

An Introduction to Oracle COREid Access and Identity

An Oracle White Paper
December 2005

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.

An Introduction to Oracle COREid Access and Identity

INTRODUCTION

Leading organizations increasingly rely on identity management solutions to increase regulatory compliance, cut operational costs and improve application delivery. A strong identity management foundation requires integrated technology for managing user lifecycles, securely storing and administering profile data, and controlling application access based on these profiles.

With the acquisition of Oblix and the integration of Oblix's product set into the Oracle Identity Management products, Oracle delivers a comprehensive solution for each of these areas. Oracle COREid Access and Identity is in deployment at many of the largest companies in the Global 1000, and powers many of the largest portals in the world. Companies rely on COREid Access and Identity to bring security, administrative control, and increased visibility to portals, extranets and intranets deployed on multiple vendor products and platforms.

COREid Access and Identity has been available since 1996, and delivers critical functionality for access control, single sign-on, and user profile management. This paper describes the main components and functions of Oracle COREid Access and Identity. Next, we describe the audit reporting framework of COREid Access and Identity and its ability to support heterogeneous vendor environments. Finally, we describe how Oracle COREid Access and Identity interoperates with OracleAS Single Sign-On, Oracle's authentication service for Oracle applications.

COREid ACCESS

COREid Access, the access management component of COREid Access and Identity, includes WebGate, Access Manager and Access Server.

Access Manager

COREid Access Manager is a graphical tool for creating and managing access policies, setting up resources to be protected, and simulating user access to ensure correct policy functionality.

Oracle COREid Access is the only policy-based access management solution that is heterogeneous and pre-integrated with Oracle technology stack.

Oracle COREid Access and Identity includes user self-service, delegated administration, personalization and audit capabilities.

Access Server

COREid Access Server is a standalone software server that enforces access policies on Web and non-Web resources. The Access Server can be deployed in a single or clustered (load balancing/failover) configuration, and provides dynamic policy evaluation as users access Web applications. It also provides authentication, authorization, and auditing services.

Oracle COREid Access supports biometric and two-factor authentication.

Authentication Plug-ins

COREid Access provides a plug-in API for integrating a variety of authentication methods and devices. Support for smart cards such as SecurID is included out of the box. With the plug-in API, customers can extend COREid to support nearly any form of authentication possible, including biometrics and two-factor authentication.

COREid IDENTITY

COREid Identity provides key identity administration functions to directory administrators. Customers that deploy large-scale portals or extranets, with hundreds of thousands or millions of users, find that standard administrative tools break down under this type of load. The only way to scale user data stores (be they LDAP or relational databases) is to bring special-purpose features such as delegated administration, dynamic group management, and user self-service and self-registration. Each of these functionalities of COREid Identity is described below.

Delegated Administration

When a user directory is scaled to thousands or millions of users, it becomes impossible for a centralized administration team to manage the constant profile changes that occur throughout the day. Firms at this scale would have to employ dozens of directory administrators to keep up with the load. A much better way to handle this is through delegated administration, where responsibility for managing a group of users is pushed out to the various group administrators. For example, if a manufacturer operates a supplier portal for a thousand suppliers, the manufacturer might delegate responsibility for users in each supplier firm to an administrator at each supplier. The result is distributed work, more accurate data, and administrative scalability.

Oracle COREid Identity delivers delegated administration, essential for supporting large user populations.

COREid Identity has the most flexible and scalable delegated administration functionality in the market today, proven in production in many of the largest portals in the world. In fact, COREid Identity's delegated administration features are so strong that many customers who have already purchased access control solutions from another vendors have chosen to deploy COREid Identity for the delegated administration abilities.

Oracle COREid Access and Identity includes powerful and flexible authorization features such as dynamic groups and attribute access control.

Dynamic Group Management

A very useful and common identity management need is the ability to assign users to groups, for better access control and usage analysis. However, assigning large numbers of users to static groups does not scale well. A better approach is to use dynamic groups based on user attributes. For example, in a wireless phone company's customer portal with millions of users, a dynamic group might be called "SMS users" containing all customers who currently have SMS messaging activated for their accounts. Users in this group would be automatically granted access to additional support web pages. Since customers may continually activate and deactivate SMS messaging, it would be impractical to assign users to this group manually. COREid Identity's dynamic group management functionality can be used to assign and de-assign users to the "SMS users" group automatically based on profile attributes. As a customer activates SMS messages in her account, a flag would be activated in her directory profile, and COREid Identity would instantly include this customer in the group.

User Self-Service/Self-Registration

Allowing users to manage their own profiles also enhances administrative scalability. COREid Identity's out-of-the-box self registration screens enable users to add themselves to a directory without administrative intervention. Self-registration can use COREid Identity's workflow capability to ensure that controls and processes are enforced as users add their profiles. COREid Identity also allows users to change their attributes, within the access levels granted. For example, some users may be allowed to update their own phone numbers but not their titles. Managers of these employees may change titles but not their salary, and so on. COREid Identity supports unlimited access control flexibility for user attributes, and also links workflow to these changes. The result is increased user power and flexibility, all under the desired level of administrative control.

AUDIT REPORTING

For audit reporting, COREid Access and Identity includes a reporting framework, so that all security and profile management activity can be logged to a centralized relational database. Auditors now demand significant proof of compliance with regulations and internal policies, and administrators also wish to analyze security and identity operations for holes. Pre-built reports are available for the most common audit functions, including:

- Authentication statistics (success/failed rates across all COREid Access Servers)
- Authorization statistics (success/failed rates across all COREid Access Servers)
- Failed authorizations (by user)
- Failed authorizations (by resource)

Oracle COREid Access and Identity can support compliance efforts by logging security and profile management activity to a centralized relational database.

- Access testing
- Group history (all changes to all group profiles)
- Identity history (by user)
- Locked-out users
- Password changes (in a particular interval of time)
- Users created/deactivated/reactivated/deleted
- User profile modification history (for all users)
- Deactivated users report
- Workflow execution time

Oracle COREid Access integrates seamlessly with a number of third party web servers, application servers, directory servers and packaged applications.

HETEROGENEOUS SUPPORT

COREid Access and Identity includes many integration agents for managing and securing applications running on a variety of platforms. These integration components include out-of-the-box agents for all leading Web servers, application servers, and portal servers, running on multiple platforms.

COREid WebGates and AccessGates plug into third-party and custom infrastructure products to intercept requests and apply COREid access policies. WebGates are pre-built web server agents, while an Access SDK enables customers to build their own AccessGates for custom applications, broadening the reach of COREid's policy management and enforcement. No other identity vendor provides this level of breadth, covering multiple versions, products, and operating systems to protect real-world production environments.

Oracle COREid Access and Identity is fully interoperable with OracleAS Single Sign-On, providing Oracle customers with single sign-on to all their enterprise applications.

INTEROPERABILITY WITH ORACLE SINGLE SIGN-ON

Oracle COREid Access and Identity is fully interoperable with OracleAS Single Sign-On, Oracle's built-in authentication service for Oracle applications. This means that Oracle customers using Oracle Portal, Oracle Collaboration Suite, Oracle E-Business Suite Release 11i, or other Oracle applications can deploy Oracle COREid Access and Identity to provide a single point of access control, and user single sign-on, or all of their enterprise applications.

CONCLUSION – ORACLE'S COMMITMENT TO PRODUCT SUPPORT

While Oracle works towards creating a new generation of integrated product offerings, we are committed to the continued support for both product lines. As upgraded products become available, we will work with our customers to ensure a smooth transition from the existing products.

With the introduction of COREid Access and Identity Oracle provides the most comprehensive identity management solution on the market, covering full lifecycle management of user identity information, from creation, to usage, to reporting, to deletion. In conjunction with Oracle Internet Directory and the Oracle Identity

Management platform, COREid provides a complete solution for managing identities across both Oracle and non-Oracle platforms and applications.

ORACLE FUSION MIDDLEWARE

An Introduction to Oracle COREid Access and Identity
December 2005

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 © 2005, 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.