ORACLE ACCESS MANAGEMENT SUITE PLUS

KEY FEATURES:

- Most comprehensive and integrated, best-in-class access management suite
- Authentication, single sign-on (SSO) and identity assertion for heterogeneous enterprise applications
- SSO for native mobile applications and REST API for custom application development
- OAuth Authorization and Resource Services
- Cross-platform Web SSO portal
- Relying party support for sign-on from popular social networks
- Industry-leading enterprise fraud prevention, risk-aware authentication, and real-time risk analytics
- Innovative external authorization solution that centralizes policy management while distributing policy enforcement
- Standards-based solution for federated authentication across security domains and rapid enrollment of new federation partners
- Sets the industry standard for securing SOA and web services and providing a complete SOA governance solution
- A complete solution for issuing, validating, and exchanging security tokens across multiple tiers of the enterprise

Oracle Access Management Suite Plus is the industry's most advanced solution for securing applications, data, Web services, and cloud-based services. Through a broad feature set—which includes authentication and single sign-on, mobile and social sign on, entitlement management and fine-grained authorization, fraud detection and risk-aware authentication, security tokens services and identity federation—Oracle Access Management Suite Plus provides an integrated, modular architecture that enables customers to deploy a complete access solution. It is the most comprehensive solution—tightly integrated and engineered together to protect access from the endpoint to the cloud.

Introduction

Today's enterprises are facing access management challenges that require new levels of protection. For example, enterprises need to provide employees with access to company resources from personal mobile devices. Similarly, some organizations need to grant customers access to applications on the basis of the user's identities on social networking sites. And most organizations need to manage sign-on to cloud services as they would for on-premise applications. Further, organizations are being transformed by the need to provide end-to-end, standards-based security services to their applications, data, web services, and cloud-based or Software as a Service (SaaS) applications. Such business demands are driving organizations to externalize security services, integrate with partners, and evaluate the risk of internal and external transactions. Oracle Access Management Suite Plus addresses these challenges with a complete solution for controlling access to applications, data, web services, and cloud-based services across and beyond the enterprise. Oracle Access Management Suite Plus provides:

- Pluggable authentication and Web SSO
- Cross-platform Web SSO portal
- SSO for native mobile applications on iOS and Android
- Federated identities and integration with social networks
- Fine-grained authorization for internal and external resources
- Proactive fraud prevention and authentication security
- Real-time risk analytics and risk-aware, multifactor authentication
- Comprehensive security for Web services and SOA infrastructure
- Security Token Service (STS) for secure identity and token propagation

ORACLE®

The integrated suite of best-of-breed functionality offers several compelling benefits to customers including:

- End-to-End Access Security for enterprise, cloud, mobile and social ecosystems

- Suite-wide Interoperability

- Innovative anomaly detection for real-time transactions

- Centralized security and authorization

- Lower operational costs and better IT agility

Authentication and Web SSO

Oracle Access Management Suite Plus delivers an enterprise-grade web access management (WAM) solution for authentication, SSO, policy administration, policy enforcement, agent management, session control, systems monitoring, reporting, logging, and auditing. Multi-data-center load balancing and failover capability enable enterprises to support mission-critical infrastructure. The solution works in existing enterprise heterogeneous environments with Web agents certified on a variety of web servers and application servers as well as applications. A cross-platform Access Portal provides SSO to web resources including SaaS and federated partners.

Mobile and Social Sign On

The proliferation of mobile devices and competitive reasons are compelling enterprises to offer access to commonly used business applications for customers and employees using personal mobile devices. But many applications don't have visibility into the security posture of the device making it challenging to enforce audit, compliance, and privacy requirements. With the innovative Mobile and Social capability in Oracle Access Management Suite Plus, organizations can extend SSO to mobile applications and secure applications and data regardless of which device is being used. Also organizations can consume identities from popular social networks (Facebook, Google, Yahoo, Twitter, and LinkedIn) for signing on users to consumer-facing and other low risk applications, providing a seamless user experience for users without the burden of forcing additional registration and logins. The solution also comes with an SDK with REST APIs that developers can leverage to integrate custom mobile applications with commonly used identity management functions like authentication, credential management, secondary authentication, device fingerprinting, and session management. The SDK supports OAuth and OpenID, two of the most commonly used user-centric identity frameworks in the industry. So developers can use the SDK to enable applications to consume social identities.

ORACLE®

Adaptive Access and Fraud Detection

Organizations face the constantly growing threat of fraud and misuse of online systems. Failure to implement effective access monitoring and management can even impact the business' bottom line. Oracle Access Management Suite Plus delivers superior protection for businesses and their customers through strong multifactor authentication security and proactive, real-time fraud prevention. It provides online applications with device-free, strong mutual authentication and real-time risk scoring to identify potential fraud at multiple points in a transaction. Oracle Access Management Suite Plus provides organizations a cost-effective solution to meet current security needs that is extendable to meet future requirements as they move critical business processes to the web.

Identity Federation

Building federated user communities that span company boundaries represents an opportunity for businesses to implement consumer product cross-selling strategies, streamline supplier access to their extranet applications, and respond quickly to organizational changes such as mergers and acquisitions. With support for industry federation standards, Oracle Access Management Suite Plus makes these kinds of interactions possible with a multi-protocol federation server implementing standards-based web technology including SAML and OAuth. This enables organizations to securely link accounts and identities across security boundaries without a central user repository or the need to synchronize data stores. Oracle Access Management Suite Plus provides an interoperable way to implement cross domain single sign-on for vendors, customers and business partners without the overhead of managing, maintaining and administering their identities and credentials.

External Authorization

As enterprises successfully gain control over their access management requirements, more are looking to centralize management of fine-grained authorization policies embedded within the applications themselves. Support for industry standards like XACML, NIST RBAC and Enterprise RBAC help make this feasible across heterogeneous vendor environments. Oracle provides centralized, standards-based policy management and distributed policy enforcement across enterprise applications resulting in a more secure enterprise environment, improved ease of administration, consistent policy enforcement and improved compliance.

Web Services Security

Service Oriented Architecture (SOA) provides loose coupling between application components across heterogeneous environments and makes standards-based interoperable security a must. Oracle Access Management Suite Plus fills that need with a large number of features out-of-the-box for access control and message-level encryption and protection. It also includes deep integration with Oracle and third-party identity management infrastructure. Runtime SOA Governance is provided through a comprehensive set of policy management features with centralized auditing,

ORACLE®

logging, and reporting of runtime security enforcement metrics.

Security Token Service

Secure Token Service (STS) is a foundational component to an organization's web services security infrastructure where it becomes a trusted authority that provides issuance and management of security tokens. Oracle STS is a standards-based security solution that issues, validates, or exchanges security tokens and acts as a trusted authority that an enterprise web services infrastructure may use to enforce appropriate security token policies across web service providers and consumers. STS also provides a means for propagating identity and security information across infrastructure tiers, for example by converting a web SSO token issued for the enterprise portal to a SAML token that is consumed by applications or web services.

Conclusion

Oracle Access Management Suite Plus strengthens information security, helps enterprises satisfy audits and improves user experience, all delivered with the backing of the world's largest enterprise software company. Visit www.oracle.com/identity for more information.

Contact Us

For more information about Oracle Access Management Suite Plus, visit oracle.com/identity or call +1.800.ORACLE1 to speak to an Oracle representative.

SOFTWARE. HARDWARE. COMPLETE.

ORACLE®