ORACLE IDENTITY MANAGEMENT 11*g*

Oracle Identity Management provides unified, integrated security and identity services designed to manage user identities, provision resources to users, secure access to corporate resources, enable trusted online business partnerships, and support governance and compliance across the enterprise.

KEY FEATURES

- ***Identity Administration***: Identity life cycle management (provisioning and reconciliation); workflow; self-service account request and password management; enterprise role management.
- ***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.
- ***Identity and Access Governance***: Audit and compliance reporting; segregation of duties; conflict-resolution management; attestation; role mining and engineering; identity and fraud-prevention analytics.
- ***Manageability***: Service-level configuration; dashboard-based user interaction and environment monitoring; performance automation; patch management; diagnostics and tuning.
- ***Directory Services***: Persistent storage, identity virtualization, synchronization; database user security.

KEY BENEFITS

- ***Complete***: Comprehensive set of best-in-class identity management and access control services.
- ***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 WebCenter, Oracle SOA, Oracle Business Intelligence).
- ***Hot-Pluggable***: Oracle Identity Management's standards-based products are designed to support multiple-vendor development and runtime environments, including operating systems, web servers, application servers, directory servers, and database management systems.

Introduction

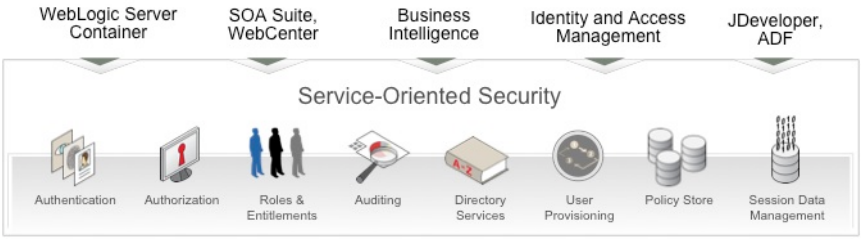
Oracle Identity Management ensures the integrity of large application grids by enabling new levels of security and completeness to address the protection of enterprise resources and the management of the processes acting on those resources. Oracle Identity Management provides enhanced efficiency through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

Oracle Identity Management 11g establishes the Oracle Identity Management product suite as a security development platform offering end-to-end integration between identity management 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, audit and reporting.

Oracle Identity Management is available as a fully integrated suite including the whole range of services described in this data sheet. Each suite service (or product) can be licensed separately.

Service-Oriented Security

Key to Oracle Identity Management 11g is the concept of Service-Oriented Security (SOS). SOS provides a set of low-level, independent security services leveraged by Oracle Fusion Middleware components (Identity Management, SOA, WebCenter), as well as new-generation Oracle Fusion Applications, as shown in the figure below.



The foundation for SOS is Oracle Platform Security Services (OPSS), described in the next section.

- ***Best-Of-Breed***: In addition to Oracle Identity Management'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 Identity Management 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 Identity Management suite to take advantage of its enhanced integration.

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" the OPSS framework's services. OPSS-based authorization policies are administered by Oracle Authorization Policy Manager (OAPM). OAPM provides delegated administration and advanced life cycle management. OAPM is based on industry standards (JAAS permissions and enterprise RBAC) and is intended for customers relying on Oracle Fusion Middleware products based on OPSS, custom or in-house applications built with Oracle ADF, and Oracle Fusion Applications.

Oracle Identity Management Products and Services

Oracle Identity Management leverages Oracle's SOS platform to provide shared identity services delivered by the various products described in this section. In turn, Oracle's identity services are leveraged by other Oracle Fusion Middleware components as well as Oracle Fusion Applications ("application-centric security").

Oracle Identity Manager

Oracle Identity Manager (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 a company's resources using traditional clients (e.g., browsers) or smart phones. OIM 11g includes new features such as *Universal Delegated Administration* (through embedded Oracle Entitlement Server), and *Request Templates* for persona-specific request catalogues.

Oracle Identity Analytics

Oracle Identity Analytics (OIA) brings a new dimension to Oracle Identity Management in the area of identity and access governance. OIA helps you address regulatory mandates, automate processes, and quickly make compliance a repeatable and sustainable part of business. OIA provides a comprehensive solution for certification, role governance, enterprise-level segregation of duties (SoD) enforcement, a 360-degree view of user access (*Cert360*), and an *Identity Warehouse* designed to consolidate identities, resources, and entitlement information.

Oracle Access Manager

Oracle Access Manager (OAM) provides centralized, policy-driven services for web applications' 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. High-performance access to distributed session data is ensured by *eCO Grid* (embedded Oracle Coherence grid), and *SSO Security Zones* prevents unauthorized access from spreading to multiple applications.

Oracle Web Services Manager

Oracle Web Services Manager (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 BPEL and enterprise service bus (ESB) processes; and Oracle WebCenter's remote portlets.

IDENTITY AS A SERVICE: IDENTITY MANAGEMENT COMPONENT INTEGRATION

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

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 Server Integration

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

Oracle Access Manager and Oracle Adaptive Access Manager Integration

The combination of OAM and OAAM enables fine control over the authentication process and provides full capabilities of pre- and post-authentication checking against OAAM policies. In the context of this integration, OAM acts as the authenticating and

Oracle Identity Federation

Oracle Identity Federation (OIF) is a self-contained solution enabling browser-based, cross-domain single sign-on using industry standards (SAML, Liberty ID-FF, WS-Federation, Microsoft Windows CardSpace). In addition, with Oracle OpenSSO Fedlet packaged as a Web Archive (WAR), a service provider can immediately federate with an OIF identity provider without requiring a full-blown federation solution in place.

Oracle OpenSSO Security Token Service

Oracle OpenSSO Security Token Service (STS) establishes a trust relationship between online partners through web services. STS provides both standard (e.g., SAML, Kerberos) and proprietary (e.g., PeopleSoft, Siebel) security token issuance, validation, and exchange.

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 SSO to both thick- and thin-client applications with no modification required to existing applications. *eSSO Anywhere* simplifies deployment to very large numbers of client desktops and automates updates.

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).

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. In addition, OAAM provides real-time and offline risk analysis, proactive actions to prevent fraud at critical log-in and transaction checkpoints, one-time password (*OTP Anywhere*) to add sophisticated security to basic flows in a few easy steps, and *AnswerLogic* to provide needed security to "unprotected" password reset pages.

Oracle Directory Services

Oracle Directory Server Enterprise Edition (ODSEE) offers best-of-breed Lightweight Directory Access Protocol (LDAP)-based services recommended for heterogeneous applications and multi-vendor environments. ODSEE is the industry's leading carrier-grade directory solution.

Oracle Internet Directory (OID) provides Oracle Fusion Middleware components, Oracle Fusion Applications and in-house enterprise applications with a highly-scalable 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 Management Pack for Identity Management

Oracle Management Pack for Identity Management leverages Oracle Enterprise Manager's broad set of capabilities to administer end-to-end identity management components along with the rest of Oracle Fusion Middleware and Applications. Key capabilities include configuration and patch management, diagnostics and tuning, and monitoring with SLA management.

authorizing service, while OAAM provides the rich, strong authenticators and performs risk and fraud analysis.

Oracle Access Manager and Oracle Identity Manager Integration for Password Management

A user tries to access a resource protected by OAM. An OAM agent (WebGate) intercepts the (unauthenticated) request. WebGate redirects the user to the OAM log-in service, which performs validation checks. If OAM finds any password management trigger conditions, such as password expiry, it redirects users to OIM. OIM interacts with the user to establish the user's identity and carry out the appropriate action, such as resetting the password. OAM logs the user in by means of auto-log-in, and redirects the user to the OAM-protected resource the user was trying to access in the first place.

Oracle Identity Manager and Oracle Adaptive Access Manager Integration

The integration between OIM and OAAM allows OAAM challenge questions to be invoked while using OIM for password validation, storage, and propagation.

The integration of Oracle Identity Management services 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.

Oracle Identity Management And Other Oracle Technologies

Oracle Identity Management is at the intersection of several complementary Oracle technologies. It 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 Oracle Identity Management for user provisioning and entitlements, and 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 compliance management. OIM, OIA, and OAM 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 application-level segregation of duty (SoD) policies for enterprise resource planning (ERP). 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 user directories. 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* (data is encrypted within the database.), allowing Oracle to provide the only directory services with complete security from storage to client.

Contact Us

For more information about Oracle Identity Management, 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

SOFTWARE. HARDWARE. COMPLETE.

ORACLE