

Identity Management Solutions for Oracle E-Business Suite

An Oracle White Paper
January 2008

NOTE:

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Identity Management Solutions for Oracle E-Business Suite

EXECUTIVE OVERVIEW

In today's fast-paced business environment, companies are increasingly turning to automating business operations using a range of enterprise applications such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Supply Chain Management (SCM). While these applications help to streamline businesses processes, if not properly managed they can also create an environment where user and access information is fragmented and difficult to manage centrally. Further compounding the problem is the business-driven need to make internal applications available to partners and customers while assuring the security of critical corporate resources.

This paper outlines how Oracle Identity Management solutions enable organizations to meet these challenges working in conjunction with Oracle E-Business Suite.

By addressing the cost and complexity of securing disparate and heterogeneous IT environments existing in your company and at your partners – customers, suppliers, external service providers – Oracle Identity Management enables you to maximize the value of your investment in Oracle E-Business Suite applications.

INTRODUCTION

Enterprise Resource Planning (ERP) applications have become a ubiquitous element in modern corporate strategy to automate business processes with software solutions. From benefits, payroll, and performance management to recruiting and talent management, training, and employee self-service, many critical business processes surrounding lifecycle events for all members of the enterprise are automated and managed by an organization's ERP solution.

However for most companies, process automation and quality data management for personnel lifecycle events ends where the ERP application ends. The business processes outside of ERP that are concerned with "identities" – role and access management, risk management and compliance, resource and account provisioning, authentication and authorization – also have a critical impact on a company's business yet more often than not these processes remain labor intensive, expensive, inefficient and error-prone. They are not scalable or easily distributed and are inherently difficult to secure and to audit.

Consider the following questions:

- How long does it typically take for a new employee to be provided access to the applications and systems necessary for his or her job?
- Are employees and contractors given the correct access according to policy? Is their access changed as their roles and responsibilities within the company change? Is their access ever revoked when they leave the company?
- Are key applications made available to partners and customers? Is this access extended while assuring the security of critical corporate resources.?
- How easy is it to generate reports at the requests of auditors to show who has access to what in your critical business applications?

Relying on traditional processes and systems to manage the challenges of granting and maintaining such access for thousands of users connecting to thousands of systems, applications and devices creates far-reaching problems for even the smallest of organizations. The result is that most companies have no idea of the answers to these questions, and what's worse, no easy way of finding out.

While ERP applications help to streamline businesses processes, if not properly managed, they can also create an environment where user information is fragmented and difficult to manage centrally.

IDENTITY MANAGEMENT CHALLENGES

This situation results in a number of business challenges:

Increased costs

No single source of truth for identity information for persons of interest (inclusive of user groups such as employees, contingent workers, partners, etc.) usually exists. Since applications have no reliable means of locating the data needed to make important decisions such as personalization, authentication, and authorization, local application administrators end up manually collecting and managing such information for themselves. The burden of password management falls upon system administrators, who are inundated with requests for password resets and changes.

Once new identity and organization events occur, the changes take weeks or months to propagate through all of the relevant systems that need to consume this information. Updates to data are necessarily manual and therefore error-prone. The maintenance of all of this duplicate data with multiple, overlapping processes represents an enormous hidden cost for both the business and IT and a significant source of frustration for the IT staff.

Increased security risks

The security picture that emerges from such a situation is grim. Administrators need to cope with complex and error prone manual processes for managing user privileges across disparate systems. Users have to maintain far too many passwords, which increases the likelihood that they will be managed in an insecure manner. As employees move from position to position, or as contractors leave one organization and rejoin another, access privileges are not changed to reflect these changes in business function and responsibilities. Privileges are therefore accumulated over time, leading to a classic security hole.

Compliance and audit risks

Many organizations are subject to independent audits of their IT systems as part of a wider 'governance' imperative. These audits can be internally imposed, for example in the government sector, or externally imposed, for example by regulations such as Basel II, Sarbanes Oxley, EU Privacy Directives, etc. At a minimum, such audits expect an organization to be able to demonstrate that only the appropriate people have access to specific resources (applications, information, services).

In order to demonstrate compliance businesses need to show that access controls have been in place and working as required. Without a centralized process in place to manage access policies and without an infrastructure designed to assign and track user entitlements in applications and systems, most companies have to start from scratch for each audit. This "pick up all the pieces and put them back together" approach is not only time-consuming and costly, but is increasingly causing organizations to fail standards of compliance that are currently being demanded by auditors.

Lack of business agility

Organizations must derive as much value as possible from their existing IT investments while at the same time compete more effectively by adding new business functionality quickly and at reasonable cost. One way of doing this is to modularize pieces of business functionality by moving to a Services-Oriented Architecture (SOA). A major obstacle to effectively implementing SOA is that user information is spread across applications and systems. New services can be introduced more quickly and more securely if user management, authentication, authorization, and provisioning are core services that are made available to service developers and therefore do not need to be duplicated on a case by case basis.

Oracle leads the industry with award-winning Identity Management offerings that constitute the most comprehensive solution offered by any vendor.

ORACLE IDENTITY MANAGEMENT SOLUTIONS

Oracle Identity Management solutions addresses these business challenges by helping enterprises

- Maximize productivity by ensuring that new employees have the tools and information they need to do their jobs on day one.
- Mitigate security risks by ensuring that proper access is enforced through a consistent set of security policies that are linked to business operations.
- Reduce the cost of compliance and the risk of audit by establishing a centralized and comprehensive view of people, roles, and privileges that certifies who has access to what, granted by whom, and when
- Lower operational costs by helping companies manage their environments efficiently through centralized user management, delegated administration, self-service password resets and account requests, automated provisioning and identity federation
- Enhance business agility through a standards-based and flexible integration framework that securely links partners, suppliers, customers and virtual teams

Oracle has a unique approach to Identity Management – it provides enterprise-wide solutions that support the heterogeneous IT environments prevalent in most organizations. 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 Access Manager

Oracle Access Manager is a state-of-the-art solution for centralized identity administration and access control. Oracle Access Manager delivers the functionalities of web single sign-on, access policy creation and enforcement, user

self-registration and self-service, delegated administration, password management, and reporting and auditing.

Oracle Adaptive Access Manager

Oracle Adaptive Access Manager is a comprehensive solution for pure web-based strong authentication and proactive, real-time fraud prevention.

Oracle Identity Federation

Oracle Identity Federation is an industry-leading federation solution providing a self-contained and flexible multi-protocol federation server deployable with existing identity and access management systems. Oracle Identity Federation is Liberty Alliance certified for Liberty ID-FF and SAML 2.0.

Oracle Web Services Manager

Oracle Web Services Manager is a comprehensive solution for adding policy-driven best practices to existing or new web services, and provides the key security and management capabilities necessary to deploy Service-Oriented Architectures across applications.

Oracle Role Manager

Oracle's Role Manager provides unique features to speed the process of role discovery and to deliver automated enterprise role management solutions. Oracle Role Manager serves as a centralized role management repository and synchronizes roles and polices with privileges in target systems.

Oracle Identity Manager

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 provides the functionalities of identity administration, approval and request management, policy-based entitlement management, technology integration, and audit and compliance automation..

Oracle Identity Manager includes a library of pre-configured adapters that support applications such as Oracle E-Business Suite, Peoplesoft, Siebel, SAP, IBM Lotus Notes, and many others.

Oracle Virtual Directory

Oracle Virtual Directory allows you to rapidly deploy secure directory enabled applications by providing a real-time, virtual view of identity data from any data-store including directories, databases and Web Services without synchronization. With Oracle Virtual Directory, you can logically join identity attributes stored in multiple data-stores as well as prioritize requests to back-end directories on a per-server or per-connection basis, to maximize the native directory's processing potential.

Oracle Internet Directory

Oracle Internet Directory is an LDAP v3 service that combines the mission-critical strength of Oracle's database technology with the flexibility and compatibility of the LDAP v3 directory standard. Supporting heterogeneous environments, Oracle Internet Directory can be synchronized against third party directories including Microsoft Active Directory, SUN Java System Directory Server, Novell eDirectory and OpenLDAP.

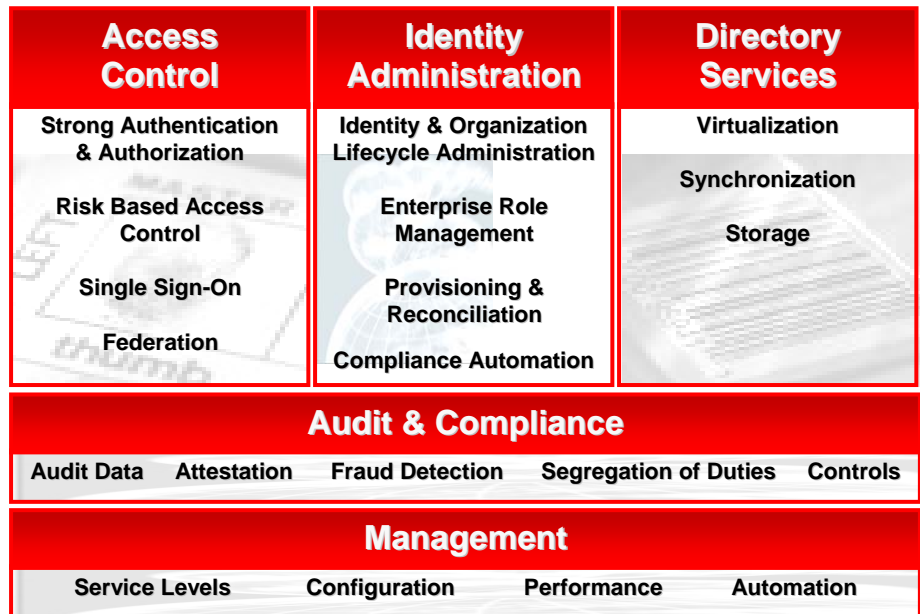


Figure 1. Oracle's Comprehensive Identity and Access Management Solutions

ORACLE IDENTITY MANAGEMENT FOR E-BUSINESS SUITE

Let's look at a few solutions in depth to see how Oracle Identity Management products can be used to deliver real-world solutions for Oracle E-Business Suite.

Access Management for E-Business Suite

With the introduction of Oracle Access Manager and Oracle Virtual Directory, existing E-Business customers can establish a single, comprehensive authentication, authorization, and auditing infrastructure that can protect all of the web-based applications in their environment (Figure 1).

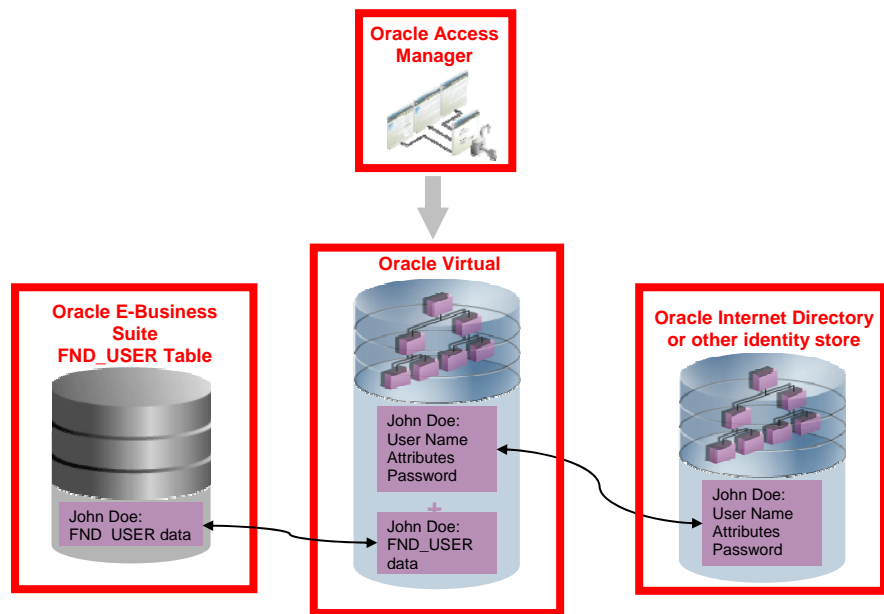


Figure 2. Oracle Access Manager working in conjunction with Oracle Virtual Directory

Authentication

Using agents on a variety of web platforms such as web servers and reverse proxy servers, Oracle Access Manager (OAM) can control all access requests and, based on centrally stored and managed policies, challenge the end user for authentication according to the required security level. Delegated administrators can easily maintain enterprise security policies by making use of pre-configured authentication types such as form-based login, smart cards, SecurID tokens, one-time passwords or biometrics to protect the resources at the appropriate level. OAM integrates directly with the Oracle Single Sign-On (OSSO) capabilities offered with the Oracle E-Business Suite. This provides a seamless user experience for single sign-on.

Authorization

Oracle Access Manager also provides a central policy store for authorization of users to applications, protecting HTTP, J2EE and other resource types. The authorization policies are enforced by standard agents as well as modules integrated with application servers. For fine-grained entitlement and application specific permissions, Oracle Identity Manager can be used to provide role and profile information to E-Business Suite, so that it is able to enforce the right application access once the Oracle Access Manager has established the session and completed the initial user authorization.

Auditing

Oracle Access Manager provides master audit rules for identity administration, policy management, and access events. The auditable events include authentication success/failure, and authorization success/failure; and each audit trail entry can be

configured to capture various details about the event, such as user profile information, the network where the request originated, on which web server, at what authentication level, etc. In addition to master audit rules, individual audit rules can be enforced to capture additional information as required by each protected application. Thus, all roles, permissions and access events can be audited for E-Business Suite and for all other applications managed by Oracle Access Manager.

User Provisioning Driven from E-Business Suite

Oracle Identity Manager (OIM) is a robust provisioning solution that works with E-Business Suite and heterogeneous third-party systems, and provides the management activities, business processes, and technologies governing the creation, modification and deletion of user access rights and privileges across an organization's IT systems. By automating these activities, companies gain better control over user access rights, enforce organizational security policies and ensure adherence to regulatory standards. Working in conjunction with Oracle Role Manager, it offers the industry's only integrated and automated role-based provisioning solution.

For example, this allows an HR application such as E-Business Suite HRM to be the primary entry point for establishing, changing and removing access rights for employees. Changes made in the HR system are automatically synchronized in the Corporate Directory or other authoritative identity repository.

Similarly, Oracle Identity Manager automates the process of provisioning users with IT resources across heterogeneous business policies and managed platforms. It connects users to the resources they need to be productive ("user on-boarding"), and revokes unauthorized access ("user off-boarding") to protect proprietary information and enhance security. As change occurs in your organization – employees are promoted, change locations, gain new job responsibilities, and so on – they automatically gain or lose access based on changes in roles, ensuring that they are granted the right access at the right time.

As shown in Figure 3 below, Oracle Identity Manager provides two connectors to Oracle E-Business Suite:

- An Employee Reconciliation connector pulls newly-created employee and contractor records from the EBS HR store and creates identities from them. This process is known as Trusted Source Reconciliation.
- Once the identity is created, the User Management connector can be automatically invoked using OIM access policies. This connector provisions EBS accounts along with their responsibilities. It also links this newly-created account record with the corresponding employee record so that EBS applications can leverage the additional employee data if needed. Additionally, existing EBS accounts can be matched to OIM identities using a process called target resource reconciliation.

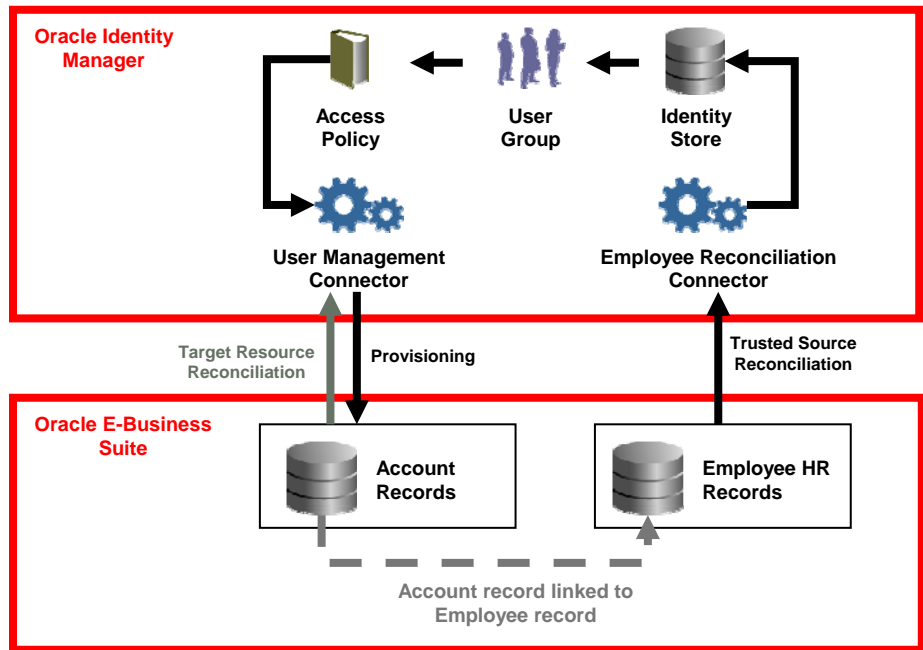


Figure 3. Oracle Identity Manager Connectors for E-Business Suite

In order to automate provisioning to applications outside of the E-Business Suite, Oracle Identity Manager offers an extensive and rapidly expanding library of pre-configured connectors which are used to automate the provisioning and de-provisioning of user privileges across a wide array of applications. Each connector supports a range of identity management functions and uses the most appropriate and supportable integration technology recommended for the target resource. These connectors enable out-of-the-box integration, but can be further modified using an ‘Adapter Factory’ integration generator to suit each enterprise’s unique integration requirements. Agent-less connectors are used wherever possible, reducing support and maintenance costs by avoiding installation of software on target systems.

Attestation for E-Business Suite Entitlements

Oracle provides a common framework for attestation across the entire Identity Management infrastructure. Attestation is a process for reviewers to verify the entitlements that users have on target systems. Attestations may be scheduled or manually initiated. Responsibility to perform regular reviews and attestation of user entitlements within E-Business Suite and other enterprise applications can be assigned to individuals or groups of participants. User-centric or application-

centric reviews may be conducted. All events are recorded and are reportable, allowing attestation processes (Figure 4) to be automated and compliance measured.

Oracle Identity Manager automates attestation scheduling, notification, supply of data to be audited, execution, auditing and reporting for all integrated applications or external entities.

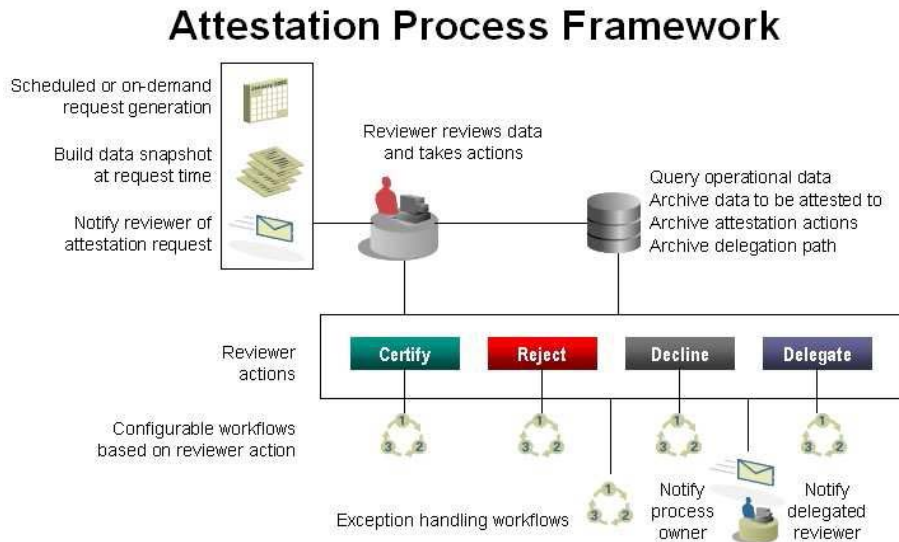


Figure 4. Attestation Process Framework

Looking Forward

Oracle is in the process of certifying new deployment approaches for Oracle Identity Management products that will make the integration with Oracle E-Business Suite version R12 even easier, and add new capabilities as well. Oracle Access Manager will integrate directly with E-Business Suite, removing the need to deploy and manage the native OSSO. Likewise, the new Oracle Identity Manager connectors will enable quicker and easier synchronization of identity information within Oracle E-Business Suite deployments and to other identity stores, such as Microsoft Active Directory. This unique approach will allow organizations to realize rapid return on investment (ROI) and significantly reduce the total cost of ownership (TCO).

Oracle's new product for strong authentication and risk management, Adaptive Access Manager, will also support an out-of-the-box integration with Oracle E-Business Suite. Oracle Adaptive Access Manager (OAAM) provides superior protection for businesses and their customers through strong multifactor authentication security and proactive, real-time fraud prevention.

Companies who grant their employees, partners, or customers remote access to E-Business Suite need to protect these access points with strong authentication. OAAM provides a powerful set of next-generation strong authentication tools that ensure that only authorized individuals can gain access to critical transactions and data. On top of this added security, OAAM conducts risk analysis and scoring at authentication and in session to verify users by their device, location, and behavior. This real-time scoring is used to authorize, deny, or put on hold suspicious online logins and transactions, preventing fraudulent activity before it has a chance to do any damage.

Key Oracle Differentiators in Identity Management:

- **“Application-Centric”.** Oracle Identity Management solutions are integrated to work seamlessly with your Oracle E-Business Suite applications, helping you achieve the benefits of Identity Management more quickly with less risk and cost. Oracle Identity Management solutions also integrate out-of-the-box with other leading applications and infrastructure components, providing a common layer of security and control across your entire environment.
- **Complete, unified solution.** The Oracle Identity Management suite is a complete and integrated set of best-of-breed components that can be deployed individually and in tandem. It is the only suite in the marketplace with an integrated Enterprise Role Management solution.
- **Proven in the real world.** The solutions are proven for large-scale deployments, and leverage Oracle’s expertise in providing large-scale information solutions for the world’s largest organizations. Oracle Identity Management solutions enjoy a broad and referenceable customer base.
- **Best long-term investment.** This breadth and depth offers the best long-term investment for a company’s Identity Management strategy. Oracle is committed to its strong support of open standards and the “hot-pluggable” strategy.

CONCLUSION

Oracle leads the industry with the most complete suite of Identity Management solutions. Built on an open-standards architecture, Oracle Identity Management supports heterogeneous environments ensuring interoperability with multiple IT systems, a key requirement for today’s leading companies.

Oracle Identity Management solutions integrate out-of-the-box with your E-Business Suite applications, offering a unique set of capabilities that:

- Maximize productivity by ensuring that new employees have the tools and information they need to do their jobs on day one

- Increase security and compliance by ensuring that user access is based on business policy
- Reduce administration costs and increase the security posture of the organization by automating employee and contractor on-boarding, transfer, and off-boarding processes
- Minimize the total cost of compliance and reduce the risk of a failed audit by providing accurate documentation of who has access to what, granted by whom, and when



Identity Management Solutions for Oracle E-Business Suite

January 2008

Author: Steve Wolford

Contributing Authors: Stephen Lee

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 © 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 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.