Oracle® Identity and Access Management

Introduction

10*g* (10.1.4.0.1)

B31291-01

July 2006

ORACLE®

Oracle Identity and Access Management Introduction 10*g* (10.1.4.0.1)

B31291-01

Primary Author: Ellen Desmond

Contributors: Francisco Abedrabbo, Pradeep Bhoj, Sidharth Choudhury, Rohit M. Gupta, Hasan Rizvi, Ashish Koli, Michael Mesaros, Sanjay Rallapalli, Olaf Stullich, Frank Villavicencio

Contents

4 Oracle Virtual Directory

5 Oracle Directory Integration Platform

6 Oracle Access Manager

10 Oracle Delegated Administration Services

Index

List of Figures

List of Tables

Preface

This document is an introduction to Oracle Identity and Access Management.

Audience

This document is intended for the following audience:

- Identity and access management administrators
- Oracle application developers
- Enterprise security architects

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

Please see Chapter 2 for information about related documentation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview of Oracle Identity and Access Management

Oracle Identity and Access Management is a product set that allows enterprises to manage and automate the end-to-end lifecycle of user identities, and provides users with secure, fine-grained access to enterprise resources and assets. Oracle introduced the first product in this set, Oracle Internet Directory, in 1999. Since then, Oracle has developed and introduced a number of identity and access management features including directory synchronization, secure directory administration, and a Web single sign-on service, all of which were integrated with the Oracle product stack. In 2005 and 2006, Oracle further enhanced its identity and access management offerings through strategic acquisitions. Oracle has made significant investments in best-of-breed solutions for identity federation, Web access management, delegated identity administration, user identity provisioning and virtual directory technology.

This chapter includes the following topics:

Oracle Identity and Access Management Products

This section provides an introduction to the individual products comprising Oracle Identity and Access Management. The products can be grouped by function into three broad categories:

Directory Services

Directory services, based on the Lightweight Directory Access Protocol (LDAP) are central to an identity and access management strategy. Oracle provides scalable directory and integration technology that meets the requirements of general enterprise deployment, and is also leveraged by other Oracle products in the stack. Oracle Directory Services includes the following components:

Oracle Internet Directory

Oracle Internet Directory is a scalable, robust LDAP V3-compliant directory service that leverages the scalability, high availability and security features of the Oracle Database. Oracle Internet Directory can serve as the central user repository for identity and access management deployment, simplifying user administration in the Oracle application environment. In can also serve as a highly scalable standards-based directory for the heterogeneous enterprise.

Performance, high availability, and security are some of the outstanding characteristics of Oracle Internet Directory. The Oracle Internet Directory Server employs a multi-process, multi-instance architecture that enables scalability with the number of CPUs, whether deployed on an SMP platform or as nodes in a hardware cluster. This is unique in the industry and a clear differentiation from directories employing single process architectures. Data management is another area where Oracle Internet Directory excels. As user populations grow, so do the challenges associated with configuring pilot installations, rapidly deploying new directory nodes, backing up directory data, and performing on-line bulk provisioning operations. Oracle Internet Directory leverages the data management capabilities of the Oracle Database to support hot backups and parallel load operations. In addition, Oracle Internet Directory provides specialized directory management tools such as high-speed multi-threaded client tools that facilitate on-line bulk user provisioning. Finally, Oracle Internet Directory exploits the security functionality of the Oracle Database, providing secure directory processes and data stores.

Oracle Internet Directory is a key component of the Oracle product stack used in applications such as OracleAS Portal, Oracle E-Business Suite, Oracle Collaboration Suite, and the Oracle Database for services such as user and credential management, e-mail address storage, and name resolution. In addition, Oracle Internet Directory is supported as a directory store for PeopleSoft applications.

Oracle Virtual Directory

Creating a secure application environment often requires integration of existing user identity information that may be scattered across multiple locations and services. Oracle Virtual Directory, formerly known as OctetString Virtual Directory Engine, provides a single, dynamic access point to these data sources through LDAP or XML protocols. It does this by providing a real-time data join and an abstraction layer that exposes a single logical directory, without the need to synchronize or move data from its native location. Oracle Virtual Directory can provide multiple application-specific views of identity data stored in, for example, Oracle Internet Directory, Microsoft Active Directory and Sun Java Systems Directory instances, and can also be used to secure data access to the application-specific sources and enhance high-availability to existing data-sources. These capabilities accelerate the deployment of applications and reduce costs by eliminating the need to consolidate user information before an application can be deployed. Oracle Virtual Directory can constantly adapt those applications to a changing identity landscape as user repositories are added, changed, or removed.

Oracle Virtual Directory facilitates the integration of applications into existing identity infrastructures. Oracle Virtual Directory accomplishes this integration without requiring changes to existing directories or user repositories, allowing enterprises to deploy these services quickly without having to deal with the political issues of data ownership and representation. Oracle Virtual Directory can also be deployed to provide multiple application centric views of directory information optimized for the specific needs of individual applications.

Oracle Directory Integration Platform

Oracle Directory Integration Platform is a component of Oracle Internet Directory designed to perform directory synchronization and application integration across various directories and compatible Oracle products. Oracle Directory Integration Platform allows applications that rely on Oracle Internet Directory to leverage user data managed in other directories and enterprise user repositories. The synchronization feature enables customers to synchronize data between various directories and Oracle Internet Directory. The application integration feature notifies target applications of changes to a user's status or information. Oracle Directory Integration Platform can also be used to implement a corporate meta-directory, where the entries of several departmental or application-specific directories are stored and managed centrally. Oracle Internet Directory includes agents for out-of-the-box synchronization with Oracle Human Resources, Oracle Database, and third-party LDAP servers, such as Sun Java System Directory Server Microsoft Active Directory, Novell eDirectory, and OpenLDAP.

Access Management

Access management is the means for controlling user access to enterprise resources. Access management products provide centralized, fine-grained access management for heterogeneous application environments, as well as out-of-the-box integration with Oracle products such as Oracle Portal, Oracle Collaboration Suite, and Oracle E-Business Suite.

Oracle access management products include the following:

- Oracle Access Manager
- Oracle Identity Federation
- Oracle Application Server Single Sign-On
- Oracle Enterprise Single Sign-On Suite

Oracle Access Manager

Oracle Access Manager, formerly known as Oracle COREid Access and Identity, provides Web-based identity administration, as well as access control to Web applications and resources running in a heterogeneous environments. It provides the user and group management, delegated administration, password management and self-service functions necessary to manage large user populations in complex, directory-centric environments. Access Manager supports all popular authentication methods including browser forms, digital certificates, and smart cards, and integrates seamlessly with most application servers and portals, including OracleAS 10g, BEA WebLogic, IBM WebSphere, Vignette and others. User identities and credentials can be accessed from a number of repositories including Oracle Internet Directory, Microsoft Active Directory and Sun Java System Directory. With Access Manager, user access policies can be defined and enforced with a high degree of granularity through centralized management.

Access System The Access System enables you to protect resources such as URLs and legacy, non-HTTP applications. It uses the information stored by the Identity System to control which users, groups, and organizations can access a resource. It stores information about configuration settings and security policies that control access to resources in a directory server that uses Oracle Access Manager-specific object classes. You can use the same directory to store the Access System configuration settings, access policy data, and user data, or you can store this data on separate directory servers.

Identity System The Identity System is a set of applications that provide delegated administration, user self-service, and real-time change management. The Identity System stores information about users, groups, and organizations. For example, you can create, manage, and delete groups in the directory server. You can define a subscription policy for a group, including self-service with no approval needed, subscription with approvals, rule-based subscription, and no subscription allowed.

Oracle Identity Federation

As more companies move their business processes to the Web, many organizations have a greater need to extend the boundaries of their enterprise to include partner applications. Federated identity management allows companies to operate independently and cooperate for business purposes by enabling cross-domain single sign-on and allowing companies to manage user identities and vouch for them as they access resources managed by another domain.

Oracle Identity Federation, formerly known as COREid Federation, provides a self-contained federation solution that combines the ease of use and portability of a standalone application with a scalable, standards-based proven interoperable architecture. It helps corporations securely link their business partners into a corporate portal or extranet while also increasing their compliance with privacy and security regulations. Identity Federation enables companies to manage multiple partners and choose from industry standard federated protocols. Identity Federation provides built-in integration with customer's identity management infrastructure (Oracle and non-Oracle) to deliver an end-to-end user experience, addressing scenarios like automatic registration, identity mapping, seamless access control navigation, and others.

Oracle Application Server Single Sign-On

Oracle Application Server Single Sign-On (OracleAS Single Sign-On) is a component that provides single sign-on access to Oracle and third-party Web applications. OracleAS Single Sign-On enables Web single sign-on for Oracle applications such as Oracle Portal, Oracle Collaboration Suite and Oracle E-Business Suite. It delivers a lightweight authentication solution to Oracle-only environments, supporting basic username and password authentication and X.509 certificate based authentication. OracleAS Single Sign-On supports authentication against user identities and credentials stored in Oracle Internet Directory, with integration to other repositories such as Microsoft Active Directory and Sun Java System Directory though the Oracle Directory Integration Platform.

Oracle Enterprise Single Sign-On Suite

Oracle Enterprise Single Sign-On Suite (eSSO Suite) is an upcoming product that provides true single sign-on for all the applications and resources in an enterprise, with no modification required to existing applications. It enables seamless retrofitting of strong, multifactor authentication to the desktop and to all legacy applications. eSSO Suite saves users from having to remember and manage multiple passwords and usernames. It also saves helpdesk time and money in responding to user requests to reset forgotten passwords. With the Oracle eSSO Suite, users log on once, and eSSO does the rest, automating every password management function, including logon, password selection, and password change and reset.

Identity Management

Oracle Identity Management is a product set that allows enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources both within and beyond the firewall.

Automating user identity provisioning can reduce IT administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Compliance initiatives focus on the enforcement of corporate policies as well as the demonstration of compliance with these standards. An enterprise identity management solution can provide a mechanism for implementing the user management aspects of a corporate policy, as well as a means to audit users and their access privileges.

The Oracle Identity and Access Management Suite includes the following identity management products:

- Oracle Identity Manager
- Oracle Delegated Administration Services

Oracle Identity Manager

The Oracle Identity Manager platform automates user identity provisioning and deprovisioning and allows enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources, both within and beyond the firewall. It provides an identity management platform that automates user provisioning, identity administration, and password management, wrapped in a comprehensive workflow engine.

Automating user identity provisioning can reduce IT administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Key features of Oracle Identity Manager include password management, workflow and policy management, identity reconciliation, reporting and auditing, and extensibility through adapters.

Oracle Identity Manager also provides attestation support. Attestation is the process of having users or system managers confirm people's access rights on a periodic basis. Existing Sarbanes-Oxley requirements demand enterprises to perform attestation for all financially significant systems every three to six months. Identity Manager includes a highly flexible attestation solution to help enterprise customers meet these regulatory requirements in a cost-effective and timely manner. By setting up attestation processes in Identity Manager, enterprise customers can automate the process of generation, delivery, review, sign-off, delegation, tracking, and archiving of user access rights reports for reviewers on a scheduled or ad-hoc basis.

Oracle Delegated Administration Services

Oracle Delegated Administration Services, part of Oracle Internet Directory, provides trusted proxy-based administration of directory information by users and application administrators. Oracle Delegated Administration Services are implemented as a set of pre-defined, Web-based units that are embedded in the administrative interfaces for Oracle products such as OracleAS Portal, Oracle Collaboration Suite, the Oracle Database Security Manager and Oracle E-Business Suite. Included with Oracle Internet Directory is the DAS Self-Service Console, an easy-to-use, Web-based tool built on the Oracle Delegated Administration Services framework. The DAS Self-Service Console allows end users and application administrators to search for and manage data in the directory and provides Oracle Application Server administrators with a means of managing end users in the Oracle environment.

Packaging of Oracle Identity and Access Management Products

Oracle's Identity and Access Management solution consists of two packages:

- Oracle Identity and Access Management Suite, a comprehensive set of best of breed components aimed at addressing the Identity and Access Management requirements of a heterogeneous enterprise
- A set of components included as part of the Oracle Application Server infrastructure installation

This section describes these two packages. It contains the following topics:

Oracle Identity and Access Management Suite

The Oracle Identity and Access Management Suite includes the following products, which are described in this book:

- Oracle Internet Directory
- Oracle Virtual Directory
- Oracle Access Manager
- Oracle Identity Federation
- Oracle Identity Manager

In addition, the Oracle Identity and Access Management Suite includes Oracle Security Developer Tools, which provides an API for developing federation and secure Web services applications.

Oracle Application Server Infrastructure Components

Four of the identity and access management products described in this book are components of the Oracle Application Server infrastructure, which is included with Oracle Application Server, Oracle Database, and Oracle Collaboration Suite. These four products are:

- Oracle Internet Directory
- Oracle Directory Integration Platform
- Oracle Application Server Single Sign-On
- Oracle Delegated Administration Services

When you install the Oracle Application Server infrastructure, you can choose to install these components on the same server or on different servers.

> **See Also:** The "Installing OracleAS Infrastructure" chapter in *Oracle Application Server Installation Guide*.

Note: Oracle Internet Directory is included in both the Oracle Identity and Access Management Suite and Oracle Application Server Infrastructure.

As of Oracle Application Server 10*g* (10.1.4.0.1), these four products can be managed with Identity Management Grid Control Plug-in, which uses the features of Oracle Enterprise Manager 10*g* Grid Control.

> **See Also:** The "Identity Management Grid Control Plug-in" chapter in *Oracle Identity Management Infrastructure Administrator's Guide*.

The Oracle Application Server Infrastructure also includes Oracle Application Server Certificate Authority, which issues, revokes, renews, and publishes X.509v3 certificates to support PKI-based strong authentication methods

2

Documentation Roadmap

This chapter provides pointers to other documentation. It consists the following sections, for different categories of users:

- Oracle Identity and Access Management Administrator
- Oracle Application Developer
- Enterprise Security Architect

Oracle Identity and Access Management Administrator

This section lists documentation that an Oracle Identity and Access Management Administrator should read. The Oracle Identity and Access Management Administrator tasks are divided into two broad topics:

- Installing and Upgrading Oracle Identity and Access Management Products
- Administering Oracle Identity and Access Management Products

Installing and Upgrading Oracle Identity and Access Management Products

This section lists the documentation that an Oracle Identity and Access Management Administrator should read before installing or upgrading specific products.

Table 2–1 Read Before Installing or Upgrading

Task	Documentation
Installing Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, or Oracle Application Server Single Sign-On	*Oracle Application Server Enterprise Deployment Guide* *Oracle Application Server Release Notes* *Oracle Application Server Quick Installation Guide* *Oracle Application Server Installation Guide*
Upgrading Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, or Oracle Application Server Single Sign-On	*Oracle Application Server Release Notes* *Oracle Application Server Upgrade and Compatibility Guide*
Installing or upgrading Oracle Virtual Directory	*Oracle Virtual Directory Server Installation Guide*

Table 2–1 (Cont.) Read Before Installing or Upgrading

Task	Documentation
Installing or upgrading Oracle Access Manager	*Oracle Access Manager Upgrade Guide* *Oracle Access Manager Installation Guide*
Installing or upgrading Oracle Identity Federation	The Installation chapter in *Oracle Identity Federation Administrator's Guide*
Installing or upgrading Oracle Identity Manager	*Oracle Identity Manager Installation and Upgrade Guide for JBoss* *Oracle Identity Manager Installation and Upgrade Guide for WebLogic* *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*

Administering Oracle Identity and Access Management Products

This section lists the documentation that an Oracle Identity and Access Management Administrator should read before administering specific products. Before administering Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, or Oracle Application Server Single Sign-On, please read the documentation listed in the first row as well as the specific documentation for each product.

Table 2–2 Read Before Administering

Task	Introductory Documentation	Advanced Documentation
Administering Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, or Oracle Application Server Single Sign-On	*Oracle Identity Management Infrastructure Administrator's Guide* *Oracle Application Server Quick Administration Guide*	*Oracle Application Server Administrator's Guide* *Oracle Application Server Enterprise Deployment Guide* *Oracle Application Server Performance Guide* *Oracle Application Server High Availability Guide*
Administering Oracle Internet Directory	*Oracle Internet Directory Administrator's Guide*, Chapters 1 and 2.	The remaining chapters in *Oracle Internet Directory Administrator's Guide*.
Administering Oracle Directory Integration Platform	*Oracle Identity Management Integration Guide*, Chapter 1.	The remaining chapters in *Oracle Identity Management Integration Guide*.
Administering Oracle Delegated Administration Services	Chapter 1 in *Oracle Identity Management Guide to Delegated Administration*	The remaining chapters in *Oracle Identity Management Guide to Delegated Administration*
Oracle Application Server Single Sign-On	Chapter 1 in *Oracle Application Server Single Sign-On Administrator's Guide*	The remaining chapters in *Oracle Application Server Single Sign-On Administrator's Guide*
Administering Oracle Virtual Directory	Chapter 1 in O*racle Virtual Directory Server Product Manual*.	The remaining chapters in *Oracle Virtual Directory Server Product Manual*.

Table 2–2 (Cont.) Read Before Administering

Task	Introductory Documentation	Advanced Documentation
Administering Oracle Access Manager	Chapter 1 in *Oracle Access Manager Introduction*	The remaining chapters in *Oracle Access Manager Introduction* *Oracle Access Manager Identity and Common Administration Guide* *Oracle Access Manager Access Administration Guide* *Oracle Access Manager Deployment Guide* *Oracle Access Manager Customization Guide* *Oracle Access Manager Integration Guide* *Oracle Access Manager Schema Description*
Administering Oracle Identity Federation	Chapter 1 in *Oracle Identity Federation Administrator's Guide*	The remaining chapters in *Oracle Identity Federation Administrator's Guide*
Administering Oracle Identity Manager	Chapter 1 in *Oracle Identity Manager Design Console Guide* Read Chapter 1 in *Oracle Identity Manager Administrative and User Console Guide*	The remaining chapters in *Oracle Identity Manager Administrative and User Console Guide.* The remaining chapters in *Oracle Identity Manager Design Console Guide.* *Oracle Identity Manager Administrative and User Console Customization Guide* *Oracle Identity Manager Tools Reference Guide* *Oracle Identity Manager Audit Report Developer Guide* *Oracle Identity Manager Best Practices Guide*

Oracle Application Developer

This section lists documentation that an Oracle application developer should read.

Table 2–3 Read Before Developing Applications

Task	Documentation
Developing Applications for Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, or Oracle Application Server Single Sign-On	*Oracle Identity Management Infrastructure Administrator's Guide* *Oracle Application Server Application Developer's Guide* *Oracle Containers for J2EE Security Guide* Java Naming and Directory Interface (JNDI) documentation at Sun Developer Network: `http://java.sun.com/products/jndi` *Oracle Containers for J2EE Services Guide* *Oracle Identity Management Application Developer's Guide* *Oracle Internet Directory API Reference* Any API-specific notes in *Oracle Application Server Release Notes*
Developing Applications for Oracle Virtual Directory	Chapters 8, 9, and 10 in *Oracle Virtual Directory Server Product Manual.*

Table 2–3 (Cont.) Read Before Developing Applications

Task	Documentation
Developing Applications for Oracle Access Manager	*Oracle Access Manager Developer Guide* *Oracle Access Manager Customization Guide*
Developing Applications for Oracle Identity Federation	*Oracle Security Developer Tools Reference*, Chapters 9 and 11 *Oracle Security Developer Tools Liberty SDK 1.1 Java API Reference* *Oracle Security Developer Tools Liberty SDK 1.2 Java API Reference* *Oracle Security Developer Tools SAML 1.0/1.1 Java API Reference* *Oracle Security Developer Tools SAML 2.0 Java API Reference*
Developing Applications for Oracle Identity Manager	*Oracle Identity Manager Audit Report Developer's Guide* *Oracle Identity Manager Application Development API Usage Guide* *Oracle Identity Manager Tools Reference* *Oracle Identity Manager Design Console Guide*

Enterprise Security Architect

This section lists the documentation that an enterprise security architect should read to determine which identity and access management products to use.

Table 2–4 Read to Determine Which Products to Use

Documentation
Oracle Application Server High Availability Guide
Oracle Application Server Enterprise Deployment Guide
Oracle Identity Management Infrastructure Administrator's Guide
Oracle Internet Directory Administrator's Guide, Chapters 1 and 2.
Oracle Identity Management Integration Guide, Chapter 1.
Chapter 1 in *Oracle Identity Management Guide to Delegated Administration*
Chapters 1, 2, and 3 in *Oracle Virtual Directory Server Product Manual*
Chapter 1 in *Oracle Access Manager Introduction*
Oracle Access Manager Deployment Guide
Oracle Access Manager Integration Guide
Oracle Access Manager Access Administration Guide
Chapter 1 in *Oracle Application Server Single Sign-On Administrator's Guide*
Chapter 1 in *Oracle Identity Federation Administrator's Guide*
Chapter 1 in *Oracle Identity Manager Design Console Guide*
Chapter 1 in *Oracle Identity Manager Administrative and User Console Guide*
Oracle Identity Manager Best Practices Guide

3

Oracle Internet Directory

Oracle Internet Directory is a general purpose directory service that enables fast retrieval and centralized management of information about dispersed users and network resources. It combines Lightweight Directory Access Protocol (LDAP) Version 3 with the high performance, scalability, robustness, and availability of an Oracle Database.

This chapter contains these topics:

Benefits of Oracle Internet Directory

Among its more significant benefits, Oracle Internet Directory provides scalability, high availability, security, and tight integration with the Oracle environment.

- **Scalability**—Oracle Internet Directory exploits the strengths of an Oracle Database, enabling support for terabytes of directory information. In addition, such technologies as shared LDAP servers and database connection pooling enable it to support thousands of concurrent clients with subsecond search response times.

  Oracle Internet Directory also provides data management tools, such as Oracle Directory Manager and a variety of command-line tools, for manipulating large volumes of LDAP data.

- **High Availability**—Oracle Internet Directory is designed to meet the needs of a variety of important applications. For example, it supports full multimaster replication between directory servers: If one server in a replication community becomes unavailable, then a user can access the data from another server. Information about changes to directory data on a server is stored in special tables on the Oracle Database. These are replicated throughout the directory environment by Oracle Database Advanced Replication, a robust replication mechanism.

  Oracle Internet Directory also takes advantage of all the availability features of the Oracle Database. Because directory information is stored securely in the Oracle Database, it is protected by Oracle's backup capabilities. Additionally, the Oracle Database, running with large data stores and heavy loads, can recover from system failures quickly.

- **Security**—Oracle Internet Directory offers comprehensive and flexible access control. An administrator can grant or restrict access to a specific directory object

or to an entire directory subtree. Moreover, Oracle Internet Directory implements three levels of user authentication: anonymous, password-based, and certificate-based using Secure Sockets Layer (SSL) Version 3 for authenticated access and data privacy.

- **Integration with the Oracle Environment**—Through Oracle Directory Integration Platform, Oracle Internet Directory provides a single point of integration between the Oracle environment and other directories such as NOS directories, third-party enterprise directories, and application-specific user repositories.

Features of Oracle Internet Directory

Oracle components use Oracle Internet Directory for easier administration, tighter security, and simpler integration between multiple directories.

Features of Oracle Internet Directory include:

- Management with Identity Management Grid Control Plug-in
- Referential Integrity
- Server Chaining
- Integration with Other Oracle Products
- Security
- Globalization Support
- Distributed Directories

Management with Identity Management Grid Control Plug-in

As of Oracle Application Server 10*g* (10.1.4.0.1), you can manage Oracle Internet Directory with Identity Management Grid Control Plug-in, which uses the features of Oracle Enterprise Manager 10*g* Grid Control.

> **See Also:** The "Identity Management Grid Control Plug-in" chapter in *Oracle Identity Management Infrastructure Administrator's Guide*.

Referential Integrity

If you enable Referential Integrity, whenever you update an entry in the directory, the server also updates other entries that refer to that entry.

Server Chaining

This feature enables you to map entries that reside in third party LDAP directories to part of the directory tree and access them through Oracle Internet Directory, without synchronization or data migration.

Integration with Other Oracle Products

Oracle Internet Directory is integrated with several Oracle products, including the following:

- **Oracle Virtual Directory** can use Oracle Internet Directory as one of its target repositories.
- **Oracle Access Manager** uses Oracle Internet Directory to provide scalable, highly available back end identity storage.

- **Oracle Identity Federation** can use Oracle Internet Directory as an identity repository. It uses Oracle Internet Directory to create SAML assertions when running as an identity provider.
- **Oracle Identity Manager** uses Oracle Internet Directory as an LDAP target system to which it can provision identities and from which it can reconcile identity changes.
- **Oracle Web Services Manager** uses Oracle Internet Directory as a repository of identity information which can be used to drive authentication and authorization.
- **OracleAS Portal** enables self-service, integrated enterprise portals to store common user and group attributes in Oracle Internet Directory. The Oracle Portal administration tool also leverages the Oracle Delegated Administration Services for certain tasks.
- **Oracle Collaboration Suite** uses Oracle Internet Directory for:
  - Centralized management of information about users and groups
  - Provisioning Oracle Collaboration Suite components—that is, notifying them whenever changes of interest are applied to data in Oracle Internet Directory
  - Centralized integration for enterprises connecting other directories with any Oracle Collaboration Suite component

  Integrating Oracle Internet Directory and Oracle Collaboration Suite provides a common framework for user management and provisioning across all Oracle products.
- **Oracle Net Services** uses Oracle Internet Directory to store and resolve database services and the simple names, called net service names, that can be used to represent them.
- **Database Enterprise User Security** allows customers to easily manage database access for thousands of enterprise users. Database Enterprise users are stored in the directory together with authentication and authorization information, including database roles and privileges. When a user accesses an Oracle database, the database retrieves the user's information from Oracle Internet Directory and uses it to set the security context of the user's session on that server. Such centralized administration of database access makes it easy for administrators to control all access.
- **Oracle E-Business Suite** is integrated with Oracle Internet Directory to provide a common framework for user management and provisioning across all Oracle products.
- **Oracle Secure Enterprise Search** (SES) provides uniform search capabilities over multiple repositories. Oracle Internet Directory provides the basic infrastructure for SES user authentication and authorization. All users and roles defined in the Access Control Lists used by SES are stored in Oracle Internet Directory.

Security

Oracle Internet Directory is a key element of the Oracle Identity Management Infrastructure. This enables you to deploy multiple Oracle components to work against a shared instance of Oracle Internet Directory and associated infrastructure pieces. This sharing allows an enterprise to simplify security management across all applications.

In addition to the role it plays in the Oracle Identity Management infrastructure, Oracle Internet Directory provides many powerful features for protecting information.

These security features within Oracle Internet Directory itself include:

- Data integrity: Ensuring that data is not tampered with during transmission
- Data privacy: Ensuring that data is not inappropriately observed during transmission between Oracle Internet Directory and other components in the network.
- Authentication: Ensuring that the identities of users, hosts, and clients are correctly validated
- Authorization: Ensuring that a user reads or updates only the information for which that user has privileges
- Password policies: Establishing and enforcing rules for how passwords are defined and used
- Password protection: Ensuring that passwords are not easily discovered by others

You can use all these features to enforce a uniform security policy for multiple applications enabled for Oracle Internet Directory, and do so in either an enterprise or hosted environment. You do this by deploying the directory for administrative delegation. This deployment allows, for example, a global administrator to delegate to department administrators access to the metadata of applications in their departments. These department administrators can then control access to their department applications.

Globalization Support

Oracle Internet Directory follows LDAP Version 3 internationalization (I18N) standards. These standards require that the database storing directory data use Unicode Transformation Format 8-bit (UTF-8) character set. With Oracle9*i*, Oracle added a new UTF-8 character set called AL32UTF8. This database character set supports the latest version of Unicode (3.2), including the latest supplementary characters. This allows Oracle Internet Directory to store the character data of almost any language supported by Oracle Globalization Support. Moreover, although several different application program interfaces are involved in the Oracle Internet Directory implementation, Oracle Internet Directory ensures that the correct character encoding is used with each API.

Distributed Directories

Although an online directory is logically centralized, it can be physically distributed onto several servers. This distribution reduces the work a single server would otherwise have to do, and enables the directory to accommodate a larger number of entries.

A distributed directory can be either replicated or partitioned. When information is replicated, the same naming contexts are stored by more than one server. When information is partitioned, one or more unique, non-overlapping naming contexts are stored on each directory server. In a distributed directory, some information may be partitioned and some may be replicated.

How Oracle Internet Directory Works

This section includes the following topics:

- An Oracle Directory Server Instance

Components of Oracle Internet Directory

Oracle Internet Directory includes:

- Oracle directory server, which responds to client requests for information about people and resources, and to updates of that information, by using a multitiered architecture directly over TCP/IP
- Oracle directory replication server, which replicates LDAP data between Oracle directory servers
- Directory administration tools, which include:
  - Oracle Directory Manager, which simplifies directory administration through a Java-based graphical user interface
  - A variety of command-line administration and data management tools invoked from LDAP clients
  - Directory server management tools within Oracle Enterprise Manager 10*g* Application Server Control Console. These tools enable you to:
    - Monitor real-time events and statistics from a normal browser
    - Start the process of collecting such data into a new repository
- Oracle Internet Directory Software Developer's Kit

See Also: *Oracle Identity Management Application Developer's Guide* for information about the Oracle Internet Directory Software Developer's Kit.

Oracle Internet Directory Connections

An Oracle Internet Directory node consists of one or more directory server instances connected to the same directory store. The directory store, that is, the repository of the directory data, is an Oracle Database.

Oracle directory server runs as an application on an Oracle Database. It communicates with the database by using Oracle Net Services, Oracle's operating system-independent database connectivity solution. The database may or may not be on the same host. Figure 3–1 shows these relationships. It shows Oracle Internet Directory running as a server application. LDAP clients and the directory administration client connect to the Oracle directory server by using LDAP. The Oracle directory server connects to the Oracle database by using Oracle Net Services.

Figure 3–1 Oracle Internet Directory Overview

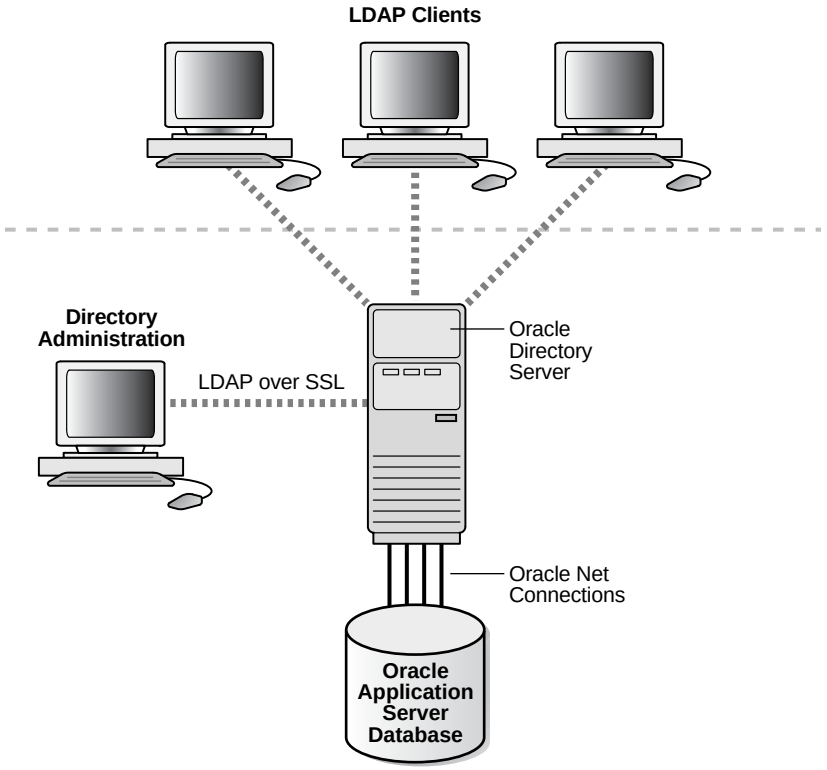


Figure 3–2 shows the various directory server components and their relationships running on a single node.

Oracle Net Services is used for all connections between the Oracle database server and:

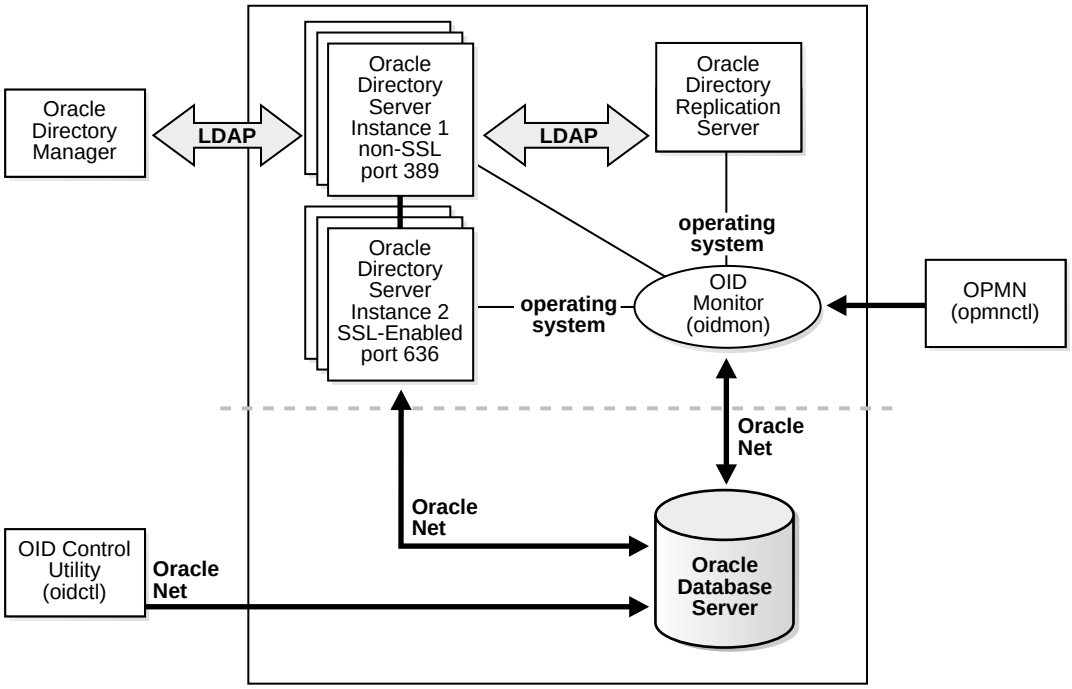
- The object class
- The Oracle directory server instance 1 non-SSL port 389
- The Oracle directory server instance 2 SSL-enabled port 636
- The OID Monitor

LDAP is used for connections between directory server instance 1 on non-SSL port 389 and:

- Oracle Directory Manager
- Oracle directory replication server

The two Oracle directory server instances and the Oracle directory replication server connect to OID Monitor by way of the operating system.

Figure 3–2 A Typical Oracle Internet Directory Node



As shown in Figure 3–2, an Oracle Internet Directory node includes the following major components:

Table 3–1 Components of an Oracle Internet Directory Node

Component	Description
Oracle directory server instance	Also called either an LDAP server instance or a directory server instance, it services directory requests through a single Oracle Internet Directory dispatcher process listening at specific TCP/IP ports. There can be more than one directory server instance on a node, each listening on different ports.
Oracle directory replication server	Also called a replication server, it tracks and sends changes to replication servers in another Oracle Internet Directory system. There can be only one replication server on a node. You can choose whether or not to configure the replication server.
Oracle Database Server	Stores the directory data. Oracle strongly recommends that you dedicate a database for use by the directory. The database can reside on the same node as the directory server instances.
Oracle Process Manager and Notification Server (OPMN)	Manages Oracle Internet Directory as an Oracle Application Server component. OPMN uses the directives in the OID component snippet in `$ORACLE_HOME/opmn/conf/opmn.xml` and invokes OIDMON and OIDCTL as required. It is unaware of the Oracle Internet Directory Server instances.

Table 3–1 (Cont.) Components of an Oracle Internet Directory Node

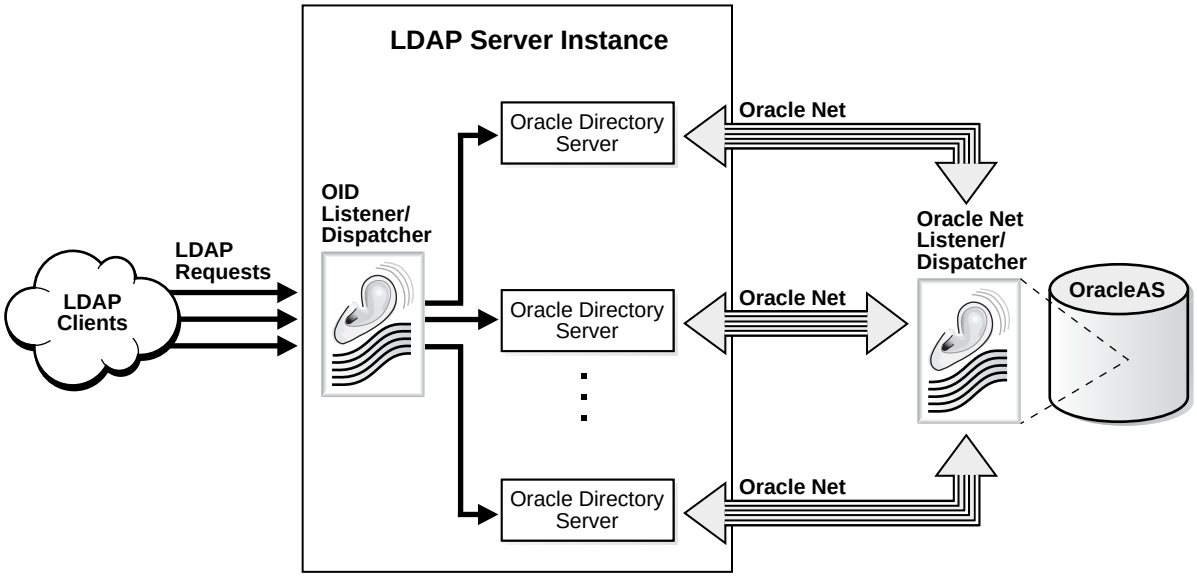
Component	Description
OID Monitor (OIDMON)	Initiates, monitors, and terminates the LDAP server processes. If you elect to install a replication server, OID Monitor controls it. When you issue commands through OID Control Utility (OIDCTL) to start or stop directory server instances, your commands are interpreted by this process. OID Monitor executes the LDAP server instance startup and shutdown requests that you initiate from OID Control Utility. OID Monitor also monitors servers and restarts them if they have stopped running for abnormal reasons. When it starts a server instance, OID Monitor adds an entry into the directory instance registry and updates data in the process table. It also starts any servers that it finds in the process table. When it shuts down the directory server instance, it updates the process table. If OID Monitor restarts a server that has stopped abnormally, it updates the registry entry with the start time of the server. All OID Monitor activity is logged in the file `$ORACLE_HOME/ldap/log/oidmon.log`. This file is on the Oracle Internet Directory server file system. OID Monitor checks the state of the servers through mechanisms provided by the operating system.
OID Control Utility (OIDCTL)	Communicates with OID Monitor by placing message data in Oracle Internet Directory server tables. This message data includes configuration parameters required to run each Oracle directory server instance.

The Oracle directory replication server uses LDAP to communicate with an Oracle directory (LDAP) server instance. To communicate with the database, all components use OCI/Oracle Net Services. Oracle Directory Manager and the command-line tools communicate with the Oracle directory servers over LDAP.

An Oracle Directory Server Instance

Each Oracle directory server instance, also called an LDAP server instance, looks similar to what Figure 3–3 illustrates.

Figure 3–3 Oracle Directory Server Instance Architecture



One instance comprises one dispatcher process and one or more server processes. By default, there is one server process for each instance, but you can increase this number. Oracle Internet Directory dispatcher and server processes can use multiple threads to distribute the load.LDAP clients send LDAP requests to an Oracle Internet Directory listener / dispatcher process listening for LDAP commands at its port.

The Oracle Internet Directory listener / dispatcher sends the request to the Oracle directory server which, in turn creates server processes. A server process handles an LDAP operation request and connects to the Oracle database instance to access the directory store. The directory server handles the client request by generating one server process for each operation.

Multiple server processes enable Oracle Internet Directory to take advantage of multiple processor systems. The number of server processes created is determined by the configuration parameter ORCLSERVERPROCS. The default is 1 (one).

Database connections from each server process are spawned as needed, depending on the value set for the configuration parameter ORCLMAXCC. The number of database connections spawned by each server is equal to ORCLMAXCC + (ORCLMAXCC / 2) + 1. The default value of ORCLMAXCC in configset0 is 2. The server processes communicate with the data server by way of Oracle Net Services. an Oracle Net Services Listener / Dispatcher relays the request to the Oracle Database.

4

Oracle Virtual Directory

Oracle Virtual Directory is an LDAPv3-enabled service that provides virtualized abstraction of one or more enterprise data sources into a single directory view. Oracle Virtual Directory provides the ability to integrate LDAP-aware applications into diverse directory environments while minimizing or eliminating the need to change either the infrastructure or the applications.

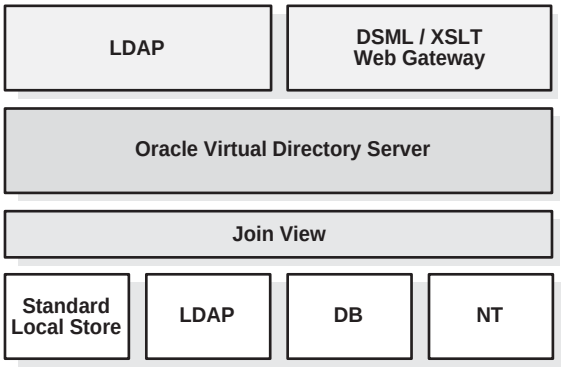
This chapter contains the following sections:

Benefits of Oracle Virtual Directory

Oracle Virtual Directory provides the following benefits:

- **Consolidates multiple directories**—Oracle Virtual Directory can translate existing directory data to match application directory requirements, as shown in Figure 4–1. Oracle Virtual Directory communicates with multiple directory sources through its adapter architecture. It provides full schema and namespace translation services, ensuring that data presented to applications from multiple proxied sources has a common and consistent format.

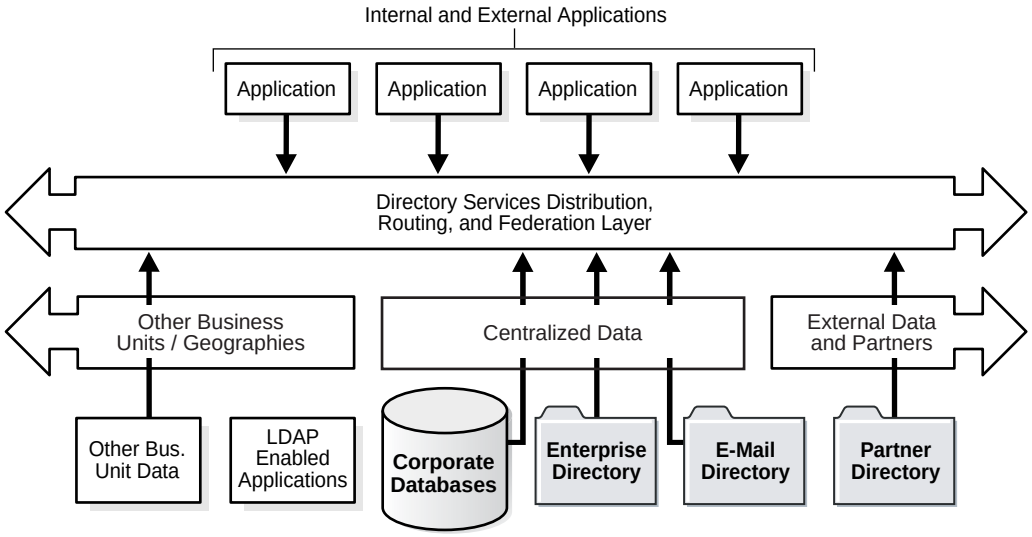
Figure 4–1 Oracle Virtual Directory Server Architecture



- **Provides virtualization and distribution of directory services**—As shown in Figure 4–2, an enterprise might have many directory sources in different formats and different geographies, and owned by different parties. Added to these traditional enterprise directories are LDAP enabled applications, relational

databases and email systems. Oracle Virtual Directory provides a directory service integration layer to handle practical issues such as distributed security, routing, integration, and data-level federation.

Figure 4–2 Directory Services Virtualization and Distribution



- **Reduces administrative cost and improves security**—Oracle Virtual Directory eliminates issues with updates from duplication, synchronization and replication. Data is up-to-date and consistent at all times.
- **Extends enterprise applications quickly**—Oracle Virtual Directory supports enterprise directory applications and legacy data. Secure accurate data access is available for corporate resources, suppliers and customers.
- **Provides ubiquitous access to information**—The software is fully LDAPv3 compliant. It works with most applications and is compatible with many directory products, tools, and applications.
- **Lowers cost of implementation**—Oracle Virtual Directory is less expensive to acquire or implement than a custom or synchronization-based solution. Oracle Virtual Directory Server can be deployed tactically to solve a specific application integration issue, or strategically in an overall directory infrastructure architecture.

Features of Oracle Virtual Directory

Features of the Oracle Virtual Directory Server include:

- Data Federation
- Data Ownership
- Multiple Data Adapters
- Flexible Security Domains
- Secure Data Publication
- High Availability Support
- Application Integration
- Flexible Deployment

- Custom Application Programming Interfaces
- Low-Cost, High-Value Solutions

Data Federation

Oracle Virtual Directory Server acts as a directory gateway that processes client requests and dynamically re-routes them to one or more existing directories, regardless of format (LDAP, RDBMS, etc). Oracle Virtual Directory Server does this by presenting a virtual directory hierarchy to its clients and then assigning hierarchy branches of that tree to designated LDAP or RDBMS servers. Oracle Virtual Directory Server handles the issues of inter-directory security, protocol, and data translation so that LDAP-clients assume that all information comes from a single trusted LDAP directory, the Oracle Virtual Directory Server.

Data Ownership

One of the least obvious but most important benefits of virtualization is data ownership. Directories are often set up by organizations with specific purposes and objectives in mind. When another organization wishes to access data owned by the first, questions arise as to who owns the data and who controls it. Politics can occur when different parties wish to use and share information. Everyone acknowledges the value in re-using existing data, but re-using data brings up many care and control issues. Many organizations that own data are very concerned when copies of their data go to other organizations or outside parties. Who is responsible for it? Who will ensure its accuracy? Who will ensure its security and confidentiality? If the information is copied, how does the owning organization assure itself about how the information is being used and controlled by the other party?

Virtualization through proxy technology solves many of these political problems by keeping data where it belongs – with the owner. At any time, the owner can restrict or cut off access to this data. Additionally, the owner is free to revise this information at will and can be assured that partners are always working with the latest relevant information. Most importantly, by keeping information with the owner, the use of that information can be continuously monitored and controlled by the owner. Oracle Virtual Directory Server supports this type of solution by not copying information. Information accessed by Oracle Virtual Directory Server occurs in real time. This assures the consumer and provider that the information is current, accurate, and authorized.

Multiple Data Adapters

Oracle Virtual Directory Server supports an unlimited number of directory data connection components known as adapters. Each adapter is responsible for managing a particular namespace that is represented by a specific parent distinguished name (DN). Multiple adapters can be combined and overlapped to present a customized directory tree.

Oracle Virtual Directory Server supports the following adapter types:

- **LDAP Adapter**—provides proxied access to LDAPv2/LDAPv3 directory servers such as Microsoft Active Directory, Novell® eDirectory™, Sun™ONE Directory, or IBM/Tivoli SecureWay® Directory as well other Oracle Virtual Directory Servers. The LDAP Proxy provides namespace translation as well as advanced connection pooling and operation level load-balancing.

- **Database Adapter**—provides LDAP virtualization of relational database data. Almost any data structure can be mapped into a hierarchy of LDAP objects. DB Adapter also provides automatic schema mapping and attribute value translation.
- **Local Store Adapter**—provides a local directory store that enables Oracle Virtual Directory Server to operate as a standalone directory server. The Standard Adapter supports single-master replication and is compatible with other directory servers (such as IBM / Tivoli SecureWay® or Netscape Directory) that support SLURPD replication.
- **Windows NTLM Adapter**—provides LDAP virtualization of a Microsoft Windows domain (NOTE: available only on Win32 platform).
- **JoinView Adapter**—provides real-time join capabilities between entries located in other Oracle Virtual Directory Server adapters. The JoinView Adapter provides an extendible API that allows the development of customer specific joiners. JoinView Adapter comes with three out-of-the-box Joiners: Simple, OneToMany, and Shadow. These joiners demonstrate the widely ranging capabilities of the Oracle Virtual Directory Server joiner and the different join functionalities that can be performed. More information on these joiners can be found later in the guide.

In addition to the listed adapters, Oracle Virtual Directory Server also supports the ability to create custom adapters using plug-ins that can connect to almost any data source with a defined API. For example, custom adapters can be used to abstract information available through Web services.

Flexible Security Domains

When deploying new business applications across multiple business organizations, identity and security can be complicated by the existence of multiple directory security infrastructures. As Microsoft Active Directory administrators know, having multiple windows infrastructures (forests) is great for administration and performance, but has a downside in that there is no automatic trust between forests and no inter-forest global catalogue.

> **See Also:** Microsoft TechNet Paper: Design Considerations for Delegation of Administration in Active Directory, http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/addeladm.mspx.

Oracle Virtual Directory Server is able to create a new transitive security context with fine-grained access controls built to support all IETF standards for access control, while supporting the IETF draft model for implementation. Oracle Virtual Directory Server is also designed to properly integrate with security restrictions from the source directories that it proxies. This results in a multi-layer or multi-domain security concept that gives administrators the ultimate security control.

Oracle Virtual Directory Server supports a wide array of authentication models. In addition to SSL / TLS (including StartTLS) and certificate-based authentication, Oracle Virtual Directory Server is able to use server-to-server authentication with proxied servers (authenticating itself), or alternatively is able to pass user context through to source directories. By providing user-context at the Oracle Virtual Directory Server and source directory, both directories can provide end-user contextual security control.

Secure Data Publication

Oracle Virtual Directory Server offers standard features such as:

- **SSL/TLS**—Oracle Virtual Directory Server offers SSL/TLS capabilities that provide for secure communication sessions with LDAP clients. This allows you greater security by allowing Oracle Virtual Directory Server to be the trusted transport mechanism.
- **Transaction Cleansing**—Oracle Virtual Directory Server is based on a protocol conversion engine, which means that it deconstructs every query, recompiling and assessing validity before transmission to trusted proxied directory sources. This protects source LDAP servers from malformed or unauthorized queries. After cleaning the "garbage" requests, Oracle Virtual Directory Server is able to protect limited resources from exposure to huge loads from malicious attacks by providing the ability to set limits on items such as:
  - Maximum operations per connection
  - Maximum concurrent connections
  - Maximum total connections in a specified period for a particular subject
  - Maximum total connections in a specified period for a particular address

Oracle Virtual Directory Server implements its own access controls and provides filtered access to internal proxied directory data.

High Availability Support

Oracle Virtual Directory provides the following high availability support:

- **Fault Tolerance and failover** —Oracle Virtual Directory Servers provide fault tolerance in two forms:
  - they can be configured in fault tolerant configurations
  - they can manage flow to fault tolerant proxied sources

  Multiple Oracle Virtual Directory Servers can be quickly deployed simply by copying, or even sharing configuration files. When combined with round-robin DNS, redirector, or cluster technology, Oracle Virtual Directory Server provides a complete fault-tolerant solution.

  For each proxied directory source, Oracle Virtual Directory Server can be configured to access multiple hosts (replicas) for any particular source. It intelligently fails over between hosts and spreads the load between them. Flexible configuration options allow administrators to control percentages of a load to be directed toward specific replica nodes and to indicate whether a particular host is a read-only replica or a read/write server (master). This avoids unnecessary referrals resulting from attempts to write to a read-only replica.
- **Load-Balancing**—Oracle Virtual Directory Server been designed with powerful load balancing features that allow it to spread load and manage failures between its proxied LDAP directory sources.

  Oracle Virtual Directory Server's virtual directory tree capability allows large sets of directory information to be broken up into multiple distinct directory servers. Oracle Virtual Directory Server is able to recombine the separated data sets back into one virtual tree by simply "gluing" together the separate directory tree branches. In scenarios where either an application or the data doesn't support this, or the directory tree from separate directories needs to overlap, Oracle Virtual Directory Server supports "routing".

  "Routing" means search filters can be included in addition to the search base to determine optimized search targets. In this mode, Oracle Virtual Directory Server

automatically routes queries to the appropriate virtualized directory sources enabling the ability to work with many millions of directory entries.

Application Integration

A directory is only useful if the applications it serves can gain access to the data it needs, in a form that has consistent formats or schema. But the typical enterprise environment contains a myriad of directory repositories with different schema, namespace, and data designs. In addition to providing a secure bridge to existing directory information, Oracle Virtual Directory Server provides "meta-directory"-like functionality to translate and transform data on-the-fly. This functionality enables administrators to easily normalize differences in data found between different organizations and directory infrastructures.

The resulting virtualized directory view contains all the directory information an application needs to run, without needing drastic changes or integration technology to be built into the application.

Flexible Deployment

Oracle Virtual Directory Server's management console, the Oracle Virtual Directory Manager, is a rich and extensible management environment based on the open source Eclipse platform. It simplifies deployment and management whether using a single Oracle Virtual Directory Server in a single environment, or in an environment with tens of servers in multiple data centers and at multiple stages of deployment.

Management can also be performed through a Web Services API with a published WSDL specification. This gives administrators the ability to script or otherwise programmatically access Oracle Virtual Directory Servers without walking through the GUI.

Custom Application Programming Interfaces

Oracle Virtual Directory Server provides 3 main areas of extensibility within the product. This allows customers and consultants to enhance the functionality of Oracle Virtual Directory Server to meet specific business or technical integration needs.

- **Oracle Virtual Directory Server Plug-ins**—Oracle Virtual Directory Server provides a flexible plug-in framework modeled on Java Servlet Filters. Plug-ins can be used to provide custom logic as part of a transaction or simply to connect to a custom data source. Plug-ins can be inserted globally or only for specific adapters. The ordering of plug-ins can be changed and plug-ins can be isolated to particular types of transactions. Oracle Virtual Directory Server's management tools provide wizards for creating new plug-ins along with examples that can be used to get started quickly.
- **Custom Joiners**—The Oracle Virtual Directory Server JoinView Adapter is based on an extensible model known as Joiners. Custom Joiners can be written providing different joiner behaviors. Joiners provide functions such as mapping, joining and pre / post / handler event handling. Joiners can be written to provide simple entry level joins, or can be extended to provide complex join logic, or transaction handling and rollback capability.
- **Web Gateway**—Oracle Virtual Directory Server includes a customizable DSML / XSLT based gateway. This gateway provides basic Web server support based on the Apache Web server model that supports static HTML and XSLT rendered content. The gateway includes a directory-enabled interface allowing for

queries as well as modification operations. Web server security enables custom delegated administration applications to be developed based on this interface.

Low-Cost, High-Value Solutions

Traditional directory integration solutions require complex LDAP provisioning and replication schemes and even synchronization to operate. These new directories then become yet another directory source that has to be maintained and managed.

As a light, real-time service, Oracle Virtual Directory Server improves efficiency by reusing existing directory infrastructure, rather than synchronizing and duplicating it. Oracle Virtual Directory Server extends the reach of existing enterprise directories and capitalizes on their value.

How Oracle Virtual Directory Works

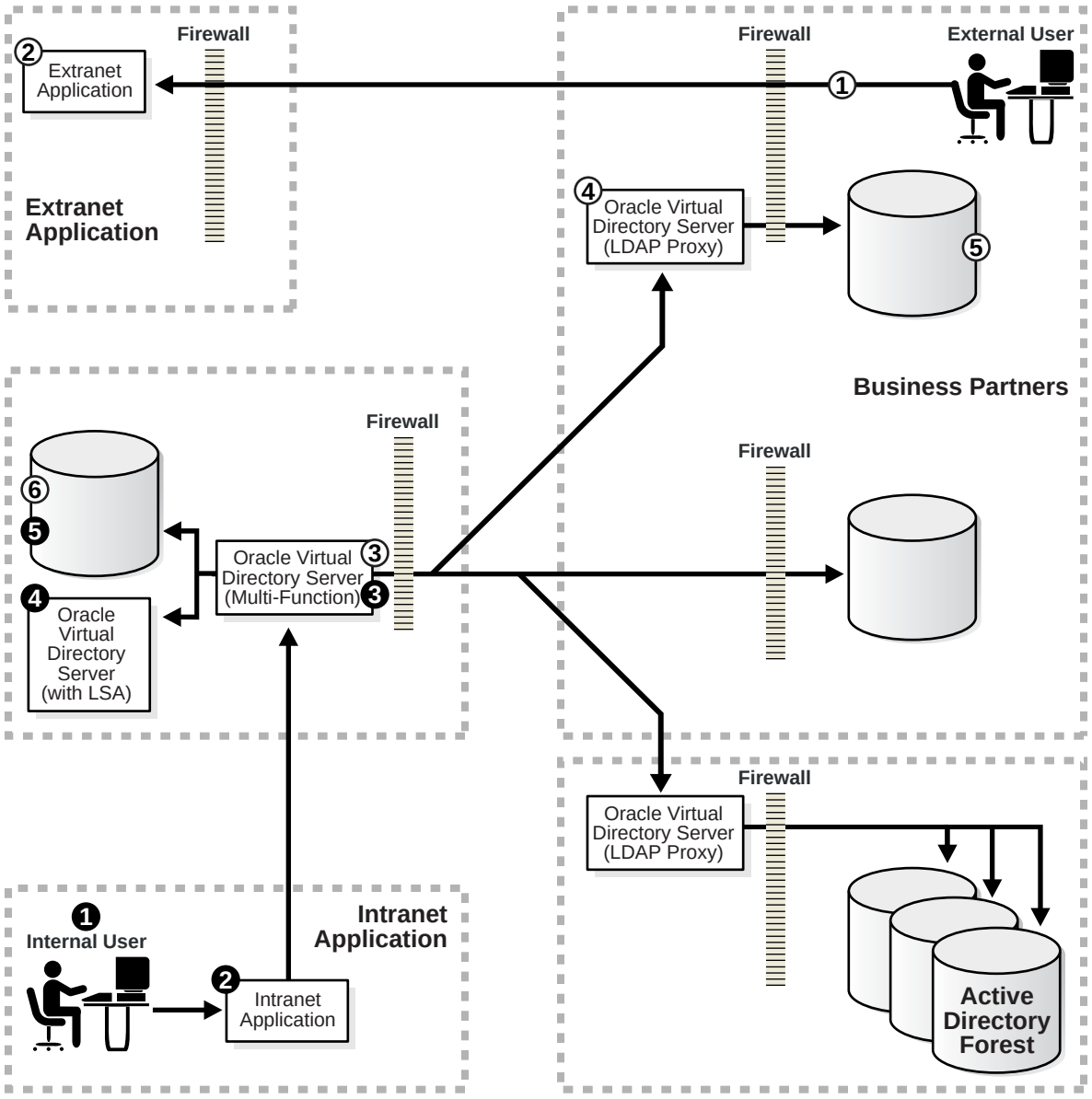
This section contains the following topics:

- Intranet Identity Example
- Extranet Identity Example
- Scenario Review

Intranet Identity Example

In Figure 4–3, Oracle Virtual Directory Server is used in several ways. In the bottom left corner, there is an internal end user (1) accessing an intranet based Web application (2).

Figure 4–3 Environment with Intranet and Extranet Applications



During the access, the application (or policy service) requests the user's id and password. The application or policy service then accesses the Oracle Virtual Directory Server (3) using LDAPv3 to validate the credentials using an LDAP bind request. Oracle Virtual Directory Server in turn routes this request to the local directory server store (4) and validates the credentials. On validation, Oracle Virtual Directory Server returns the verified results to the application (2).

In a further request, the application requests the user's directory entry from Oracle Virtual Directory Server so that their application profile and rights can be retrieved. To do this, Oracle Virtual Directory Server performs a transparent join, bringing together attributes from both the local directory server (4), as well information from a RDBMS (5). Once collected, Oracle Virtual Directory Server merges the result into a single virtual entry and returns it to the Intranet Application.

Note: The application may or may not include a policy server as part of its own infrastructure.

Extranet Identity Example

In the external identity example shown in Figure 4–3, we have an external organization or business partner user (1) accessing an extranet-based Web application (2). The application contacts Oracle Virtual Directory Server (3) using LDAPv3 to verify the user's credentials using an LDAP "bind".

At this stage, Oracle Virtual Directory Server recognizes that the credential maps to an external directory. Oracle Virtual Directory Server connects to the external Oracle Virtual Directory Server directory (4) at the business partner using an SSL encrypted link and uses it's own credentials to validate the interbusiness unit query. Once the business partner's Oracle Virtual Directory Server has validated the Oracle Virtual Directory Server (3), it recognizes the request and passes it on to the internal LDAPv3 directory (5). Oracle Virtual Directory Server applies the appropriate inter-business access control and returns the filtered results from the directory back to Oracle Virtual Directory Server, which is then able to validate the password of the business partner user and return success or failure to the application (2).

Finally, as in the Intranet Application example, the application might then query Oracle Virtual Directory Server for additional attributes about the user. Oracle Virtual Directory Server performs a join linking client-supplied information from the business partner directory (5) with locally stored information in the corporate database(6).

Scenario Review

This scenario demonstrates capabilies across quite a complex scenario. We see Oracle Virtual Directory Server acting as an information router and joiner, brokering information from multiple secure sources to meet the needs of an application or security infrastructure. Not only can Oracle Virtual Directory Server bring together information from within a single intranet, it can also leverage information from business partners. This is particularly important because it allows business partners to use the extranet application without having to be provisioned or managed in the host business's directory. Business partner users are authenticated by their own local directory in real time.

Oracle Virtual Directory Server can also play an important role as an LDAP Proxy server. Oracle Virtual Directory Server may optionally be used by business partners to act as a directory firewall. Oracle Virtual Directory Server properly authenticates and authorizes external access to internal directory information. In the bottom right of the diagram we also see how Oracle Virtual Directory Server's own routing capabilities allow it to route to multiple internal directories or Windows Active Directory Forests keeping this information away from the client. As a firewall, Oracle Virtual Directory Server controls and limits access to information as seen by authorized external parties. As a virtual-directory component, Oracle Virtual Directory Server simplifies and restructures data for publication of data to be used by business partners.

5

Oracle Directory Integration Platform

This chapter introduces Oracle Directory Integration Platform, its components, structure, and administration tools. It contains these topics:

Benefits of Oracle Directory Integration Platform

Oracle Directory Integration Platform enables you to reduce administrative time and costs by integrating your applications and directories, including third-party LDAP directories, with Oracle Internet Directory. Benefits offered by Oracle Directory Integration Platform include:

- **Directory Synchronization**—You can keep employee records in Oracle Human Resources consistent with those in Oracle Internet Directory.
- **Application Integration**—Oracle Directory Integration Platform can notify certain LDAP-enabled applications, such as OracleAS Portal, whenever incremental changes are applied to a subset of data in Oracle Internet Directory.
- **Integration with Third-party LDAP Directories**—You can integrate with various directories, including Microsoft Active Directory, Sun Java System Directory, Novell eDirectory, and OpenLDAP. For example, in an Oracle Application Server environment, where access to Oracle components relies on data stored in Oracle Internet Directory, you can still use Microsoft Active Directory as the central enterprise directory. Users of that directory can access Oracle components because Directory Integration Platform can synchronize the data in Microsoft Active Directory with that in Oracle Internet Directory.

Features of Oracle Directory Integration Platform

Features of Oracle Directory Integration Platforminclude:

- **Identity Management Grid Control Plug-in**—As of Oracle Application Server 10*g* (10.1.4.0.1), you can manage Oracle Directory Integration Platform with Identity Management Grid Control Plug-in, which uses the features of Oracle Enterprise Manager 10*g* Grid Control.

  See Also: The "Identity Management Grid Control Plug-in" chapter in *Oracle Identity Management Infrastructure Administrator's Guide*.

- **Installation Options**—By default, Oracle Directory Integration Platform is installed as a component of Oracle Internet Directory. However, you can also install Oracle Directory Integration Platform as a standalone installation. You should install a standalone instance of Oracle Directory Integration Platform under the following circumstances:
  - When you need Oracle Internet Directory to run on a separate host for performance reasons
  - When the applications that you need to integrate and synchronize require intensive processing
  - When you need to run multiple instances of Oracle Directory Integration Platform for high-availability
- **Directory Synchronization**—Directory synchronization involves movement and transformation of data between Oracle Internet Directory and another LDAP-enabled directory. It ensures the consistency of entries and attributes that reside in both Oracle Internet Directory and other connected directories.

  See Also:

  - *Oracle Identity Management Integration Guide.*
  - The chapter on Oracle Directory Integration Platform tools in the *Oracle Identity Management User Reference* for information on the Directory Integration Assistant (`dipassistant`).

- **Application Integration**—Application integration involves the notification of changes to entries occurring in Oracle Internet Directory to an application interested in tracking those changes. Application integration enables you to ensure that an application is notified of directory changes, for example, user or group information. Such changes can affect whether the application allows a user access to its processes and which resources can be used.

  See Also:

  - *Oracle Identity Management Integration Guide.*
  - The chapter on Oracle Directory Integration Platform tools in the *Oracle Identity Management User Reference* for information on the Provisioning Subscription Tool.

- **Scheduling**—Processing a synchronization or integration profile based on a predefined schedule
- **Mapping**—Executing rules for converting data between connected directories and Oracle Internet Directory
- **Data Propagation**—Exchanging data with connected directories by using a connector
- **Event Notification**—Notifying an application of a relevant change to the user or group data stored in Oracle Internet Directory

How Oracle Directory Integration Platform Works

The Oracle Directory Integration Platform Server is the shared server process that provides synchronization and integration functionality.

This section contains the following topics:

Synchronization

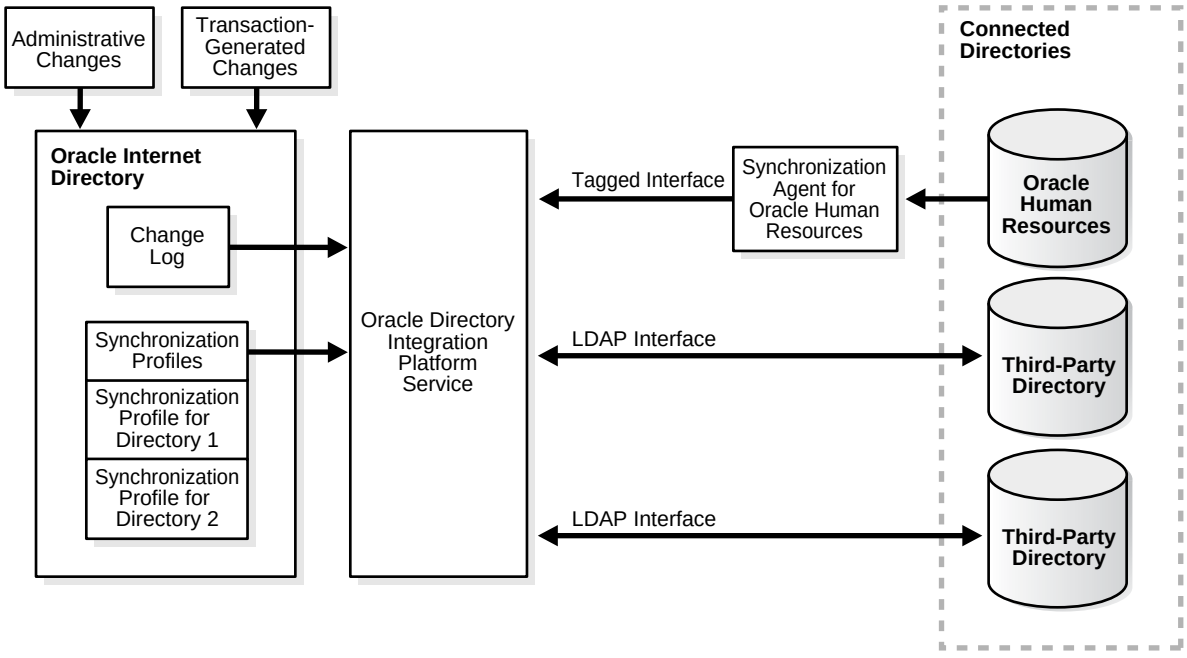
For Oracle Application Server components, Oracle Internet Directory is the central directory for all information, and all other directories are synchronized with it. This synchronization can be:

- One-way: Some connected directories only supply changes to Oracle Internet Directory and do not receive changes from it. This is the case, for example, with Oracle Human Resources as the primary repository for employee information.
- Two-way: Changes in Oracle Internet Directory can be exported to connected directories, and changes in connected directories can be imported into Oracle Internet Directory.

Certain attributes can be targeted or ignored by the Oracle Directory Integration Platform Service. For example, the attribute for the employee badge number in Oracle Human Resources may not be of interest to Oracle Internet Directory, its connected directories or client applications. You might not want to synchronize it. On the other hand, the employee identification number may be of interest to those components, so you might want to synchronize it.

Figure 5–1 shows the interactions between components in the Oracle Directory Integration Platform Service in a sample deployment in the context of directory synchronization.

Figure 5–1 Oracle Directory Integration Platform Service: Directory Synchronization



The central mechanism triggering all such synchronization activities is the Oracle Internet Directory change log. It adds one or more entries for every change to any connected directory, including Oracle Internet Directory. The Oracle Directory Integration Platform Service:

- Monitors the change log.
- Takes action whenever a change corresponds to one or more synchronization profiles.
- Supplies the appropriate change to all other connected directories whose individual profiles correspond to the logged change. Such directories could include, for example, relational databases, Oracle Human Resources, Microsoft Active Directory, Sun Java System Directory, Novell eDirectory, or OpenLDAP. It supplies these changes using the interface and format required by the connected directory. Synchronization through the Directory Integration Platform connectors ensures that Oracle Internet Directory remains up-to-date with all the information that Oracle Internet Directory clients need.

Additionally, the Oracle Directory Integration Platform Service ensures that each integrated application is notified of changes in, for example, user or group information. To do this, it relies on the information contained in an integration profile. Each profile:

- Uniquely identifies the application and organization to which it applies
- Specifies, for example, the users, groups, and operations requiring the application to be notified

The profile must be created when the application is installed, by using the Provisioning Subscription Tool.

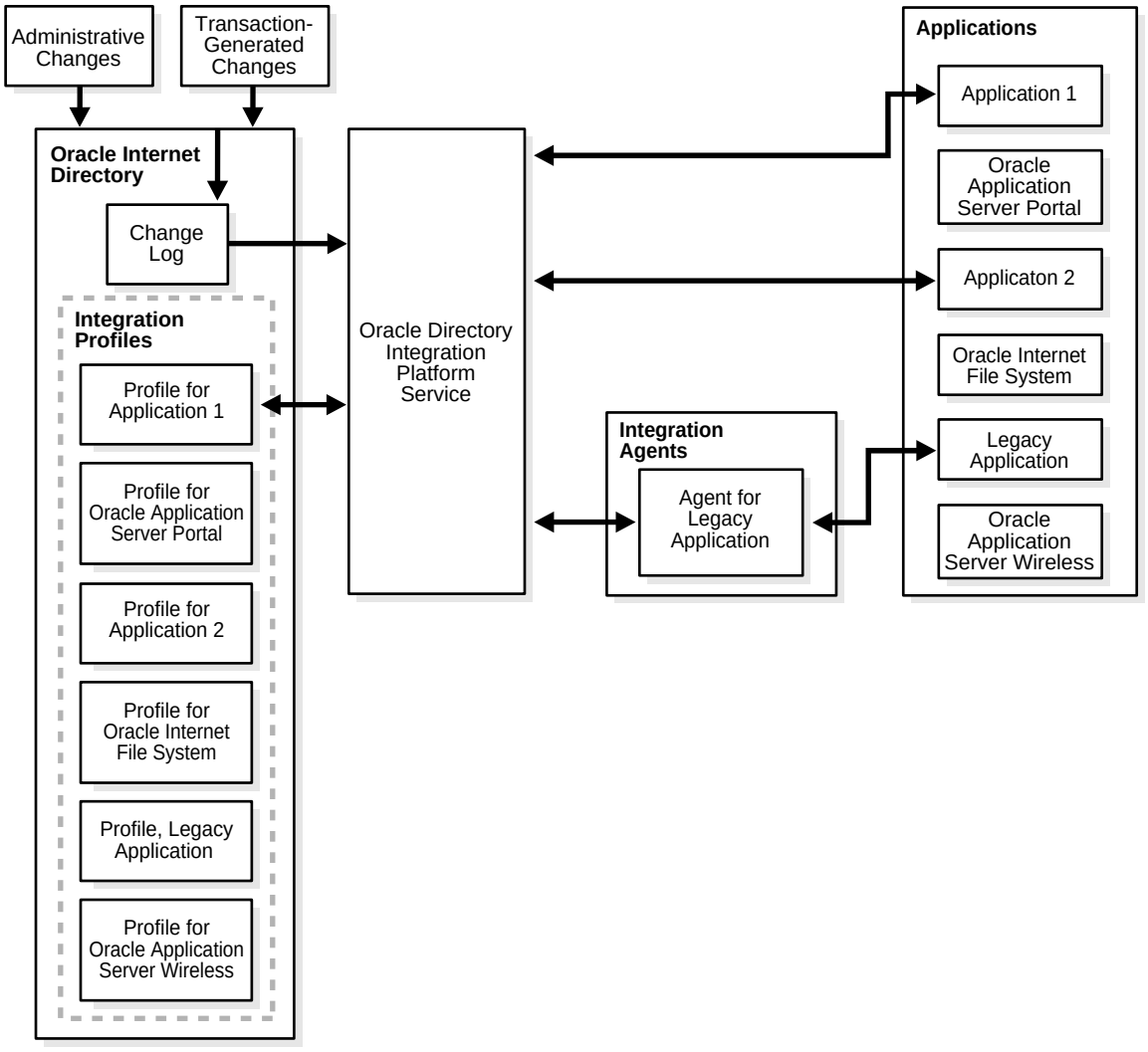
> **See Also:** The chapter on Oracle Directory Integration Platform tools in the *Oracle Identity Management User Reference* for information about the Provisioning Subscription Tool.

When changes in Oracle Internet Directory match what is specified in the integration profile of an application, the Oracle Directory Integration Platform Service sends the relevant data to that application.

Integration

Figure 5–2 shows the interactions between components in an Oracle Directory Integration Platform Service environment, including the special case of an integration agent for a legacy application. This illustration shows the interactions between Oracle Internet Directory, the Oracle Directory Integration Platform Service, integration agents, and applications. Oracle Internet Directory is shown as containing a change log and integration profiles for several applications, including OracleAS Portal, Oracle Internet File System, and Oracle9iAS Wireless. Administrative and Transaction-generated changes are entered into Oracle Internet Directory. Change log data and integration profile data in Oracle Internet Directory are sent to the Oracle Directory Integration Platform Service. The Oracle Directory Integration Platform Service sends data to integration agents, specifically to an integration agent for a legacy application. That information is, in turn, sent to the legacy application itself. The Oracle Directory Integration Platform Service also sends data to various other integrated applications.

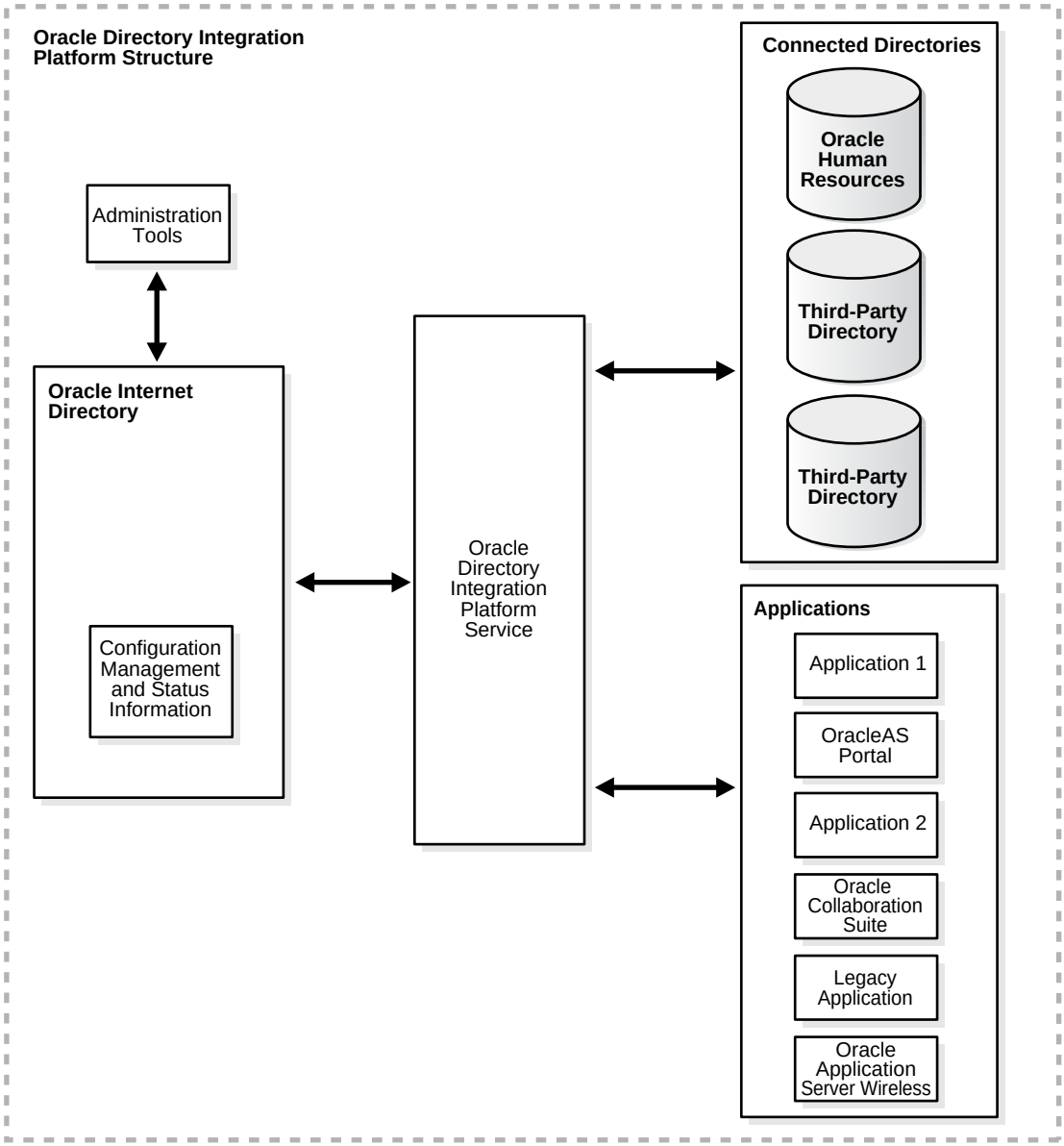
Figure 5–2 Oracle Directory Integration Platform Service: Application Integration



Oracle Directory Integration Platform Example

Figure 5–3 shows a sample deployment of Oracle Directory Integration Platform. This illustration shows the relation between components in the Oracle Directory Integration Platform. On the left is Oracle Internet Directory, which stores configuration management and status information. A bidirectional arrow shows the reciprocal relationship between Oracle Internet Directory and the administration tools. A bidirectional arrow also shows the relationship between Oracle Internet Directory and the Oracle Directory Integration Platform Service. An arrow points from the latter to examples of connected directories: Oracle Human Resources, Sun iPlanet, and Microsoft Active Directory. Another bidirectional arrow points from the Oracle Directory Integration Platform Service to examples of integrated applications: Integrated Application 1, OracleAS Portal, Integrated Application 2, Oracle Files, a legacy application, and Oracle Application Server Wireless.

Figure 5–3 Example of an Oracle Directory Integration Platform Environment



In the example in Figure 5–3, Oracle Internet Directory is synchronized with connected directories by way of the Oracle Directory Integration Platform Service In this example, the connected directories are Oracle Human Resources, Sun Java System Directory, and Microsoft Active Directory. Similarly changes in Oracle Internet Directory are sent to various applications by using the same service. In this example, the integrated applications include OracleAS Portal, Oracle Files, Oracle Application Server Wireless, two unspecified integrated application, and a legacy application.

6

Oracle Access Manager

Oracle Access Manager (formerly known as Oblix NetPoint and Oracle COREid) provides a full range of identity administration and security functions. These functions include Web single sign-on, user self-service and self-registration, workflow, auditing and access reporting, policy management, dynamic group management, and delegated administration.

Oracle Access Manager consists of two systems:

- **Access System**—You use the Access System to configure single- and multi-domain single sign-on to Web- and non-Web-based applications, Web pages, and other resources. You can configure user authentication schemes that require a user name and password, a certificate, or you can design a custom login form. Users are authorized based on schemes that you define. The authorization schemes are based on criteria such as header variables, the time, or data retrieved from external sources. You can use external authorization plug-ins in an authorization scheme. You can configure audits and reports of authentication and authorization activity. Third-party integrations enable use of smart cards and other technologies.
- **Identity System**—You use the Identity System to enable users to manage their profiles, perform self-registration, subscribe to and manage group memberships, and manage other organizational assets. The Identity System contains functionality for creating and managing password policies including self-service for lost password retrieval. You can configure delegated administration to enable management of millions of users. Workflow functionality enables Identity System functions to be routed for additional information and approval, and workflow steps can send calls to external applications.

This chapter provides an overview of Oracle Access Manager 10*g* (10.1.4.0.1) and includes the following topics:

Benefits of Oracle Access Manager

Oracle Access Manager enables you to change from a perimeter defense model, in which you unilaterally block outside access to your resources, to a security model based on business rules. You can securely provide business systems and data to employees, customers, and suppliers.

Oracle Access Manager helps your enterprise facilitate delivery of corporate functions to extended groups of employees, customers, partners, and suppliers; maintain a high level of security across applications; enable users and business partners to access the information they need.

For example, suppose that your internal users, your suppliers, and your customers require access to unique data sets. In addition, suppose that you also have common data that everyone should see. Using Oracle Access Manager, your identity-based policies can provide the right levels of access to each group while ensuring that everyone can securely access only the data that they need and that they have the right to access.

Using Oracle Access Manager, you can manage a corporate portal that is open to external business partners. For instance, for a portal that allows customers to order manufacturing materials and equipment, all applications exposed through the portal are protected with one platform (Oracle Access Manager) which grants access rights. Administration of the access policies protecting these resources can be delegated throughout the corporation so that business units, rather than the IT department, make decisions about the customers, suppliers, and partners who are to be given access rights. This is possible even if you need to manage millions of people, including your customers, employees, and suppliers.

Using Oracle Access Manager, you can also grant different types of privileges to different classes of users. For instance, a health-care organization can manage its data so that different groups can view different kinds of data, as follows:

- Health-care plan members can view their health-care information.
- Companies providing health-care services to their employees can manage their health-care plans.
- Doctors and hospitals can view patient information.

An organization can use Oracle Access Manager to aggregate application accounts. For example, financial institutions can configure self-service portals to allow their customers to access different accounts from a single login, including online banking, mortgage information, and insurance.

Oracle Access Manager Access System Features

The Access System enables you to centralize access policy creation while decentralizing policy management and enforcement. The following types of resources can be protected using the Access System:

- HTTP resources including directories, pages, Web-based applications, query strings, and so forth
- J2EE application server resources, including Java server pages (JSPs), servlets, and enterprise Java beans (EJBs)
- Other resources, including standalone programs (Java, C, C++), ERP applications, CRM applications, and the like

This section outlines key access-control features.

- **Authentication Services**—Provide a generalized means to authenticate users and systems attempting to access resources protected by Oracle Access Manager. Authentication services support both the basic username and password authentication method as well as stronger methods such as digital certificates or SecurID cards.

You can either use standard authentication plug-ins or create your own custom plug-ins using the Authentication Plug-In API. Each custom plug-in implements the authentication interface to pass relevant information between the Access Server and the plug-in. Methods within the interface parse the data.

Once a user is authenticated, Oracle Access Manager creates a single-sign-on (SSO) session for the client that frees the user from having to sign on again to access other resources or applications.

- **Authorization Services**—Deliver centralized, consistent management of policies across applications, while providing users granular access to Web-based content and resources. You can secure sensitive information while helping ensure that users and systems have the easy access they need.

  Authorization is governed by a policy domain that includes an authorization expression among a set of default rules that specify how resources for this domain are protected. You can use the authorization scheme provided by the Access System or configure one or more custom schemes that include custom plug-ins created using the Authorization Plug-In API. See also *Oracle Access Manager Developer Guide*.

  Once authorization is confirmed, the user is granted access to the resource.

- **Auditing Services**—Provide flexible and detailed reporting, auditing, and logging of events in Oracle Access Manager with out-of-the-box reports for Crystal Reports. The auditing and log files enable you to perform threat and intrusion detection, security monitoring, and business-level reporting by integrating with third-party products.

- **Personalization Services**—Enable personalization for other applications through HTTP header variables and redirection URLs. When Oracle Access Manager authenticates or authorizes user requests, the URL it returns can contain HTTP header variables which in turn can contain any user data stored under the authenticated user's ID in the directory.

  The downstream application can decode this information and use it to personalize the user experience. You can include a redirection URL in the URL returned by Oracle Access Manager, which may take the user to another Web page tailored to the identity of the user.

- **Single Sign-On**—Enables users and groups of users to access multiple applications after a single login and authentication, which improves the user experience by eliminating multiple logins. Users needing access to single-domain servers store a generated cookie for subsequent requests to the Web site. Users needing access to multi-domain servers store a cookie generated by a central Web login server; this occurs transparently for each accessed server within the associated Web system.

- **Delegated Access Administration**—Enables distribution of administrative tasks. When the responsibility for managing the Access System falls on a few people, you may want these people to appoint others to share the work. For example, you can delegate the ability to modify the revoked user list and to add, modify, or delete configuration details and schemes.

For more information and a sample Access System installation, see "How the Oracle Access Manager Access System Works" on page 6-3.

How the Oracle Access Manager Access System Works

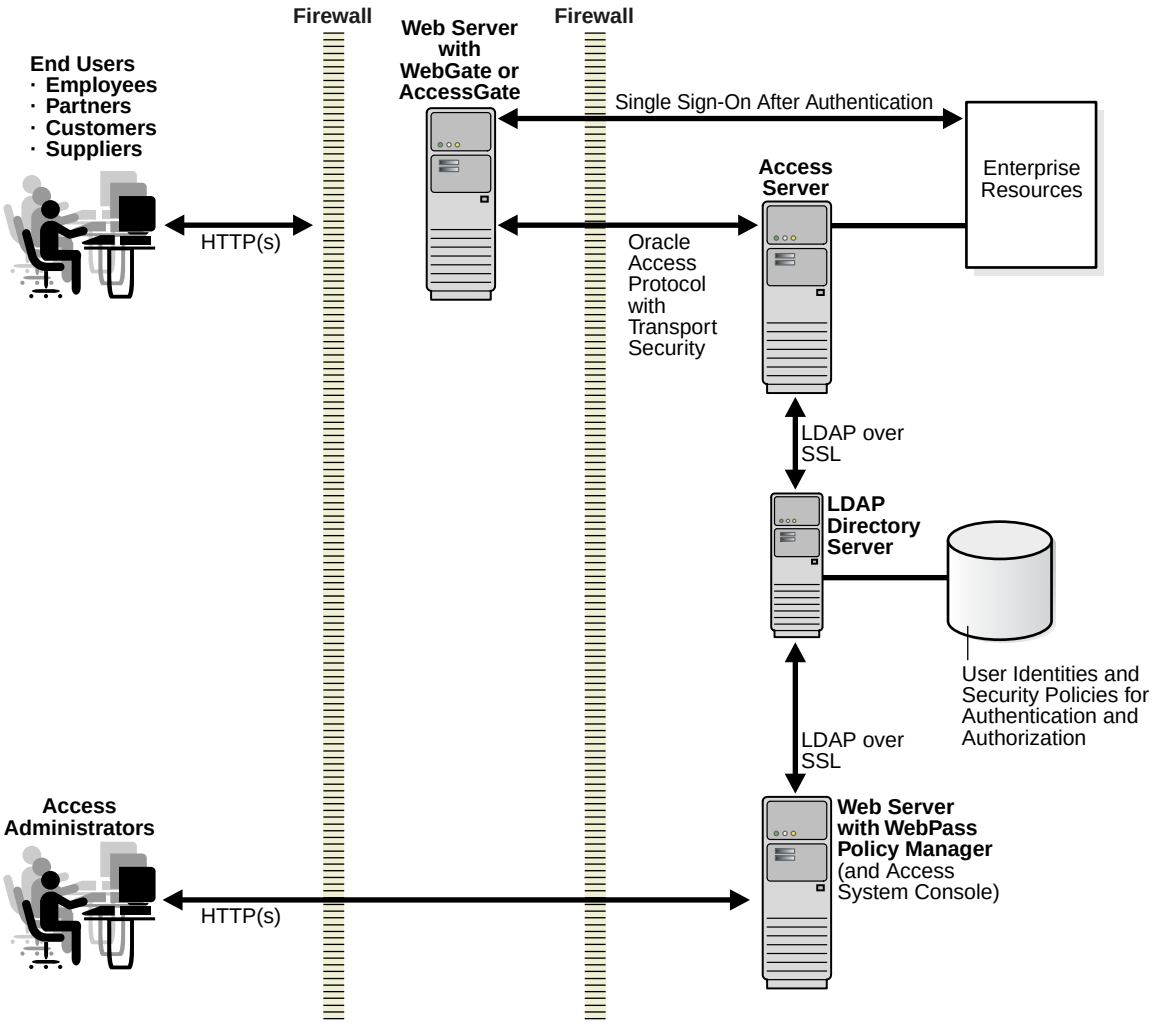
This section includes the following topics:

- Policy Manager and Access System Console
- The Access Server
- WebGates and AccessGates
- Access System Operation

Components of the Oracle Access Manager Access System

Figure 6–1 shows the basic components of the Access System. The WebGate communicates with the Access Server; the Access Server communicates with the directory server; the Policy Manager communicates with the directory server through a WebPass.

Figure 6–1 Basic Access System Installation



The Oracle Access Protocol (formerly known as the NetPoint or COREid Access Protocol) enables communication between Access System components during user authentication and authorization. Transport security between Web clients (Policy Manager and WebPass; Access Server and WebGate) can be Open, Simple (Oracle-provided), and Cert (third-party CA). In both Simple and Cert mode, Oracle Access Manager components use X.509 digital certificates only.

Transport security between Access Servers and the directory server (and Policy Managers and directory server) may be either open or SSL-enabled. The same mode must be used between all Policy Managers and the directory server.

During Policy Manager installation and setup, the LDAP directory server is updated to include policy data (access policy data). All access policy definitions defined in the Policy Manager are stored in the directory server.

Policy Manager and Access System Console

This discussion introduces the Policy Manager, Access System Console, and functions available with each.

Policy Manager—The Policy Manager provides the login interface for the Access System, communicates with the directory server to write policy data, and communicates with the Access Server over the OAP to update the Access Server when you make certain policy modifications.

Master Access Administrators and Delegated Access Administrators use the Policy Manager to:

- Create and manage policy domains that consist of:
  - Resource types to protect
  - Authentication, authorization, and audit rules
  - Policies (exceptions)
  - Administrative rights
- Add resources to policy domains
- Test access policy enforcement

The Policy Manager must be installed on a machine hosting a Web server instance with a WebPass (installed at the same directory level as the Policy Manager). Oracle recommends that you install multiple Policy Managers for fault tolerance. For details about installing the Policy Manager, see the *Oracle Access Manager Installation Guide*.

Access System Console—Included with the Policy Manager. Provides a login interface to the Access System Console and the functions that allow any Master Administrator, Master Access Administrator, and Delegated Access Administrator to use the following functional options:

- **System Configuration**—Enables a Master Oracle Access Manager Administrator to assign users to be a Master Access Administrator, as well as add or remove Delegated Access Administrators and their rights. Responsibilities of a Master Access Administrator include defining resource types, policy domains, and authentication and authorization schemes.

  From the System Configuration tab, administrators can also view and change server settings from this tab. For example, you can specify email addresses for bug reports, user feedback, and the company Web master. You can change the default logout URL for single sign-on, configure directory server settings, and view cache settings.
- **System Management**—Enables a Master Administrator to manage:
  - Diagnostics—Show Access Server details, including connection information.
  - Manage Reports—Create, view, or modify user access privilege reports.

  - Manage Sync Records—Archive or purge synchronization records generated by the Policy Manager before a given date. To help you manage the space these records consume on the directory server, it is a good idea to periodically archive or purge all the records before a specified date.

- **Access System Configuration**—Enables a Master Access Administrator or Delegated Access Administrators to complete the following tasks:
  - View, add, modify, and delete AccessGates, Access Servers, Access Server clusters, Host Identifiers
  - View and modify authentication and authorization parameters; Web resource user rights; and common information
  - Configure common information, including:

    Shared Secret: Generate a cryptographic key that encrypts cookies sent from an AccessGate or WebGate to a browser.

    Master Audit Rule: Create the default Master Audit Rule for this installation.

    Resource type Definitions: Define and manage resource types.

    Flush Password Policy Cache: Select a password policy and flush all associated caches or select a Lost Password Management policy and flush all associated caches.

    Duplicate Actions: Select a policy for handling Duplicate Action Headers

The Access Server

The Access Server plays a key role in authentication and authorization:

- Authentication involves determining what authentication method is required for a resource and gathering credentials from the directory server, then returning an HTTP response based on the results of credential validation to the access client (WebGate or AccessGate).
- Authorization involves gathering access information and granting access based on a policy domain stored in the directory and the identity established during authentication.

To perform these operations, you may have one or more standalone Access Server instances that communicate with both the directory server and WebGate. Before you can install an Access Server instance, you must define it in the Access System Console.

Note: Oracle recommends that you install multiple Access Servers for failover and load balancing.

Process overview: Access Server functions

1. Receives requests from an access client (WebGate or AccessGate)
2. Queries authentication, authorization, and auditing rules in the directory server to determine whether:
   a. The resource is protected (and if so, how)
   b. The user is already authenticated (if the user is not yet authenticated, a challenge is provided)
   c. The user credentials are valid

   d. The user is authorized for the requested resource, and under what conditions

3. Responds to the access client as follows:
   a. Sends the authentication scheme
   b. Validates credentials
   c. Authorizes the user
   d. Audits
4. Manages the session, by:
   a. Helping the WebGate terminate user sessions
   b. Re-authenticating when there is a time out
   c. Tracking user activity during a session
   d. Setting session timeouts for users

WebGates and AccessGates

Throughout Oracle Access Manager manuals, the terms AccessGate and WebGate may be used interchangeably. However, there are differences worth noting:

- A WebGate is a Web server plug-in access client that intercepts HTTP requests for Web resources and forwards them to the Access Server for authentication and authorization. A WebGate is shipped out-of-the-box with Oracle Access Manager.
- An AccessGate is a custom access client that is specifically developed using the Software Developer Kit (SDK) and Access Manager APIs, either by you or by Oracle. An AccessGate is a form of access client that processes requests for Web and non-Web resources (non-HTTP) from users or applications.

A WebGate intercepts requests for resources from users or applications and forwards requests to the Access Server for authentication and authorization. See "Access System Operation" on page 6-7 for more information.

Before you can install a WebGate, you must define it in the Access System Console and associate it with an Access Server or cluster of Access Servers. For details, see *Oracle Access Manager Installation Guide.*

Access System Operation

The following description explains how Access System components work in concert during authentication and authorization. See also Figure 6–2.

Process overview: When a user requests access

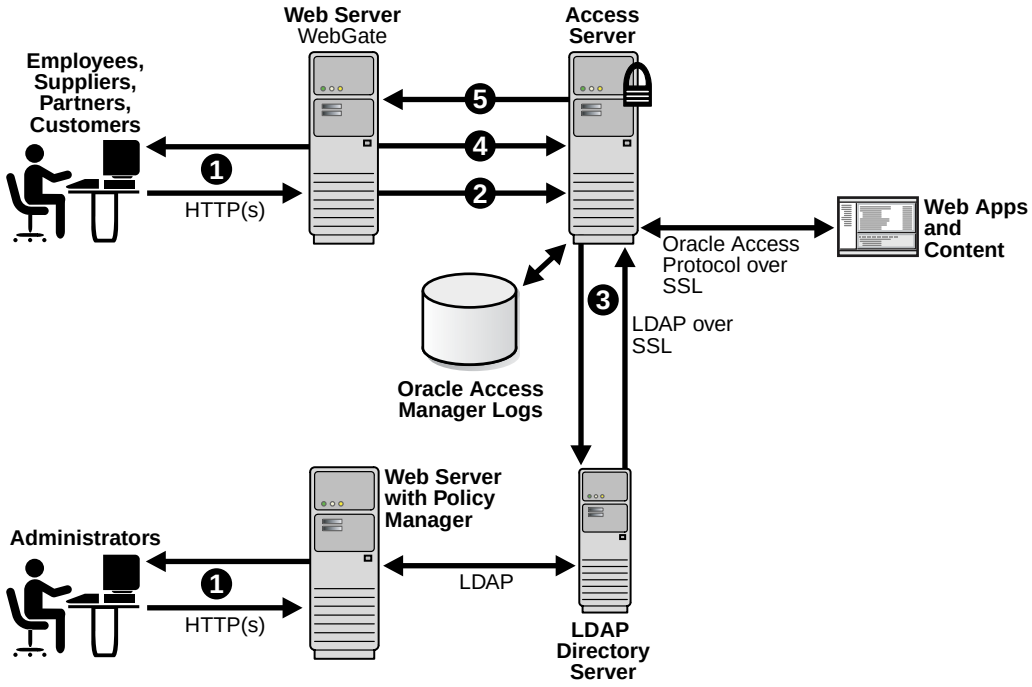
1. The WebGate intercepts the request.

   Servers that can be protected include Web servers, application servers, and FTP servers (using the Access Manager SDK), among others.
2. The WebGate forwards the request to the Access Server to determine whether the resource is protected, how, and if the user is authenticated (if not, there is a challenge).
3. The Access Server checks the directory server for credentials such as a user ID and password, sends the information back to WebGate, and generates an encrypted cookie to authenticate the user.

The Access Server authenticates the user with a customer-specified authentication method to determine the identity, leveraging information stored in the directory server. Oracle Access Manager authentication supports any third-party authentication method as well as different authentication levels. Resources with varying degrees of sensitivity can be protected by requiring higher levels of authentication that correspond to more stringent authentication methods.

4. Following authentication, the WebGate prompts the Access Server to look up the appropriate security policies, compare them to the user's identity, and determine the user's level of authorization.
   - If the access policy is valid, the user is allowed to access the desired content or applications.
   - If the policy is false, the user is denied access and redirected to another URL determined by the organization's administrator.

Figure 6–2 Basic Access System Operations



As mentioned earlier, the Policy Manager provides the login interface for the Access System, communicates with the directory server to write policy data, and communicates with the Access Server over the OAP to update the Access Server when you make certain policy modifications. The WebPass intercepts and forwards administrator requests for the Policy Manager and Access System Console.

Oracle Access Manager Identity System Features

Administrators can build password management and other functions on top of the Oracle Access Manager identity management system. You can integrate other applications with the primary Identity System components using a single identity management system so that access cards, computer accounts, and payroll functions can all be modified from one identity change function when an employee leaves an organization. Customization and XML-based integration features are included.

End users can search for and view other users and groups, depending on the rights granted to them by an administrator; modify personal information such as phone numbers and passwords; and display organizational information such as floor plans and asset lists.

Identity System administration features include:

- **Centralized User, Group, and Organization (object) Management**—Enables you to provide different access policies for different people and groups and to manage organizational entities, such as assets and maps. Information in the Oracle Access Manager Identity System can then be leveraged by the Oracle Access Manager Access System to manage access privileges based on user attributes, group membership, or association with an organizational entity.
- **Dynamic Role-Based Identity Administration**—Provides security guided by user identity-based access privileges. For example, a role may include all users or all managers or direct-reports only, and so on.
- **A Customizable Multi-Step Identity Workflow Engine**—Enables you to map and automate business processes, policies, and approvals relating to identity data. For example, you can model your business processes in the Identity System using workflows to:
  - Create, delete, and modify users, groups, and organizations
  - Implement self-registration of users and organizations
  - Subscribe and unsubscribe to groups
- **Multi-Level Delegation of Identity Administration**—Enables you to scale up to millions of users by delegating identity administration activities. Administrators can delegate all or some of the rights they have been granted, and they can choose whether or not to allow their delegates to pass these rights on to others. The tasks that are delegated are specific to the right, the target, and the tree path.
- **Self-Service**—Enables you to implement a secure self-service model for organizational functions such as password change. Users with self-service permissions can manage their own information without the use of a workflow.
- **Self-Registration**—Provides limited access to your system through the initiation and processing of a self-registration workflow.

  For example, you can set up a self-registration workflow such that when a user self-registers, the registration request is forwarded to appropriate people for approval. Upon approval, the user is immediately and automatically granted access to all appropriate resources based on his or her identity attributes.
- **Data Management Layer**—Supports multiple LDAP environments, RDBMS databases, and split-directory profiles. This feature is also known as Data Anywhere and is available with Oracle Virtual Directory. Data Anywhere aggregates and consolidates data from RDBMS and LDAP directories into a virtual LDAP tree. The tree can be managed by the Oracle Access Manager Identity System and used to support authentication and authorization with the Oracle Access Manager Access System. For complete details, see the *Oracle Access Manager Identity and Common Administration Guide*.
- **Password Management Services**—Enables you to specify multiple password policies, constraints on password composition, a configurable password validity period and notification, forced password change, lost password management setup, and password creation / change rules.

- **User Interface Customization**—Provides several methods you can use to change the appearance of Oracle Access Manager applications and control operations, and connect CGI files or JavaScripts to Oracle Access Manager screens. For details, see the *Oracle Access Manager Customization Guide*.
- **Extensive APIs for Identity Integration**—Enables you to gain access and interact with Oracle Access Manager without using a browser, and implement functions and executables triggered by events within Oracle Access Manager. For details, see the *Oracle Access Manager Customization Guide*.

Unless otherwise indicated, you can find more information about these features and how to configure them in the *Oracle Access Manager Identity and Common Administration Guide*. For a simple installation diagram, see the next discussion: "How the Oracle Access Manager Identity System Works".

How the Oracle Access Manager Identity System Works

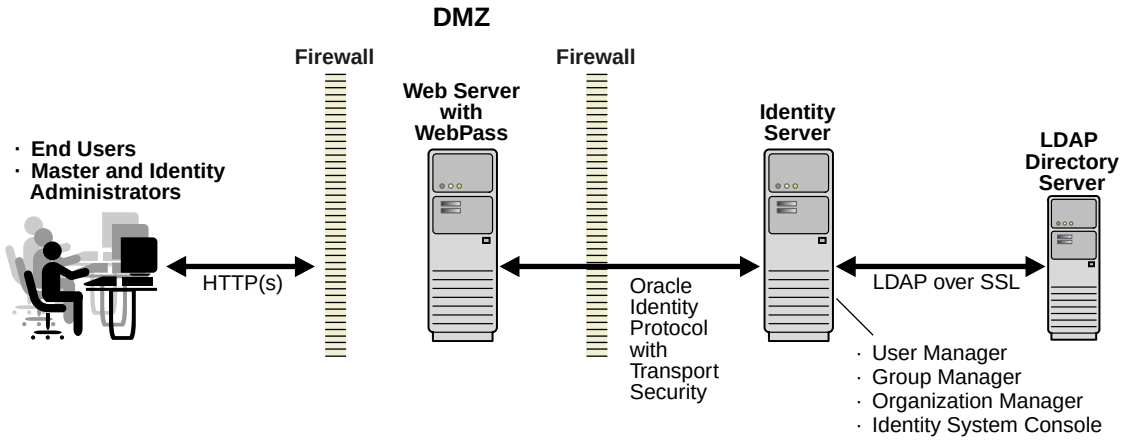
The Oracle Access Manager Identity System provides the infrastructure needed for other applications and systems to leverage user identity and policy information across the enterprise. This eliminates the need to create and manage separate user identity repositories for each application.

This section contains the following topics:

Oracle Access Manager Identity System Components

Figure 6–3 illustrates the basic Identity System components in a simple environment, as well as transport security between components over the Oracle Identity Protocol (formerly known as the NetPoint or COREid Identity Protocol). The end users and Administrators are separated from components by a firewall. The Web server with WebPass installed resides in the DMZ. The Identity Server and directory server reside behind the second firewall.

Figure 6–3 Components in a Simple Environment



The Oracle Identity Protocol facilitates communication between Identity Servers and associated WebPass instances. Transport security between Oracle Access Manager Web

clients (WebPass and Identity Server) may be specified as Open, Simple (Oracle-provided), or Cert (third-party CA). In both Simple and Cert mode, Oracle Access Manager components use X.509 digital certificates only. Transport security between Identity Servers and the directory server may be either open or SSL-enabled.

During Oracle Access Manager installation and setup, the LDAP directory server is updated to include the Oracle Access Manager schema with object classes and attributes for the entire system. Oracle Access Manager enables you to store various types of data on the same directory server type, or separate directory server types. Data types include:

- **User Data**—User directory entries managed by Oracle Access Manager
- **Configuration Data**—Oracle Access Manager configuration details stored in the directory and managed by the Identity System
- **Policy Data**—Access policy definitions defined in the Policy Manager are stored in the directory server

During Oracle Access Manager installation and setup, the Master Oracle Access Manager Administrator (Master Administrator) is assigned. The Master Administrator is a super user who is empowered to configure the deployment and assign administrative tasks. Using the System Console, the Master Administrator can create additional Master Administrators, as well as Master Identity Administrators and Master Access Administrators. For example, a Master Identity Administrator can delegate authority to other administrators, which enables management of millions of users.

In addition to managing identity information, you can use the Identity System to manage access privileges for a user based on a specific user attribute, membership in a group, or association with an organization. Administrators can link privileges together into a workflow so that, for example, when a user self-registers, the registration request is forwarded to appropriate people for signoff.

The Identity Server and Identity Applications

Your Oracle Access Manager installation must include at least one Identity Server. You use the Identity Server to manage identity information about users, groups, organizations, and other objects. Your installation may include one or more Identity Server instances. The Identity Server performs three main functions:

- Reads and writes to your LDAP directory server across a network connection
- Stores user information on a directory server and keeps the directory current
- Processes all requests related to user, group, and organization identification

Each instance of the Identity Server communicates with a Web server through a WebPass plug-in, as discussed in "WebPass" on page 6-12.

The Identity Server provides the following Identity applications, which are accessed through a Web-based interface. All have a reporting capability:

- **User Manager**—Enables complete management of all identity information related to individual network users.

  The User Manager enables administrators to add, modify, deactivate, and delete user identities. In addition, the User Manager enables administrators to provide users with access privileges based on their directory profiles (and substitute rights), as well as view and monitor requests.

Typically, end users can view other users and modify their own identity information. The users that a person can view and the identity information that someone can modify depends on the privileges granted by the Master Administrator.

- **Group Manager**—Enables authorized personnel to create, manage and delete static, dynamic, or nested groups or to delegate group administration.

  Administrators can create or delete groups, and enable users to subscribe or unsubscribe from groups.

  End users can view groups and subscribe to membership in a group. The groups that a person can view, and subscription rights, are granted by a Master Administrator.

- **Organization Manager**—Helps you manage system rules, access privileges, and workflows to manage ongoing changes for entire organizations.

  Administrators can create and delete organizations and other objects (such as floor plans and assets) that do not belong in the User Manager or Group Manager.

  End users can view organizational entities. The organizational entities that a person can view depend upon the rights granted by a Master Administrator.

- **Identity System Console**—Provides Web-based administration and configuration that is used to create administrators and assign the right to delegate administrative tasks. Tabs in the Identity System Console provide access to specific identity administration functions.

WebPass

A WebPass is an Oracle Access Manager Web server plug-in that passes information back and forth between a Web server and the Identity Server. Depending upon its configuration, the Identity Server processes the request either as an XML or HTML file.

A WebPass can communicate with multiple Identity Servers. Each Web server instance that communicates with the Identity Server must be configured with a WebPass. In a Oracle Access Manager installation:

- At least one WebPass must be installed on a Web server and configured to communicate with at least one Identity Server.
- A WebPass is required on each machine hosting an Oracle Access Manager Policy Manager.

After installing an Identity Server and a WebPass, you must complete an initial Identity System setup process so the Identity Server and WebPass can communicate.

Process overview: WebPass functions

1. The WebPass receives the user request and maps the URL to a message format.
2. The WebPass forwards the request to an Identity Server.
3. The WebPass receives information from the Identity Server and returns it to the user's browser.

7

Oracle Identity Federation

Although single sign-on (SSO) enjoys wide adoption for its ability to cut down the need for redundant logins, mere SSO is insufficient for companies that operate in a federated environment, that is, an environment where services are shared with business partners, while protecting those same services from unauthorized access.

Oracle Identity Federation is a standalone, self-contained federation server that enables single sign-on and authentication in a multiple-domain identity network. Oracle Identity Federation supports multiple federated identity protocols including the Liberty ID-FF and SAML protocols. This allows users to federate in heterogeneous environments and business associations, whether or not they have implemented other Oracle Identity Management products in their solution set.

This chapter provides an introduction to federated identity management and describes key features and benefits of Oracle Identity Federation. It contains the following sections:

Benefits of Oracle Identity Federation

A federated environment enables business partners to achieve integration in the identity management realm by providing a mechanism for companies to share identity information across their respective security domains.

Federated identity management is the evolution of the SSO paradigm in response to users' growing needs for access to computing resources and services that reside outside their own company's boundaries. In a federated environment, enterprises offering such a service can reliably obtain identity information about an individual or other entity from the user's home organization or security domain. This provides twin benefits:

1. The end user does not need to supply login credentials to access each entity where business is conducted. This also eliminates the need to remember and manage multiple logins / passwords. (Users still need accounts at the sites so that the accounts can be linked.)
2. Enterprises do not need to create additional accounts to manage the identities of users who are already known to a partner organization. In the example cited earlier, the service provider could simply leverage the employee data maintained internally by its client health care organizations.

Features of Oracle Identity Federation

Key features of Oracle Identity Federation include:

- **Cross-Site Capability**—You can implement cross-site access and authentication in an environment containing both identity providers and service providers.
- **Configurability**—You canconfigure, enable, and disable external sites.
- **Single Sign-On**—Users can access applications at destination sites using a single sign-on.
- **Federation Protocol Support**—Oracle Identity Federation supports these leading federation protocols:
  - Liberty ID-FF 1.1
  - Liberty ID-FF 1.2
  - SAML 1.0
  - SAML 2.0, including a SAML 2.0 responder
  - WS-Federation
- **Integration with Other Products**—Oracle Identity Federation is integrated with Oracle Internet Directory, Oracle Access Manager, and OracleAS Single Sign-On. It also supports:
  - A range of authentication engines, including Oracle Access Manager and CA eTrust SiteMinder
  - User data repositories, including LDAP Stores such as Microsoft Active Directory and Sun Java System Directory Server
  - Relational databases
- Support for cross-protocol single sign-on and sign-out.
- **Affiliations**—Oracle Identity Federation supports affiliations, which reduce the number of federations by allowing service providers to share their federation information.
- **Certificate Validation**—Oracle Internet Directory supports X.509 certificate validation.

How Oracle Identity Federation Works

This section contains the following topics:

Federation Use Cases

Use cases in this section explain how federation can provide a seamless end-user experience by authenticating once for multiple applications.

Use Case 1: Single Sign-On to Partner Site

Figure 7–1 Single Sign-On from Employee Portal to Partner

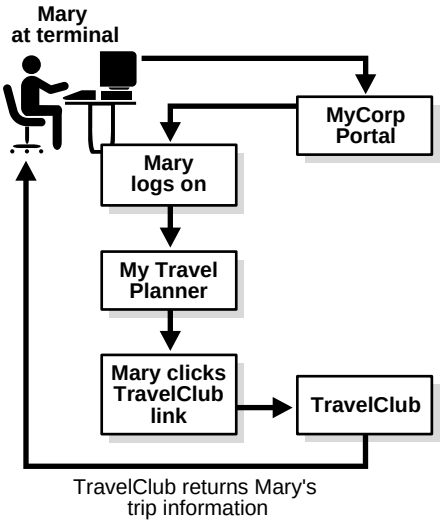


Figure 7–1 describes a situation where Mary, an employee of MyCorp, wishes to plan an upcoming business trip. She is able to achieve this seamlessly, in a single session, by performing the following steps:

1. Mary accesses her company's MyCorp employee portal from her terminal.
2. The portal, which is enabled with WS-Federation, presents her with a sign-on dialog.
3. After Mary signs on, the portal returns a page personalized with her information.
4. Mary commences travel planning by clicking on a link inside the portal for TravelClub, which is a partner organization providing access to a range of travel services for MyCorp employees. Mary has already established a federated relationship with TravelClub.
5. TravelClub requires authentication before Mary can access her account, and requests the same from MyCorp, which returns the necessary identity information to the travel site. Mary is then automatically authenticated to the TravelClub site. TravelClub returns a page with Mary's travel account information.
6. When Mary is done, she can log out of both her TravelClub and MyCorp sessions using a single global logout feature at the MyCorp home page.

In this way, Mary is able to authenticate once to her company's Web site, connect with another site and perform necessary tasks, without the need for any additional authentication at the second site.

Use Case 2: New Federated Account at Partner Site

Figure 7–2 Creating a Federated Account

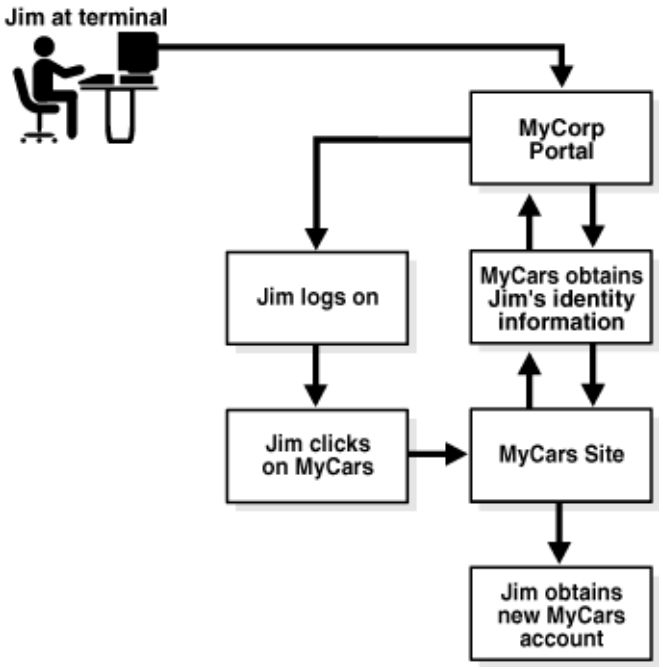


Figure 7–2 illustrates a use case where Jim, another employee at MyCorp, wishes to set up a new account at MyCars, an external site which provides discount auto repair services to MyCorp employees. The steps are as follows:

1. Jim signs on to the MyCorp portal.
2. After doing some work within the portal, Jim elects to move to the "Vendors" page of the portal to look for automotive services, and clicks on the MyCars link.
3. Information is required to set up a new account at MyCars. With Jim's permission, MyCars communicates with MyCorp to obtain information relevant to Jim's identity.
4. Jim now has an account at MyCars, which he can access in a manner similar to that outlined in the previous use case.

These use cases are typical examples of the application of federated single sign-on and federated identity management. In subsequent sections we take a closer look at the key concepts of federation technology, and how they are leveraged in Oracle Identity Federation.

Federation Event Flow

This section describes a typical message flow in a federated interaction.

Elaborating on the use case in Figure 7–1, consider that Mary is already authenticated at mycorp.com, and goes to travelclub.com where she is not logged in. travelclub.com requires Mary to be authenticated before she can access her local account, and redirects Mary with a SAML 2.0 message to mycorp.com requesting a single sign-on for travelclub.com. Since Mary is already logged in at the identity provider, mycorp.com retrieves Mary's account and federation data and redirects her back to travelclub.com. Using the Provider Identifier `mycorp.com` and the User Identifier `xyz123` provided

with the redirect, travelclub.com can uniquely retrieve Mary's federation data and her local account.

Federation Protocol Profiles

Identity providers and service providers exchange assertions using profiles and services defined in a federation protocol such as SAML or Liberty ID-FF. Assertion functions include:

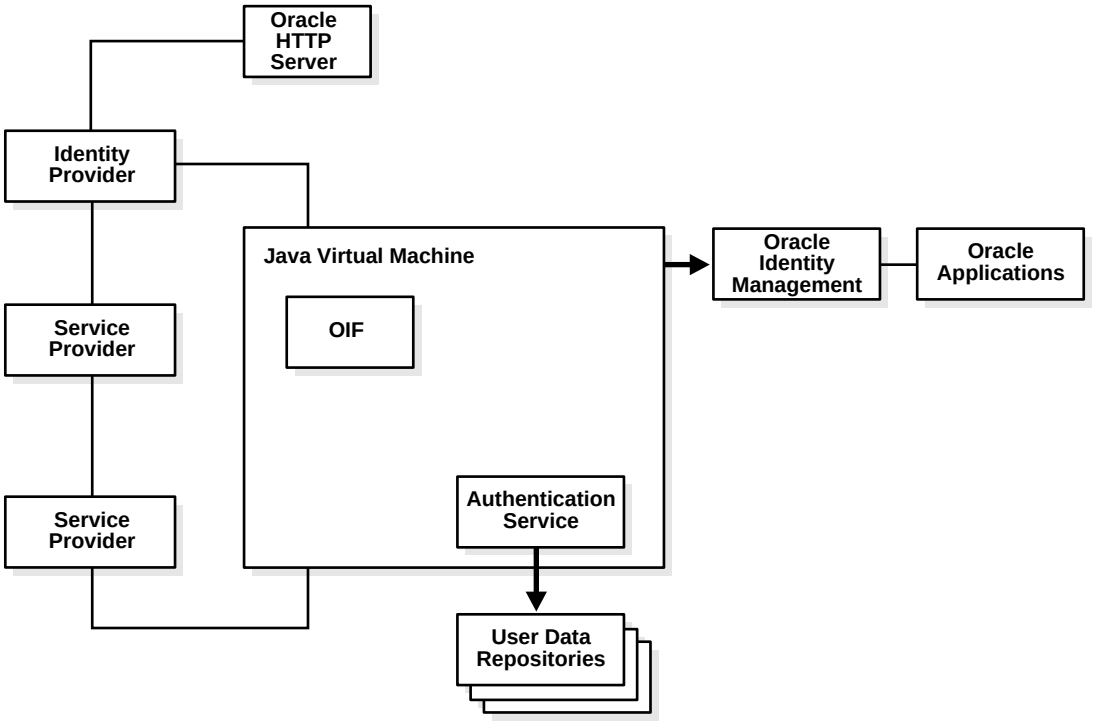
- establishing secure connections
- conveying authentication data across those connections
- receiving and interpreting assertions from other SAML domains

Profiles describe the types of exchanges required to transfer assertions between IdP and SP. This section takes a closer look at the assertion profiles available in Oracle Identity Federation.

Federation Architecture

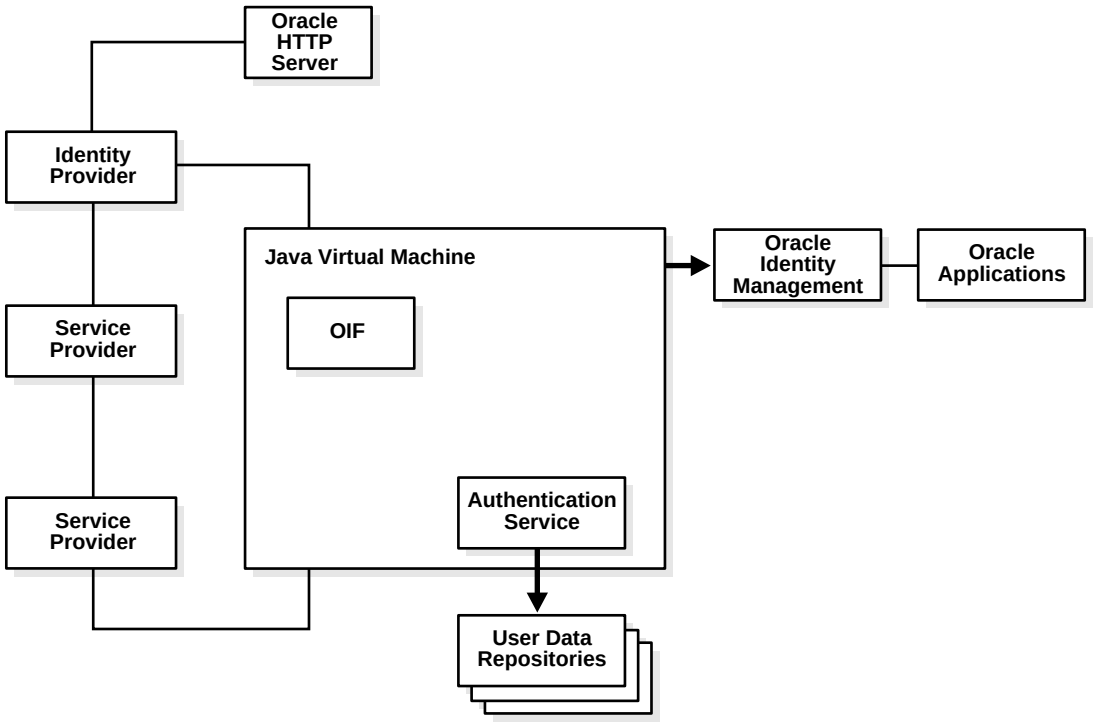
Figure 7–3 shows the architecture of Oracle Identity Federation (OIF) and its relationship to other federation components. Here Oracle Identity Federation is a member of a circle of trust containing other identity providers and service providers, which can be additional Oracle Identity Federation instances or third-party providers.

Figure 7–3 Oracle Identity Federation



Oracle Identity Federation includes a self-contained, lightweight authentication service. Based on IdMBridge, this service—illustrated in Figure 7–4—is deployed in a WAR (Web Application aRchive) file with Oracle Identity Federation and runs in the same Java Virtual Machine as the server.

Figure 7–4 Oracle Identity Federation 3rd Party Integration



Oracle Identity Federation can communicate with a range of authentication mechanisms and user data repositories:

1. Oracle Identity Management

   You can configure the Oracle Identity Federation authentication service to enable single sign-on access to resources protected by OracleAS Single Sign-On or Oracle Access Manager, including:

   - Oracle Collaboration Suite
   - Oracle E-Business Suite
   - PeopleSoft modules
   - and more

   In addition to Oracle Application Server Single Sign-On (with the Oracle Internet Directory user repository) or Oracle Access Manager (with various repositories), this configuration can also leverage third-party access management solutions when OracleAS Single Sign-On is deployed for use with those solutions.

Note: In an environment where Oracle Identity Federation and OracleAS Single Sign-On both protect resources, you can configure either component to serve as the authentication mechanism when a user requests access to a protected resource. For example, Oracle Identity Federation can forward authentication requests to OracleAS Single Sign-On; or, OracleAS Single Sign-On can request Oracle Identity Federation to locate an appropriate identity provider. For details, see *Oracle Application Server Single Sign-On Administrator's Guide*.

Likewise, environments containing both Oracle Identity Federation and Oracle Access Manager provide similar functionality.

2. Data Stores

   You can configure Oracle Identity Federation to access:

   - LDAP directories
   - RDBMS databases
   - Oracle Access Manager
   - eTrust SiteMinder

8

OracleAS Single Sign-On

Oracle Application Server (OracleAS) Single Sign-On enables you to use a single user name, password, and optionally a realm ID to log in to all features of OracleAS as well as to other Web applications.

Oracle components delegate the login function to the OracleAS Single Sign-On server. When a user first logs into an Oracle component, the component redirects the login to the OracleAS Single Sign-On server. The OracleAS Single Sign-On server authenticates the user by verifying the credentials entered by the user against those stored in Oracle Internet Directory. After authenticating the user, and throughout the rest of the session, the OracleAS Single Sign-On server grants the user access to all the components the user both seeks and is authorized to use.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide* for information about OracleAS Single Sign-On.

This chapter contains the following topics:

Benefits of Oracle Application Server Single Sign-On

OracleAS Single Sign-On provides the following benefits:

- **Reduced administrative costs**—The single sign-on server eliminates the need to support multiple accounts and passwords.
- **Convenient login**—Users do not have to maintain a separate user name and password for each application that they access.
- **Increased security**—When a password is required only once, users are less likely to use simple, easily exposed passwords or to write these passwords down.

Features of Oracle Application Server Single Sign-On

Oracle Application Server Single Sign-On provides the following features:

- **Federated Authentication**—You can implement federated authentication using Oracle Application Server Single Sign-On and . Federated single sign-on permits users to access information on different corporate Web sites while authenticating to only one of those sites. You can configure either Oracle Application Server

Single Sign-Onor to be the authentication mechanism for users who want to access resources that are protected by either product.

- **Identity Management Grid Control Plug-in**—As of Oracle Application Server 10*g* (10.1.4.0.1), you can manage Oracle Directory Integration Platform with Identity Management Grid Control Plug-in, which uses the features of Oracle Enterprise Manager 10*g* Grid Control.

  See Also: The "Identity Management Grid Control Plug-in" chapter in *Oracle Identity Management Infrastructure Administrator's Guide*.

- **Global User Inactivity Timeout**—The global user inactivity timeout is a feature that enables applications to force you to reauthenticate if you have been idle for a preconfigured amount of time. This timeout is a useful feature for sensitive applications that require a shorter user inactivity timeout than the single sign-out session timeout.
- **Wireless Option**—You can use mobile, or wireless, devices such as personal digital assistants, cellular phones, and voice recognition systems to access OracleAS applications. If you select the wireless option when installing OracleAS, Portal-to-Go, the gateway for mobile devices, is registered with the single sign-on server automatically.

  See Also:

  - *Oracle Application Server Wireless Administrator's Guide*
  - *Oracle Application Server Wireless Developer's Guide*

  for more information about Oracle Application Server Wireless.

- **Single Sign-Off**—You can terminate a single sign-on session and log out of all active partner applications simultaneously. Clicking **Logout** in a partner application takes you to the single sign-off page, where logout occurs.
- **Changing Passwords**—When a your password is about to expire, Oracle Application Server Single Sign-On presents the change password screen. To change or reset a password under other circumstances, a nonadministrative user can use Oracle Delegated Administration Services.

How OracleAS Single Sign-On Works

This section contains the following topics:

Components of the Single Sign-On System

OracleAS Single Sign-On interacts with several components. They include:

- **Single Sign-On Server**—The single sign-on server consists of program logic that enables users to log in securely to single sign-on applications such as expense reports, mail, and benefits. The single sign-on server program logic resides in the Oracle Application Server database, Oracle HTTP Server, and OC4J server.

- **Partner Application**—an Oracle Application Server application or non-Oracle application that delegates the authentication function to the OracleAS Single Sign-On server. This type of application spares users from reauthenticating by accepting headers from an authentication module named mod_osso. Examples of partner applications include OracleAS Portal, OracleAS Discoverer, and Oracle Delegated Administration Services.
- **External Application**—a non-Oracle application that displays an HTML login forms that ask for application user names and passwords. At the first login, a user can select the **Remember My Login Information For This Application** check box. On subsequent logins, the server uses the single sign-on user name to locate and retrieve application names and passwords and to log the user in without requiring the user to authenticate.
- **mod_osso**—an Oracle HTTP Server module that provides authentication to OracleAS applications. Mod_osso works only with the Oracle HTTP listener. You can use OracleAS SSO Plug-in to protect applications that work with third-party listeners such as Sun One and IIS.

  See Also: *Oracle Identity Management Application Developer's Guide* for more information about mod_osso.

- **Oracle Internet Directory**—the repository for all single sign-on user accounts and passwords, both administrative and nonadministrative. The single sign-on server authenticates users against their entries in the directory. At the same time, it retrieves user attributes from the directory that enable applications to validate users.

Accessing the Single Sign-On Server

Nonadministrative users first gain access to the single sign-on server by entering the URL of a partner application such as OracleAS Portal. Entering such a URL invokes the single sign-on login screen. Once they have entered the correct user name and password, users gain access to other partner applications and to external applications without having to provide credentials again.

Administrative users can access the administration home page for single sign-on by typing a URL of this form:

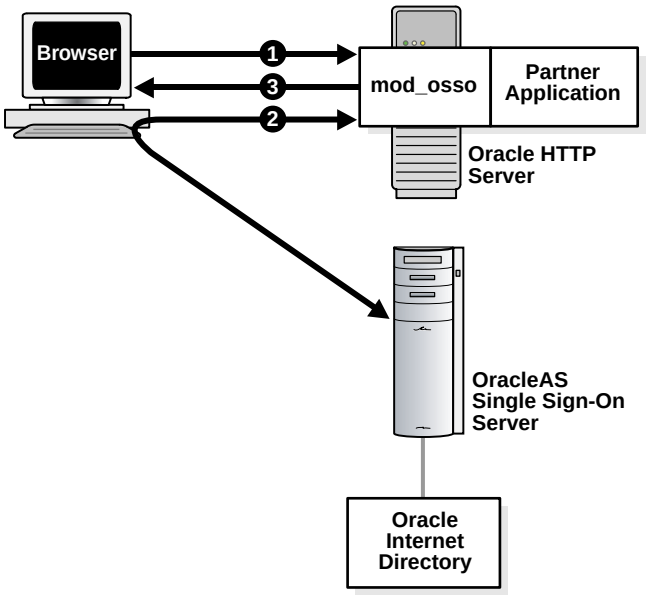
`http://host:port/sso`

where *host* is the computer where the single sign-on server is located and *port* is the port number of the server. If the server is enabled for SSL, `https` must be substituted for `http`. If the port number is `80` or `443` (SSL), it may be omitted from the URL. These numbers are the defaults.

Accessing a Partner Application

Figure 8–1 shows what happens when the user requests the URL of a partner application that is protected by mod_osso. This illustration shows the single sign-on server and the partner application server residing on separate computers, one placed above the other. To the left of the partner application server is the browser. Attached to the single sign-on server is a box that represents Oracle Internet Directory. Arrows show the browser requesting an application, being redirected to the single sign-on server, and, finally, being redirected back to the partner application.

Figure 8–1 Single Sign-On with mod_osso



1. The user tries to access a partner application.
2. The user is redirected to the single sign-on server. The server challenges the user for credentials. After verifying the credentials in Oracle Internet Directory, the server sets the SSO session cookie and passes an authentication token to the partner application.
3. The application serves up the requested content.

Authenticating to a Partner Application After the First Time

Requesting access to a partner application initiates the partner application login process. The following occurs if you are accessing a new partner application after having already logged in to the Single Sign-On server:

1. The user tries to access a partner application.
2. The user is redirected to the single sign-on server. The server does not challenge the user for authentication credentials. The SSO session cookie is used to validate the user identity.
3. The server passes an authentication token to the partner application.
4. The application serves the requested content.

Logging Out of an Partner Application

Unlike external applications, partner applications cede logout control to the single sign-on server. When the user logs out of one partner application, he or she is automatically logged out of the other partner applications.

Accessing an External Application

External applications are available through OracleAS Portal, a single sign-on partner application.

This section contains these topics:

- Accessing the External Applications Portlet in OracleAS Portal

Accessing the External Applications Portlet in OracleAS Portal

To gain access to an external application, you select the External Applications portlet on the OracleAS Portal home page; then, from the list of external applications that appears, you select an application.

Authenticating to an External Application for the First Time

Selecting an application in the External Applications portlet initiates the external application login procedure. The following occurs if you are accessing the application for the first time:

1. The external application login procedure checks the single sign-on password store for your credentials. If it finds no credentials, the single sign-on server prompts you for them.
2. You enter your user name and password. You can save these credentials in the password store by selecting the **Remember My Login Information** check box on the application login screen.
3. If you elect to save your credentials in the password store, the server uses these credentials to construct a login form to submit to the login processing routine of the application. This routine has been preconfigured by the administrator and is associated with the requested application.
4. The server sends the form to the client browser, with a directive to post it immediately to the external application.
5. The client posts the form to the external application and logs you in.

If you decline to save your credentials in the password store, you must enter a user name and password each time that you log in.

Authenticating to an External Application After the First Time

If you saved your credentials when accessing an external application for the first time, the single sign-on server retrieves your credentials for you during subsequent logins. The process works like this:

1. You click one of the links in the External Applications portlet of OracleAS Portal.
2. The external application login procedure checks the password store for your credentials.
3. The single sign-on server finds your credentials and uses them to construct a login form to submit to the login processing routine of the application. This routine has been preconfigured by the administrator and is associated with the requested application.
4. The server sends the form to the client browser, with a directive to post it immediately to the external application.
5. The client posts the form to the external application and logs you in.

Logging Out of an External Application

Unlike partner applications, external applications do not cede logout control to the single sign-on server. It is the user's responsibility to log out of each of these applications.

9

Oracle Identity Manager

The Oracle Identity Manager platform automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager instantly connects users to resources they need to be productive and revokes and restricts unauthorized access to protect sensitive corporate information.

The identity audit and compliance automation component of Oracle Identity Manager also provides automated attestation and reporting.

This chapter describes the architecture, benefits, and key features of Oracle Identity Manager. It contains the following topics:

Benefits of Oracle Identity Manager

Automating user identity provisioning can reduce IT administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Compliance initiatives focus on the enforcement of corporate policies as well as the demonstration of compliance with these standards. An enterprise identity management solution can provide a mechanism for implementing the user management aspects of a corporate policy, as well as a means to audit users and their access privileges. Oracle's enterprise user provisioning solution is Oracle Identity Manager.

Due to a number of recent government and industry initiatives, corporations must stringently enforce internal controls and regulatory compliance. All organizations with trade-able securities in US markets are required to authorize and validate user identity information for all internal and external users, including their entitlements, as well as the access policies and workflow processes defined by and in use within various divisions in the organization. The process of authorizing established internal controls, processes, policies, programs, and data, is commonly referred to as attestation.

In most corporate entities, attestation is performed by using manual processes and spreadsheets, which can be very time consuming and costly. Such manual processes are subject to human errors and must be repeated at every audit. By automating these routine tasks, organizations can realize significant time and cost savings. Oracle provides automated attestation using the identity audit and compliance automation component of Oracle Identity Manager .

Automated attestation capabilities allow organizations to quickly generate reports across the organization's business and IT environment. Automated attestation complements existing internal control mechanisms and provides a means of verifying the data, practices and policies put in place for ensuring compliance. This is particularly critical when the user population is large and dynamic. The use of automated attestation features enables organizations to create and follow standard practices and policies across various departments within an organization, while ensuring that the organization is meeting diverse regulatory compliance requirements. This can be achieved without costly, time-consuming, and error-prone manual processes

Features of Oracle Identity Manager Provisioning

Key features and functionalities of Oracle Identity Manager provisioning are:

Scalable Architecture—The J2EE application server model of Oracle Identity Manager provides scalability, failover, and load-balancing, and inherent Web deployment. Based on an open, standards-based technology, and featuring a three-tier architecture (the Client application, Oracle Identity Manager supported J2EE-compliant Application Server and ANSI SQL-compliant database), Oracle Identity Manager can provision both LDAP and non-LDAP enabled applications.

Extensive User Management—Oracle Identity Manager includes unlimited user organizational hierarchies and user groups with inheritance, customizable User ID policy management, password policy management, and user access policies that reflect customers' changing business needs. Oracle Identity Manager also provides a resource allocation history, and the ability to manage application parameters and entitlements. Delegated administration is also a key element of user management with comprehensive permission settings.

Web-based User Self-Service—Oracle Identity Manager contains a customizable Web-based user self-service portal with the ability to manage user information, change and synchronize passwords, reset forgotten passwords, request available applications, review and edit available entitlements, and effect or react to workflow tasks.

Powerful and Flexible Process Engine—With Oracle Identity Manager, you can create business and provisioning process models in easy-to-use applications, such as Microsoft Project and Microsoft Visio. Process models include support for approval workflows and escalations. You can track the progress of each provisioning event, including the current status of the event and error code support. Oracle Identity Manager provides support for complex, branching, self-healing processes, and nested processes with data interchange and dependencies. The process flow is fully customizable and does not require programming.

Integration Using the Adapter Factory™—Attempting to support all systems with hand-coded adapters is impractical. Thus, Oracle has developed an automated tool for adapter generation. This tool, the Adapter Factory, supports a wide range of interfaces and virtually any application or device. These adapters run on the Oracle Identity Manager server, and do not require agents to be installed or updated on target platforms. In situations where the target application resource does not have a network-enabled interface, you can create remote integration by using UDDI/SOAP-based support. With the Adapter Factory, integrations that take months to implement can now be accomplished in a few days. Numerous adapters can be generated instantly. With the Adapter Factory, not only can you keep existing integrations updated, you can also support new integration needs quickly. Oracle Identity Manager has the ability to run programs on external third-party systems using the remote managers.

Built-in Change Management—Oracle Identity Manager enables you to package new processes, import and export existing ones, and move packages from one system to another.

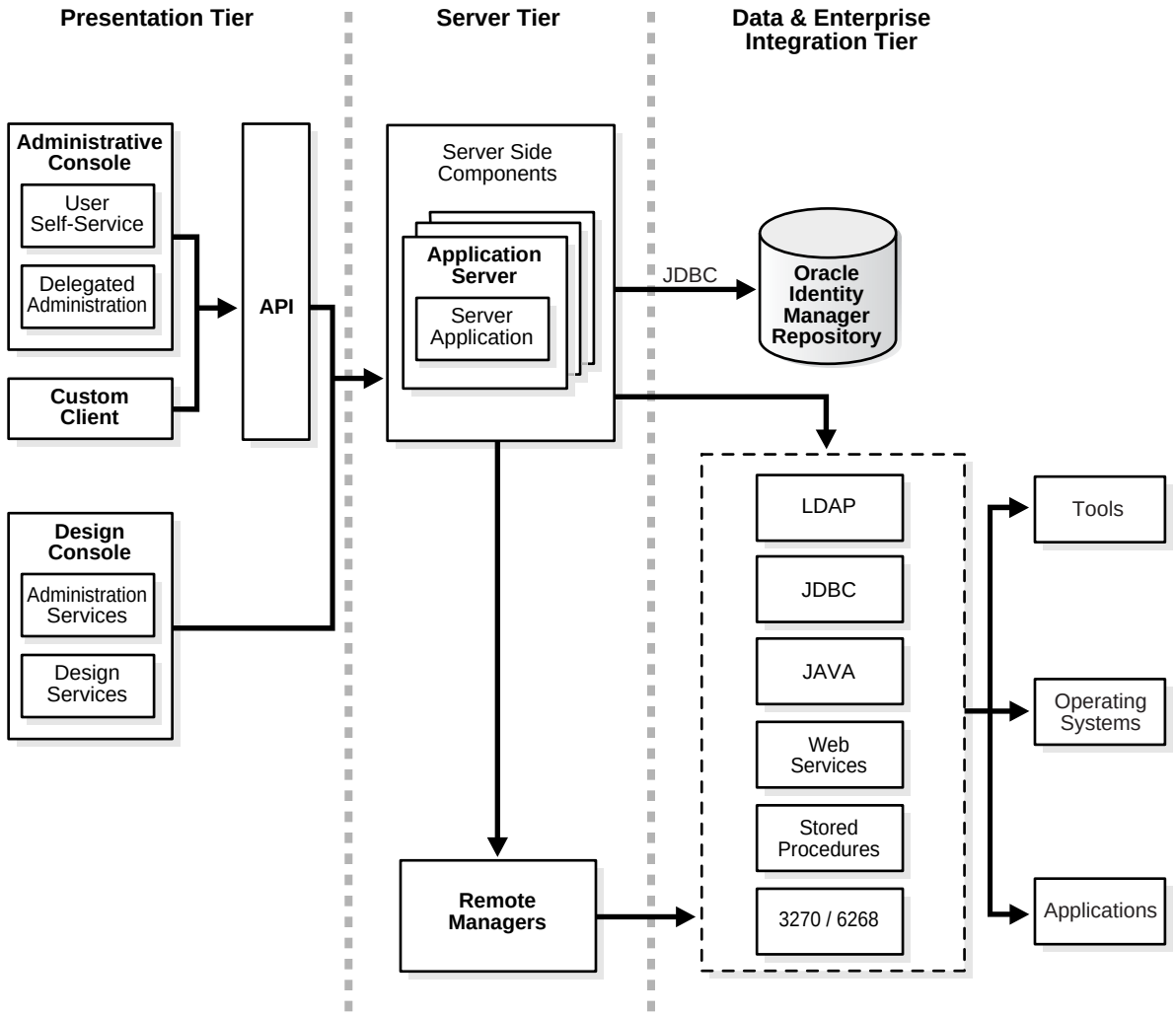
How Oracle Identity Manager Provisioning Works

The Oracle Identity Manager architecture consists of three tiers:

- Tier 1: Client
- Tier 2: Application Server
- Tier 3: Database

The Oracle Identity Manager three-tier architecture shown in Figure 9–1.

Figure 9–1 Oracle Identity Manager Three-Tier Architecture



Tier 1: Client

The first tier provides two distinct interfaces, the Java Administrative and User Console applications.

Note: This guide contains information related solely to the behavior of the Design Console edition of the Oracle Identity Manager product. For information on the functions and usage of the Oracle Identity Manager Administrative and User Console, refer to the *Oracle Identity Manager Administrative and User Console Guide*.

The Oracle Identity Manager application GUI component reside in this tier. Users log in by using the Oracle Identity Manager client. By doing so, the Oracle Identity Manager client interacts with the Oracle Identity Manager server, providing it with the user's login credentials. The Oracle Identity Manager server then validates these credentials. In addition, through the Oracle Identity Manager client, you can submit requests to search for information in the database as well as save, edit, or delete that information.

Tier 2: Application Server

The second tier implements the business logic, which resides in the Java Data Objects that are managed by the supported J2EE application server (JBoss application server, BEA WebLogic, and IBM WebSphere). The Java Data Objects implement the business logic of the Oracle Identity Manager application, however, they are not exposed to any methods from the outside world. Therefore, to access the business functionality of Oracle Identity Manager, you can use the API layer within the J2EE infrastructure, which provides the lookup and communication mechanism.

The Oracle Identity Manager supported J2EE-compliant application server is the only component that interacts with the database and is responsible for:

- **Logging into Oracle Identity Manager**: The Oracle Identity Manager supported J2EE-compliant application server connects the Oracle Identity Manager client to the database.
- **Handling Client Requests**: The Oracle Identity Manager supported J2EE-compliant application server processes requests from the Oracle Identity Manager client. It then sends the appropriate information from these requests to the database. The Server also delivers responses from the database to the client.
- **Scalability (Connection Pooling/Sharing)**: The Oracle Identity Manager supported J2EE-compliant Application Server supports single- or multi-application usage in a manner that is transparent to Oracle Identity Manager clients. Connection pooling improves database connectivity performance and dynamically resizes the **connection pool** by optimizing resources for usage scalability.
- **Securing System-Level Data (Metadata)**: Oracle Identity Manager employs **row-level** security to prevent unauthorized access by users who might otherwise accidentally delete or modify system-level information (system metadata).

Note: If an unauthorized user attempts to add, modify, or delete system-level information, the following message is displayed:

"**The security level for this data item indicates that it cannot be deleted or updated.**"

Tier 3: Database

The third tier consists of the database. This is the layer that is responsible for managing the storage of data within Oracle Identity Manager.

Features of Oracle Identity Manager Attestation and Reporting

Attestation is the process of having people or system managers confirm people's access rights on a periodic basis. Existing Sarbanes-Oxley requirements demand enterprises to perform attestation for all financially significant systems every 3 to 6 months. Identity Manager includes a highly flexible attestation solution to help enterprise customers meet these regulatory requirements in a cost-effective and timely manner. By setting up Attestation Processes in Identity Manager, enterprise customers can automate the process of generation, delivery, review, sign-off, delegation, tracking, and archiving of user access rights reports for reviewers on a scheduled or ad-hoc basis.

This section contains the following topics:

General Features

Key features of Oracle's current attestation offering include:

- Step-by-step definition of attestation processes
- On-demand or periodic scheduling of attestation tasks and processes
- Attestation of users' fine-grained entitlements across multiple resources
- Ability to tag resources as "financially significant" for participation in the attestation process
- Ability to certify, reject, decline, or delegate each item in an attestation request
- Fine-grained attestation actions for each entitlement for each user for each resource
- Notifications to reviewers, users, and process owners regarding attestation actions
- Reports on attestation requests processed, summarized by reviewer, by user, and by resource
- Archiving of attestation data, for periodic auditing and reporting
- Archiving of attestation actions taken, for periodic auditing and reporting

Types of Reports

Oracle Identity Manager currently provides two types of attestation reports:

- **Operational Reports**—Present a snapshot of current status. They include:
  - **User Entitlements** (Who Has What)—This report provides administrators or auditors the ability to query entitlements for users that match the query parameters. This report can be used for operational and compliance purposes. This is an operational report, not a historical report.
  - **Resource Access List**—This report provides administrators or auditors the ability to query all existing users provisioned to a resource. This report can be

used for operational and compliance purposes. This is an operational report, not a historical report.

- **Group Membership**—This report provides administrators or auditors the ability to view lists of groups and their members, across all resources in the provisioning environment. This report can be used for operational and compliance purposes. This is a group membership snapshot report across all resources, not a historical report.

- **Historical Reports**—Provide a view of historical data. They include:
  - **User Access History** (Who Had What)—This report provides administrators or auditors the ability to view user's resource access history over user's lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a user access profile snapshot report. This is a lifetime report showing entire history of user's entitlements.
  - **Resource Access List History**—This report provides administrators or auditors the ability to query all users provisioned to a resource over its lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a resource access list snapshot report. This is a lifetime report showing entire history of resource's access list / entitlements.
  - **User Profile History**—This report provides administrators or auditors the ability to view user's profile history over user's lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a user profile snapshot report. This is a lifetime report showing entire history of user's profile.
  - **User Membership History**—This report provides administrators or auditors the ability to view user's membership history in user groups over user's lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a membership snapshot report. This is a lifetime report showing entire history of the user's group memberships.
  - **Group Membership History**—This report provides administrators or auditors the ability to view a user group's historical membership over the group's lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a group membership snapshot report. This is a lifetime report showing entire history of the group's membership.
  - **User Lifecycle**—This report provides administrators or auditors the ability to obtain full information detailing all account-related data about a specific user (user identity lifecycle) within the corporate environment. This report can be used for compliance and forensic auditing purposes. This is not a user profile snapshot report. This is a lifetime report showing entire history of user's profile and user's entitlements in various resources.

How Oracle Identity Manager Attestation and Reporting Work

An attestation process, as defined in Oracle Identity Manager (OIM), includes the reviewers, the data to be attested to, and the schedule for attestation tasks.

Oracle's automated attestation capabilities involve presenting user identity and fine-grained entitlement data to authorized reviewers for sign-off on the accuracy of the data and providing reviewers with the means to document and correct any inaccuracies. Attestation processes can be run on demand or can be scheduled for periodic execution at regular intervals, whether it is once a year, once every six months, or once every quarter.

The data to be attested to can range from basic user profile data to access privileges or entitlements assigned to users and roles. Specific actions that can be undertaken by a reviewer for attestation include the ability to certify, reject, decline or delegate each entry in the attestation request. Reviewers can enter specific comments for each entry in the request to justify the action taken, and they can enter generic comments that apply to all entries in the request.

Each attestation request may contain a number of entries, for instance, to include each entitlement assigned to each user. The reviewer has the ability to take one of four actions—certify, reject, decline, or delegate—for each of these entries. The reviewer can select responses for some of the entries in the request, save the selections, then review the request again at a later time to complete the actions for other entries, and finally submit the entire attestation request for processing. E-mail notifications are sent to the reviewer and the users affected, so they are aware of the actions taken on the data. Each of these attestation requests is archived for subsequent auditing and reporting.

Resources can be tagged as "financially significant" and the user entitlements for such resources are automatically selected to participate in attestation processes. Optionally, specific resources that are not tagged as financially significant also can be selected for attestation on demand.

All data and actions taken on attestation requests are also archived for subsequent auditing and reporting purposes.

The process flow is as follows. First, a scheduled or on-demand attestation request is generated and a snapshot of the data required for the attestation task is compiled. The reviewer is then notified of the attestation request. The reviewer logs into the system and views the attestation request displayed in his/her attestation inbox. The attestation request is typically composed of a number of entries, one for each item of user profile data or user entitlement data to be attested to for each user. The reviewer can make one of four selections for each entry:

- **Certify**—reviewer attests to the data as accurate
- **Reject**—reviewer marks the data as inaccurate
- **Decline**—reviewer refuses to perform any attestation on this entry
- **Delegate**—reviewer delegates the attestation task for this entry to an alternate reviewer

The reviewer has the option of making the selections only for a subset of the entries in the request, saving the actions taken, and then returning at a later time to complete the attestation request. The reviewer can also enter individual comments for each entry or a generic comment for all entries in the request. Once the reviewer has completed taking an action for each entry, he/she can submit the entire attestation request for further processing. At this point, e-mail notifications are sent to the reviewers, the users, and the process owners associated with this attestation request.

10

Oracle Delegated Administration Services

This chapter describes Oracle Delegated Administration Services, a framework consisting of pre-defined, Web-based units for building administrative and self-service consoles. These consoles can be used by delegated administrators and users to perform specified directory operations.

It contains these topics:

> **Note:** Oracle Delegated Administration Services is only used for managing information that is stored in Oracle Internet Directory. To manage information that is stored in third-party or heterogeneous directory environments, consider using Oracle Access Manager, which provides a full range of identity administration and security functions. Oracle Access Manager functionality includes Web single sign-on, user self-service and self-registration, sophisticated workflow functionality, reporting and auditing, policy management, dynamic group management, and delegated administration.

Benefits of Oracle Delegated Administration Services

Delegated administration enables you to store all data for users, groups, and services in a central directory, while distributing the administration of that data to various administrators and end users. It does this in a way that respects the various security requirements in your environment.

Suppose, for example, that your enterprise stores all user, group, and services data in a central directory, and requires one administrator for user data, and another for the e-mail service. Or suppose that it requires the administrator of Oracle Financials to fully control user privileges, and the administrator of OracleAS Portal to fully control the Web pages for a specific user or group. Delegated administration as provided by the Oracle Identity Management infrastructure enables all of these administrators with their diverse security requirements to administer the centralized data in a way that is both secure and scalable.

Features of Oracle Delegated Administration Services

Oracle Delegated Administration Services is a set of pre-defined, Web-based units for performing directory operations on behalf of a user. It frees directory administrators from the more routine directory management tasks by enabling them to delegate specific functions to other administrators and to end users. It provides most of the functionality that directory-enabled applications require, such as creating a user entry, creating a group entry, searching for entries, and changing user passwords.

Features of Oracle Delegated Administration Services include:

- Management with Identity Management Grid Control Plug-in
- Oracle Internet Directory Self-Service Console
- Privilege Delegation Levels
- Centralization of Proxy User

Management with Identity Management Grid Control Plug-in

As of Oracle Application Server 10*g* (10.1.4.0.1), you can manage Oracle Directory Integration Platform with Identity Management Grid Control Plug-in, which uses the features of Oracle Enterprise Manager 10*g* Grid Control.

> **See Also:** The "Identity Management Grid Control Plug-in" chapter in *Oracle Identity Management Infrastructure Administrator's Guide*.

Oracle Internet Directory Self-Service Console

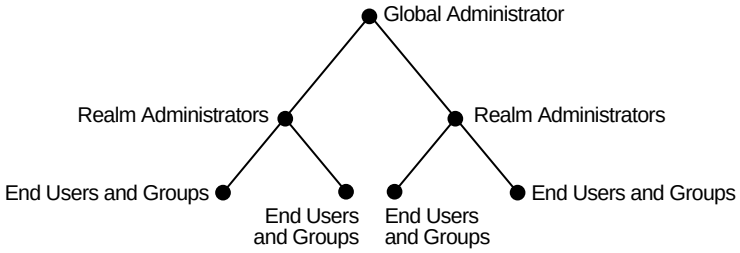
You can use Oracle Delegated Administration Services to develop your own tools for administering application data in the directory. Alternatively, you can use the Oracle Internet Directory Self-Service Console, a tool based on Delegated Administration Services. This is a self service application that allows administrated access to the applications data managed in the directory. This tool comes ready to use with Oracle Internet Directory.

> **See Also:** *Oracle Identity Management Guide to Delegated Administration*.

Privilege Delegation Levels

Applications built by using Oracle Delegated Administration Services enable you to grant a specific level of directory access to each type of user. For example, look at Figure 10–1, which shows the various administrative levels in a hosted environment. This illustration shows a directory information tree, the root of which is the entry for the global administrator. From that node, there are two branches, both extending to subscriber administrator nodes. Under each subscriber administrator node are two nodes, both of which are for end users and groups.

Figure 10–1 Administrative Levels in a Hosted Environment



The global administrator, with full privileges for the entire directory, can delegate to realm administrators the privileges to create and manage the realms for hosted companies. These administrators can, in turn, delegate to end users and groups the privileges to change their application passwords, personal data, and preferences. Each type of user can thus be given the appropriate level of privileges.

The following privileges can be delegated with Oracle Delegated Administration Services:

- Creation, editing, and deletion of users and groups
- Assignment of privileges to users and groups
- Management of services and accounts
- Configuration of Oracle Delegated Administration Services
- Resource management of Oracle Reports and Oracle Application Server Forms Services

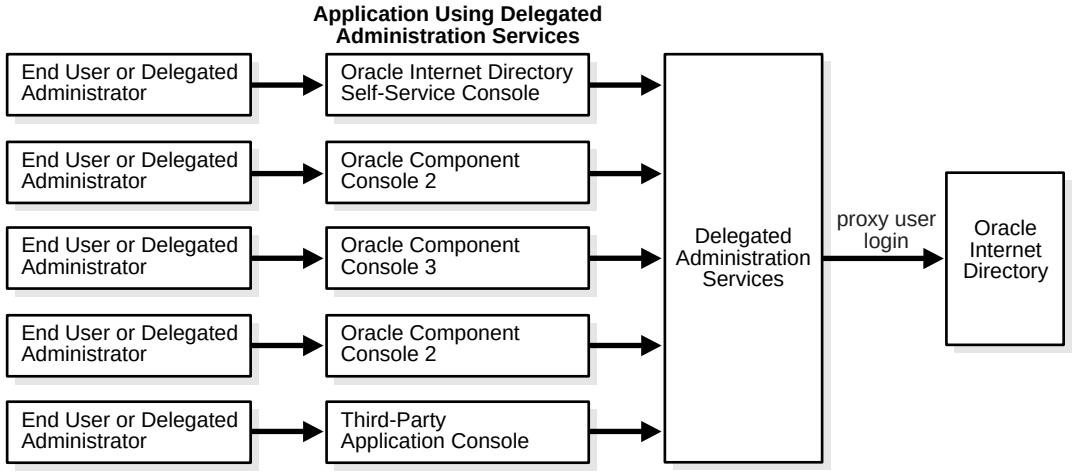
Centralization of Proxy User

When a user logs into an Oracle component, that component may need to obtain information from the directory on the end user's behalf—for example, the password verifier. To do this, the component typically logs into the directory as a proxy user, a feature that enables it to switch its identity to that of the end user.

In a Oracle Delegated Administration Services environment, each component, instead of logging into the directory as a proxy user, logs into the central Oracle Delegated Administration Services. Oracle Delegated Administration Services then logs into the directory as a proxy user, switches its identity to that of the end user, and performs operations on that user's behalf. Centralizing proxy user directory access in this way replaces the less secure strategy of granting proxy user access to every component accessing the directory.

Figure 10–2 shows the proxy user feature in an Oracle Delegated Administration Services environment. End users or delegated administrators log in to a central Oracle Delegated Administration Services. They do this by using the Oracle Internet Directory Self-Service Console, the consoles of other Oracle components such as OracleAS Portal, or those of third-party applications. The Oracle Delegated Administration Services then logs into Oracle Internet Directory as a proxy user.

Figure 10–2 Proxy User Feature in Oracle Delegated Administration Services



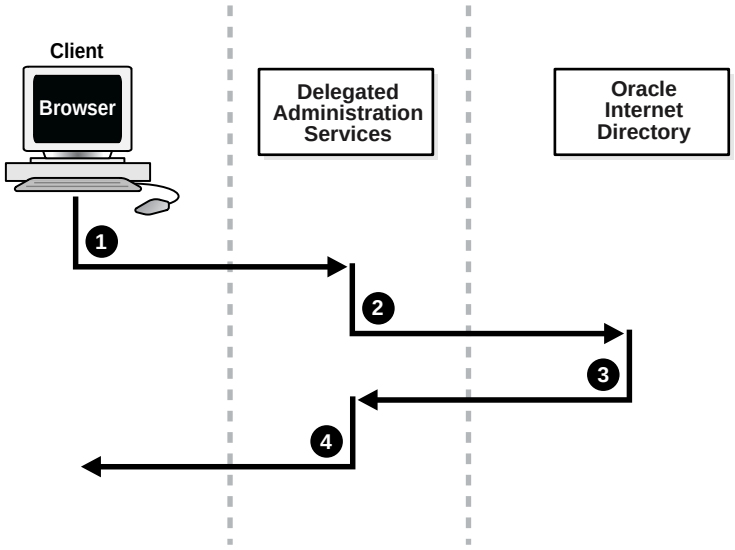
How Oracle Delegated Administration Services Works

Oracle Delegated Administration Services is a J2EE application that is deployed on an Oracle Containers for J2EE (OC4J) instance. Oracle Delegated Administration Services performs the following basic tasks:

1. Receive requests from clients
2. Process those requests—by either retrieving or updating data in Oracle Internet Directory—and compile the LDAP result into an HTML page
3. Send the HTML page back to the client Web browser

Figure 10–3 shows the flow of information between components in an Oracle Delegated Administration Services environment.

Figure 10–3 Information Flow in an Oracle Delegated Administration Services Environment



As Figure 10–3 shows:

1. The user, from a browser and using HTTP, sends to Oracle Delegated Administration Services a request containing a directory query.
2. Oracle Delegated Administration Services receives the request and launches the appropriate servlet. This servlet interprets the request, and sends it to Oracle Internet Directory by using LDAP.
3. Oracle Internet Directory sends the LDAP result to the Oracle Delegated Administration Services servlet.
4. The Oracle Delegated Administration Services servlet compiles the LDAP result into an HTML page, and sends it to the client Web browser.

Index

F

G

H

I

L

M

N

O

P

R

S

U

W