ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

Oracle Mobile Security

What's New in OMSS 11gR2 Patch Set 3

ORACLE WHITE PAPER | MAY 2015

ORACLE

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.

Oracle Mobile Strategy

Provide a comprehensive mobile platform to address todays advanced mobile solution requirements; developing apps, integrating with enterprise resources, providing advanced security for the apps with full fledged Enterprise Mobility Management (EMM) capabilities, deploying, managing and analyzing from a unified console. Oracle Mobile Suite provides tools to abstract the application from the underlying OS, enabling "write-once, run-anywhere" capabilities for mobile devices. Customers can focus on building highly effective, multi-channel mobile apps that leverage their existing skill sets in HTML5 or Java and which can easily integrate with their existing corporate resources. They can leverage one middleware infrastructure for their enterprise wide security and integration needs. Oracle provides enterprise-grade reliability, performance, and availability to handle the high volume of traffic from existing web and mobile channels.

What's New in Oracle Mobile Security Suite PS3

Identity-centric Enterprise Mobility Management Platform

OMSS now provides an Identity-centric Enterprise Mobility Management (EMM) Platform that includes Mobile Device Management (MDM) in addition to Mobile App Management (MAM), Mobile Content Management (MCM) and Mobile Identity. It can fully integrate and leverage customers existing identity management platform, for superior security and enhanced user experience.

Mobile Device Management

Provides the ability to secure corporate-owned mobile devices. Enforces device policies and restrictions that conform to corporate security policies and provides remote controls to manage mobile devices. Compliance with policies can be tracked and remediation actions enforced. Android MDM functionality relies on Google Cloud Messaging (GCM); iOS MDM functionality relies on Apple Push Notification Service (APNS). Features include:

- Device Configurations – Use Device Configurations to create pre-configured E-mail, VPN, calendar, and Wi-Fi settings profiles that can be added to mobile security policies.
- Device Restrictions – For Android: camera only. For iOS: camera, app install, assistant (Siri), cloud backup, cloud doc sync, cloud Keychain sync, diagnostic submission, explicit content, fingerprint unlock, lock screen control center, lock screen notifications view, lock screen today view, ad tracking, iTunes, iTunes Store password entry, untrusted TLS prompt, Shared Stream, screenshot, Safari, Photo Stream, Passbook while locked, over-the-air PKI updates.
- Device passcode – Passcode policy restrictions, including minimum length, history, idle timeout, failed attempts, expiry, expiry duration, and password complexity.
- Android Device Encryption – Enables device encryption for Android devices.

Note: OMSS can co-exist with other MDM solutions enabling customers to continue using it for MDM functionality but leverage OMSS for advanced application and content level security functionalities.

Servers on Oracle Fusion Middleware

The server components of the Oracle Mobile Security Suite (Mobile Security Manager and Mobile Security Access Server) have been rebuilt on top of the Oracle Fusion Middleware technology stack for this release. Oracle Mobile Security Suite can now be installed, configured, and managed using mechanisms that are consistent with other Oracle Identity and Access Management products.

Support for additional LDAP directories

Oracle Mobile Security Suite now supports the following LDAP directories:

- Microsoft Active Directory 2008, 2008R2, and 2012R2
- Oracle Unified Directory 11gR2 (11.1.2.2+)
- Oracle Internet Directory 11gR1 (11.1.1.7 and 11.1.1.9)
- Oracle Directory Server Enterprise Edition (ODSEE) 11gR

Support for additional Database versions

Oracle Mobile Security Suite now supports the following Oracle Database versions:

- Oracle 11.1.0.7+
- Oracle 11.2.0.1+
- Oracle 12.1.0.1+

Oracle Access Manager/Oracle Identity Governance console integration

The Oracle Mobile Security Suite and Oracle Access Manager UI consoles have been combined in this release into a single unified Policy Manager console. Mobile Security Suite console pages can also be deployed with Oracle Identity Governance self-service console. This provides centralized administrative, helpdesk, and self-service UI functionality from these products in a single place. A unified console improves the user experience and reduces management costs.

Risk-based step-up authentication

Oracle Mobile Security Suite can now use the capabilities of Oracle Access Manager to perform context aware risk-based step-up authentication at the time the user registers or logs in to the Secure Workspace app. Step-up authentication is an additional authentication factor on top of the primary password, and can take the form of either Knowledge-Based Authentication (KBA) or a One Time Password (OTP). This feature is available when the Secure Workspace app is configured to use OAuth2 Mobile Client authentication.

Mobile Security Access Server as an OAM 11g WebGate

The Mobile Security Access Server can optionally be enabled as an Oracle Access Manager 11g WebGate. This allows the Mobile Security Access Server to protect access to otherwise unprotected web applications, and provide single sign-on to them relying on the standard Oracle Access Manager login page, tokens, and HTTP redirects.

Containerized app recovery

If the Secure Workspace app has been deleted and reinstalled, automatic recovery of the encrypted data underlying containerized mobile apps is now supported. End-users can now reinstall the Secure Workspace app after

mistakenly—or intentionally—deleting it without any loss of service or data by the set of containerized apps that are part of the Workspace.

Support for Android 5.0

This release of Oracle Mobile Security Suite now fully supports the Secure Workspace app and App Containerization on Android 5.0 devices.

Containerization of Oracle Mobile Application Framework (MAF) apps

Oracle Mobile Security Suite 11g Release 2 (11.1.2.3.0) has a tight integration with the Oracle Mobile Application Framework (MAF) 2.1.3 or higher to support containerization of MAF apps across both iOS and Android. This integration enables the Oracle Mobile Security Suite functionality for secure networking, security storage, and data leakage prevention within MAF apps at both the virtualized and native levels.

Localized User Interfaces

All Oracle Mobile Security Suite user interfaces, including both the MSM console UI, as well as the mobile UI exposed by the Secure Workspace app and the app containerization functionality, have been translated and can now be displayed in the standard sets of Oracle Fusion Middleware localized languages.

Accessibility Compliance

This release includes significant investment across all components of the Oracle Mobile Security Suite in the area of accessibility. More information on the Oracle Accessibility Program is available at the following website:

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc

Localized User Interfaces

All Oracle Mobile Security Suite user interfaces, including both the MSM console UI, as well as the mobile UI exposed by the Secure Workspace app and the app containerization functionality, have been translated and can now be displayed in the standard sets of Oracle Fusion Middleware localized languages.

Kiosk Mode (Workspace Launcher)

For Android devices only. Minimizes interaction with the operating system outside of the Workspace and prevents the user from closing the Secure Workspace app, making this mode suitable for public environments where supervision is minimal, such as lobbies, exhibit spaces, and show rooms. Addresses retail, healthcare, manufacturing, and other use cases where a single device is used by multiple users to access corporate data.

Basic authentication for Secure E-mail and Mobile File Manager

Support for ActiveSync-enabled e-mail servers and file share servers that are protected with Basic authentication, in addition to the Windows authentication supported in previous releases. This enables Secure E-mail and Mobile File Manager features to be used in environments where the Secure Workspace app is configured for OAM/OAuth password authentication instead of Windows authentication.

Shared Workspace Mode

Allows multiple users to share a single installed Secure Workspace app on a shared device. This feature addresses retail, healthcare, manufacturing, and other use cases where multiple users need to access online resources in an authenticated and secure fashion on a shared device, but do not require data to be locally stored between authenticated sessions. Locally stored data is securely wiped when each authenticated session ends or when the user logs out of the session.

Custom Web URLs for password management prior to Secure Workspace login

Ability to customize the Secure Workspace app with a set of web URLs accessible to the end-user prior to login. When selected, these web URLs will be opened in an embedded Web view within the Secure Workspace app, and can be used to expose password change, password reset, forgot user id, and other functionality that needs to be used prior to login. These web URLs can point to the password management functionality exposed by Oracle Access Manager, or another system.

Secure storage using Android NDK containerization

A new native-level mechanism for securing the storage of containerized apps on Android devices. This native-level secure storage is complementary to the Java-level secure storage present in previous releases, and together they enable securing a wider range of locally stored data.

Role-based mobile access authorization

Oracle Mobile Security Suite can now check for mobile-only access authorization. Use this feature to allow or deny users access to specific web apps and web services based on their role assignments. For example, you can deny users access to an internal resource if they have the Contractor role.

For more information, please visit Oracle's website at http://www.oracle.com/identity.

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

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

Hardware and Software, Engineered to Work Together

Oracle Mobile Security – What's new in PS3
May 2015