

ORACLE IDENTITY MANAGEMENT 11g

KEY FEATURES AND BENEFITS

FEATURES

- **Identity Administration:** Identity life cycle management (provisioning and reconciliation); workflow; self-service account request and password management; enterprise role management and role mining.
- **Authentication and Trust Management:** Multifactor, strong authentication; identity assertion; single sign-on; federation; privacy.
- **Access Control:** Risk-based authorization; fine-grained entitlements, web services security
- **Audit and Compliance:** Audit and compliance reporting; segregation of duties; conflict-resolution management; attestation; fraud-prevention analytics.
- **Manageability:** Service-level configuration; dashboard-based user interaction and environment monitoring; performance automation; patch management.
- **Directory Services:** Persistent storage, identity virtualization, synchronization; database user security.

BENEFITS

- **Complete:** Comprehensive set of best-in-class identity management and access control components.
- **Integrated:** Oracle Identity Management components are designed to work tightly together. In addition, the product suite's components integrate seamlessly with Oracle applications (e.g., Oracle's PeopleSoft, Oracle E-Business Suite, Oracle's Siebel) and other Oracle Fusion Middleware components (e.g., Oracle

As part of Oracle Fusion Middleware 11g, Oracle extends Oracle Identity Management to provide a unified, integrated security platform designed to manage user identities and entitlements, provision resources to users, secure access to corporate resources, and support extensive audits across enterprise applications.

Introduction

Oracle Identity Management (IM) 11gR1 ensures the integrity of large application grids by enabling new levels of security and completeness to address the protection of enterprise resources and the management of the processes acting on those resources. Oracle IM 11gR1 provides enhanced efficiency through a higher level of integration, consolidation, and automation, and increased effectiveness in terms of application-centric security, risk management, governance, and database integration.

Oracle IM 11gR1 is characterized from its predecessor (10g) by the following: establishment of the Oracle IM product suite as a security development platform; enhanced integration between Oracle IM components and other Oracle Fusion Middleware components, Oracle applications, Oracle Database, and third-party security providers; enhanced functionality streamlining enterprise-wide deployments; common technology infrastructure uptake across the product suite for critical operational and functional areas including installation, configuration, user interface, workflow, and reporting.

Oracle Identity Management 11gR1 Components

Oracle Identity Management 11gR1 includes the following suite of products.

Oracle Identity Manager

Oracle Identity Manager (OIM) typically answers the question "*Who has access to What, When, How, and Why?*". OIM is designed to administer both intranet and extranet user access privileges across a company's resources throughout the entire identity management life cycle, from initial on-boarding to final de-provisioning of an identity. In extranet environments, OIM's superior scalability allows enterprises to support millions of customers accessing the company's resources using traditional clients (e.g., browsers) or smart phones.

Oracle Role Manager

Oracle Role Manager (ORM) provides a comprehensive feature set for enterprise role life cycle management, and business and organizational relationships. ORM is the authoritative source for enterprise roles in Oracle IM's suite of products. Oracle Identity Manager and ORM complement each other to ensure that provisioning events are based on roles.

Oracle Access Manager

Oracle Access Manager (OAM) provides centralized, policy-driven services for

WebCenter, Oracle SOA, Oracle Business Intelligence).

- **Hot-Pluggable:** Oracle Identity Management's standards-based products are designed to support heterogeneous, multiple-vendor development and runtime environments, including operating systems, web servers, application servers, directory servers, and database management systems.
- **Best-Of-Breed:** In addition to Oracle IM's level of completeness, integration, and hot-pluggability, the components of the suite deliver functional depth and sophistication that, even taken individually, makes them market-leading, best-of-breed products. Customers, especially those looking for advanced capabilities to support their application grid, can choose the best-in-class Oracle IM component to meet their specific requirements and integrate that component with the rest of their existing identity management portfolio, or they can deploy the best-of-breed Oracle IM suite to take advantage of its enhanced integration.

authentication, single sign-on (SSO), and identity assertion. OAM integrates with a broad array of authentication mechanisms, third-party web servers and application servers, and standards-based federated SSO solutions to ensure maximum flexibility and a well-integrated, comprehensive web access control solution. OAM complements its own coarse-grained authorization and attribute assertion capabilities by integrating with Oracle Entitlements Server to provide fine-grained authorization to applications, portals, databases, and web services.

Oracle Web Services Manager

Oracle Web Services Manager (OWSM) is to web services what Oracle Access Manager is to web applications. OWSM is designed to protect access to multiple types of resources including standards-compliant web services (Java EE, Microsoft .NET, PL/SQL, etc.); service-oriented architecture (SOA) composites including Business Process Execution Language (BPEL) and enterprise service bus (ESB) processes; and Oracle WebCenter's remote portlets.

Oracle Identity Federation

Oracle Identity Federation (OIF) is a self-contained solution enabling browser-based, cross-domain single sign-on using industry standards (Security Assertion Markup Language -- SAML, Liberty ID-FF, WS-Federation). OIF 11gR1 introduces support for Microsoft Windows CardSpace (for example, an OIF identity provider can challenge a user for log-in via the CardSpace protocol and then return a SAML assertion based on the CardSpace authentication and claims).

Oracle Enterprise Single Sign-On

Oracle Enterprise Single Sign-On (eSSO) is a Microsoft Windows desktop-based suite of products providing unified authentication and single sign-on to both thick- and thin-client applications with no modification required to existing applications. Using Oracle eSSO, enterprise users benefit from single sign-on to all of their applications, whether users are connected to the corporate network, traveling away from the office, roaming between computers, or working at a shared workstation.

Oracle Entitlements Server

Oracle Entitlements Server (OES) is a fine-grained authorization engine that externalizes, unifies, and simplifies the management of complex entitlement policies. OES secures access to application resources and software components (such as URLs, Enterprise JavaBeans, and Java Server Pages) as well as arbitrary business objects (such as customer accounts or patient records in a database). OES provides a centralized administration point for complex entitlement policies across a diverse range of business and IT systems.

Oracle Adaptive Access Manager

Oracle Adaptive Access Manager (OAAM) provides resource protection through real-time fraud prevention, software-based multifactor authentication, and unique authentication strengthening. OAAM consists of two primary components that together create one of the most powerful and flexible weapons in the war against fraud. Adaptive Strong Authenticator provides multifactor authentication and protection mechanisms for sensitive information such as passwords, tokens, account numbers, and other credentials. Adaptive Risk Manager provides real-time and offline risk analysis, and proactive actions to prevent fraud at critical log-in and transaction checkpoints.

ORACLE IDENTITY MANAGEMENT COMPONENTS INTEGRATION

Following are examples of how multiple Oracle Identity Management components can work together to provide a seamless security solution.

Oracle Identity Manager and Oracle Role Manager Integration

OIM and ORM complement each other to ensure that provisioning events are based on roles. The former emphasizes end-to-end identity management and provisioning while the latter focuses on role life cycle management.

Oracle Access Manager and Oracle Identity Federation Integration

First, OAM challenges the user for credentials. Upon successful authentication, OAM sets an SSO cookie and asserts the authenticated identity to the federation service (OIF). OIF then generates an authentication ticket (a SAML assertion) based on the information provided by OAM, and sends the SAML assertion to a service provider.

Oracle Access Manager and Oracle Web Services Manager Integration

A user is authenticated to an application protected by OAM and the application makes a service call on behalf of the user. An OWSM client agent intercepts the call and inserts the necessary security information in the SOAP message header (e.g., a SAML assertion), based on the asserted identity information provided by OAM.

Oracle Access Manager and Oracle Entitlements Manager Integration

OAM asserts an authenticated user's identity and passes an authorization request to OES. OES retrieves information about

Oracle Directory Services

Oracle Internet Directory (OID) provides Oracle Fusion Middleware components, Oracle Fusion applications and in-house enterprise applications with a standard Lightweight Directory Access Protocol (LDAP)-based mechanism for storing and accessing identity data such as user credentials (for authentication), access privileges (for authorization), and profile information.

Oracle Virtual Directory (OVD) is designed to provide real-time identity aggregation and transformation without data copying or data synchronization. OVD hides the complexity of underlying data infrastructures by providing industry-standard LDAP and XML views of existing enterprise identity information, without moving data from its native location.

Oracle Platform Security Services

Oracle Platform Security Services (OPSS) provides enterprise product development teams, systems integrators, and independent software vendors with a standards-based, portable, integrated, enterprise-grade security framework for Java Platform, Standard Edition (Java SE) and Java Platform, Enterprise Edition (Java EE) applications. OPSS insulates developers from the intricacies of tasks not directly related to application development by providing an abstraction layer in the form of standards-based application programming interfaces. OPSS is the security foundation for Oracle Fusion Middleware: all Oracle Fusion Middleware 11g components and Oracle Fusion applications “consume” OPSS’s services.

Oracle Management Pack for Identity Management

Oracle Management Pack for Identity Management leverages Oracle Enterprise Manager's broad set of capabilities to control end-to-end Oracle Access Manager, Oracle Identity Manager, and Oracle Identity Federation environments.

Oracle Identity Management and Other Oracle Technologies

Oracle Identity Management is at the intersection of several complementary Oracle technologies. The following sections describe how Oracle Identity Management integrates with Oracle Information Rights Management, Oracle’s Governance, Risk, and Compliance (GRC) platform, and Oracle Database security.

Oracle Identity Management and Oracle Information Rights Management

Oracle Information Rights Management (IRM) safeguards information directly. It uses encryption to shrink the access control perimeter down to the actual units of digital information, e.g., documents, emails, and web pages. Oracle refers to the process of protecting digital documents as “sealing”, which includes encrypting the document, digitally signing the file containing that document, and including indelible URL hyperlinks into each sealed file that point back to the customer-operated Oracle IRM Server. Oracle IRM leverages the following Oracle IM components: Oracle Identity Manager to centrally provision IRM users and entitlements; Oracle Virtual Directory to synchronize IRM users and groups from existing enterprise LDAP and non-LDAP directories; and Oracle Enterprise Single Sign-On for desktop single sign-on and additional support for strong authentication.

Oracle Identity Management and Enterprise Governance

Oracle’s Governance, Risk, and Compliance (GRC) platform integrates business intelligence, process management, and automated controls enforcement to enable sustainable risk and

the trusted subject, resource request, and security context, and executes a dynamic role evaluation. OES checks the application authorization policy against the subject and role, and enforces the fine-grained resource access.

Oracle Entitlements Manager and Oracle Web Services Manager Integration

OWSM can delegate a service access decision to OES by passing down the identity of the user and contextual parameters that tell OES how to unpack data from the message itself when making an entitlement decision. OES can then take the message information and its own policies into account and provide a *grant* or *deny* response back to OWSM. OWSM can then enforce that decision.

The integration of Oracle Identity Management components can involve more than two products. For example, in order to support a full-blown web transaction, OAM can rely on OES for fine-grained authorization and at the same time rely on OWSM to secure requests to internal or external web services or service-oriented architecture (SOA) composites.

compliance management. With Oracle Identity Management 11gR1, Oracle Identity Manager, Oracle Role Manager, and Oracle Access Manager are part of the multiple products making up Oracle GRC's infrastructure controls. Oracle Application Access Controls Governor, a key product in the Oracle GRC platform, allows customers to manage, remediate, and enforce enterprise resource planning segregation of duty (SoD) policies. Typically, Oracle Identity Manager integrates with Oracle Application Access Controls Governor to perform real-time SoD validation prior to provisioning roles and responsibilities to Oracle E-Business.

Oracle Identity Management and Oracle Database Security

One of the key differentiators of Oracle's identity management offering is its ability to provide customers greater flexibility and choice by integrating Oracle Virtual Directory (OVD) with Enterprise User Security (EUS), a feature of Oracle Database, enabling organizations to centrally manage database-user identities through their existing corporate directories such as Oracle Internet Directory (OID), Microsoft Active Directory, and Sun Java System Directory Server. Thanks to the integration of OVD with EUS, organizations can leverage identity virtualization to manage database-user identities and their privileged roles across diverse identity stores without having to migrate or synchronize data. In addition, OID leverages two unique database security features: Oracle Database Vault (enforcing separation of duties for database administrators) and Oracle Transparent Encryption. Oracle Database Vault prevents identity data from being accessed or manipulated outside of the OID protocol listener(s). Transparent Data Encryption encrypts data within the database. Even if users get unauthorized access to the database, they can't read the data. Oracle Database Vault and Oracle Transparent Data Encryption allow Oracle to provide the only directory services with complete security from storage to client.

Contact Us

For more information about Oracle Identity and Access Management Suite, please visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
0109