

# Oracle Access Management

Complete, Integrated, Scalable Access Management Solution

ORACLE WHITE PAPER | MAY 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

Executive Summary	2
Introduction	3
Typical Use-Case Scenarios	5
Oracle Access Management Overview	6
Oracle Access Management Core Services	7
Intelligent Access Management	8
Adaptive Access and Fraud Prevention	12
Identity Federation	13
Mobile Security	16
API and Web Services Security	20
Cloud Security	22
Enterprise Single Sign-On	24
Scalability and High Availability	25
Conclusion	26



## Executive Summary

In the recent past, Access Management was mainly focused on web authentication, single sign-on, and access to intranet 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 and technologies transforming the way organizations access and expose business-critical services and data. In today's enterprise environment, organizations increasingly depend on the cloud for delivery of applications in addition to existing on-premise deployments, and more and more users leverage multiple types of devices to access those applications. In order to increase traffic to their corporate portals, enterprises often leverage less-secure social network identities. Finally, a growing number of large corporations need to support the proliferation of smart devices ("Internet of Things"), with new approaches to security controls and the management of increasingly large amounts of information.

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 cloud-based 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 concurrently protect on-premise and cloud resources, mobile apps, and APIs or web services, will 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.

This paper introduces Oracle Access Management, a complete solution designed to securely enable business transformation with mobile and social networking technologies, hybrid on-premise and cloud applications deployment, and hybrid Access Management deployment while preserving a seamless user experience, centralized administration, and market-leading performance and scalability.

## Introduction

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 access to SOA applications. Various industry-standard specifications including Security Assertions Markup Language (SAML) 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 following example illustrating the need for seamless client and system interactions across enterprise and cloud resources:

- » A user located in his office accesses the corporate portal.
- » In the corporate portal, the user clicks on a link for a new business intelligence Software-as-a-Service (SaaS) application, which redirects the user to the cloud application.
- » 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.
- » Finally the cloud application presents the data on the user's dashboard.

While this process appears to be straightforward and seamless to the user, it can only be achieved through the integration of various access management services, including Web Access Management; Identity Federation and Cloud Single Sign-On; API (or Web Services) Security and XML / JavaScript Object Notation (JSON) Firewalling; Fine-Grained Authorization and Entitlements Management.

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.

Oracle Access Management 11gR2 represents a major milestone in Access Management technology that is unique in the industry. Oracle Access Management is designed to meet the requirements of the new Access Management paradigm.



Figure 1: New Access Management Paradigm

Oracle Access Management provides innovative new services that complement traditional access management capabilities. For example, adaptive authentication, federated single-sign on (SSO), 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. Services can be licensed and enabled as required to meet the specific needs of your organization.

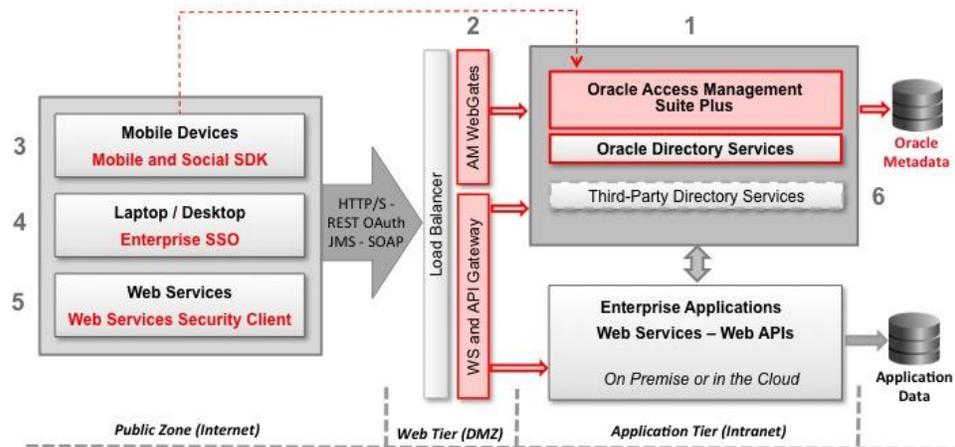


Figure 2: Oracle Access Management Overview

- 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 service client SDK, installed on mobile devices.
- 4- Enterprise SSO Suite installed on PCs (desktops and laptops).
- 5- Web Services 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 SAML, OAuth, and OpenID. Social log-on using social network identities is supported.
- » **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 adaptive authentication, SSO, fine-grained authorization, risk analysis and fraud detection.
- » **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 transformation, API firewalling, 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.

## Typical Use-Case Scenarios

This section describes four typical scenarios emphasizing Oracle Access Management's strengths: cloud, mobile, employee-facing intranet and customer-facing extranet.

### Cloud

As enterprises increasingly embrace cloud applications, both cloud 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 intellectual property (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 Overview

Oracle Access Management is part of the Oracle Identity Management pillar. Oracle Identity Management enables organizations to effectively manage the end-to-end lifecycle of user identities across all enterprise resources, both within and beyond the firewall and into the cloud. The Oracle Identity Management platform delivers scalable solutions for Identity Governance, Access Management (the subject of this paper), and Directory Services. This

modern platform helps organizations strengthen security, simplify compliance, and capture business opportunities around mobile and social access involving hybrid on-premise and cloud environments.

As part of the Oracle Fusion Middleware family of solutions, Oracle Access Management provides all the security services for Oracle Fusion Middleware components using a common development framework (Oracle Application Development Framework –ADF), and providing a single user interface across all Oracle Fusion Middleware components. Oracle Access Management leverages the scalability of Oracle’s application container (Oracle WebLogic Server) and Oracle Fusion Middleware’s cross-solution systems management environment (Oracle Enterprise Manager), as shown in Figure 3.

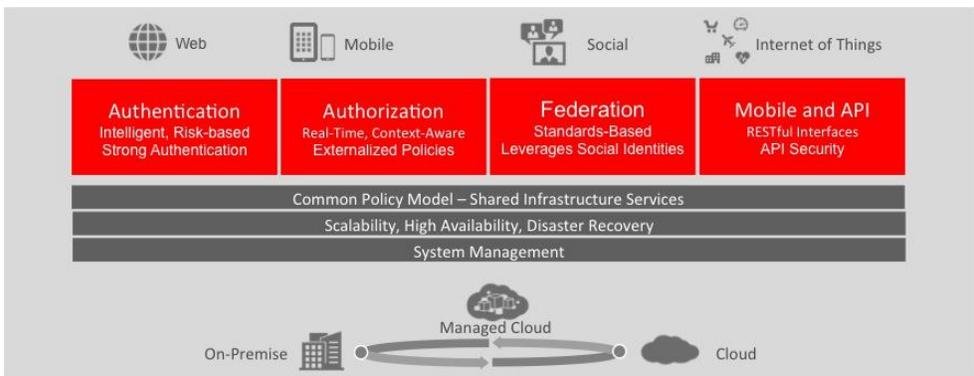


Figure 3: Oracle Access Management: Oracle Fusion Middleware's Security Pillar

The following sections describe Oracle Access Management services in detail.

### Oracle Access Management Core Services

Oracle Access Management core services provide the primary perimeter access control services for the whole Oracle Access Management platform, including web authentication, web single sign-on (SSO), and coarse-grained authorization. As shown in Figure 4, Oracle Access Management core services are deployed in a layered architecture across web, application, and data tiers.

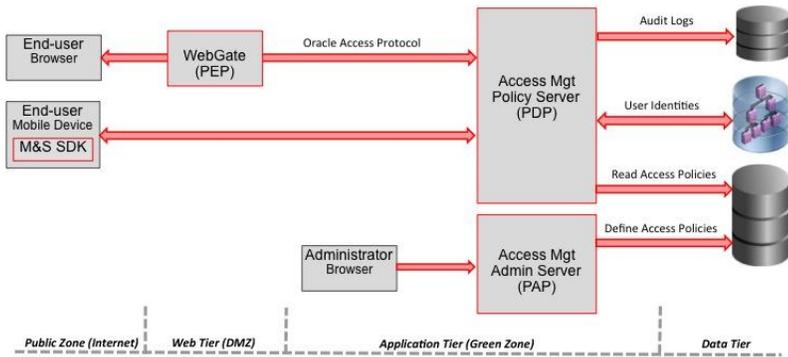


Figure 4: Oracle Access Management Deployment Overview



Users access protected web applications by authenticating to Oracle Access Management. The user request is intercepted by a filter referred to as WebGate acting as a Policy Enforcement Point (PEP) deployed in the DMZ. The WebGate communicates with Oracle Access Management's policy server, which acts as the Policy Decision Point (PDP). The administrator sets up security policies and selects authentication schemes from the administration console, which acts as the Policy Administration Point (PAP). If authentication is successful, a cookie is returned to the user's browser to enable repeated log-ins to the same application or SSO with other web applications similarly protected by Oracle Access Management. For authorization, the WebGate prompts the Access Management policy server to look up authorization policies. The Access Management policy server evaluates the user's identity and determines the user's level of authorization for the requested resource (coarse-grained authorization).

Oracle Access Management lets users log in without credentials after first-time log-in based on configurable cookie technology. This capability, known as "persistent log-in," is enabled by the application domain's system administrator. Oracle Access Management supports Windows Native Authentication (WNA) whereby a client logs in to their Windows desktop, opens an Internet browser, navigates to an Access Management protected HTTP resource, and is let in using the Kerberos Service Ticket without being challenged.

Credentials are sent to the Access Management runtime servers for collection, regardless of where the login pages are (sample log-in pages are provided out-of-the-box). Oracle Access Management extends WebGate 11g with a detached credentials collector (DCC) capability enabling the decoupling of credential collection from the server thus providing additional security (end-user HTTP sessions get terminated in the DMZ), and reducing overhead on the server in addition to improving performance.

## Session Management

Oracle Access Management supports the session management life cycle (session life time, idle timeout, maximum number of sessions, database persistence of active sessions). Server-side session management allows for advanced session management across nodes via Oracle Coherence-based caching. Client-side session management stores the session details in the browser cookie with no information saved on the server side (stateless session), providing higher performance and smaller footprint than server-side session management.

## Intelligent Access Management

Intelligent access management includes identity context, dynamic authentication, and content-aware authorization.

### Identity Context

Identity Context is an innovative feature of Oracle Access Management. Identity Context allows organizations to meet growing security threats by leveraging the context-aware policy management and authorization capabilities built into the Oracle Access Management platform. Identity Context secures access to resources using traditional security controls (roles and groups) as well as dynamic data established during authentication and authorization (authentication strength, risk levels, device trust). Contextual information controlled by the Oracle Access Management platform includes:

- » Presence (location, historical patterns)
- » Authentication strength (weak, strong)
- » Level of assurance (NIST levels, X509 certificates)
- » Risk assessment (pattern analysis)
- » Federation (partner attributes)
- » Device characteristics (fingerprint, device health, device protection, trusted data)

- » Assertions from trusted partners (SAML tokens, JWTs)
- » SSO sessions (session timeouts)

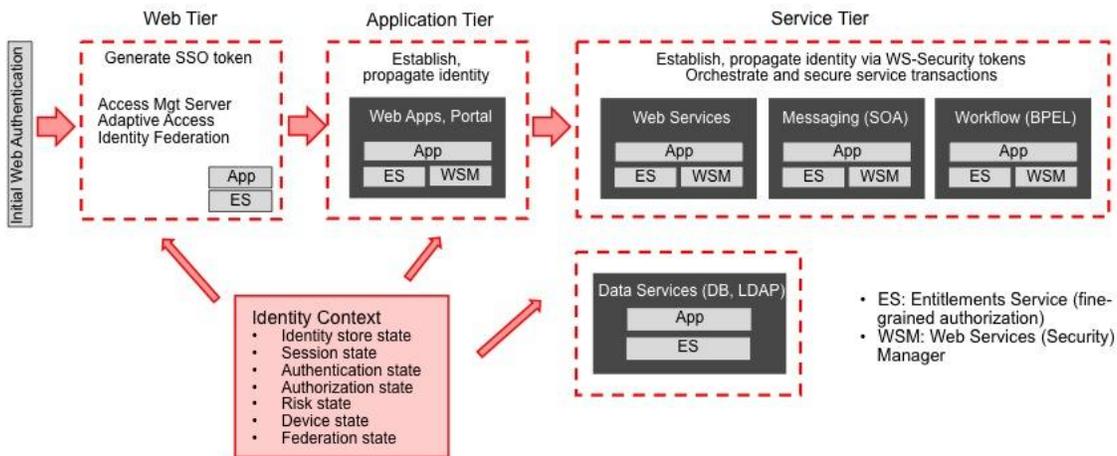


Figure 5: Identity Context Overview

The following typical examples illustrate how Identity Context data is used to ensure security throughout your environment.

- » Disable a particular business function if the user is not authenticated using a strong credential such as a smart card.
- » Secure access to a transaction based on the identity data supplied by a business partner (via Identity Federation) with whom the organization does business.
- » Request additional authentication credentials if the Identity Context detects that access is originating from a location known for fraudulent activities.
- » Limit the scope of administrative authority if the administrator's industry certification (as maintained by a third party) has expired.
- » Disable certain business functions if the Identity Context detects that access is originating from an unknown device.

### Dynamic Authentication

Dynamic authentication uses advanced rules to switch authentication schemes dynamically.

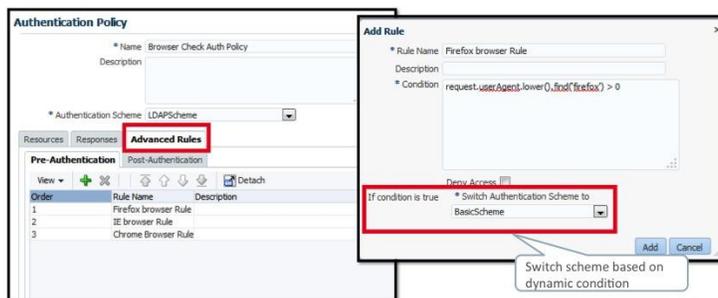


Figure 6: Dynamic Authentication

Advanced rules include pre- and post-authentication rules where a condition is specified based on request or user attributes. For example, a post-authentication rule can be used to step up authentication to require a one-time password (see next section).

## Context- and Content-Aware Authorization

Context- and content-aware authorization leverages Oracle Access Management's attribute-based fine-grained authorization service (Entitlements Server).

Entitlements Server is an externalized, fine-grained authorization service granting or denying access to a protected resource based on the authorization request context. Protected resources can be deployed on-premise or in the cloud. Entitlements Server enforces controls on multiple types of resources: software components (URLs, servlets, JSPs, EJBs) and business objects (e.g., patient records in a health care application) or anything used to define a business relationship. Entitlements Server provides the following business benefits:

- » Business agility: Security service infrastructure that closely fits with your business model and rapidly adapts to changing corporate or regulatory requirements without impacting the code of the applications you protect.
- » Enhanced security and compliance: The administrator manages fine-grained authorization from a single point of control across the enterprise, whether protected applications reside on-premise or in the cloud. Entitlements Server allows the separation of application security from the application's code, thus increasing IT efficiency and reducing development costs (administrators control the security environment, not developers).

Entitlements Server leverages existing identity management infrastructures and integrates seamlessly with Oracle Access Management's core services described earlier in this document. As any Oracle Access Management service, Entitlements Server (described in Figure 7) runs in Oracle WebLogic Server.

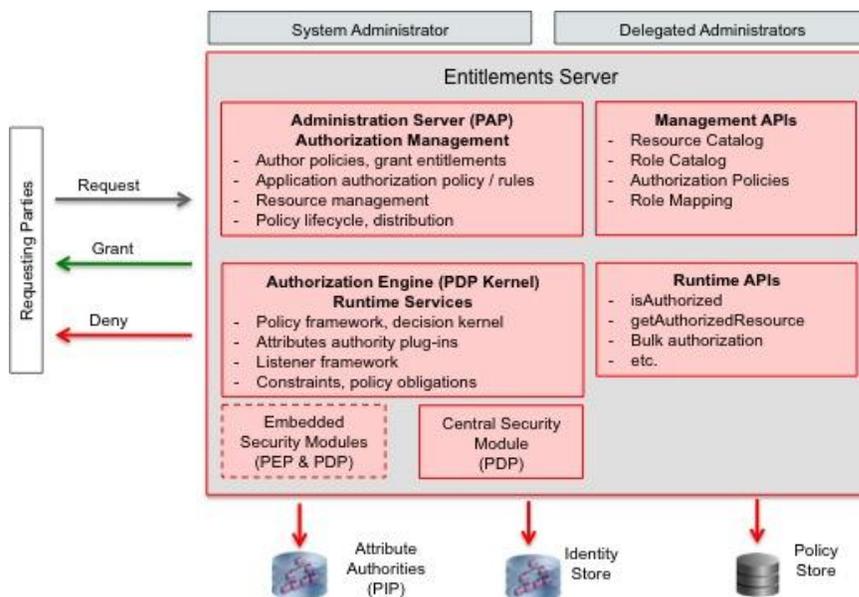


Figure 7: Fine-Grained Authorization Service (Entitlements Server)

Entitlements Server includes Security Modules (SMs) providing the policy enforcement point (PEP) and policy decision point (PDP) functionality. SM components can be invoked in several ways:

- » Java Security Module: A generic PDP that provides authorization decisions using the Java API. This SM type is supported in Java, Standard Edition (SE), IBM WebSphere, and RedHat JBoss environments.
- » Multi-Protocol Security Module: A PDP wrapped around a Java Security Module, providing authorization decisions using Extensible Access Control Markup Language (XACML).
- » WebLogic Server Security Module: A custom made Java Security Module that includes both a PDP and a PEP. This SM type can receive requests directly from WebLogic Server without the need for explicit authorization API calls.

As shown in Figure 8, Entitlements Server can be deployed flexibly: Centrally-controlled PDPs (SMs) or autonomous PDPs (local or remote), across multiple data centers supporting extreme scalability, high availability and failover.

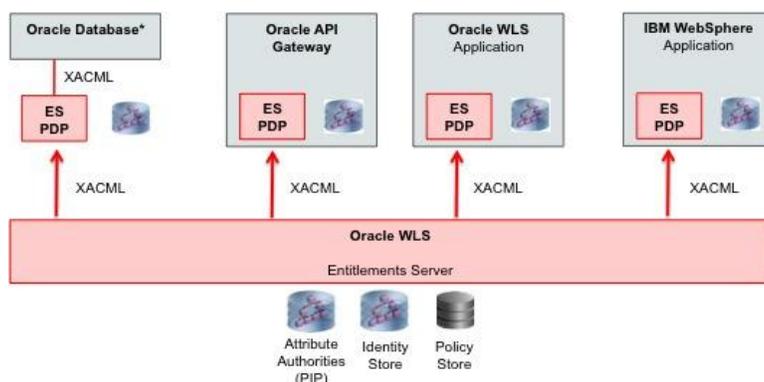


Figure 8: Entitlements Server Deployment

Entitlements Server provides intelligent access through context-aware and content-aware fine-grained authorization:

- » Context-Aware Authorization: Security policies need access to contextual identity information. For example, an application should disable a business function if the requester's device (e.g., a smart phone) can't be trusted; a web service request should be denied if the requester's risk score computed during log-in is too high; Database queries should be rewritten to not return sensitive or private information (e.g., social security #) if the requester's level of assurance established during authentication is below an acceptable limit.
- » Content-Aware Authorization: Security policies are based on the content of a protected resource, as shown in Figure 9. Entitlements Server provides seamless integration with document management systems such as Oracle WebCenter and Microsoft SharePoint.

Name	Sensitivity	Department
World Domination Strategy.ppt	Top Secret	Strategy, Development
Cost Analysis.xls	Secret	Accounting
Planning Assumptions.doc	Top Secret	Development
Progress Report.ppt	Top Secret	Strategy
Public Statement.ppt	Public	Marketing

Fine-Grained Access Policy:

```

Permit read access to documents
if document.sensitivity <= employee.clearance_level
and document.department = employee.department
and user.authenticationType = 'Multifactor'

```

Figure 9: Content-Aware Fine-Grained Authorization

## Adaptive Access and Fraud Prevention

Adaptive Access delivers risk-aware, context-driven access management. The Adaptive Access service is built on a scalable, fault-tolerant, multi-tier deployment architecture including the following components:

- » Adaptive Access Administration for managing the Adaptive Access Server.
- » Adaptive Access Server consisting of three layers: Presentation leveraging the strong authenticator functionality using the interfaces provided by the business layer to access its services; Business Logic containing the core application logic that implements the risk-analyzing engine; and Data Access connecting the environment to the supported relational database systems.

Adaptive Access supports the following functionality:

- » Real-time and batch risk 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.
- » Risk-based authentication methods including knowledge-based authentication (KBA) challenge infrastructure with server-generated one-time passwords (OTP).
- » Standard integration with Oracle Identity Management (Identity Governance and Access Management).
- » Leverages Access Management's core services and enhances its authentication methods.
- » Key support for mobile devices using Access Management's Mobile and Social service.

Adaptive Access includes the following features:

- » Auto learning: A mixture of real-time and predictive auto-learning technology is used to profile behavior and detect anomalies (recognize high risk activity and proactively take actions to prevent fraud and misuse). Auto-learning automates risk evaluations and keeps track of changing behaviors.
- » Configurable risk engine: Flexible architecture supporting three methods of risk evaluation that work concurrently to evaluate risk in real-time: configurable rules, real-time behavioral profiling, and predictive analysis.
- » Virtual authentication devices: Server-driven services (i.e., no client-side software or logic that can be compromised by key-loggers and other common malware – personalized images and phrases are known only to the server and the end user). The security of the user credentials during entry is ensured by not capturing or transmitting the actual credential of the end user (strong authentication). Virtual authentication devices include TextPad, a personalized device for entering a password or PIN using a regular keyboard (defends against phishing); PinPad, a lightweight authentication device for entering a numeric PIN; QuestionPad, a personalized device for entering answers to challenge questions using a regular keyboard; and KeyPad, a personalized graphics keyboard used to enter alphanumeric and special characters (passwords and other sensitive data such as credit card numbers).
- » Device fingerprinting: Designed to support desktops, laptops, mobile devices or other web-enabled devices, providing standard browser-based access and mobile browser-based access without additional client software. Adaptive Access device fingerprinting integrates with the Access Management Mobile and Social SDK and REST interface, and monitors multiple device attributes.
- » Knowledge-based authentication (KBA): Secondary authentication in the form of KBA questions presented after successful primary authentication. The KBA infrastructure handles registration, answers, and the challenge of questions. Adaptive Access Management's rules engine and organizational policies are responsible for determining if it is appropriate to use challenge questions to authenticate the customer.
- » Answer Logic: Increases the usability of KBA questions by accepting answers that are fundamentally correct but may contain a small typo, abbreviation, or misspelling.
- » OTP Anywhere: Risk-based challenge mechanism consisting of a server-generated one-time password (OTP) delivered to an end user via SMS, email, or instant messaging. The challenge processor framework supports

custom risk-based challenge solutions combining third-party authentication products with Adaptive Access real-time risk evaluations.

- » Mobile access security: Security policies available with Adaptive Access can dynamically adjust when user access originates from a mobile device. IP geo-location velocity rules behave differently if the access request is via a cellular connection or Wi-Fi. When used with Mobile and Social, Adaptive Access provides device fingerprinting, device registration, risk-based challenge mechanisms, and lost and stolen device.
- » Universal Risk Snapshot: Allows an administrator to instantly save a full copy of all Adaptive Access policies, dependent services, and configurations for backup, disaster recovery, and migration.
- » Fraud investigation: Forensic interface for security analysts and compliance officers allowing agents to save “case” information in a repository.
- » Adaptive policy management: Policies and rules are designed to handle patterns or practices, or specific activities. The administrator can define when rules should be executed, the criteria used to detect various scenarios, the group to evaluate, and the appropriate actions to take when suspicious activity is detected.

### Adaptive Authentication with Oracle Mobile Authenticator

Oracle Mobile Authenticator is a token-based authentication mobile app available for download from the Apple Store and Google Play. Oracle Mobile Authenticator enables organizations to cost-effectively provide strong authentication and prevent unauthorized access to vital company and customer data by generating a time-based security code or one-touch notification enabling soft-token authentication. As part of the Oracle Access Management platform, Oracle Mobile Authenticator leverages adaptive, dynamic authentication and strong authentication services.

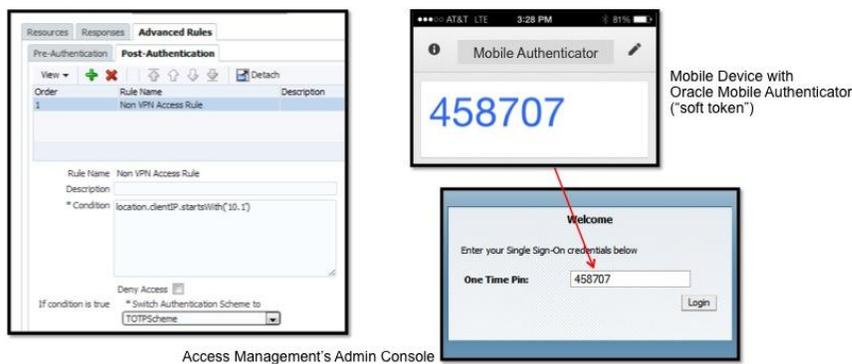


Figure 10: Oracle Mobile Authenticator

## Identity Federation

The Identity Federation service is an integral part of the Oracle Access Management platform, leveraging the authentication core services described earlier in this document, such as credential collectors and authentication plug-ins. Identity Federation services can protect both on-premise and cloud resources leveraging several industry standards:

- » SAML-based federation (authentication, attribute sharing)
- » OpenID-based federation (delegated authentication)
- » OAuth-based federation (delegated authorization)
- » Social-identity-based federation (redirected authentication)
- » Form-fill-based federation (Access Portal)

Identity Federation services are enabled from the central access management console, as shown in Figure 11.

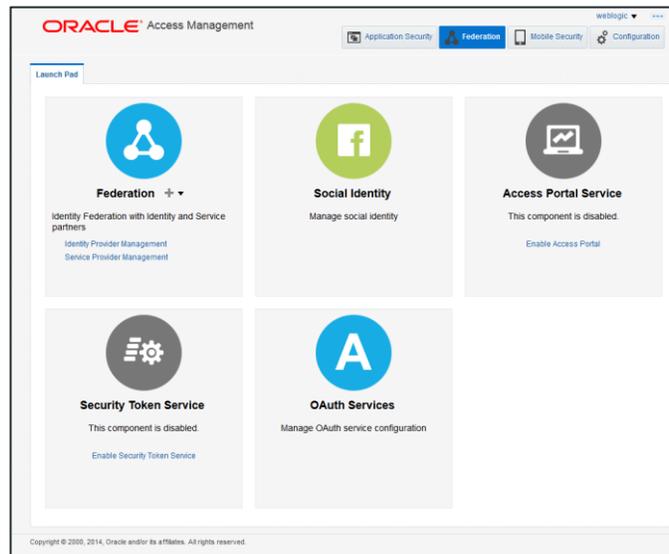


Figure 11: Oracle Access Management Identity Federation Services Launchpad

Identity Federation services are seamlessly weaved into the authentication and authorization process. Identity Federation leverages the Access Management platform's shared services.

### SAML-Based Federation

The Security Assertion Markup Language (SAML) is an open framework for sharing security information on the Internet through XML documents. SAML was originally designed to address the following requirements:

- » Limitations of web browser cookies to a single domain: SAML provides a standard way to transfer security information across multiple Internet domains (**Note:** Cross domain SSO can be supported by Oracle Access Management (without federation) if all domains leverage the same Access Management server – in all other cases, Access Management Identity Federation is required).
- » Proprietary web single sign-on (SSO): SAML provides a standard way to implement SSO within a single domain or across multiple domains.
- » Federation: SAML facilitates identity management (e.g., account linking when a single user is known to multiple web sites under different identities).
- » Web Services Security: SAML provides a standard security token (a SAML assertion) that can be used with standard web services security frameworks (e.g., WS-Security, WS-Trust, etc.).
- » Identity propagation: SAML provides a standard way to represent a security token that can be passed across the multiple steps of a business process or transaction.

Typically, SAML involves two parties:

- » Identity Provider (IdP): Asserting party that provides identity information to other services.
- » Service Provider (SP): Relying party that consumes the identity information sent by the asserting party to grant access to services hosted by the SP.

Oracle Access Management Identity Federation supports a large set of use-case scenarios:

- » Known name or attribute: Email address, X.509 Subject Name, Windows Domain Qualified Name, Kerberos Principal name, Attribute (e.g., employee number).
- » Opaque identifier: The principal is identified by a persistent randomized string private to the identity provider and service provider pairs.
- » Anonymous user: The principal is never explicitly identified by a persistent identifier, i.e., there's no need to maintain a user (principal) entry at the service provider.
- » Attribute Sharing: Identity Federation's attribute-sharing plug-in allows Oracle Access Management to request user attributes from an identity provider.
- » Identity Provider Proxy: This use case involves three parties: Original Service Provider; Proxying Identity Provider (Oracle Access Management Federation acting as Identity Provider and becoming a Service Provider); and Proxied Identity Provider (Oracle Access Management services that authenticate the user).

### Oracle Access Management Fedlet

Fedlet provides a standalone, light-weight SAML 2.0-compliant component for a Service Provider (SP) interacting with Access Management Identity Federation or a third-party SAML Identity Provider (IdP). Fedlet can be embedded and integrated with an application at development time. Fedlet can be deployed on premise or in the cloud supporting multiple environments:

- » Java version deployable as a Web Archive (WAR) on Oracle WebLogic Server and other market-leading Java EE containers.
- » .NET version designed to support asp.net applications, deployable to Microsoft IIS (DLL) .

Additionally, Fedlet can be deployed in conjunction with an IdP Discovery Service allowing users to select a preferred IdP.

### OpenID-Based Delegated Authentication

OpenID is a delegated authentication standard that any web site can leverage without having to develop its own authentication system. As a user, the OpenID standard allows you to log in to multiple OpenID-enabled sites with a single OpenID token. Identity data is communicated through the exchange of an OpenID identifier (a URL or XRI chosen by the end-user) and the Identity Provider provides OpenID authentication. Oracle Access Management Identity Federation support the following functionality:

- » OpenID 2.0 Authentication and SSO: An OpenID token contains the NameID of the user and (optional) attributes, outgoing tokens (or "assertions") are signed.
- » OpenID 2.0 NameID Format: OpenID defines the NameID as being a random string. Identity Federation uses one of the following as the value for the NameID: A hashed user attribute (such as DN); a generated random value stored in the Federation Data Store (requires the use of a Federation Data Store).

### OAuth Delegated Authorization

OAuth (Open Authorization) is an industry standard designed to support delegated authorization. Before OAuth, if a third-party (e.g., a money manager) wanted to access your account, you'd have to share your credentials with them, thus compromising your environment. OAuth was originally designed to allow a User (Resource Owner) to transparently share his private data stored on one site (Service Provider, or Resource Server) with another site (Consumer, or Client). With the advent of OAuth 2.0, the original consumer-centric delegated authorization use case extends to the enterprise and the cloud. OAuth 2.0 enables a third-party application to obtain access on its own behalf (two-legged process) or obtain limited access to an HTTP service on behalf of a Resource Owner by orchestrating an approval interaction between the Resource Owner and the HTTP Service Provider (three-legged process). Although focusing on mobile clients, OAuth was originally intended for web applications that need access to resources owned by private users.

## Oracle Access Management's Support for OAuth

OAuth is supported by multiple Oracle Access Management services:

- » Oracle Access Management Identity Federation (license for web clients only (i.e., non-mobile)).
- » Oracle Access Management Mobile and Social (license for both web clients and mobile clients).
- » Oracle API Gateway (typically, OAG acts as the resource server while the Oracle Access Management OAuth service acts as the authorization server; an OAG filter validates the Access Management OAuth token before allowing access to the resource).
- » Web Services Manager (future release): OAuth client-side support and integration with Oracle Access Management OAuth service for obtaining an access token, propagating it to a WSM-protected resource, and verifying the access token on the service side.

### Identity Federation OAuth Service

The Identity Federation OAuth service extends the Access Management server (both administration and runtime) to provide *Token Issuance*, *Token Validation*, *Token Revocation* and *User Flows* in accordance with the OAuth 2.0 standard. The OAuth service increases security by eliminating the use of end-user passwords in many service-to-service interactions and reduces administrative costs by centralizing trust policies and associations in a large deployment. The standard OAuth Service is implicitly enabled if the Oracle Access Management Identity Federation service is enabled, To also enable Mobile OAuth, the Mobile and Social service (described later in this document) must be enabled, in addition to the Identity Federation service.

### Oracle Access Management Cloud Federation

- » Microsoft Office 365 SAML 2.0 federation: Oracle Access Management Identity Federation is the Identity Provider, MS Office 365 is the Service Provider
- » WS-Federation Passive Requester Profile: Cross-domain Web SSO (HTTP Redirect, HTTP Post), local log out supported (i.e., log out is not broadcast to all WS-Federation endpoints in the circle of trust).
- » Web Services and APIs Security: Support for federation and delegated authorization with Salesforce, Google, Amazon AWS, SQS.

## Mobile Security

Oracle provides a full, integrated mobile security solution to support both employee and consumer use-case scenarios.

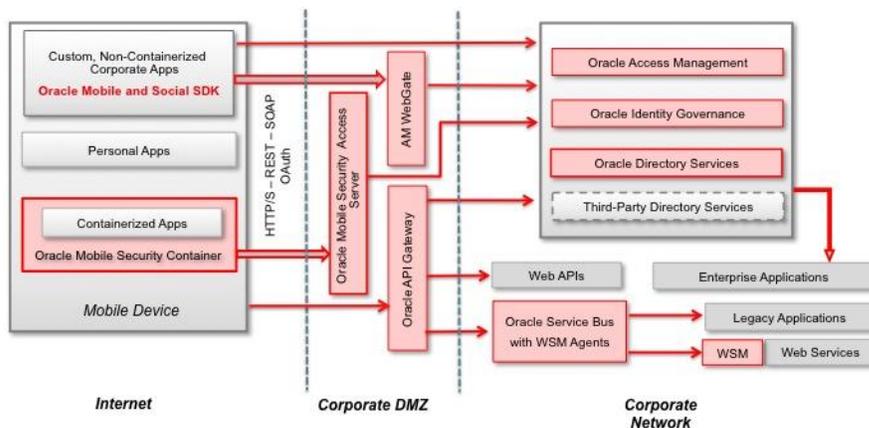


Figure 12: Oracle Mobile Security Overview

Three services are involved:

- » Oracle Mobile Security Suite: A BYOD, employee-centric mobile security suite that separates personal apps from secure, “containerized” corporate, “off-the-shelf” apps and data, avoiding device lock-down. Containerized apps are Oracle and/or third-party enterprise applications accessed by employees through the corporate network (intranet). Oracle Mobile Security Suite is described in a dedicated Oracle Mobile Security Suite white paper.
- » Oracle Access Management Mobile and Social: A consumer-centric service part of the Access Management platform that provides a software development kit (SDK) allowing corporate developers to secure custom enterprise apps for Apple’s iOS and Google’s Android devices, bridging the gap between mobile devices, social networks, and the enterprise’s backend identity management infrastructure.
- » Oracle API Gateway, intercepting mobile requests in the DMZ and supporting protocol and data format transformations.

### Oracle Access Management Mobile and Social Service

As an integral part of the Oracle Access Management platform, the Mobile and Social service leverages multiple platform components, including:

- » Access Management’s core services for web application authentication, authorization, and single sign-on.
- » Adaptive Access for mobile device fingerprinting and registration, risk-based authentication factoring in the mobile device context, and fraud detection.
- » Oracle API Gateway (OAG) for first line of defense supporting multi-protocol and multi-format web services and web application programming interfaces (APIs), security gateway to cloud services, data redaction (in conjunction with the attribute-based entitlements server), identity propagation, and access to legacy applications. OAG is described in detail in a later section.
- » Entitlements Server for fine-grained, attribute-based authorization policies and access to mobile apps based on the mobile device context.
- » Oracle Directory Services for direct access of mobile applications to LDAP-based user directories.

Mobile and Social enables enterprises to securely leverage social identities as some websites may require users to provide access tokens obtained from Facebook or Google in order to be authenticated to their services relying on more lightweight security standards than enterprise identities but are better adapted to the requirements of social networks.

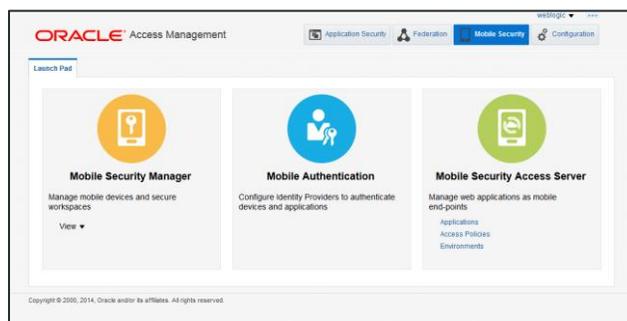


Figure 13: Oracle Access Management Mobile and Social Services Launchpad

Oracle Mobile and Social includes the following functionality:

- » Delegated authorization leveraging the OAuth 2.0 standard.

- » Mobile Services connecting browser-based (HTML5) and native mobile apps to the enterprise identity management infrastructure, typically the Oracle Access Management platform.
- » Internet Identity Services providing functionality that allows Mobile and Social to be used as the relying party when interacting with popular, cloud-based identity services, such as Google, Facebook, Twitter, or LinkedIn
- » By deploying Oracle Mobile and Social, you provide the user with multiple log-in options without the need to implement access functionality for each identity provider individually.
- » User Profile Services providing a REST interface for LDAP CRUD operations, user self-service functions such as self-registration, profile maintenance, password management, and account deletion (User Profile Services are also available as an OAuth resource).
- » Access Management Integration Services for leveraging Oracle Access Management through a runtime REST interface provided by an agent software development kit (SDK).

### Mobile and Social Service Support for OAuth

Oracle Mobile and Social leverages the Oracle Access Management platform's OAuth 2.0 service described earlier in this document. Oracle Access Management Mobile and Social provides enhanced security support when the OAuth client resides on a mobile device. This enhanced security support is in addition to the baseline security measures defined in the OAuth 2.0 specification.

On a mobile device, the OAuth client must obtain a client verification code before the authorization endpoint on the Access Management server interacts with the mobile app. The Mobile and Social server component can restrict token delivery to a specific app installed on a specific device by sending part of a token through HTTPS, and sending the other part through push notification using either the Apple Push Notification Service (APNS) or Google Cloud Messaging (GCM). Mobile OAuth single sign-on allows multiple mobile apps on a device to share the same user session, which securely resides on the server, not the client.

The user has an option to give his authorization to register each mobile OAuth app installation instance on a mobile device. Upon registration, the app is issued a client assertion token. The mobile client submits the client assertion token as an input parameter to use all of the OAuth access service endpoints. Upon mobile client registration, the client performs the OAuth access service interaction to obtain the access token used to access protected resources. The mobile devices and apps are checked against fraud using the Adaptive Access (fraud detection) service of the Oracle Access Management platform.

### Mobile and Social Client SDK

The Mobile and Social service provides client libraries that allow developers to add feature-rich authentication, authorization, and identity capabilities to registered mobile apps. On the backend, the Mobile and Social server's pluggable architecture lets system administrators add, modify, and remove identity and access management services without having to update software installed by the user. The Mobile and Social service provides separate client software development kits (SDKs) for Apple's iOS, Google's Android, and generic Java for desktop applications. These client SDKs are designed to build identity security features into your mobile apps and enable you to use your existing identity infrastructure for authentication, authorization, and directory-access services.

## ORACLE MOBILE AND SOCIAL USE-CASE SCENARIOS

Components Involved	Use Case Description
<ul style="list-style-type: none"> <li>» <i>Access Management Core Services</i></li> <li>» <i>Mobile and Social</i></li> </ul>	<p><b>Authentication</b></p> <p>Mobile and Social supports multiple types of resources by offering two token types to secure the path between mobile apps and resources: Access Management tokens (HTTP cookies) and JSON Web Tokens (JWT).</p>



	<ul style="list-style-type: none"> <li>» <i>The Mobile and Social client SDK handles authentication programmatically after the SDK collects user credentials.</i></li> <li>» <i>The SDK then uses the Mobile and Social REST interfaces to authenticate the user with the token service configured for the app.</i></li> <li>» <i>Access Management-generated tokens are delivered as JSON payload by the Mobile and Social service.</i></li> <li>» <i>When presented to an Access Management interceptor (WebGate) by a mobile app, these tokens are validated by the Access Management policy server, and they allow access to any type of resource protected by Access Management without the AM interceptor requesting a browser redirection for authentication.</i></li> </ul>
<ul style="list-style-type: none"> <li>» <i>Access Management Core Services</i></li> <li>» <i>Adaptive Access</i></li> <li>» <i>Mobile and Social</i></li> </ul>	<p><b>Strong and Step-up Authentication</b></p> <p>Mobile and Social enforces new layers of authentication by requiring both device and app registration. Each app communicating with Mobile and Social downloads configuration parameters and obtains an app registration handle that is required for all subsequent requests from that app. When SSO is configured, the app registration for SSO serves as a device registration, and that device registration handle is required for all subsequent requests. Device registration is also subject to the policies and risk assessments available from the Adaptive Access service. These policies can trigger step-up challenges such as knowledge-based authentication (KBA) or one-time passwords (OTP).</p> <ul style="list-style-type: none"> <li>» <i>Adaptive Access policies can be implemented for first-time access, so new device registrations require KBA, or more sensitive applications can require OTP.</i></li> <li>» <i>Policies can also be defined for specific users, allowing users with lower levels of access in with a username and password, but requiring an OTP for users with more privileged access (step-up authentication).</i></li> <li>» <i>Devices can be required to be pre-registered in the Adaptive Access service before their applications can authenticate or obtain tokens.</i></li> </ul>
<ul style="list-style-type: none"> <li>» <i>Access Management Core Services</i></li> <li>» <i>Adaptive Access</i></li> <li>» <i>Mobile and Social</i></li> </ul>	<p><b>Device Loss or Theft</b></p> <p>Smart phone loss and theft create a high security risk for users and companies, particularly when these devices are used to access corporate resources. Mobile and Social working in conjunction with Adaptive Access addresses this risk by providing a way to mark a device lost or stolen, and then implement specific policies that are enforced when a stolen device tries to access enterprise applications.</p> <p>Since device Identity Context data is delivered to the Adaptive Access service each time a device attempts to communicate with Mobile and Social, Adaptive Access has the ability to challenge a user if the device has been reported lost, or deny any access from a device if the device has been reported stolen.</p>
<ul style="list-style-type: none"> <li>» <i>Mobile and Social</i></li> <li>» <i>Oracle API Gateway</i></li> </ul>	<p><b>Web Services and Web APIs Security</b></p> <p>Mobile apps typically access corporate information through lightweight REST-based APIs as mobile devices lack support for more involved applications, web services, and SOA-based infrastructures using the SOAP, Java Message Service (JMS), Message Queue (MQ), or even File Transfer Protocol (FTP) technologies that existing corporate systems often rely on. With Oracle API Gateway (OAG), organizations can expose internal systems and corporate data as fully secure REST-based APIs (using JSON payloads) without the need for any coding; this is achieved by virtualizing the existing backend SOAP or JMS services as REST APIs through OAG. Existing transport protocols and security tokens required for authentication, identity propagation, and user claims (attribute assertions) can also be automatically transformed to address mobile requirements without changing existing backend systems. For example, an organization may only want to accept REST-based JWT tokens issued by the Oracle Access Management platform; once authenticated the tokens can be converted to SAML or any other type of token required by the SOAP-based backend systems.</p>
<ul style="list-style-type: none"> <li>» <i>Mobile and Social</i></li> <li>» <i>Directory Services</i></li> </ul>	<p><b>Exposing Directory Data Through User Profile Services</b></p> <p>LDAP directory services are used for many functions, including user self-service, company white pages, or help-desk user account maintenance. Mobile and Social makes directory services available to mobile devices, without a need for building LDAP clients (you still need a mobile client app such as a white-list app).</p> <p>Mobile and Social provides REST interfaces to Oracle Directory Services as well as third-party directory services such as Microsoft Active Directory. Mobile and Social's User Profile</p>

	Services gives users and administrators access to configured directories for many common functions, and provides additional outward-facing security layered on the directory's own security.
<ul style="list-style-type: none"> <li>» <i>Mobile and Social</i></li> <li>» <i>Access Management Core Services</i></li> </ul>	<p><b>Mobile and Social Services Complementarity</b></p> <ul style="list-style-type: none"> <li>» <i>Use Social Identity services to let users authenticate with Google, Facebook, or Twitter.</i></li> <li>» <i>Use Mobile services to provide local authentication functionality, or generate a user token by accepting a user identity assertion from a social identity provider.</i></li> </ul>

## API and Web Services Security

Web Application Programming Interfaces (APIs) are designed for developers to access third-party public applications programmatically to integrate a company's offering (e.g., Google maps) with their own business website (e.g., a dentist office). Because they are accessed by multiple kinds of clients (e.g., portable devices), APIs leverage REST as a lightweight infrastructure (a REST API is a method of allowing communication between a web-based client and an HTTP server that uses REST constraints).

Web services are self-contained applications that process client requests directly or front-end legacy applications. Web services are secured through various protocols: XML/SOAP leveraging WS-Security standards and tokens such as SAML assertions, and RESTful environments and light-weight security protocols such as OAuth.

API and web services security is supported by several Oracle Access Management components: Oracle API Gateway; Oracle Web Services Manager; and Oracle Secure Token Service, as shown in Figure 14.

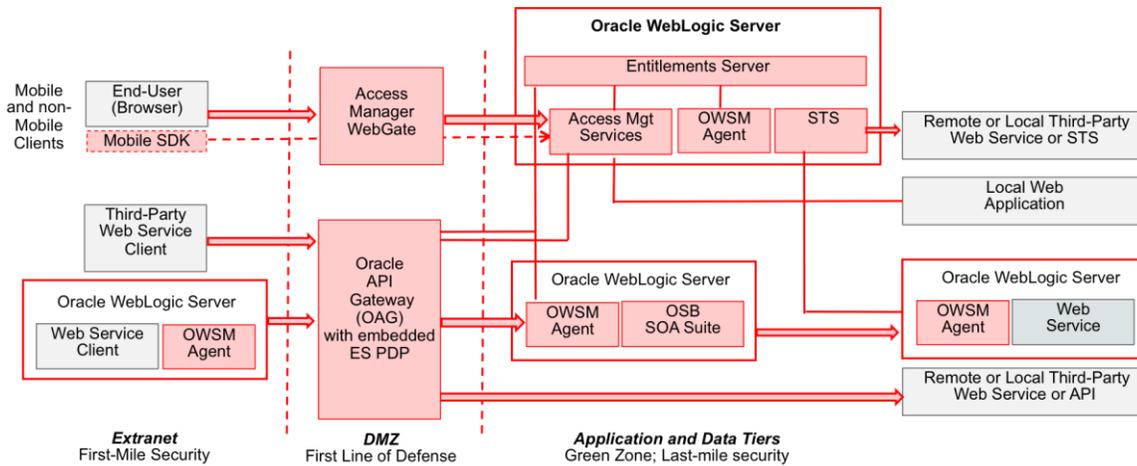


Figure 14: Oracle Layered Security Overview

### Oracle API Gateway

Oracle API Gateway (OAG) secures access to web APIs and web services deployed on premise or in the cloud. OAG detects and prevents message-level threats for REST API traffic:

- » Scan HTTP headers, HTTP QueryString parameters, and HTTP POST data.
- » Enable selective restriction of HTTP methods to detect and block inappropriate usage.
- » Scan payloads and attachments for harmful content, virus, and JSON/XML schema validation.

- » Integrate with virus detection software to detect and prevent common REST APIs security exploits.

OAG extends Access Management to REST API leveraging context-aware authentication, content-aware authorization, security tokens, data redaction, and audit services. OAG also extends access to web services and APIs from mobile devices (tablets or smartphones). OAG provides simplified deployment of the gateway in cloud environments such as Oracle Cloud or Amazon Web Services Cloud computing platform. In addition to API and web services security, OAG provides XML firewalling, data format transformations (XML to JSON and vice-versa) and protocol bridging (REST, SOAP, JMS).

OAG integrates with multiple environments to provide a complete, end-to-end solution: Oracle Access Management core services and Web Services Manager, and third-party identity and access management infrastructures. OAG can be deployed on premise and access APIs hosted in the cloud or it can be deployed in the cloud on Oracle or third-party Cloud services.

### Oracle Web Services Manager (WSM)

WSM provides a policy-driven, standards-based web services security framework for Oracle Fusion Middleware and Oracle Fusion Applications. WSM is part of Oracle Fusion Middleware's "lower" stack, i.e., infrastructure (the "upper" stack includes application pillars such as Oracle Access Management).

WSM includes a Policy Manager, a stateless component deployed on at least one node in the domain (managed server) which reads and writes predefined and custom security policies from the WSM repository, and WSM Agents (client- and server-side) natively available on every Fusion Middleware managed server. WSM agents provide a policy enforcement point (PEP) via the policy interceptor pipeline and they cache information from the Policy Manager. When a protected web service is accessed by a client application, the WSM agent queries the policy cache and enforces the applicable policies. Based on the policies, the request is authenticated, encrypted, decrypted, authorized or logged (the agent does not need to connect to the Policy Manager for any of these operations). Runtime availability of the Policy Manager does not affect the functioning of the WSM agents.

WSM presents the following benefits:

- » Visibility, control, governance: Centralized management with a single unified console (Enterprise Manager) for administering, monitoring, and auditing web services security throughout the Oracle stack.
- » Open, extensible, integrated: Interoperability with third-party environments (e.g., Security Token Service) based on industry standards; Extensible to support custom policies; Integrated with multiple Oracle components as part of the Oracle Layered SOA Security strategy.
- » Service security enabler for Oracle Fusion Applications SaaS offering; Oracle Java Cloud Service; Oracle Application Development Framework (ADF); and Oracle Service Bus (OSB) PaaS offering.

WSM leverages Entitlements Server to support attribute-based authorization. WSM applies attribute-based authorization to SOAP-based web services. The Entitlements Server authorization policy provides a grant or deny decision for a subject to perform a certain action on a given resource, based on context attributes, e.g., information from the SOAP request message extracted using XPath statements, or HTTP headers. Entitlements Server helps mask (with characters of your choice) certain information in the response following a web service request.

### Security Token Service

Security Token Service (STS) is an integral part of the Oracle Access Management platform. STS brokers trust between a Web Service Consumer (WSC) and a Web Service Provider (WSP) and provides security token lifecycle management services to both. STS enables the creation of a consistent and streamlined model for security token acquisition, validation, cancellation, and renewal implementing the WS-Trust specification.

### STS-OAG Interoperability: Token Translation and Identity Propagation

In this case, OAG acts as a WS-Trust client to Access Management STS (or any other third-party STS).

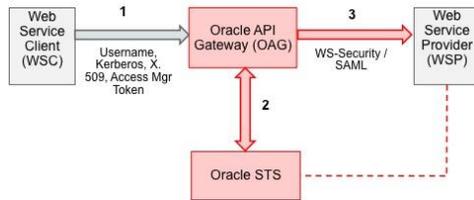


Figure 15: STS-OAG Interoperability

All communication between OAG and STS are based on WS-Trust. A trust relationship between OAG and the web service provider is brokered by STS to facilitate identity propagation from the client side to a web service endpoint. The web service endpoint (WSP) can additionally be protected by a WSM agent (last-mile security).

### STS-Core Services-OWSM Interoperability: Web App to Web Service Identity Propagation

In this case, the user's identity needs to be propagated from a web application protected by Oracle Access Management to a web service provider protected by WSM (or a WS-Trust-compliant third-party agent).

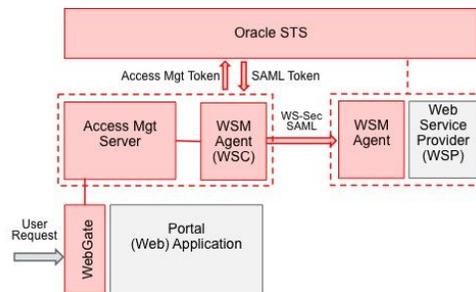


Figure 16: STS-Access Management-WSM Interoperability

The user logs onto the portal application (username / password) and clicks on a procurement application to make a purchase via web services (the web service provider may or may not reside in the same domain). STS is used to exchange the Access Management token for a SAML assertion. WSM is used to propagate the user's identity between the portal and the web service provider.

## Cloud Security

Cloud computing enables companies to purchase software and IT resources as a service. Users are able to access their business applications at any time and from multiple locations, track their usage levels, and scale capacity as needed without large up-front costs. Identity management, access control, and cross-enterprise security are at the core of Oracle's broader cloud offerings.



Figure 17: Cloud Security Deployment Options

Oracle recognizes that customers are not going to migrate their environments to the cloud in one fell swoop. Most enterprise customers proceed at their own pace to meet their specific requirements and priorities. As shown in Figure 17, Oracle supports three access control and identity management options: Cloud Ready, Managed Cloud, and Public Cloud.

- » Cloud-Ready Identity Services: On-premise or private cloud including Identity Governance, Access Management, Mobile Security, Directory Services.
- » Managed Identity Services: Pre-configured, Oracle-managed Identity-as-a-Service (MIDaaS) including distinct offerings for full enterprise Identity Governance and Access Management functionality (powered by Oracle Identity Management 11gR2). This deployment option enables organizations to leverage their Oracle investments to extend into the cloud and transform their business processes while letting Oracle run Oracle.
- » Public Cloud Identity Services: Identity-as-a-Service (IDaaS) hosted in the Oracle cloud, designed to extend enterprise controls by automating SaaS account provisioning and de-provisioning, simplify the user experience to access SaaS applications (SSO), provide seamless integration with enterprise identity stores and authentication services, and facilitate compliance activities by clearly reporting on SaaS application usage.

### Cloud Access Portal

Cloud Access Portal is a mobile and cloud solution part of the Oracle Access Management platform designed to address the following customer challenges:

- » Simplify the user experience to access corporate web and cloud resources.
- » Adapt to different PC and mobile form factors.
- » Enable integration with existing corporate portals.
- » Provide wizard-driven tools to accommodate integration with SaaS, partner, and cloud applications.

Access Portal is designed for on-premise deployment to build a private SSO portal, providing a singular, secure way for users to access enterprise applications from any device supporting a browser (PC, Mac, Linux workstation, tablet, and smartphone). Access Portal supports intranet and extranet applications and seamless access to SaaS, partner, and Oracle Access Management protected applications. Access Portal leverages multiple Single Sign-On methods depending on the application type:

- » Applications with login forms (no federation): Oracle's form-fill technology enabled via the Oracle Traffic Director (OTD) gateway (OTD's admin interface defines routes to web servers and configures rewrite policies if required).
- » Federation-enabled applications: Identity-Provider-initiated links via Access Management Identity Federation.
- » Corporate web resources protected by Access Management: SSO via Oracle Access Management policy and session identifiers.

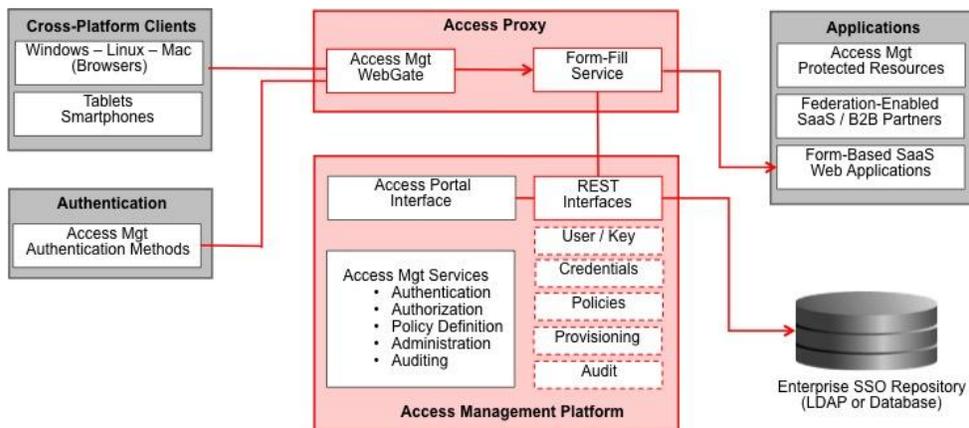


Figure 18: Cloud Access Portal Overview

As an integral part of the Oracle Access Management platform, Access Portal provides the following functionality:

- » Add end-user credential management services to the Access Management platform (Web Logon Manager - WLM).
- » Provide full integration of REST services and APIs for wallet and application / policy CRUD with Access Management's administration and managed servers.
- » Enable native notion of apps, app catalog, dashboard, and wallet.
- » Support Access Management authentication tokens allowing users to access their credential management services.
- » Provide key foundation for stronger integration with Access Management core services such as Adaptive Access as well as Privileged Access Management.
- » Provide a foundation for migrating Enterprise SSO's administration into the Access Management administration console (Enterprise SSO is described later in this document).
- » Provide a foundation for authorized service access to credential management services on behalf of a user.

Access Portal extends traditional, rich-client-based Enterprise SSO beyond the Microsoft Windows desktop:

- » Web, mobile, Windows and non-Windows desktops, customizations.
- » Web-based UI for end users to manage and access their credentials and applications (Enterprise SSO Web Logon Manager).
- » Support for web applications without having to install a client component (access proxy, which can be viewed as "Enterprise SSO for web apps").
- » Ensure compatibility and coexistence with existing Enterprise SSO deployments (data stores, policies) allowing for simplified migration and adoption without compromising forward flexibility.

## Enterprise Single Sign-On

Enterprise Single Sign-On (SSO) provides a suite of desktop-based components to handle all tasks related to granting users access to enterprise applications: automatic sign-on, application password change, Windows password reset, kiosk session management, application credentials provisioning, as well as strong authentication inside and outside of the session. Enterprise SSO uses any LDAP directory, Microsoft Active Directory, or any SQL database server as its user profile and credentials repository and seamlessly integrates with Oracle Identity Management for common security policy enforcement and compliance reporting across applications.

The Enterprise SSO Suite includes the following functionality:

- » Logon Manager (ESSO-LM): Authentication and single sign-on.
- » Password Reset (ESSO-PR): Self-service Windows password-reset and Windows account unlock.
- » Provisioning Gateway (ESSO-PG): Remotely provisions application credentials for ESSO-LM users via external identity management systems such as Oracle Identity Manager and provides session and application management for kiosk environments.
- » Kiosk Manager (ESSO-KM): Adds user-level granularity for session and application sign-on and state in "kiosk" environments (e.g., hospitals where a single workstation is shared by multiple users).
- » Universal Authentication Manager (ESSO-UAM): Strong-authentication solution that replaces the standard Windows logon mechanism with a SmartCard, proximity card, token, or a biometric logon method.
- » ESSO Anywhere: Provides a way to deploy ESSO-LM and ESSO-PG to end users without administrator intervention.
- » ESSO Reporting: Captures event data and stores them to a remote database.

The close integration of Enterprise SSO with the Access Management platform's core services provides organizations with the ability to implement a single SSO session no matter what type of application is being accessed, thus increasing cross-enterprise security and compliance. The Oracle Access Management platform can leverage the strong authentication support of Enterprise SSO for a web SSO session. After a successful authentication to Enterprise SSO, the Enterprise SSO agent obtains an Access Management cookie and automatically injects it into the user's web browser to grant the user seamless access to Access Management-protected applications. Upon expiration of the Enterprise SSO session, the cookie is removed from the browser thus ending the Access Management session as well.

Enterprise SSO and the Cloud Access Portal (described earlier in this document) are complementary solutions. Access Portal uses secure REST interfaces to access Enterprise SSO application and configuration stores and proxy technology to replace the traditional ESSO-LM client mentioned earlier (a customizable user interface interacts with the REST interfaces and acts as a cross-platform presentation layer to Enterprise SSO application configurations and credential stores).

## Scalability and High Availability

Oracle Access Management is architected to provide Internet-level performance, scalability, and high availability. 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 3,000 to 5,250.

High Availability (HA) refers to the system or components ability to continuously operate for long periods of time, even in the event of a system or component failure. 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 Access Management supports the full range of HA strategies:

- » Active – Active, Passive – Passive or Active – Hot Standby
- » Seamless SSO and global log-out
- » Master-Clone configuration for clusters across data centers
- » Test-to-production (T2P) process for initial set up and automated replication for ongoing synchronization
- » Behavior is configurable based on session adoption policy

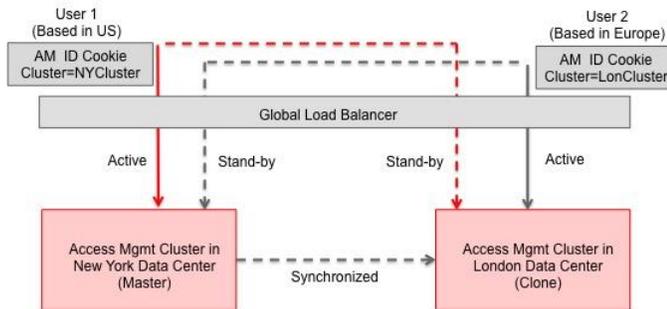


Figure 19: Oracle Access Management High Availability

## Conclusion

Oracle Access Management represents a major milestone in Access Management technology that is unique in the industry. 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 across multiple data centers.
- » 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.



**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](http://blogs.oracle.com/oracle)
- [facebook.com/oracle](https://facebook.com/oracle)
- [twitter.com/oracle](https://twitter.com/oracle)
- [oracle.com](http://oracle.com)

### Hardware and Software, Engineered to Work Together

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0515

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