

ORACLE INTERNET DIRECTORY

KEY FEATURES AND BENEFITS

ORACLE INTERNET DIRECTORY

- LDAP v3 Compliant
- Common Criteria EAL4
- OpenGroup LDAP Certified
- Ease of deployment for Clusters
- Fan-out and partial replication support
- Replication Management Tools
- Management integration with Oracle Enterprise Manager
- Integration with the Microsoft Windows environment
- Directory Integration and Provisioning
- External authentication support
- Flexible Password Policies Management
- Server Side Entry Cache
- Garbage collection framework
- Extensible via plug-in framework

Oracle Internet Directory is an LDAPv3 directory that leverages the scalability, high availability and security features of the Oracle Database. Oracle Internet Directory serves as the central user repository for Oracle Identity Management, a component of Oracle Fusion Middleware, simplifying user administration in the Oracle environment and providing a standards-based application directory for the heterogeneous enterprise. Additionally, Oracle Directory Synchronization allows seamless integration with other directories and enterprise user repositories, allowing users to leverage identity information wherever it resides.

Oracle Directory Integration and Provisioning

This feature enables you to synchronize various directories with Oracle Internet Directory. It also makes it easier for third party metadirectory vendors and developers to develop and deploy their own connectivity agents.

Improved integration with other components

With features like service-to-service authentication, service registry, and verifier generation using dynamic parameters, you will benefit from improved integration with components such as Oracle Collaboration Suite.

Support for Certificate Matching Rules

External authentication using certificates can now take either of two forms: an exact match, in which the subject DN of the client certificate is used to authenticate the user, or a certificate hash, in which the client certificate is hashed and is then compared with a certificate hash stored in the directory.

Enforcing access control for Oracle Internet Directory super user

The super user is now subject to access control policies like any other user. New ACL keywords allow you to restrict super user access through privileged groups.

Integration with the Microsoft Windows environment

You can integrate the Oracle Application Server infrastructure with the Microsoft Windows Operating System--including Microsoft Active Directory and Microsoft Windows NT 4.0. This integration is achieved by using the Active Directory Connector in the Oracle Directory Integration and Provisioning platform and plug-ins.

ORACLE IDENTITY MANAGEMENT PRODUCTS

Oracle Identity Management

is an integrated, scalable and robust identity management infrastructure that includes LDAP V3 directory services, directory synchronization, access management, user administration and a certificate authority.

Oracle COREid Access and Identity

delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment. COREid Access and Identity provides the key functions for creating, managing, and enforcing access policies.

Oracle COREid Federation

enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the box. Oracle COREid Federation enables customers to manage multiple business partners and link them into corporate portals or extranets, securely and quickly.

Oracle COREid Provisioning

automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases, and ERP. It provides key functions for user lifecycle management, and is fully integrated with the rest of the Oracle Identity Management components.

Oracle Web Services

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

External authentication support

You can store user security credentials in a repository other than Oracle Internet Directory--for example, a database or another LDAP directory such as Microsoft Active Directory or SunONE Directory Server. You can then use these credentials for user authentication.

Password policy enhancements

Password policy capabilities in Oracle Internet Directory include:

- Configurable Password History
- Unlocking of accounts
- Forced password change upon first login
- Self-resetting of password in case of account lockout or forgotten passwords
- IP-based account lockout
- Password policy enablement or disablement by using a single attribute in the password policy entry

Standards Supported

Oracle Internet Directory supports a comprehensive range of security standards and protocols.

- LDAP v2 and v3
- SSL v3
- TLS 1.0
- SASL

A Component of Oracle Fusion Middleware

Oracle Fusion Middleware is a family of proven middleware products that help organizations achieve greater agility, make better informed business decisions and more easily integrate data and processes across disparate IT systems - including technologies from Oracle and other vendors. Oracle Fusion Middleware features Oracle Application Server 10g, related Application Server products and options, Data Hubs and Oracle Collaboration Suite. These products are available today and are being used by thousands of customers and partners throughout the world.

Additional information can be found at www.oracle.com/middleware.

Packaging and Availability

Oracle Internet Directory is part of the Oracle Identity Management option. Oracle Identity Management is bundled with Oracle Application Server 10g Enterprise Edition. It can also be licensed separately as an option for the Oracle Application Server 10g Standard Edition.