ORACLE DATA SHEET

Oracle Access Management

ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

Oracle Access Management is 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.

KEY FEATURES

Cores Services

- Multiple authentication schemes
- Web single sign-on (SSO)
- Session management life cycle
- Coarse-grained authorization

Intelligent Access Management

- Context-aware (device context, geo-location, session context, transaction context)
- Content-aware (leveraging content classification)
- Risk-aware (real-time risk assessment based on context and policies)
- Context, content, and risk driven, dynamic, step-up authentication and fine-grained authorization

Adaptive Access

- Device fingerprinting
- Predictive auto-learning
- Knowledge-based authentication (KBA)
- One-time password (OTP) using SMS, email, or Oracle Mobile Authenticator (a soft token OTP mobile app)

Fraud Detection and Investigation

- Real-time and batch analysis (heuristic behavior analysis)
- Universal risk snapshot

Identity Federation

Introduction

Oracle Access Management is part of the Oracle Fusion Middleware Identity Management pillar. Oracle Access Management provides innovative, fully integrated new services that complement traditional access management capabilities by extending security from enterprise to mobile to cloud. For example, adaptive authentication, federated single sign-on (SSO), risk analysis, and fine-grained authorization are all extended to mobile clients and mobile applications, and Access Portal allows customers to build their own cloud SSO service.

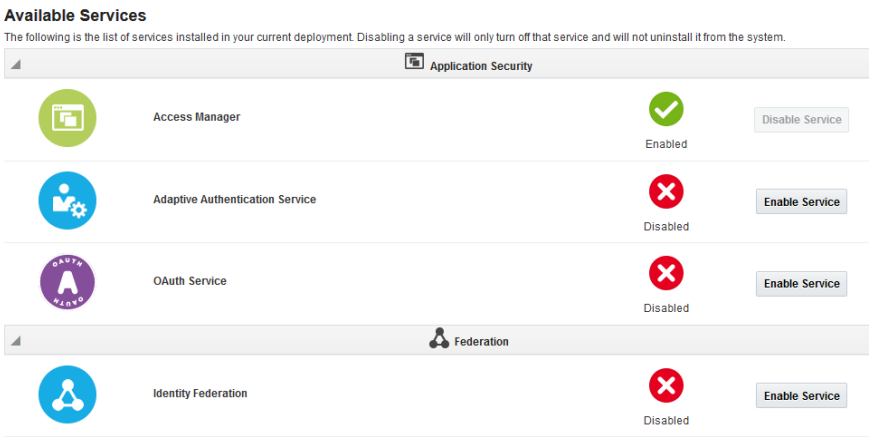

Figure 1: Oracle Access Management Launching Pad

Oracle Access Management is designed to meet the needs of your organization in typical use-case scenarios involving the cloud (allowing both on-premise and cloud resources to be secured from a single set of controls), mobile access (native or browser-based apps), employee-facing intranet, and customer-facing extranet.

Oracle Access Management provides the following functionality, licensed and enabled as required:

- Support for SAML 2.0, OpenID 2.0, OAuth 2.0
- Integration with Identity Cloud Service(IDCS)

Mobile Security

- Client-side SDK for authentication, SSO, and delegated authorization (OAuth)
- Support for Adaptive Access features

API and Web Services Security

- Authentication, authorization
- Data format (XML, JSON) and transfer protocol translation
- XML firewalling and throttling

KEY BENEFITS

- Scalability (support for up to 250 million user accounts).
- High availability with active-active multiple data center support.
- Dynamic, proactive security posture, avoiding the common pitfalls of reactive, static security systems.

RELATED PRODUCTS

- *Oracle Directory Services*: All-in-one directory solution with storage, proxy, synchronization, and virtualization capabilities.
- *Oracle Identity Governance*: User administration (provisioning), privileged account management, identity intelligence and analytics.
- ***Oracle Identity Cloud Service***: Cloud native, comprehensive, next - generation security and identity management platform. https://www.oracle.com/cloud/paas/identity-cloud-service.html

STATEMENT OF DIRECTION

- Oracle Privileged Account Manager Doc ID 2306738.1
- Oracle Enterprise Single Sign-On Suite Plus Doc ID 2308888.1
- Oracle Adaptive Access Manager Doc ID 2305294.1

- **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.
- **Adaptive Access and Risk Analysis**: Strong, multi-factor authentication and heuristic fraud detection service. Oracle Mobile Authenticator provides a soft-token OTP solution with one-touch notification services.
- **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.
- **Password Management**: Reset and Forgot password capability with second factor authentication methods. Support for Multiple password policies.
- **Integration with Identity Cloud Service (IDCS)**. Single Sign On between apps protected by IDCS and OAM using Federation.

CONTACT US

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

CONNECT WITH US


blogs.oracle.com/oracle


facebook.com/oracle


twitter.com/oracle


oracle.com

Hardware and Software, Engineered to Work Together


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