ORACLE MOBILE AND SOCIAL ACCESS MANAGEMENT

Oracle Mobile and Social Access Management is designed to secure mobile access to applications leveraging the enterprise's existing back-end identity management infrastructure.

KEY FEATURES

- Authenticating mobile users
- Authorizing mobile users
- Mobile single sign-on
- Device fingerprinting and registration
- Device blacklist/whitelist
- Device-context based fine-grained authorization
- Log on using Social Identity from Facebook, Google, Twitter, LinkedIn or Yahoo
- REST-based directory interface for User Profile Services
- Mobile and Social Client SDKs
- Mobile OAuth flows and server-side credential store
- Offline authentication

KEY BENEFITS

- Improves compliance and lowers TCO by extending existing access management services to mobile devices
- Enhances user experience with Mobile Single Sign-on for both native and browser-based applications
- Strengthens security with device fingerprinting and device context-based authentication and authorization
- Controls risk with risk-based control and investigative analysis
- Offers flexible authentication with knowledge-based access (KBA) and one-time password (OTP)
- Integrates with Oracle Access Management OAuth Services
- Enables Social Identity authentication and access without programming
- Manages server features through the integrated Oracle Access Management Console
- Packaged Security that frees the mobile developer to focus on functionality

Introduction

Mobile computing gradually allows us to make the elusive “anytime, anywhere access” mantra a reality, while online social identities allow us to access web sites on the Internet using existing identity from leading social networks such as Facebook, Google, Twitter, LinkedIn or Yahoo.

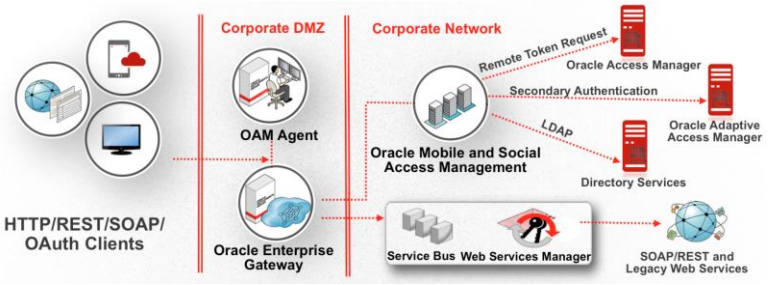
As part of its Access Management platform, Mobile and Social Access Services are designed to secure mobile access to applications leveraging the existing back-end identity management infrastructure. Oracle's Mobile and Social Access Services also provide client software development kits (SDKs) used by developers to weave security into native mobile applications for tight integration with identity management.

Oracle's Mobile and Social solution secures mobile access to corporate resources by leveraging the services of Oracle Access Management in terms of single sign-on between browser-based and native mobile applications, device fingerprinting and registration, device context based fine-grained authorization and REST interface Security. In addition, the Mobile and Social Access Services enable enterprises to securely leverage social identity for personalization and federated sign-on. The Mobile and Social Access Services support standards like OAuth and JWT.

Extending Enterprise Security to Mobile Applications

By extending Oracle’s unique identity and access management platform approach to mobile, customers can securely bring advanced mobile computing into the enterprise.

As shown below, Oracle Mobile and Social Access Services leverage the whole Oracle Access Management Platform



Authenticating Mobile Users

The Mobile and Social Access Services provide authentication and authorization services that let you extend an existing authentication and authorization infrastructure to mobile and non-mobile applications. Mobile services support User Tokens, Access Tokens, Client Tokens, OAM Master Tokens and client registration handles.

CLIENT SDKS

- Apple iOS
- Android
- JAVA
- Social Identity

SUPPORTED ACCESS CONTROL STANDARDS

- REST
- JSON, JWT
- OpenID
- OAuth
- SAML
- WS-Security
- Web API

Authorizing Mobile Users

Authorization is handled by Oracle Entitlement Server (OES), a policy-based, fine-grained authorization server designed to externalize authorization from applications and make decisions regarding the access of an authenticated party to protected applications.

Mobile single sign-on

Mobile single sign-on (SSO) allows a user to run multiple mobile applications on the same device without having to provide credentials for each application. Both native, hybrid and browser-based applications can participate in mobile SSO.

Integrating with User Directories

The Mobile and Social Access Services make directory services available to mobile devices, protected by a token, without a need for building LDAP clients. User Profile services includes the ability to search, view, create, update and delete users, groups and relationships, subject to permissions.

Integration with OAM

Mobile and Social Access Services support OAM tokens (HTTP cookies) to secure the path between mobile applications and resources. Credentials are collected on the mobile device using native interfaces, then presented to the Mobile and Social Access server via REST interfaces, which returns the OAM token. When the token is presented to an OAM WebGate by a mobile application, access is granted without a browser redirection for authentication.

Integration with OAG

Mobile and Social Access Services together with Oracle API Gateway can support JWT or OAM tokens to secure the path between mobile applications and SOAP/SAML or REST resources. Credentials are collected on the mobile device using native interfaces, then presented to the Mobile and Social Access server via REST interfaces, which issues a token. Oracle API Gateway (OAG) can protect REST and SOAP/SAML resources with these JWT or OAM tokens.

Validating Device Identities

Mobile and Social Access Services can enforce new layers of authentication by requiring both device and application registration. Registrations are also subject to the policies and risk assessments available in OAAM. These policies can trigger step-up challenges such as knowledge-based authentication (KBA) or one-time passwords (OTP) delivered via email or SMS text.

Addressing Device Loss and Theft

Smart phone loss and theft create a high security risk for users and companies. Oracle Mobile and Social Access Services address this risk by providing a way to blacklist a device, and then implement policies to challenge the user, block the device, or initiate a selective wipe of security information.

Mobile and Social Client SDKs

Mobile and Social Access Services are built on REST interfaces available from any platform without an SDK. However, the SDKs add feature-rich platform-aware authentication, authorization, and identity capabilities to registered mobile applications. The Mobile and Social Access solution provides separate client software development kits (SDKs) for iOS and Android devices and Java.

Contact Us

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

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

Hardware and Software, Engineered to Work Together

ORACLE