reconciliation engine. Reconciliation refers to the process by which Oracle Identity Manager "polices" the resources under its management. If it detects any accounts or changes to user access privileges affected outside of Oracle Identity Manager's control, it can immediately take corrective action, such as undo the change or notify

an administrator. The reconciliation engine also helps to detect and map existing accounts in target resources, enabling the creation of an enterprise-wide identity and access profile for each employee, partner or customer user.

Rogue/Orphan Account Management

A rogue account is an account created “out of process” or outside of the provisioning system’s control. An orphan account is an operational account without a valid user. These accounts represent serious security risks to an enterprise. Oracle Identity Manager can provide continuous monitoring of rogue and orphan accounts. By combining denial access policies, workflows and reconciliation, an enterprise can execute the requisite corrective actions when such accounts are discovered, in accordance with security and governance policies. Oracle Identity Manager can also manage the lifecycle of special service accounts, also known as administrator accounts, which have special life cycle requirements that extend beyond the lifecycle of an assigned user and across the lifecycles 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. 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. When combined with the transaction data generated and captured by Oracle Identity Manager’s workflow, policy, and reconciliation engines, an enterprise has all the required data to address any identity and access related audit inquiry. 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.

Attestation / Recertification Automation

Attestation, also referred to as recertification, is a key part of Sarbanes-Oxley compliance and a highly recommended security best-practice. Enterprises are meeting these attestation requirements today largely with manual processes based on spreadsheet reports and emails. These manual processes tend to be fragmented, are difficult and expensive to manage, and have little data integrity and auditability. Oracle Identity Manager offers a best-in-class attestation feature that can be deployed quickly to enable an enterprise-wide attestation process that features 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 reviewers’ actions are captured for future auditing needs. Reviewer actions can

optionally trigger corrective action by configuring Oracle Identity Manger's workflow engine.

Integration Solutions

A scalable and flexible integration architecture is critical for successful deployment of enterprise provisioning solution. Oracle Identity Manager offers a proven integration architecture featuring Adapter Factory and large assortment of pre-configured connectors for fast and low cost deployments. Today Oracle Identity Manger powers the largest known user provisioning solution with more than 650 targets systems under management.

Adapter Factory

Integrating most provisioning systems with managed resources can be a daunting task. Connecting to proprietary systems can often be near impossible. Oracle Identity Manager'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. Once connectors have been created, their definitions are maintained within the Oracle Identity Manager repository, creating self-documenting views. These views make extending, maintaining and upgrading connectors a manageable and straightforward process.

Pre-configured Connectors

For the most popular commercial applications and interface technologies, Oracle Identity Manager offers an extensive and rapidly expanding library of pre-configured connectors. With these connectors, an enterprise can get a head start on application integration. Each connector supports a wide range of identity management functions and uses the most appropriate integration technology recommended for the target resource, whether it's proprietary or based on open standards. These connectors enable out-of-the-box integration, but can be further modified using the Adapter Factory to work with each enterprise's unique integration requirements.

ORACLE IDENTITY MANAGER ARCHITECTURE

Oracle Identity Manager's architecture provides a number of compelling technical benefits when deploying a provisioning solution as part of an identity and access management architecture. Oracle Identity Manager offers the most flexible and scalable open architecture on the market.

Ease of Deployment

Leveraging its maturity in the provisioning market, 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 may be staging or production. The XML files can be used to archive and version configurations, as well as replicate integrations. The Deployment Manager offers great flexibility over what to import and export and identifies data object dependencies during both import and export steps. This flexibility makes it possible to merge integration work done by multiple people in-transit, and ensures the integrity of any migration.

Flexible and Resilient

Oracle Identity Manager can be deployed in single or multiple server instances. Multiple server instances provide optimal configuration options, in support of geographically dispersed users and resources, for increased flexibility, performance and control. Oracle Identity Manager's multi-server system implementations also provide fault tolerance, redundancy, fail-over and system load balancing. As deployments grow, moving from a single server to a multi-server implementation is a seamless operation.

Maximum Reuse of Incumbent 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 an organization's IT infrastructure. For example, if an implementation requires integrating with an existing customer portal, Oracle Identity Manager's advanced API offers 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 enterprise's specific needs.

Modular Architecture

Oracle Identity Manager makes it easy to keep up with the changing needs of a dynamic enterprise. Oracle Identity Manager's breakthrough technology separates what "needs" to be done from "how" it is actually done (called "abstraction"). This 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 "evolution without revolution" approach that allows IT to implement their provisioning system to fit today's requirements, and be assured that it 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 enterprise's ongoing evolution of processes and systems.

Built-in Audit and Compliance

Identity management is a key part of any audit and compliance solution. Thus, auditing and compliance capabilities need to be integrated into the core identity management architecture; it should not be an “add-on” or a “bolt-on” for the identity provisioning platform, or worse, be a separate product. Oracle Identity Manager is a fully integrated platform for identity provisioning and identity audit and compliance. An integrated application means once a resource is brought under management, the connection can be leveraged for both provisioning and compliance use, avoiding duplication of integration cost. An integrated application means the audit and compliance features need not be restricted to just reporting. It means no additional product integration effort is required to enable corrective actions as part of an audit and compliance process. For example, when using Oracle Identity Manager's attestation feature, a reviewer's reject action can directly trigger workflow to send notification or de-provision a user account. An integrated platform also means all identity and transaction data is at your fingertips, enabling an enterprise to demonstrate control and visibility to its auditors without lengthy reporting lag time.

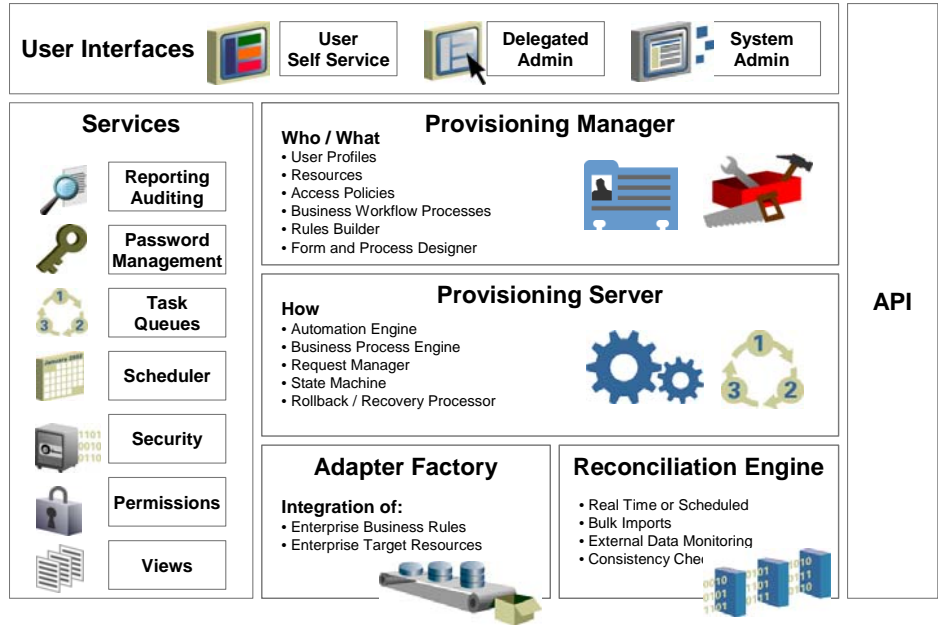
Standards-based

Oracle Identity Manager incorporates leading industry standards. For example, Oracle Identity Manager components are fully based on a J2EE architecture, so customers may 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 all its identity management products on a foundation of current and emerging standards. For example, Oracle is a Management Board Member of The 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).

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.



Oracle Identity Manager User Interfaces define and administer the provisioning environment. Oracle Identity Manager offers two feature-rich 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

ProvisionManager

ProvisionManager is where provisioning transactions are assembled and modified. The ProvisionManager maintains the “who” and “what” of provisioning. User profiles, access policies and resources are defined through the ProvisionManager, as are business process workflow and business rules.

ProvisionServer

ProvisionServer is Oracle Identity Manager’s run-time engine, which executes the provision process transactions as defined through the Design Console and

Figure 1: Oracle Identity Manager Functional Architecture maintained within the ProvisionManager.

Adapter Factory

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. The Adapter Factory allows administrators and subject matter experts to work at a higher level of abstraction by mapping the Oracle Identity Manager provisioning process directly to the target application's configuration requirements. Once mapped, the Adapter Factory will generate the necessary integration code. Modifications and extensions to adapters are accomplished by working with the integration map - not with the code.

Reconciliation Engine

Reconciliation Engine ensures consistency between Oracle Identity Manager's provisioning environment and Oracle Identity Manager managed resources within the enterprise. The Reconciliation Engine discovers illegal accounts created outside of Oracle Identity Manager. Reconciliation Engine will also synchronize business rules located inside and outside the provisioning system to ensure consistency.

CONCLUSION

Oracle Identity Manager is the most flexible and scalable enterprise user provisioning application available on the market. It powers some of the largest and most complex, award-winning identity deployments. Oracle Identity Manager helps an enterprise to reduce security risk, reduce the cost of compliance, and improve service level and end-user experience. Oracle Identity Manger should be a key component of every enterprise IT security architecture.

ORACLE FUSION MIDDLEWARE

Oracle Identity Manager
Dec 2008

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2006, 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 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 Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.