ORACLE
FUSION MIDDLEWARE
ACCESS MANAGEMENT SUITE

# Oracle Access Management

## Buyer's Guide

ORACLE WHITE PAPER | APRIL 2015

## Disclaimer

The following is intended to outline our general product direction. It 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 features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

## Introduction

In the recent past (early 2000's), Access Management was mainly centered on web authentication, single sign-on, and access to intranet and extranet applications. However, the enterprise access management landscape has been evolving at a fast pace over the last few years to meet the requirements of new computing paradigms such as Cloud computing, in particular Software-as-a-Service (SaaS), mobile access, especially bring-your-own-device (BYOD) programs, social interaction leveraging social network identities, and the Internet of Things.

In addition, economic and market forces have compelled companies to explore ways to reduce costs via integration with partners through new standards (e.g., OAuth), new architectures (e.g., REST), new application programming interfaces (public APIs), as well as data center and license consolidation, and privately or publicly hosted Access Management services. At the same time, changes to healthcare and privacy laws along with a large set of regulatory requirements have forced corporations to rethink their approach to enterprise security and privacy.

In such challenging environments, companies must develop a holistic and proactive strategy based on risk management principles. Companies that use a reactive approach to security, selecting different identity-based solutions or point products to protect web applications, mobile applications, Cloud applications, APIs or web services, may ultimately fail. Reactive and siloed approaches result in a brittle security infrastructure that is costly to maintain and, as a consequence of inconsistent security policy management, prone to external and internal security breaches and failed compliance.

Selecting the appropriate solution goes beyond meeting immediate, basic requirements. At a high level, a single Access Management solution should be able to address the requirements for four typical scenarios including Cloud security, mobile access, employee-facing intranet and customer-facing extranet access control.

In addition to traditional web access control, Oracle Access Management offers a complete solution to securely enable business transformation with mobile, Cloud and social networking technologies. The context-aware and risk-aware nature of the solution ensures strong security while supporting better user experience.

This buyer's guide is designed to help stakeholders and decision-makers develop a clear understanding of key features and requirements when evaluating an Access Management solution.

## Business Drivers

Although there are many practical reasons to consider security solutions, it is necessary to understand how they can positively impact the business. In this section, we take a look at key business drivers for adopting an Access Management solution in today's enterprise.

- **Enable Cloud Economy**: As enterprise Cloud adoption continues to grow at an increasing pace and organizations recognize the productivity and cost savings from the Cloud, IT organizations face the same challenges they face with on-premise applications – siloed access management and control. The problem is made even worse with hybrid on-premise and Cloud deployments. To secure access, enhance user experience, and improve compliance in the Cloud era, a modern Access Management solution is required to provide security to both on-premise and Cloud applications in a single point of control and administration.
- **Secure Mobile Access**: With the promise of anytime / anywhere access, the use of mobile devices is transforming the way we live and the way we do business. Customers are doing transactions through multiple channels such as web and native mobile apps, and employees are using their own devices to access corporate applications and data. Securely enabling mobile access and providing seamless multi-channel user experience are necessary prerequisites to ensure business advantages.
- **End-to-End Security**: Today, enterprises are looking to adopt solutions that can provide end-to-end protection. A complete solution protects sensitive data every step of a transaction, from any online end-user all the way to the requested resource's endpoint.
- **Internet Scalability**: Organizations are increasingly looking for their partner network to enhance their competitive advantage or to serve their customers with new, innovative services. Access Management must be able to perform at Cloud and extranet scale to serve the modern enterprise.
- **Risk Mitigation**: Fraud and security breaches have a significant financial and reputation impact on the business. With so many types of threats facing the enterprise, a complete Access Management solution must do more than simply log risky or anomalous events. It must monitor and analyze risk in real time and take appropriate actions to prevent fraud.
- **Simplified Management**: Security should be easy to manage, ensuring timely and effective deployments and creating a uniform user experience. By establishing a simplified approach to security, the enterprise can be assured of tighter control and reduced operational costs.

## Key Considerations for Typical Scenarios

This section describes four scenarios emphasizing best practices: Cloud, mobile, employee-facing intranet and customer-facing extranet.

### Cloud

As enterprises increasingly embrace Cloud applications, both Cloud applications and on-premise applications need to be secured from a common set of controls. Following are key considerations for securing a hybrid environment.

- If the authoritative identity resides on premise, the user should log on to the corporate portal and then federate with Cloud applications. Enforcing log on to the corporate portal first and removing direct log on to Cloud applications prevents the situation where an employee continues to log on to Cloud applications after leaving the company.
- The Access Management solution should enable standards-based SAML federation or OAuth to access Cloud applications.
- If the Cloud application does not support standards-based federation, the Access Management solution should provide a form-fill capability to automatically populate credentials for the user in order to deliver a seamless SSO experience.
- A single Access Management solution for both on-premise and Cloud applications is required. A Cloud-only SSO solution to support federated access to Cloud applications is not enough as it creates a silo from existing on-premise enterprise solutions.
- The Access Management solution should provide an easy way to build an SSO portal for the user to access both on-premise and Cloud applications from a single pane without signing on again.
- Customers should have the option of deploying the Access Management solution on-premise or in Cloud.

### Mobile

Mobile is becoming an essential access channel. Users expect a seamless access experience across multiple channels and enterprises require consistent access policies across those channels. Following are some key considerations to secure mobile access.

- The Access Management and mobile solution should ensure consistent user experience for SSO operation among native apps, and between native and browser apps based on common corporate security policies.
- Mobile access presents higher risks than traditional channels due to potential lost or stolen devices. The Access Management solution should be able to automatically fingerprint and register the device as well as whitelist and blacklist devices.
- The Access Management solution should be able to understand the context of an access request such as the type of mobile device, mobile device configuration, geo-location, and transactional context for authentication and authorization decisions. For example, when a user uses a mobile device for the first time to access a resource, the user may be prompted for stronger or step-up authentication, and confidential data may optionally be redacted in the response sent back to the mobile user.
- In a Bring Your Own Device (BYOD) scenario, the Access Management solution should be able to separate corporate data from personal data without disrupting the user experience.
- The Access Management solution should be able to easily enable existing applications for mobile access through a REST interface and secure that REST interface.
- A standalone, not integrated mobile security solution will create a security silo, prevent consistent policy from being enforced across multiple channels, and deliver an inconsistent user experience.
- Organizations should be able to rely on the Access Management solution to easily attract users by leveraging social identities from Facebook, Twitter, Google, or Yahoo to better personalize services while maintaining a high level of access control and the linking of social account(s) to a local user account for added security.

## Employee-Facing Intranet

Employees, contractors and partners rely on the corporate intranet for their daily work, and security threats (whether malicious or accidental) may originate from inside the company. Following are some key considerations for maximizing productivity and ensuring security and compliance in your corporate intranet.

- Protect against insufficient intranet security that may result in IP or financial loss as well as compliance failure. The Access Management solution must prevent session hijacking and session replay by supporting cookie scoping at the host or application level and session control at the individual user level in order to prevent and contain security breaches.
- Support multi-channel access. Since corporate services may be accessed through a web channel (laptop or desktop enterprise SSO), mobile native apps, or web services in business-to-business scenarios, the Access Management solution must be able to secure all channels with consistent, centralized security policies and deliver seamless user experience throughout a business transaction for multiple categories of users (employees, contractors, partners, administrators, and line-of-business managers).
- Business agility depends on the enterprise's ability to manage and report on who has access to what at a granular level. Additionally, in order to always meet security and compliance requirements, an organization must be able to implement access policy changes quickly when needed without having to change the backend applications. This can be achieved with a fine-grained authorization capability that can externalize and centralize application authorization policies.

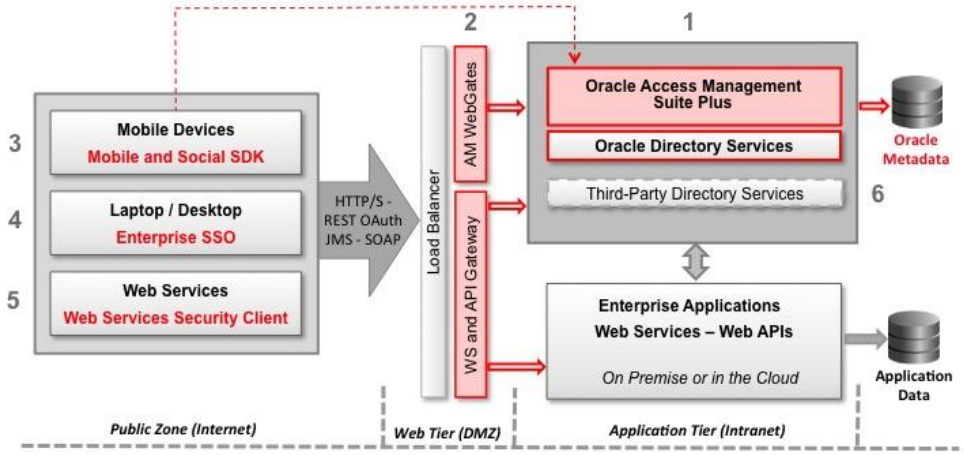
## Customer-Facing Extranet

The Internet delivers global 24x7 access to your business assets. In addition to traditional access control requirements such as authentication and federated SSO, following are some key considerations for protecting your customer-facing online applications.

- Balance security and user experience. For example, some applications or information can be accessed with a social identity, some may require a local log in, some more valuable assets may require a step-up authentication using Knowledge Based Authentication (KBA) or require multi-factor authentication, such as One Time Password/ Pin (OTP), when risk is high. An Access Management solution should be able to understand the context and risk of an access request and provide the full spectrum of services based on that context.
- The Access Management solution needs to be scalable to support your business growth. Consumer-facing applications may need to support hundreds of millions of users and performance and scalability issues may result in lost transactions and disgruntled customers. In addition, High Availability (HA) with multi-data center support is a must as downtime results in lost business opportunities and bad user experience.

## Oracle Access Management

Oracle Access Management 11gR2 represents a major milestone in Access Management technology that is unique in the industry. Oracle Access Management provides innovative new services that complement traditional access management capabilities. For example, adaptive authentication, federated single-sign on, risk analysis, and fine-grained authorization are extended to mobile clients and mobile applications, and Access Portal allows customers to build their own private Cloud SSO services. Oracle Access Management services are delivered on a single platform and can be licensed and enabled as required to meet the specific needs of your organization now and in the future.




1- Access Management's server-side services hosted in Oracle WebLogic Server.

2- Access Management's first-line-of-defense interceptors and filters (Access Management WebGates, and Web Services and API Gateway).

3- Mobile and Social client SDK, installed in mobile devices.

4- Enterprise SSO Suite installed on PCs (desktops and laptops).

5- Web Service Manager's client agents embedded in web services or applications sending requests to web services providers in the Application Tier.

6- Directory services may alternatively be deployed in the Data Tier (Note: Oracle Directory Services are not part of the Oracle Access Management Suite, they're sold separately)

Oracle Access Management is an integrated platform providing the following services:

» **Access Management Core Services**: Authentication, web SSO, coarse-grained authorization for enterprise applications deployed on premise or in the Cloud.

» **Identity Federation**: Cross-Internet-domain authentication and delegated authorization supporting industry standards such as Security Assertions Markup Language (SAML), OAuth, and OpenID. Social log-on using social network identities is supported, allowing mapping to a local user account.

» **Mobile Security**: Lightweight mobile, Cloud, and social networks interface to access corporate resources via industry standards such as OAuth. The Mobile and Social service allows mobile clients such as smart phones to

leverage the backend Access Management infrastructure for authentication, SSO, fine-grained authorization, risk analysis, and adaptive authentication.

- **Access Portal Service**: A web-based central launch pad allowing users to federate all their applications through SAML, OAuth, or Form-Fill. Access Portal provides the foundation to build a private or public cloud SSO service.
- **Adaptive Access and Fraud Detection**: Strong, multi-factor authentication and heuristic fraud detection.
- **Fine-grained Authorization**: External, centralized, fine-grained, attribute-based authorization compliant with the Extensible Access Control Markup Language (XACML) standard.
- **API Security**: First line of defense for REST APIs and web services typically deployed in the DMZ, supporting protocol and data format transformation, API firewall, authentication, and authorization.
- **SOA Security**: Last-mile security component co-located with the resource endpoint, designed to protect against man-in-the-middle attacks.
- **Security Token Service**: Trust brokerage between different, heterogeneous infrastructure tiers by creating, validating and consuming standard security tokens such as SAML assertions or Kerberos tokens.
- **Rich-Client-Based Enterprise SSO**: Standalone component suite installed on a Microsoft Windows PC to provide SSO to rich-client applications. Browser-based Enterprise SSO is available through Access Portal.

## Enterprise Access Management Checklist

This section is broken down into functional sub-sections describing the key features to consider when evaluating an Access Management solution.

**INTEGRATED SOLUTION**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Complete solution | One multi-functional solution to secure mobile, Cloud, and enterprise for consistent security and compliance, without point-product integration. |
| End-to-end security | Security layered across tiers:<br>» *Extranet: first-mile security*<br>» *DMZ: perimeter security*<br>» *Intranet: last-mile security* |
| Identity context | Context-aware security takes into consideration real-time context from each tier to make authentication and authorization decisions. This enables consistent and dynamic policies based on devices, channels, users or applications for better security and user experience. |
| Identity propagation | Allows a requester's identity (user, application, or web service) to be propagated and audited throughout a transaction, across all the tiers involved in the processing of the request and the response returned to the requester. |
| Unified administration | One administrator's console for all access management services to simplify policy administration. |
| Delegated administration | Distributed policy management allowing line-of-business owners or administrators to manage their security environment in their own domain, for their own assets. |

**SECURITY**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Session Management | Ability to set session limits and manage user session(s) at the individual level. |
| Cookie scoping | Host- or application-scoped SSO cookie to prevent security breaches on protected applications due to a stolen cookie. |

| | |
|---|---|
| Prevention against session replay | Ability to prevent cookie spoofing and prevent a stolen cookie from being replayed for unauthorized access. |
| Anti-phishing | Enable a website to mutually authenticate the user and the site through, for example, images and/or phrases. |
| Anti-key-logging | Prevent key-logging from capturing user credentials. |
| Device fingerprinting | Identify the device for better security and user experience. |

**INTELLIGENT ACCESS MANAGEMENT**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Context-aware access | Ability to collect, consume, and propagate real-time context from devices, web HTTP requests, transactions, session information, LDAP attributes to make authentication and authorization decisions for enhanced security and compliance. |
| Content-aware access | Understand a resource's metadata (e.g., classification and value) in content management systems including SharePoint or Oracle WebCenter to apply and enforce access policies accordingly. |
| Risk-aware access | Make authentication and authorization decisions based on real-time analytics to address fraud and misuse across multiple channels of access (real-time evaluation of multiple data types helps stop fraud as it occurs); device fingerprinting, real-time behavioral profiling and risk analytics harnessed across both web and mobile channels, and risk-based authentication methods including knowledge-based authentication (KBA) challenge with server-generated one-time passwords (OTP). |

**ADAPTIVE AUTHENTICATION**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Strong authentication | Provide built-in multi-factor authentication capabilities such as OTP through SMS or a mobile-application-based authenticator, as well as image- and phrase-based mutual authentication or virtual pad to prevent key logging and password phishing. |
| Step-Up authentication | Allow the administrator to make a decision for stronger authentication or validation based on the request context and the access risk. |
| Soft-token authenticator | In addition to SMS or email based OTP, a mobile application based authenticator provides a low-cost alternative to hardware based tokens for multi-factor authentication. |

**RISKS ANALYSIS**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Real-time risk analytics | Risk evaluation logic that determines the level of risk at a given moment based on multiple data points. Risk-based proactive actions can prevent fraud before it happens. |
| Auto-learning and behavior profiling | Automatically profile a user's behavior in real-time to provide immediate detection of anomalies and enable the solution to adjust quickly and single out fraud with lower false positive and negative rates. |
| Device tracking and fingerprinting | Ability to tag and track devices throughout a session resulting in enhanced protection from threats such as session hijacking. |

**EXTERNAL, FINE-GRAINED AUTHORIZATION**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| External, fine-grained authorization | Ability to externalize and centralize application authorization policies for a complete view of a user's entitlements. Allows better business agility by avoiding modification to the application when security policies need to be changed. Fine-grained authorization service granting or denying access to a resource based on the context of the authorization request such as device, location, authentication, and transaction information, as well as risk level. |
| Data redaction | Ability to control access to any database system at the data, row, and column or attribute level based on fine-grained authorization policies and real-time context. For example, private data can be redacted or specific characters can be masked in the response sent back to the requesting party. |
| Content-based authorization decisions | Applies and enforces security for content management systems such as Microsoft SharePoint and Oracle WebCenter based on file and folder classification (e.g., confidential, top secret) and specific attributes (e.g., job title or organization). |

**CLOUD SECURITY**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| SSO portal | A central logon portal providing users with SSO to on-premise and Cloud applications through federation, username / password form-filling or local access management. Provide the foundation for building private or public Cloud SSO services. |
| Identity federation | Provide federated SSO between on-premise and Cloud applications. Support for industry standards and protocols such as SAML, OAuth, OpenID, etc. Ability to support just-in-time provision of the user. |
| Delegated authorization | Externalize Cloud application authorization using an OAuth mechanism or through the claims stated in a SAML assertion so the enterprise has full control of who has access to what in a Cloud application. |
| API economy | Easily enable Cloud access to a legacy application using REST as well as secure the REST interface. |
| Secure hybrid application environment | Secure both Cloud and on-premise applications with the same access management infrastructure. |
| Hosted deployment | Flexibility to deploy the solution on-premise or in the Cloud to secure on-premise and Cloud applications. |

**MOBILE ACCESS**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Employee-centric mobile security | Ability to separate corporate data from personal data by containerizing corporate apps for BYOD users. Provide authentication, SSO, and device security policy management and enforcement. |
| Customer-centric mobile security | Ability to provide authentication and SSO among native apps and between native and browser apps. Ability to fingerprint and register the devices for added security. Strong security with context-based and risk-based adaptive authentication and authorization is needed for high-value transactions. |

**SOCIAL IDENTITY SUPPORT**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Integration with social networks | Enable enterprises to leverage social logins from social networks such as Facebook, Twitter, Google, LinkedIn, Microsoft Live, or Yahoo, to securely attract customers while providing a good user experience. |
| Delegated authorization (OAuth) | Support OAuth 2.0 for authorization claims and attributes sharing. |
| Registration | Ability to leverage social identity for user registration. |
| Local account linking | Ability to link social account(s) to a local user account for added security and compliance. |

**ENTERPRISE SINGLE SIGN-ON**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Enterprise single sign-on | Allow users to log on to networks, applications, and web sites using a single password. Once a user authenticates to Windows for the first time, the solution manages the passwords for all subsequent application logons with the ability to add layered security if required. |
| Windows application SSO | Pre-configured for Microsoft Office, Adobe Acrobat Reader, FrontRange Goldmine, Interact Act!, PKZip, and virtually all other Windows applications. |
| Web application SSO | Pre-configured for accessing web applications on Microsoft Internet Explorer and Mozilla Firefox. Also provide support for web pages including form-based and pop-up sign-ons. For web application SSO, username/ password can be form-filled without a client being installed at the endpoint. |
| Rich-client application SSO | Ability to handle form-fill for non-web applications including Windows applications, Java application and applets, and host / mainframe applications. |
| Password Reset | Provide self-service (GINA or browser) or assisted password reset for users. |
| Strong multi-factor user authentication | Multiple authentication modes for the user, including Windows login, LDAP, PKI, smart card, biometric, or token-based authentication without modifying applications for rapid deployment and low-cost adoption. |
| User access mode | Provide multiple ways for users to access enterprise applications, including desktop, offline, kiosk, or shared workstation. |
| Encryption support | Protects each user's credential store using one of several selectable encryption algorithms. |

**AUDITING AND REPORTING**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Reporting and auditing for compliance | Provide both the framework and tools necessary to track, report and verify significant events. |
| Reports generated from local audit data | Locally store audit data so that reports do not require frequent target resource accesses. |
| Data archival tools | Provide automated tools for managing high volumes of audit data and archiving data into an archiving database. |
| Integrated reporting | Single console integrating audit reporting across the entire identity and access management suite. |

| | |
|---|---|
| Customized report | Ability to customize reports to meet specific company or compliance requirements. |

**SCALABILITY, PERFORMANCE, HIGH AVAILABILITY**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| Proven large scale deployments | Scale to support business growth for tens of millions to hundreds of millions of users, and thousands of protected enterprise applications. |
| Load balancing and failover | Support agent-to-server and server-to-LDAP load balancing and failover. |
| Multi-data center deployment | Enable active-active deployment across multiple data centers for HA. Also support Active-Passive or Active-Standby deployments. |
| Automated policy replication | Allow policies and configurations to be replicated automatically across clusters and data centers. |
| Choice between session-based or cookie-only deployment | Active session management enhances security while cookie-only deployment may deliver better performance. Options for deployment based on requirements. |
| External, fine-grained authorization | Near zero impact to performance when externalizing authorization for compliance and business agility. |

**SIMPLIFIED MIGRATION, PATCHING, AND UPGRADES**

| Key Functionality | Feature Details/ Benefit |
|---|---|
| System management | Ability to discover services, monitor Access Management environments in a centralized system-monitoring console. Monitor the health of the environment including databases and the underlying host servers. Provide information on component availability, incidents, and patch recommendations. |
| Service management | Create service-level agreements (SLAs), assign service-level objectives (SLOs). |
| Dashboards | Display metrics for each service health, display hardware utilization charts for all services, report on trends in metrics change over a period of time. |

## Conclusion

As enterprises are extending their reach through new computing paradigms, Cloud, mobile, and existing enterprise applications should not be siloed in order to prevent security breaches and compliance failures, and decrease operating costs. Access Management is critical for enterprise security and compliance and needs to be modernized to support the new requirements of the extended enterprise.

Oracle Access Management has evolved to meet new requirements including Cloud deployments, mobile app access to corporate resources, integration of social networks into the corporate fabric, and integration of Access Management infrastructures with backend applications deployed on-premise or in the Cloud. Based on a homogeneous platform architecture, Oracle Access Management allows you to meet your specific requirements at your own pace, without disrupting your existing environment while supporting your enterprise's growth.

**Oracle Corporation, World Headquarters**
500 Oracle Parkway
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

**Hardware and Software, Engineered to Work Together**