

Oracle Identity Management Concepts and Architecture

*An Oracle White Paper
December 2003*

Oracle Identity Management Concepts and Architecture

Introduction	3
Identity management	3
What is Identity Management?	4
Identity Management System Components	4
Oracle Identity Management Overview	5
Oracle Identity Management Objectives.....	7
Oracle Identity Management Concepts and Architecture.....	8
Identity Management Concepts.....	8
Integrating Application Security with Identity Management.....	8
Identity and Application Provisioning Lifecycle	10
Administrative Delegation	11
Identity Management Integration with Oracle Products	11
Conclusion.....	13

Oracle Identity Management Concepts and Architecture

INTRODUCTION

Identity management is the process by which application user identities are defined and managed in the enterprise environment. Specifically, identity management describes the process by which:

- User identities are provisioned and coordinated
- User account provisioning is automated
- User roles, privileges & credentials are managed
- Administrators delegate responsibility
- Administrators deploy applications easily & securely
- Users self-manage their preferences & passwords
- Users have single sign-on access

An integrated identity management infrastructure helps enterprises perform these operations efficiently, therefore reducing administration costs and enhancing the end user experience while improving application security.

This white paper is intended for those planning an Oracle Identity Management deployment, as well as for people seeking an overview of identity management in the Oracle environment. It describes identity management, the essential components of an identity management infrastructure, and provides an overview and objectives of Oracle's identity management infrastructure for the enterprise environment. Next, concepts such as the role of identity management in application security and the identity and application provisioning lifecycle are described, as well as the topic of user administration in a distributed environment. Finally, this white paper examines how Oracle products are engineered to leverage the identity management infrastructure.

IDENTITY MANAGEMENT

This chapter introduces the concept of identity management, and the major components of an identity management system. Next it describes the Oracle

Identity Management infrastructure as well as objectives for Oracle Identity Management deployment.

What is Identity Management?

An **Identity** is the set of attributes that uniquely identifies a network entity. A network entity can have many different accounts that it uses to access various applications in the network.

These accounts can be identified by these applications by different attributes of this entity.

For example, a user can be known in the e-mail service by his or her e-mail ID, whereas that same user can be known in the human resource application by his or her employee number. The global set of such attributes constitutes the identity of the entity.

Identity management is the process by which various components in an identity management system manage the security life cycle for network entities in an organization, and most commonly refers to the management of an organization's application users. Steps in the security lifecycle include account creation, suspension, privilege modification, and account deletion.

The network entities managed can include devices, processes, applications, or anything else that interacts in a networked environment. Entities managed by an identity management process can also include users outside of an organization, such as customers, trading partners, or Web services.

By using an identity management system, an enterprise can:

- Reduce administration costs through centralized account management and automated tasks
- Accelerate application deployment by enabling new applications to leverage the existing infrastructure to provision user accounts and privileges
- Improve the user experience by allowing rapid application access to new users
- Improve security and usability by centrally managing user passwords and security credentials and customizing applications to leverage centralized authorization and policy information

Identity Management System Components

A complete identity management system includes the following components:

- A scalable, secure, and standards-complaint directory service for storing and managing user information
- A provisioning framework that can either be linked to the enterprise provisioning system, such as a human resources application, or operated in standalone mode
- A directory integration platform that enables the enterprise to connect the identity management directory to legacy or application-specific directories
- A system to create and manage public key infrastructure (PKI) certificates
- A runtime model for user authentication

- A delegated administration model and application that enables the administrator of the identity management system to selectively delegate access rights to an administrator of an individual application, or directly to a user. Security and user interface models that can support various requirements are critical.

Figure 1 shows an overview of an identity management system.

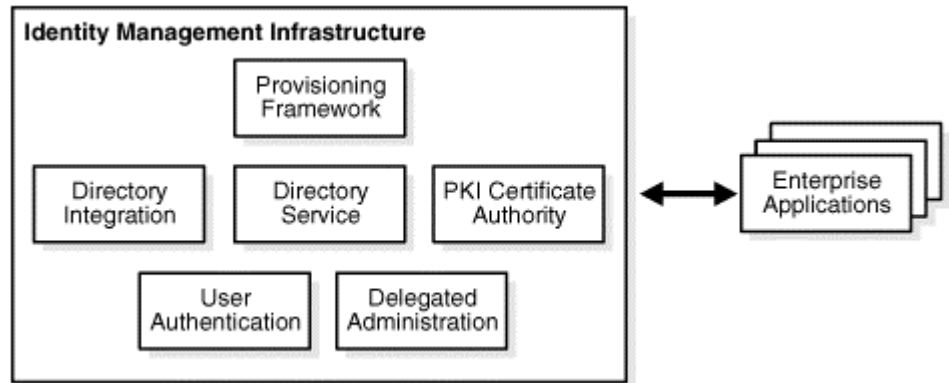


Figure 1: Overview of an Identity Management System

Oracle Identity Management Overview

Oracle Identity Management is an integrated infrastructure that provides distributed security to Oracle products. Oracle Identity Management is included with Oracle Application Server, as well as Oracle9i Database Server and Oracle Collaboration Suite.

The Oracle Identity Management infrastructure includes the following components:

- **Oracle Internet Directory:** A scalable, robust LDAP V3-compliant directory service implemented on the Oracle9i Database Server
- **Oracle Directory Integration and Provisioning:** A component of Oracle Internet Directory that enables you to:
 - Synchronize data between Oracle Internet Directory and other connected directories
 - Send notifications to target applications to reflect changes to a user's status or information
 - Develop and deploy your own connectivity agents
- **Oracle Delegated Administration Services:** A component of Oracle Internet Directory that provides trusted proxy-based administration of directory information by users and application administrators

- **Oracle Application Server Single Sign-On (OracleAS Single Sign-On):** Provides single sign-on access to Oracle and third-party Web applications
- **Oracle Application Server Certificate Authority (OCA):** Issues, revokes, renews, and publishes X.509v3 certificates to support PKI-based strong authentication methods

Many different applications, including Oracle E-Business Suite and Oracle Collaboration Suite, can leverage the Oracle Identity Management infrastructure, as shown in Figure 2.

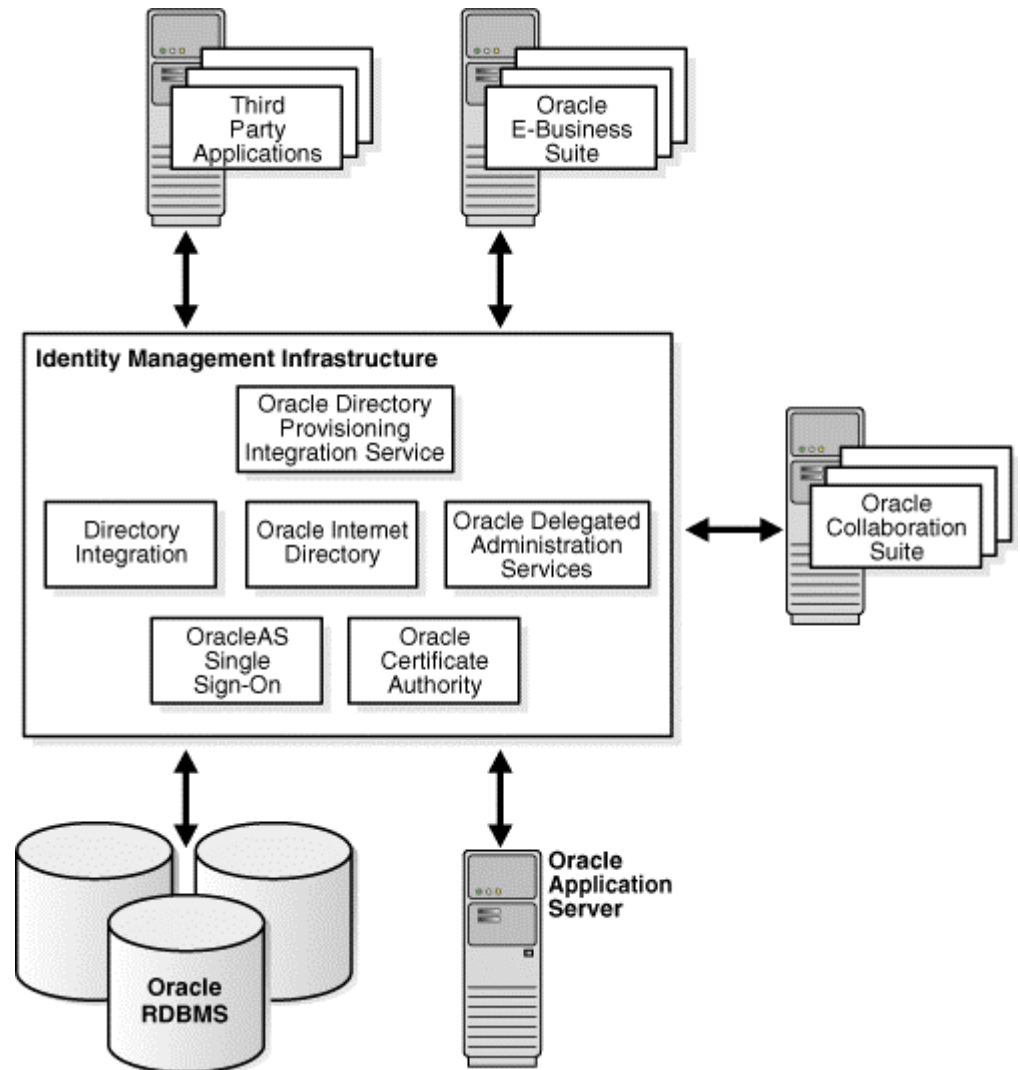


Figure 2: Oracle Identity Management

While Oracle Identity Management is designed to provide an enterprise infrastructure for Oracle products, it can also serve as a general purpose identity management solution for user-written and third-party enterprise applications.

In addition, third-party application vendors certify with Oracle Identity Management infrastructure to ensure proper operation.

Oracle Identity Management Objectives

Oracle Identity Management is designed to meet three key architectural objectives:

- Oracle Identity Management serves as a shared infrastructure for all Oracle products and technology stacks, including Oracle Application Server, Oracle9i Database Server, Oracle E-Business Suite, and Oracle Collaboration Suite. Accordingly, it is secure, reliable, and scalable, consistent with the core strengths of Oracle products and technologies.

Oracle Identity Management provides a consistent security model among all Oracle products and technology stacks. Oracle Identity Management infrastructure is planned for and deployed only once to support any current or future deployment of any Oracle product.

- Oracle Identity Management provides a secure, efficient, and reliable way to leverage and extend your investment in an existing third-party identity management infrastructure
 - Within a third-party identity management environment, Oracle Identity Management provides a single consistent point of integration for the entire Oracle technology stack, eliminating the need to configure and manage integration of various individual Oracle products with the third-party environment
 - Using Oracle Directory Integration and Provisioning, Oracle Identity Management leverages current investment in planning and deployment of a third-party enterprise directory. This provides the means to map and inherit major considerations such as directory naming, directory tree structure, schema extensions, access control, and security policies. Established procedures in an existing framework for user enrollment, identity, and account provisioning can be seamlessly incorporated into the corresponding operations of Oracle Identity Management.
 - If a third-party authentication service is in use, OracleAS Single Sign-On provides the means to integrate with the service and extend a seamless single sign-on experience to users accessing the Oracle environment. Certified interoperability solutions exist for leading third-party authentication platforms, and well defined

interfaces are available for implementing similar solutions for any new product.

- The Oracle Identity Management infrastructure can serve as an enterprise-wide foundation for identity management, to support other Oracle products as well as third-party vendor products deployed in the customer environment.

Oracle Identity Management offers lower ownership costs by streamlining the process of both user and account provisioning for all Oracle and third-party products. It also offers high levels of security, scalability, and functional richness. By supporting industry standards in all relevant interfaces, Oracle Identity Management can be customized and extended for use in many disparate application environments.

ORACLE IDENTITY MANAGEMENT CONCEPTS AND ARCHITECTURE

This chapter introduces concepts that deployment planners must understand to effectively deploy identity management. It provides an overview of the Oracle Identity Management architecture and the provisioning lifecycle of applications and users in the Oracle environment and presents the terms that are commonly used to describe identity management.

Identity Management Concepts

This section describes the fundamental concepts of identity management and contains the following topics:

Integrating Application Security with Identity Management

This section provides a blueprint for administrators of a typical application integrated with Oracle Identity Management. It provides a framework for understanding the roles of the various Oracle Identity Management components and services, and provides a basis for understanding how to engineer secure application deployments in an enterprise environment.

The application integration model is shown in Figure 3.

In this model, the following essential services are performed by the identity management infrastructure:

- **Administration and Provisioning:** Provides administration and provisioning services for the identities managed by the identity management infrastructure. In Oracle Identity Management, these services are performed using tools such as Oracle Delegated Administration Services and Oracle Directory Integration and Provisioning.

Policy Decision Services are the process that interprets any applicable entitlement policies associated with the resources to which applications secure and control access. Some applications rely on decision services that are embedded in the application itself, while others depend on centralized decision services.

- **Policy Decision Services:** Although these services are typically performed by the application, such as OracleAS Portal, in Oracle Identity Management, Oracle Internet Directory performs policy decision services for the identity management infrastructure itself.
- **Identity Policy Assertion Services:** In Oracle Identity Management these services are performed by OracleAS Single Sign-On and Oracle Application Server Certificate Authority

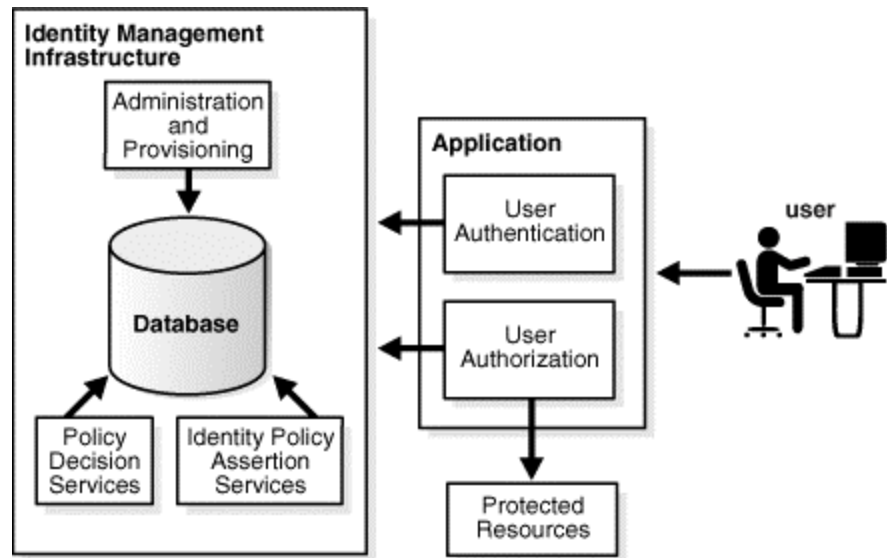


Figure 3: Application Integration Model

Applications deployed against the identity management infrastructure interact with the infrastructure in the following ways:

- **User Authentication:** When a user accesses an application, it validates the user credentials using the services provided by the identity management infrastructure. The authentication and the associated communication to the application is accomplished with the identity policy assertion services. For example, in the case of the Oracle Identity Management infrastructure, this would be validation of the credential, in the form of an encrypted browser cookie, by OracleAS Single Sign-On.
- **User Authorization:** Once authenticated, the application must also check if the user has sufficient privileges over resources protected by the application. This is performed by the application based on identity information managed in the identity management infrastructure. For example, a J2EE application uses Oracle Application Server Java Authentication and Authorization Service

Identity Management Assertion Services are the process that generates verifiable assertions about the identity of an entity or its authorizations. Network entities present these assertions to other services that the entities access.

(OracleAS JAAS Provider) to access user and role information in the Oracle Identity Management infrastructure, after authentication.

Identity and Application Provisioning Lifecycle

This section provides an overview of the user identity and application provisioning flow in the Oracle environment.

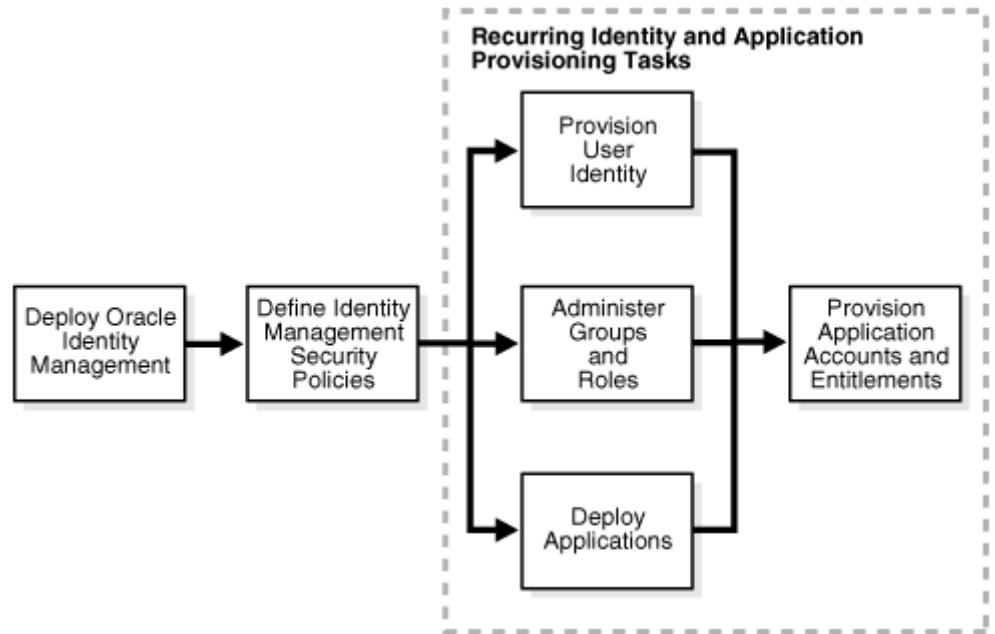


Figure 4: Identity and Application Provisioning Life Cycle

Identity Management Policies are policies affecting the management of identities in an enterprise that includes naming policies and security policies.

Following is a description of the provisioning flow shown in Figure 4:

1. The first step is the deployment of the Oracle Identity Management infrastructure using the product's installation and configuration tools.
2. The next step is to define the identity management security policies. These policies determine what data users and applications can access. They are codified as access control lists (ACLs) in Oracle Internet Directory, and are typically managed using Oracle Directory Manager.
3. The following three activities typically take place on an ongoing basis. Each of these activities can happen in parallel, and in no particular order.
 - User identities are provisioned in Oracle Internet Directory. These identities can come from multiple sources, including human resources applications, user administration tools (such as the Oracle Internet Directory Self-Service Console), through

synchronization with other directories, or through directory bulk loading tools.

- Groups and roles are administered in Oracle Internet Directory. Groups and group memberships can be defined in a number of ways, such as through the Oracle Internet Directory Self-Service Console or through synchronization with another directory service.
 - Application instances are deployed against the Oracle Identity Management infrastructure. This typically involves an identity management infrastructure administrator first granting access to the application administrator using the Oracle Internet Directory administration tools. The application administrator uses application installation and configuration tools to create the required directory objects and entries to support the application.
4. User identities, groups and roles, and applications are associated through the process of application account provisioning. This can be performed manually using application administration tools or in an automated fashion through provisioning integration.

Administrative Delegation

Oracle Identity Management requires a centralized repository for the enterprise users, groups, and services. Business requirements, however, make it difficult to manage a centralized store with a centralized set of administrators.

For example, in a business, the administrator of enterprise user management might be different from that of the e-mail service; the administrator of financials may need full control over the privileges of its users; and the OracleAS Portal administrator may need full control over the Web pages for a specific user or a specific group. To meet the needs of these various administrators, and satisfy the different security requirements, the identity management system needs delegated administration.

With delegated administration, the management of the data inside the identity management system can be distributed to many different administrators depending upon their security requirements. This combination of centralized repository and delegated privileges results in a secure and scalable administration in the identity management infrastructure.

Identity Management Integration with Oracle Products

Each of the Oracle technology stacks—Oracle Application Server, Oracle9i Database Server, Oracle E-Business Suite, and Oracle Collaboration Suite—supports a security model that is appropriate for its design. Nevertheless, they all employ the Oracle Identity Management infrastructure to implement their respective security models and capabilities, as shown in Figure 5.

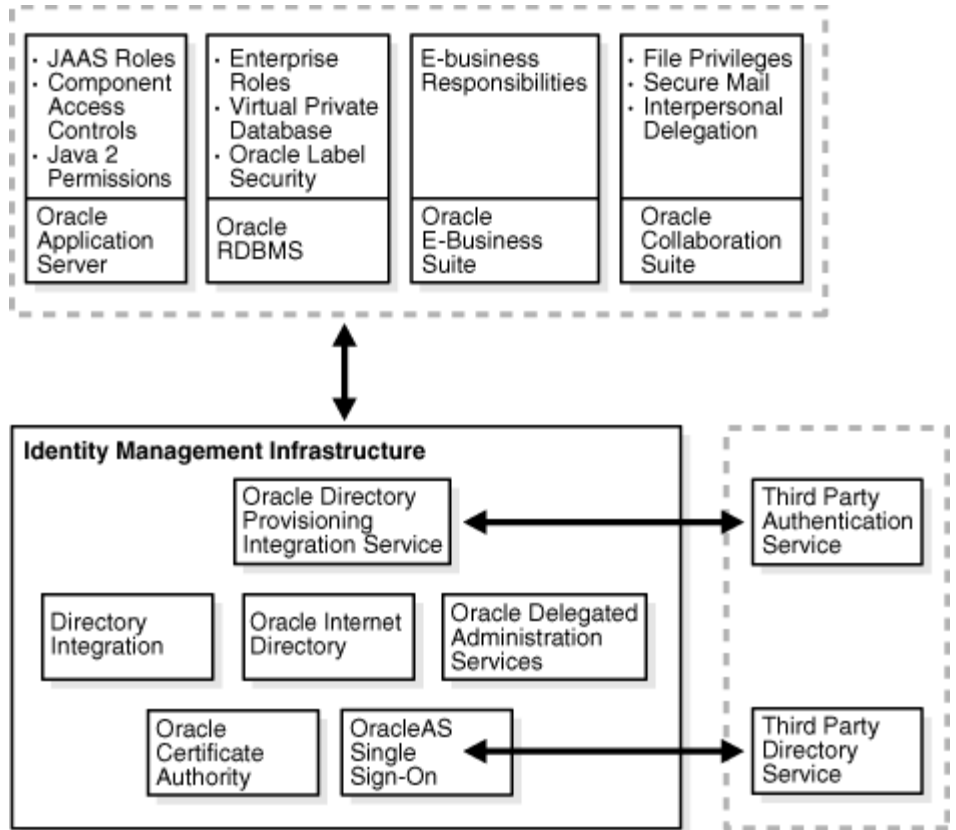


Figure 5: Identity Management Integration with Oracle Products

Oracle Application Server supports a J2EE compliant security service called Java Authentication and Authorization Service (JAAS). JAAS can be configured to utilize users and roles defined in Oracle Internet Directory.

Similarly, the database security capabilities—Enterprise User and Oracle Label Security—provide the means to leverage users and roles defined in Oracle Internet Directory. Both of these platforms facilitate the applications developed using the platforms’ respective native security capabilities to transparently leverage the underlying identity management infrastructure.

The Oracle E-Business Suite and Oracle Collaboration Suite application stacks are layered over the Oracle9i Database Server and Oracle Application Server platforms, providing a level of indirect integration with the Oracle Identity Management infrastructure. In addition, these products have independent features that rely upon Oracle Identity Management. For example, Oracle Collaboration Suite components such as Oracle Email and Oracle Voicemail & Fax use Oracle Internet Directory to manage component-specific user preferences, personal contacts, and address books.

These Oracle technology stacks also leverage Oracle Directory Integration and Provisioning to automatically provision and de-provision user accounts and privileges. Oracle Delegated Administration Services is employed extensively for self-service management of user preferences and personal contacts. Also, the security management interfaces of these products leverage the user and group management building blocks called service units.

CONCLUSION

An identity management system can provide a number of benefits to the enterprise, including reduced administrative costs, a better user experience, and improved security. Realizing the full benefits, however, requires implication on an integrated, comprehensive identity management infrastructure.

Oracle Identity Management is a complete infrastructure providing directory services, directory synchronization, user provisioning, delegated administration, web single sign-on, and an X.509v3 certificate authority. Oracle Identity Management is designed to provide ready, out-of-the-box deployment for Oracle applications, as well as serve as a general-purpose identity management infrastructure for the enterprise and beyond.



Oracle Identity Management Concepts and Architecture
December 2003

Author: Michael Mesaros, Richard Strohm
Contributing Authors: Uppili Srinivasan

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
www.oracle.com

Copyright © 2003, 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.