DATASHEET

appdome

ENTERPRISE MOBILITY CONTROL™

Extend the compatibility of UEM and MAM SDKs, cover more use cases and support all Android and iOS apps.

THE UEM & MAM SDK CHALLENGE

Developers build mobile apps using an ever-growing and constantly changing collection of native and non-native app development environments. This produces a heterogeneous and highly diverse range of mobile apps that utilize an equally wide range of frameworks and methods inside each app. But, UEM and MAM SDKs are typically built to support only a subset of these apps, frameworks and methods. As a result, developers face challenges and limitations when enterprise customers demand that they guarantee compatibility between their apps and the UEM or MAM SDK. Most of the time, developers are forced to decide between two equally bad outcomes: (a) drop support for UEM and MAM altogether, or (b) change their app to fit the UEM or MAM SDK.

ENTERPRISE MOBILITY CONTROL

Appdome's Enterprise Mobility Control allows enterprise IT and mobile developers to make UEM and MAM easy and get the most out of the chosen UEM or MAM vendor. First, by bridging the gaps between the SDK and the app, including the frameworks and methods in the app, Enterprise Mobility Control overcomes compatibility challenges developers and enterprise customers face in building UEM and MAM enabled apps for the workplace. With Enterprise Mobility Control, anyone can instantly build new apps or app versions that are fully compatible with all major UEM or MAM SDKs – no matter how the app was developed or what frameworks and methods are in the app. Second, Enterprise Mobility Control offers a range of UEM & MAM extensions, designed to make mobile apps compatible with UEM and MAM vendor browsers, email clients and secure document sharing protocols, as well as deliver unparalleled control over permissions granted to enterprise apps.

UEM-MAM CONTROL CENTER

UEM-MAM Control Center™ provides enterprise IT and mobile developers total control over the UEM or MAM implementation. These features of UEM-MAM Control Center are on top of the UEM-MAM SDK itself. It includes granular control over (a) routing via the UEM tunnel to accommodate latency sensitive features such as VoIP, instant messaging, WebView, push notifications, and more and (b) encryption schemes to accommodate different data classifications, including video, media and web files. UEM-MAM Control Center also provides a wide range of out of the box optimization features for container management, folder management, as well as extended control of copy-paste models, layered jailbreak and rooting and more.

BOOSTEMM

BoostEMM™ gives enterprise IT and mobile developers the option to integrate the UEM-MAM secure browsing, email, document sharing and other EMM or MAM ecosystem services to Android and iOS apps. This is extremely powerful for organizations that leverage productivity apps from their chosen UEM or MAM vendor, or for organizations that want to promote collaboration or sharing among apps.

MOBILE PERMISSION CONTROL

Mobile Permission Control™ gives enterprise IT and mobile developers the option to restrict or permit mobile app permissions, like access to camera, local contract or calendar, etc., to address specific use cases or security objectives. Using Mobile Permission Control, the entire range of mobile permissions accessed by Android and iOS apps can be changed to protect end user privacy, guard against unknown use of compromised apps and comply with regulations like GDPR, FINRA and more, all without building a new app manually.

UEM-MAM CONTROL CENTER

Dynamic Encryption and Container - Improves app performance inside an EMM container by tailoring the scope of encryption and optimizing the app's encryption model. For example, dynamically detect, adjust and optimize container settings, dynamically encrypt/decrypt or obfuscate all app files and folders including nested file systems, etc).

Adaptive App Routing - Optimizes traffic routing decisions in the app, allowing latency sensitive traffic such as VoIP or messaging to leverage the app's native routing protocol, while routing all other traffic and events via the EMM VPN tunnel and thereby significantly improving app performance. (EMM VPN tunnels are known to degrade the performance of latency sensitive traffic).

EMM Authentication and SSO - Appdome's EMM Authenticated Tunnel allows an Appdome-Built app to trust the EMM's authentication methods so that mobile end users only need to automatically sign into an app once. Appdome Pre-Authentication supports Kerberos, Kerberos Constrained Delegation (KCD), SAML and OAuth.

Method and Protocol Bridging - Today's modern apps are built with many protocols, frameworks and methods that are not supported by UEM/EMMs out of the box. Appdome provides a number of extensions to bridge the gap between apps and their EMM SDK counterparts. Supported extensions include IPv6 to IPv4 Tunneling, WKWebview, Inbound Port Multiplexing, legacy background/push (pre-iOS 9 apps), Jailbreak/Root prevention by Appdome, copy & paste prevention by Appdome, and more.

Secure Remote Access (MicroVPN) - Replaces the EMM VPN tunnel with Appdome MicroVPN and securely tunnels the mobile app traffic directly to the enterprise's existing VPN infrastructure over secure TLS encrypted channels. MicroVPN by Appdome provides true enterprise-grade features including certificate validation, Certificate Pinning, Route-to-Hosts designations, Server Validation (SSL/TLS trust chain), Session Hardening, and Protocol Checking - all of which prevent an app from connecting to insecure servers or destinations.

BOOSTEMM FEATURES

Secure Browser – When enabled, this feature ensures that web links opened in the app, will be opened using the EMM secure web browser.

Secure Email – When enabled, this feature ensures that email links opened in the app, will be opened using the EMM secure email client.

Secure Document Sharing – When enabled, this feature ensures document sharing via the EMM secure browser and blocks opening files in 3rd party apps and disables all other document sharing.

Legacy Camera Support – Supports legacy apps running with Android 6+ using Image Capture.

App Launcher – This ensures that users always use the EMM vendor's launcher app to navigate to any app in their EMM container or enterprise app store.

Analytics – This allows the app the app to use the EMM vendor's Analytics events in the app.

Events Reporting – Automatically reports events such as activation, authentication and policy updates from the EMM vendor.

MOBILE PERMISSIONS CONTROL

Prevent App Screen Sharing – Prevents the screen from being captured or projected on non-secure screens.

Blur Application screen – Obscures screenshots to prevent sensitive mobile data from being exposed.

Prohibit Local Contacts – Prevents users from importing local contacts to the app.

Prohibit Local Calendar – Prevents importing the local calendar to the app.

In-App Calls Only – Ensures all calls are made using the app's native dialer when applicable. This prevents the app from displaying alternate phone apps when a phone number is clicked within the app.

In-App Messages Only – Ensures all messages are made using the app's native messaging service, when applicable.

Prohibit Camera – Prevents access to the camera by the app.

Prohibit Camera via Image Requests (Android only) – Disables the app from accessing images from external sources including the camera app and gallery.

Prohibit Microphone – Prevents access to the microphone by the app.

Prohibit Location – Prevents access to the device's location (GPS, GLONASS, etc...).

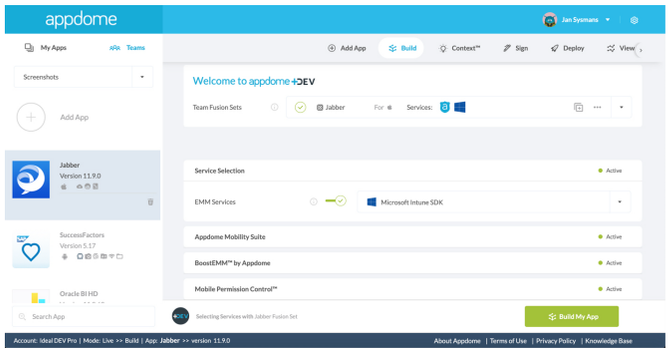

Image: Appdome Enterprise Mobility Control enabled for Microsoft Intune

Learn more about Appdome Enterprise Mobility Control at **www.appdome.com**.
Open a free Appdome account at **fusion.appdome.com** and start securing your apps!

ABOUT APPDOME

Appdome changes the way people build mobile apps. Appdome's industry defining no-code mobile development and security platform uses a patented, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new security, authentication, access, enterprise mobility, mobile threat, analytics and more into any Android and iOS app instantly. There are over 25,000 unique combinations of mobile features, kits, vendors, standards, SDKs and APIs available on Appdome. Over 150+ leading financial, healthcare, government, and m-commerce providers use Appdome to consistently deliver richer and safer mobile experiences to millions of mobile end users, eliminating complex development and accelerating mobile app lifecycles.

For more information, visit www.appdome.com

*Yehuda et al. Method and a system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.