

# An Introduction to Oracle Identity Management

*An Oracle White Paper  
June 2008*

# An Introduction to Oracle Identity Management

## **INTRODUCTION**

Oracle Identity Management's best-in-class suite of identity management solutions allows enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources both within and beyond the firewall. You can now deploy applications faster, apply the most granular protection to enterprise resources, automatically eliminate latent access privileges, and address the growing list of regulatory and compliance mandates. Leverage the suite of products in their entirety or deploy individual components to meet your unique needs.

## **BACKGROUND**

Oracle introduced its first identity management product in 1999, with the general release of Oracle Internet Directory. Since then, the product portfolio has made tremendous strides through both organic and acquisitive growth. Oracle leads the industry with award-winning identity management offerings that constitute the most comprehensive solution offered by any vendor. Not only do customers get a complete end-to-end solution, they also benefit from proven best-in-class functionality. Oracle's Identity Management solutions have received industry-wide accolades and recognition as market leaders from major analysts such as Gartner, Forrester Research and Burton Group. Many of these reports can be found at: <http://www.oracle.com/corporate/analyst/reports/infrastructure/index.html>.

This paper is meant to familiarize the reader with some of the basic functional areas of identity management and introduce the Oracle products.

## FUNCTIONAL AREAS

While the identity management industry continues to expand with new products and capabilities, many of these technologies typically fall into one of three broad functional areas: directory services, identity administration, or access management.

*Directory services* are the key building blocks for most identity management platforms. This foundational layer consists of the LDAP directory itself, which holds the user identity data, including user names and passwords. Most enterprise applications leverage data stored in an LDAP directory. Since it is common for organizations to have more than one enterprise application, you will typically find they have more than one directory. Over time, identity data becomes widely distributed across the enterprise. Further, it is quite common for enterprise applications to need data that is stored in multiple directories. One approach the development organization can take to consume this distributed data is to use a metadirectory service, which allows you to synchronize data between directories. Another approach is to use a virtual directory, which provides a single directory view for the application to consume, while pulling in data from multiple other directories without the need to synchronize.

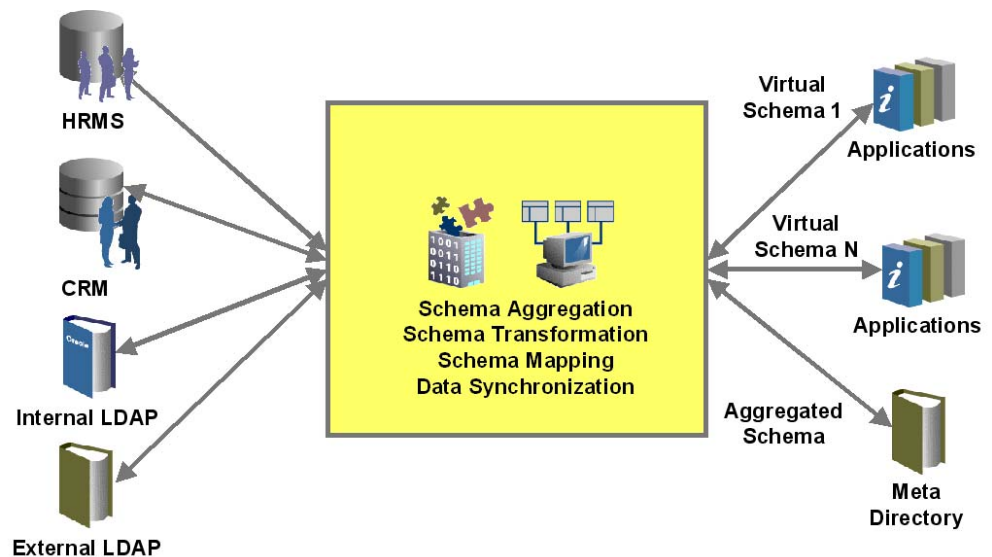


Figure 1. Directory Services

*Identity administration* is itself a broad functional area that encapsulates various activities such as user and group management, self-service, delegated administration and approval workflows. These capabilities are typically addressed by provisioning and enterprise role management technologies. If we think of the directory service as the foundational layer for holding identity data, we can think of identity administration as the area that manages the complete lifecycle of the identity data. We create and manage rules and workflows that automate the process of creating, deleting, or changing a user identity and its associated privileges in various applications. Further, an individual's ever-changing role or association in an organization can trigger these rules and workflows dynamically. While automation is a key benefit as we move away from manual processes, we still need to provide individuals the ability to self-service their own accounts and delegate certain of their responsibilities to others within their organization.

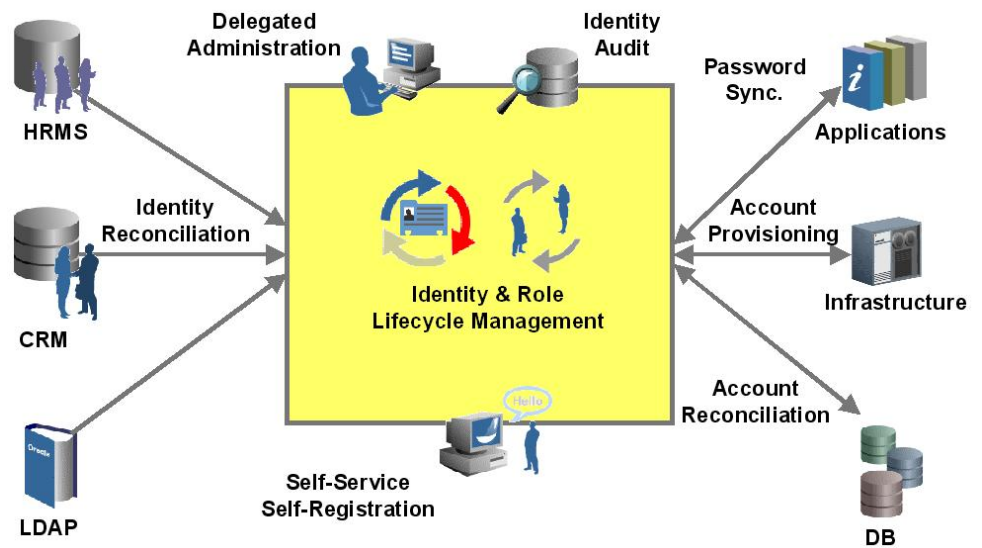


Figure 2. Identity Administration

*Access management* is the area where we control user access to enterprise resources, manage entitlements and fine-grained authorizations for enterprise applications, proactively prevent fraudulent activity and strengthen authentication security, and federate identities and user sessions across organizations. While identity administration manages the lifecycle of the identity data, access management is the guard at the door that determines which users get access to what information at what time, based on an ever-changing set of policies.

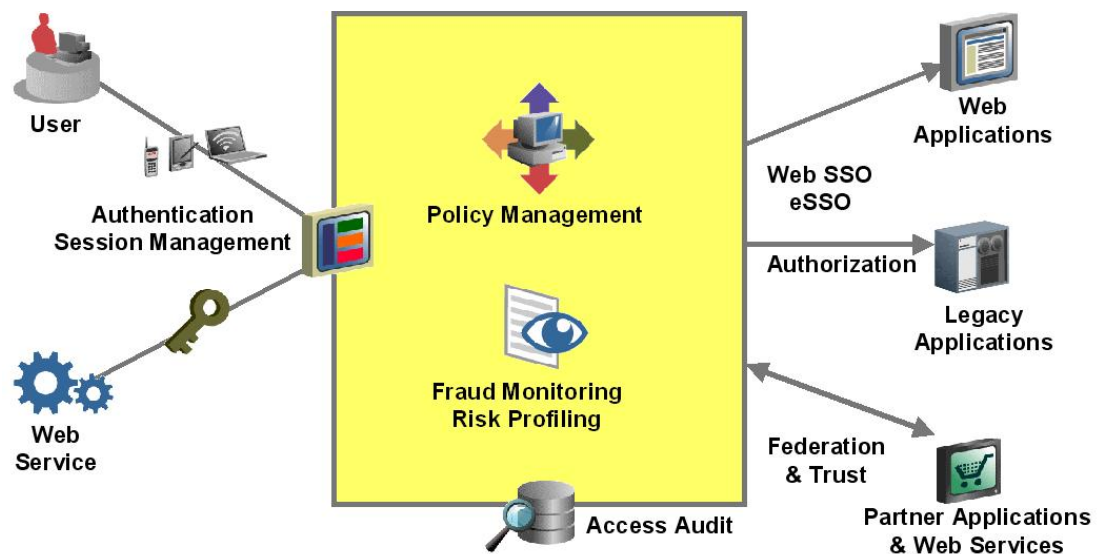


Figure 3. Access Management

## Directory Services

### Oracle Internet Directory

Oracle Internet Directory is an LDAP directory that leverages the scalability, high availability and security features of the Oracle Database. Oracle Internet Directory can serve as the central user repository for Oracle Identity Management deployments, or can serve as a highly scalable standards-based directory for the heterogeneous enterprise. Metadirectory functionality is provided through the Directory Integration Platform, thereby allowing users to synchronize data between Oracle Internet Directory and other third party directories.

### Oracle Virtual Directory

Oracle Virtual Directory is a flexible and secure service for connecting applications to existing user identity, such as directories and databases, without requiring changes to either the infrastructure or applications. Customers choose Oracle Virtual Directory to accelerate the deployment of directory-enabled applications, such as portals and single sign-on (SSO) systems. More specifically, Oracle Virtual Directory allows customers to solve specific problems around needing to unify multiple directories, allow LDAP access to databases or other proprietary identity data stores, improve directory server scalability, and provide enhanced security. Ultimately, Oracle Virtual Directory increases the reusability of your identity data, wherever it is stored, which reduces administration and integration costs.

## **Identity Administration**

### Oracle Identity Manager

Oracle Identity Manager is a highly flexible and scalable enterprise identity management system that centrally controls the lifecycle of user accounts and access privileges within enterprise resources. Oracle Identity Manager has out of the box integration with the most commonly deployed enterprise applications and infrastructure technologies. Additionally, Identity Manager ships with a graphical tool that allows you to integrate with other applications, should an out of the box integration not exist – as in the case where integration might be needed with home grown technologies.

### Oracle Role Manager

Oracle Role Manager is an authoritative role management solution, built using a scalable J2EE architecture. Oracle Role Manager provides a comprehensive feature set for enterprise role lifecycle management, multi-dimensional organization and relationship management. By using roles to abstract resources and entitlements,

Oracle Role Manager enables business users to define user access according to business policy, as well as review user's access rights in business terms. By involving the business users in the identity administration process, Oracle Role Manager brings scalability to identity related security and compliance processes.

## **Access Management**

### Oracle Access Manager

Oracle Access Manager delivers scalable access control for heterogeneous environments with an integrated, standards-based solution for authentication, web single sign-on, access policy creation and enforcement. Oracle Access Manager

supports all major web servers, application servers and directory services. It helps secure web, J2EE, and enterprise applications while reducing cost, complexity, and administrative burdens.

### Oracle Adaptive Access Manager

Oracle Adaptive Access Manager delivers superior protection for businesses and their customers through strong multifactor authentication security that can adjust dynamically based on the context of the user action as well as proactive, real-time fraud prevention. Oracle Adaptive Access Manager provides online applications with device-free, strong mutual authentication. Oracle Adaptive Access Manager also provides real-time risk scoring to identify potential fraud at multiple points in a transaction.

### Oracle Entitlements Server

As enterprises successfully gain control over their access management requirements, more are looking to centralize management of fine-grained authorization policies embedded within the applications themselves. New standards help make this feasible across vendor environments. Oracle Entitlements Server provides centralized, standards-based policy management and distributed policy enforcement across enterprise applications resulting in a more secure enterprise environment, improved ease of administration, consistent policy enforcement and improved compliance.

### Oracle Identity Federation

Building federated user communities that span company boundaries represents an opportunity for businesses to implement consumer product cross-selling strategies, streamline supplier access to their extranet applications, and respond quickly to organizational changes such as mergers and acquisitions. Oracle Identity Federation makes these kinds of interactions possible with a multi-protocol federation server implementing standards-based web technology. Oracle Identity Federation enables organizations to securely link accounts and identities across security boundaries without a central user repository or the need to synchronize data stores. Oracle Identity Federation provides an interoperable way to implement cross domain single sign-on for vendors, customers and business partners without the overhead of managing, maintaining and administering their identities and credentials.

### Oracle Enterprise Single Sign-On

Oracle Enterprise Single Sign-On provides users with unified sign-on and authentication across all their enterprise resources, including desktops, client-server, custom and host-based mainframe applications. Users can authenticate themselves once with a single credential – such as a username/password, smartcard, or biometric device – and then have secure access to all of their enterprise applications without needing to sign in again.

### Oracle Authentication Services for Operating Systems

Unix and Linux servers are widely deployed across most enterprise organizations and typically hold company sensitive data. Each of these systems can provide their own local account management, but this leads to administrative challenges not the least of which are potential security breaches due to inconsistent security policies being applied. Oracle Authentication Services for Operating Systems provides these Linux and Unix environments a centralized, secure and seamless user authentication infrastructure. Now access to operating systems can be centrally managed, enforced, and audited, providing a true end-to-end security service.

### Oracle Web Services Manager

Companies worldwide are actively implementing service-oriented architectures (SOA), both in intranet and extranet environments. While SOA offers many advantages over current alternatives, deploying networks of web services still presents key challenges, especially in terms of security and management. Oracle addresses SOA security and management with a standards-based solution known as Oracle Web Services Manager. Oracle Web Services Manager is a J2EE application designed to define and implement web services security in heterogeneous environments, provide tools to manage web services based on service-level agreements, and allow the user to monitor runtime activity in graphical charts. Oracle Web Services Manager can be used by developers to test security on individual web services at development time or systems administrators to implement company-compliant security leveraging identity management infrastructures in production environments.

## **IDENTITY MANAGEMENT 2.0**

While the industry tends to still group identity management technologies into the three functional areas as described within this paper, we are starting to see a new generation of functionality emerge. “Identity Management 2.0” is being driven by: a new era of governance, risk, and compliance; increasingly sophisticated online attacks; and corporate consolidation from merger and acquisition activities. The core platform of identity management capabilities such as authentication,

authorization, user provisioning, password management, and the like has provided us with a base for improving security and automating manual processes to drive down operational costs. Identity Management 2.0 extends the core platform to provide stronger forms of authentication, risk-based authorization and fine-grained entitlements, user provisioning based on roles and relationships, as well as the ability to virtualize identities, all in effort to address the next generation of requirements and threats.

## **CONCLUSION**

Oracle is widely recognized as the leader in the identity management space – this recognition comes from industry analysts, press, and most importantly our growing customer base. Identity management is a strategic area of focus for Oracle – in addition to providing these best of breed technologies to our global customers, Oracle Identity Management also underpins the next generation of Oracle Fusion Applications. As the identity management market continues to evolve, Oracle will continue to innovate through its leadership in the standards community, as well as through close collaboration with its customers.

With Oracle Identity Management, customers can fulfill all of their identity management requirements from a single vendor, one that offers leading products and capabilities. This means less time spent integrating disparate components, a single point of contact for support, a single license contract, and the backing of the world's largest enterprise software company.

For more information, visit [www.oracle.com/identity](http://www.oracle.com/identity)



**An Introduction to Oracle Identity Management**

**June 2008**

**Author:**

**Contributing Authors:**

**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 © 2008, 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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. 0408**