An Oracle White Paper

January 2014

Complete and Scalable Access Management
Disclaimer

The following is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions. The development, release and timing of any feature or functionality described in this document remains at the sole discretion of Oracle.
Executive Overview........................................................................................................2
Introduction ..................................................................................................................4
  Exploring the Need for Cross-Functional Interoperability .................. 4
  Meeting Demands for Mobile Access................................................................. 6
  The impact of Social Identity................................................................. 8
  Putting it all together: Complete Access Management..................... 9
A platform approach to Complete Access Management ........... 10
  Intelligent Platform Services ............................................................. 11
  Access Management Services ................................................................. 13
  Low Risk Upgrades ...................................................................................... 18
Blueprint Architecture – Complete Access Management .......... 19
Internet-level Scalability and High Availability ............... 22
  Internet-level scalability and performance .................................................... 22
  High Availability ...................................................................................... 22
Conclusion ........................................................................................................... 23
Executive Overview

Access management is critical to any effective identity and security strategy, but the complex nature of access management continues to challenge IT departments. Securing access to a diverse set of applications, services and data is particularly complex given the expansive nature of Internet technologies. The emergence of cloud computing, mobile computing, and social identity technologies has only heightened the need for access controls, because these technology trends are transforming the way organizations access and expose business critical services and data.

As access management requirements evolved, IT departments often deployed a mix of point solutions, each of which met some critical requirement for application and information security. This patchwork of access management technologies has left IT with highly complex environments to manage, stretching IT resources and budgets and hindering the ability of IT to meet the needs of the business.

With urgent demands for new IT services, departments in many organizations bypass IT altogether. The concept of “Shadow IT,” often associated with Software-as-a-Service, is causing major security and governance concerns for organizations.

Oracle recognizes the need for comprehensive access management and offers a solution that provides the market’s broadest set of access management capabilities. And as the market grows, Oracle remains dedicated to providing a complete access management solution.

As illustrated in Figure 1, Oracle’s approach to access management is to provide complete, innovative, open, and simplified services. Oracle Access Management provides IT with complete coverage of protocols to protect access over HTTP, REST, and SOAP channels seamlessly. It supports a full complement of standards for authentication and user management, including OAuth, OpenID, and SAML and also offers integration with on-premise, SaaS, cloud, and mobile applications, as well as popular social networking sites.
Oracle Access Management 11gR2 enables organizations to:

- Streamline IT by removing the need to manage multiple point products and web agents to achieve complete access management.
- Transform the business by supporting new services including mobile, cloud, and social identities.
- Meet demands for Internet-level scalability through superior architecture and optimized deployments.
- Raise assurance levels by adding risk-aware, context-driven decisions across all access management services.
- Improve IT efficiency by simplifying installation, configuration, and converging multiple products into a configurable multi-services platform.
- Provide an open architecture that enables third-party integration and customization.

This paper introduces you to Oracle’s truly unique access management platform that provides complete, Internet scale access management, innovative new services and simplified deployment and management.
Introduction

Over the past 15 years, the market has produced a collection of point products for access management, which operate independently to fulfill specific access requirements, as represented in Figure 2. However, such an independent approach is no longer viable to satisfy today’s requirements, which are demanding increased interoperability to achieve a seamless experience.

This change is being driven by the advent of cloud and mobile computing, which has transformed the way organizations access and expose business-critical applications, services, and data. In addition, pressure to leverage social identity is taxing traditional access management deployments and highlights the need for a new approach, one that Oracle is uniquely positioned to provide.

Figure 2: Access management milestones

This white paper explores the impact these new technologies are having on traditional access management deployments and helps you understand why Oracle’s new platform approach to access management is the best solution to meet your organization’s complete access management needs.

Exploring the Need for Cross-Functional Interoperability

Until recently, access management products provided access control for a single access channel. For example, Web Access Management (WAM) products secured browser-based access to web applications, whereas XML gateways secured SOA application access. Various specifications, including SAML (Security Assertions Markup Language), improved interoperability across organizational boundaries (single sign-on to partner and cloud applications), but the products continued to service a single access channel – browser-based
access or application-based access. Unfortunately this single access channel mode of operation doesn’t satisfy today’s online requirements.

To better understand these changing requirements, consider the interactions depicted in Figure 3, which illustrates the need for seamless client and system interactions across enterprise and cloud resources. The interaction starts with a user located in his office accessing a corporate portal (1). The user clicks on a link for a new business intelligence SaaS application, which redirects the user to the cloud application (2). The user adds a financial view to the cloud application’s dashboard, which pulls data from a database located at the user’s corporate office (3). Finally the cloud application presents the data on the user’s dashboard (4).

**Figure 3**: A scenario illustrating the need for cross-protocol, cross-channel access management

While this process appears to be straightforward and seamless to the user, it can only be achieved through the integration of various access management products, including:

- Web Access Management (WAM)
- Identity Federation and Cloud Single Sign-On (SSO)
- Web Services Security and XML Firewalls
• Fine-Grained Authorization and Entitlement Management

• Security Token Service (STS)

This required level of integration is far from simple for most organizations to achieve, as it often requires integrating multiple point products from different vendors, none of which can support all the requirements. The diagram below illustrates some of the necessary integration points and associated administration tasks.

Figure 4: Administration and integration points

Organizations need a solution that reduces the burden of integration cost and complexity, while completely satisfying their access management requirements.

Meeting Demands for Mobile Access

Not long ago, mobile support meant little more than the ability to identify the browser on a mobile device, in order to modify content and factor in a smaller screen size. But as device capabilities have increased, so too has the demand for richer applications and access to more confidential data. A study in 2011 found that 58% of large organizations were planning to roll
out corporate or customer-facing mobile applications, raising critical security questions for the enterprise, such as "How do we apply access management principals to mobile applications?" The answer must extend beyond traditional authentication and authorization practices to one that identifies and reacts to the level of risk associated with the requested resource.

Mobile application developers focus on the function and usability of the app rather than its security. Mobile providers tend to focus on containment of session data within each application rather than understanding larger access management requirements. The result is often weak security and poor user experience. Accordingly, organizations require a new approach to mobile security, one that can easily interface access management capabilities and provide the ability for administrators to configure rather than code risk policies that govern authentication and authorization requirements.

Mobile security is a major new service in Oracle Access Management 11gR2. The solution enables enterprises to extend their access management infrastructure to mobile devices and provides users with a seamless and consistent authentication and SSO experience. Additionally, mobile security integrates with fraud prevention capabilities that register and fingerprint devices and adapts authentication and authorization requirements based on levels of risk. For example, when a request originates from a mobile device, Oracle Access Management may prompt for stronger authentication or deny access to certain types of content.

As represented in the diagram below, when a user accesses an Oracle protected resource from a mobile device (1), Oracle Access Management detects the mobile device and subjects the request to risk analysis (2). It then determines that additional authentication is required (3), a one-time-password (OTP) is sent to the device via SMS (4), the user enters the OTP (5) and then receives content according to an adapted authorization policy (6).

![Diagram showing the process of securing mobile access with adaptive access](image_url)

**Figure 5:** Securing mobile access with adaptive access
Fraud Prevention also provides device black-listing and lost and stolen capabilities to further enhance security and reduce risk.

The impact of Social Identity
Social Identity has gained traction over the past couple of years as an identity source, with many sites accepting social identity as an initial, low security form of authentication. Social identities can be used to establish some level of personalized services (as shown in step 1 in the diagram below), but as the user navigates to higher risk services, such as an online purchase (2), a site will typically require the user to follow standard registration and verification processes (3).

![Diagram showing the impact of Social Identity](image)

**Figure 6:** Social identity as the touchstone for stronger identity

Some sites provide the ability to link a social identity with a pre-registered account to simplify future authentications, but have limited capabilities for additional identity validation, which has reduced the viability of social-linked authentication for more secure services.

Oracle recognizes the importance of social identity to enterprises and has implemented support for leading social providers including Facebook, Google, Twitter, LinkedIn and Yahoo! in Oracle Access Management 11gR2. More importantly Oracle has solved the viability issue of using social identity to access secure services, by integrating social identity with its fraud prevention service that assesses risk and determines when additional validation is required.
Putting it all together: Complete Access Management

It’s clear that a new approach to access management is required, one that consolidates the capabilities of multiple point products to simplify traditional access management, while seamlessly integrating transformational technologies to help organizations respond to new opportunities.

This new approach to access management is what Oracle delivers with Oracle Access Management 11gR2, which moves beyond the traditional suite approach of other access management vendors to deliver a complete access management platform, with innovative new services that simplifies installation and configuration and provides internet-level scalability.

As shown in the figure below, Oracle’s access management platform provides a foundation of intelligent services, including session management, risk analytics, and audit features that are shared across the markets most comprehensive set of access management services.

*Figure 7: Platform and access services*
The platform is supported by a layer of common policy, transaction and identity infrastructure, which can be virtualized to represent a single view of identity from multiple identity sources, greatly simplifying policy definition and identity interaction.

Platform interfaces have built-in security mechanisms that can be complemented by Oracle API Gateway (OAG) that centralizes API policy configuration, enforcement and monitoring. OAG also provides additional security capabilities including threat protection, protocol security, data redaction, throttling and rate metering.

The following sections further detail the benefits of Oracle’s access management platform, highlight some of the innovative new features, and detail architectural considerations for highly available, internet-scale deployments.

A platform approach to Complete Access Management

Oracle’s next generation access management technology has a number of key characteristics, including:

- A platform of intelligent services that provide session management, sharing of identity and context, risk analytics, policy definition and configuration.

- A complete set of access management services that provide web single sign-on, authentication, authorization, federation, mobile and web services security.

- Services that adapt to heightened levels of risk and prompt for additional authentication or modify access rights.

- Coarse and fine-grained policy control that supports Oracle and third-party products and extends to custom developed applications.

- APIs that facilitate developer interaction across platform and access management services.

Put these characteristics together and introduce innovative new services that provide mobile security and integration with social identity and you have just described Oracle Access Management 11gR2.
Intelligent Platform Services

Oracle’s intelligent platform provides a host of security, session-sharing, audit and configuration capabilities to Oracle’s access management services. Risk analytics is woven into the platform and determines how services adapt to increased levels of risk by combining real-time analysis with historical comparison.

Oracle Platform Security Services

Oracle Platform Security Services (OPSS) is the underlying security framework for the entire platform and is common across Oracle Fusion Middleware applications including WebLogic Server. Designed by Oracle to be portable, OPSS provides the same security services to third-party developers, including interfaces for authentication, authorization, credential management, audit and encryption.

Session Management

Session Management is responsible for managing client sessions across all access management services, maintaining sessions based on various authentication, inactivity and time-to-live policies, which can be configured as required for each resource. One new capability in Oracle Access Management 11gR2 is the ability to share information between browser-based and enterprise single sign-on services, removing the need for additional authentication as the user navigates from one service to another.

Identity Context

Identity Context (ID Context) is responsible for sharing contextual information that can be used by access management services to determine appropriate authentication and authorization decisions. Contextual information can be formed from static information, such as the user’s profile, or from dynamic information, such as device and location. Risk analytics can be applied to provide true context-driven, risk aware access management.

Security Token Service

Security Token Service (STS) is based on the Web Services-Trust (WS-Trust) specification. It allows policy-driven trust brokering and secure identity propagation through the use of token exchanges among Web services.
Trust brokering is performed between a Web Service Consumer (WSC) and a Web Service Provider (WSP) and can accept multiple forms of authentication, including UserID, X.509, Kerberos and SAML and can generate UserID, SAML and custom tokens.

STS provides seamless connectivity between web and web service-based transactions, for example a user could authentication to a portal, which in turn connects to a web service to retrieve and present information.

Risk Analytics

Risk Analytics performs real-time behavioral profiling and anomaly detection to dynamically determine additional identity verification requirements and authorization decisions.

Risk Analytics utilizes identity, session and application data to determine the risk of each access request, for example if a user is using a mobile device they have not used before or they are performing an uncharacteristic transaction the level of risk is increased, prompting additional authentication in the form of a one-time-password, more strict authorization and potentially an alert to a security analyst.

Pre-defined and self-learning risk policies interrogate a database that keeps track of resource requests and usage patterns, allowing a baseline of normal usage to be established, which becomes a key factor in risk level determination.

Policy / Entitlements

The platform provides a common policy and entitlements store to streamline policy management and authorization decisions across each access service. Coarse and fine-grained access control is available and includes support for eXtensible Access Control Markup Language (XACML), NIST, RBAC, “Enterprise” RBAC and Java2 permissions. Policy is exposed through XACML request / response, OpenAZ PEP API for Java and .NET platforms, and JAAS interfaces.

Where possible, policy definitions can be shared across services, but as policy definition tends to be service specific (a fine-grained policy for database level access is not applicable to a URL-based policy) each service will have resource specific policy definition interfaces. Identity and context data (provided by ID Context) are accessible to policy administrators and delegated administration rules can be applied where appropriate.
Audit

Audit provides a common collection and real-time monitoring point for access and platform services, which facilitates compliance activities and real-time remediation.

Administrators have the ability to configure appropriate event tracking levels and alert triggers across all services and have the ability to run pre-defined compliance or customized reports from the centralized audit database.

Virtual Identity

Virtual Identity provides an interface layer that correlates identity from various sources into a single view that can be used by Oracle and third-party access services. Similar in capabilities to Oracle’s Virtual Directory technology, which creates a single view of identity from multiple LDAP and database sources, this platform service can leverage and contribute to other platform services.

Configuration

Configuration is simplified through a centralized configuration store and administration console. Oracle is diligently working towards a single administration interface that covers all Oracle Access Management services, which customizes itself based on delegated administration policies.

Access Management Services

Oracle provides a broad range of access management services that are packaged to satisfy specific market opportunities, for example Oracle Access Management Suite Plus combines authentication, authorization, web single sign-on, identity federation, mobile security and social interfaces, with platform services including session management, identity context, policy, risk analytics, configuration and audit. Each package is built with simplified installation and centralized configuration, as represented in the screenshot below of the Oracle Access Management centralized administration console.
Figure 8: Oracle Access Management Console

Single Sign-On

The single sign-on service provides web single sign-on and enterprise single sign-on capabilities.

The web single sign-on service supports a broad range of web servers and application servers. Oracle Access Management Webgates, Access Proxy and OpenSSO modules act as credential collection and policy enforcement points and integrate with other services, including authentication, coarse-grained authorization, session management and identity to provide full WAM capabilities. Its plug-in architecture maximizes deployment flexibility and removes the need to centralize web servers, which is a typical requirement of proxy-based architectures.

Software developer kits allow developers to integrate third-party applications not directly supported by Webgates.

Enterprise single sign-on unifies authentication across most desktop, client-server, host-based mainframe and custom applications. Client-side components also permit strong methods of authentication to be assigned to applications that only support user name and password combinations and single sign-on is maintained as users roam between different workstations.
Access Portal

The Access Portal Service provides a cross-platform single sign-on service for web-based applications, including SaaS applications, Oracle Access Management protected resources and business partner applications.

Single Sign-On is achieved through a variety of methods, including Oracle Access Management tokens (SSO to Oracle Access Management protected resources), Identity Federation (SSO to federation-enabled SaaS and business partner applications) and Form-Fill (SSO to non-federation enabled web applications - including SaaS).

The Access Portal service includes RESTful interfaces to application configurations and credential store services, a customizable user interface and integration with the Access Proxy to enable Form-Fill services.

Customers can also integrate existing or newly developed user portals via the RESTful interfaces.

Authentication

Authentication services are credential collectors that interact directly with the user or interface with identity federation and other web services to validate user and service client requests.

Administrators associate authentication schemes as appropriate for the type of resource and requesting client (user or service). For browser-based access these schemes can request one or more method of identity validation. Step-up authentication is also supported as users’ navigate to more secure resources, and administrators can define authentication levels that determine when authentication requirements for one resource can satisfy the needs of another.
Authentication is integrated with platform risk analytics, which determines when additional authentication is required, based on increased levels of risk.

A broad range of basic and advanced methods of authentication is supported out-of-the-box and authentication APIs enable integration with third party and custom developed authentication solutions.

Authorization

Authorization provides coarse and fine-grained access to various policy enforcement and decision points, including Oracle Access Management Webgates, OpenSSO modules, API Gateways and Entitlement Server security modules.

The authorization engine is exposed as eXtensible Access Control Markup Language (XACML) policy decision points that can be embedded in protected applications or deployed as centralized services and using the XACML request response or binary protocols.

Externalizing authorization and policy management for custom developed applications changes policy definition from a coding exercise to one of configuration, which greatly reduces development effort, improves security, allows policies to be changed in real-time and facilitates compliance efforts.

Social Identity

The social identity service simplifies integration with social sites including Facebook, Google and LinkedIn, specifically the configuration requirements to accept the social site as a trusted identity source for authentication and personalization.

Initially used as a mechanism to identify users for low risk content, social identity has become more prevalent as an entry point to more secure resources. Dependent on the social site, a user may grant permission to share a portion of their social identity, which can be used to streamline registration processes or automate account creation.

As the level of trust of a social identity authentication may not be appropriate for all resources, step-up authentication and risk analytics can determine when additional (local account) authentication is required.
Mobile Security

Mobile Security provides mobile access to identity and access management services, enabling mobile developers to authenticate, authorize and personalize the user experience from within native mobile applications.

Platform-specific packages and developer kits complement these services and enables single sign-on between native applications and mobile browser. Developers simply need to call the Mobile Security service to provide a secure, personalized user experience.

The Mobile Security service also provides access to device and location information that can be used to fingerprint the device. Each request can then be subject to platform risk analytics, which could force additional authentication such as one-time password (OTP) via SMS or email or other knowledge-based challenges and fine-grained authorization decisions.

Fraud Prevention

Fraud prevention extends platform risk analytics with adaptive access management capabilities that complement authentication and authorization services with OTP, knowledge-based authentication (KBA), virtual keyboard / keypad entry and context-driven authorization decisions.

Fraud Prevention services can also be leveraged by third-party applications, ensuring risk aware decisions across access management services and custom developed applications.

In addition to real-time risk analytics and behavioral profiling that establishes normal usage patterns; Fraud Prevention also provides a rich set of forensic data to facilitate investigation and auditing. This data can be accessed using powerful administrative tools that include pre-defined and customizable report templates that allow administrators and fraud investigators to further drill down to specific events and compare with past activity.

Web Services Security

The Web Services Security component secures and manages Web Services (WS) / Service Oriented Architectures (SOA) across a variety of web service platforms and includes Web Services Manager (WSM) agents that act as Simple Object Access Protocol (SOAP) interceptors that leverage access and platform services including authentication, authorization,
configuration and audit. Run-time level processes increase the level of control and visibility and ensure message integrity, message confidentiality and quality of service.

Oracle API Gateway extends web services security to the network perimeter and corporate DMZ, by providing a proxy-based enforcement and decision point that supports a variety of protocols (SOAP, REST, OAuth, JMS, XML, FTP, etc) across Oracle and third-party web services and SOA infrastructure.

API Service

Even with an impressive array of out-of-the-box capabilities, Oracle understands that customization and integration may be required to make the solution a perfect fit.

As such, Oracle provides extensive Software Developer Kits (SDKs), including code examples, for all major platform and access services. Oracle is also committed to securely exposing more of its identity and access services over standard Representational State Transfer (REST) interfaces to further simplify integration efforts.

Low Risk Upgrades

Oracle Access Management 11gR2 represents the convergence point for Oracle Access Manager 10g, OpenSSO, and Oracle Single Sign-On. It provides superior capabilities and performance and includes backwards compatibility with previous versions to maximize uptime during migration.

It’s important that Oracle customers experience as smooth a transition as possible to the new access management platform; as such migration assessment and transfer tools complement detailed documentation.

Dependent on the currently deployed technology, the migration assessment tool will recommend different strategies for migration, ranging from simple upgrade to coexistence strategies that support a pragmatic approach to migration, which utilizes backwards compatibility support.
Blueprint Architecture – Complete Access Management

The high-level blueprint architecture illustrated in the figure below provides complete access management for internal and external services across a variety of clients.

To achieve this level of control, Oracle packages platform and access services into access management products that provide flexible deployment and maximum coverage.

Oracle access management products referenced in this architecture includes:


- **Oracle Entitlements Server** – XACML-based (eXtensible Access Control Markup Language) fine-grained authorization and data security.

- **Oracle API Gateway** – Security Layer for Web Services and APIs

- **Oracle Web Services Manager** – Policy control for SOA infrastructure

*Figure 9: Complete access management blueprint architecture*
Clients

Clients represent any client that connects to an Oracle protected resource from the Internet or Intranet, including:

- Users accessing resources from a web browser and/or mobile device
- Partner-affiliated users accessing resources from a web browser and/or mobile device
- Application and/or web service accessing internal or cloud resources via web service / API interaction
- Cloud provider accessing resources via web service / API interaction

Clients also represent client access to external services, including:

- Users accessing cloud applications from a web browser and/or mobile device
- Users accessing partner resources from a web browser and/or mobile device
- Application and/or web service accessing partner and/or cloud applications

Oracle manages access for all client-types regardless of origination and destination (Internet / Intranet) points.

Mobile application developers will leverage the Mobile SDK to build access management capabilities, including authentication, authorization and single sign-on into native mobile applications.

Web Tier

Web Tier represents access and policy enforcement points that are typically located in a DMZ, including:

- Web resources protected by Oracle access management agents;
- Oracle HTTP Server acting as reverse proxy to internal resources; and
- Oracle API Gateway acting as an additional security layer for Web Services and API-based resources, with hosted policy decision point to maximize performance.
Oracle API Gateway is a highly recommended component as it extends API security to the network perimeter and provides additional validation of requests before forwarding to backend resources. It also provides a central point to enforce authorization and data redaction policies and includes threat protection, client throttling and protocol security.

Application Tier

Application Tier represents Oracle Fusion and third-party applications and services protected by Oracle Web Services Management and Oracle Entitlements Server policy enforcement and decision points.

Applications and services that require fine-grained authorization decisions can leverage policy enforcement point agents that cover a variety of applications, services and databases, or can issue XACML policy requests to hosted or remote policy decision points.

Data Tier

Data Tier represents Oracle and third-party identity and application database stores. Oracle Virtual Directory provides a consolidated view of a user’s identity from multiple identity stores, which simplifies policy definition and identity interaction.

Policy decision and enforcement points can be hosted on supported databases to provide fine-grained authorization capabilities that extend to specific fields and rows in the database.

Access management infrastructure

Access management infrastructure includes the management points, policy stores, interfaces and transaction databases that provide the full range of access services across all tiers and client types, including:

- Identity Federation – Single sign-on to-and-from business partners and cloud providers.
- Mobile application security and integration with social identity.
• Fraud Prevention – Adaptive access management capabilities extend across all platform and access services and using real-time and behavioral analysis to determine risk levels and appropriate actions.

• Fine-grained authorization – Oracle Entitlements Server provides XACML-based policy decision and enforcement.

• Web Services Manager – Policy configuration and monitoring of SOA infrastructure.

Internet-level Scalability and High Availability

Oracle Access Management 11gR2 has been architected to provide internet-level performance, scalability and high availability.

Internet-level scalability and performance

Oracle conducted large scale performance testing that included a database of over 250 million user accounts and was able to demonstrate linear levels of performance as the number of Oracle Access Manager servers increased. For example, the addition of a second Oracle Access Manager server to a configuration, increased authentication transactions per second from 3000 to 5250.

High Availability

High Availability (HA) refers to the system or components ability to continuously operate for long periods, even in the event of a system or component failure, and many organizations have HA strategies that target “five 9s” (99.999%) availability, which require compliance by access management technologies.

Depending on service level requirements, HA strategies can range from standby and active server configurations all the way through to active-active between multiple data centers, which is a common configuration employed by financial organizations to achieve maximum levels of availability.
Oracle’s access management technology supports the full range of HA strategies including active-active data centers, as represented in the figure below:

![Data center configurations diagram]

**Figure 111:** Active-Active data center configurations.

You can be sure that Oracle’s access management technology has been proven to support your High Availability needs and support your “five 9s” availability goals.

**Conclusion**

Oracle Access Management 11gR2 represents a major milestone in access management technology that is unique in the industry. Oracle’s Access Management platform provides innovative new services that complement traditional access management capabilities. Services can be enabled as required to meet the specific needs of your organization.

This new platform represents key development goals for complete, innovative, simplified and scalable access management that is open to third-party customization and integration. Whether your need is to provide secure access to browser-based applications, secure mobile applications, cloud single sign-on, secure web services or federated single sign-on to and from your business partners, you can be sure that it’s a service provided by Oracle Access Management 11gR2 – Complete and Scalable Access Management.