

ORACLE ACCESS MANAGER

KEY FEATURES AND BENEFITS

- Reduces costs by automating the management of potentially millions of users in an online business environment.
- Strengthens security by eliminating latency in changes to identity policy information and by improving authentication flexibility.
- Increases visibility into identity access events throughout the enterprise to drive decisions about user and application interactions.
- Ensures compliance by enforcing consistent, streamlined business rules and practices.
- Enhances control of customer and partner relationships by limiting or expanding a user's visibility into corporate information and services.
- Improves efficiency through the use of a common workflow, administrative consoles, and reporting framework for identity and access management.
- Built-in to Oracle Fusion Middleware for seamless application integration and lower TCO.
- Open and hot-pluggable heterogeneous support. Third-party platforms supported include BEA WebLogic, IBM WebSphere and SAP.

Oracle Access Manager is a state-of-the-art solution for centralized identity administration and access management. A component of Oracle Identity Management, Oracle Access Manager delivers the functionalities of web single sign-on, access policy creation and enforcement, user self-registration and self-service, delegated administration, and reporting and auditing. It supports all leading directory servers, application servers, web servers, and enterprise applications. Oracle Access Manager is part of Oracle Fusion Middleware, Oracle's integrated solution for seamless application support.

Introduction

Oracle Access Manager addresses enterprises' needs for greater levels of business agility, business partner integration and regulatory compliance. Oracle Access Manager accomplishes this by combining services for authentication and access control with rich identity administration functionality.

Identity Administration

The identity administration service of Oracle Access Manager provides user and group management, password management and self-service. Its scalable architecture and delegated administration functionality enable it to support administration of large user populations in complex, real-world environments.

Features of the identity administration service include:

- Management of users, groups and organizations, including dynamic groups defined based on user attributes.
- Integrated workflow capability for orchestrating identity profile updates and approvals.
- User self-service administration and password management to help reduce help desk calls.
- Delegated administration, allowing unlimited ability to delegate user administration to managers and partners.
- Support for portal inserts, allowing administrative functionality to be seamlessly embedded into web applications.
- Highly customizable administration console and web service interfaces to administrative functionalities.

ORACLE IDENTITY MANAGEMENT COMPONENTS

Oracle Access Manager delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment.

Oracle Identity Manager is a powerful and flexible enterprise identity provisioning and compliance monitoring solution that automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases, and ERP.

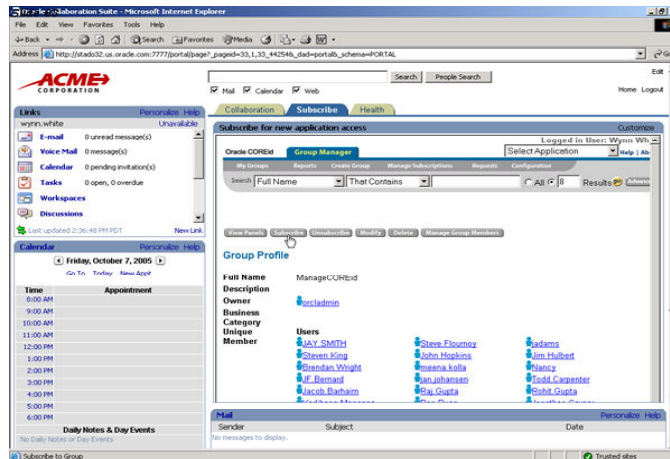
Oracle Identity Federation enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the box.

Oracle Internet Directory is a robust and scalable LDAP V3-compliant directory service that leverages the high availability capabilities of the Oracle 10g Database platform.

Oracle Virtual Directory provides Internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

Oracle Web Services Manager is a comprehensive solution for adding policy-driven security and management capabilities to existing or new Web services.

Oracle Enterprise Single Sign-On provides users with unified sign-on and authentication across all their enterprise resources, including desktops, client-server, custom and host-based mainframe applications.



Portals inserts allow the seamless insertion of identity administration functionality into enterprise web applications.

Authentication and Access Control

Oracle Access Manager provides single sign-on and policy-based access control to web applications, and J2EE resources such as EJBs and servlets. Features of the authentication and access control service include:

- Web single sign-on for secure access to multiple applications with one authentication step.
- Flexible authentication support for all popular methods including browser forms, digital certificates and smart cards.
- Centralized policy administration and enforcement that reduces cost and operational complexity for IT administrators.

Support for Enterprise Applications

Oracle Access Manager integrates with existing e-business infrastructures. It provides pre-built agents to protect, access, and manage all market leading third-party web servers, application servers, portals, LDAP directories, email systems, and relational databases. Oracle Access Manager is an integral component of Oracle Fusion Middleware, Oracle's common infrastructure for application deployment, thereby providing the lowest Total Cost of Operation (TCO).

Compliance Reporting

Oracle Access Manager includes unified and centralized audit reporting for all Access Manager components, with all operations stored and correlated in a secure database for reporting and analysis. Pre-built identity and security reports support common audit requirements.

Conclusion

Oracle Access Manager is the industry's most comprehensive identity and access management solution with integrated identity administration, single sign-on, centralized policy management and a compliance-reporting framework.. For more information, visit www.oracle.com/identity

Copyright 2006, Oracle. All Rights Reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor is it subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.