DATASHEET

appdome

Appdome for AppConfig

Implement the industry standard for enterprise mobility in a click

Appdome provides developers and publishers a true, no-code way to implement AppConfig to apps!

Appdome for AppConfig is designed to advance the business reach and usefulness of apps built for enterprise use. The service allows mobile software vendors like ISVs and enterprise developers to avoid spending any time manually adding the app configuration and security features included in the AppConfig standard, and more time building better and richer versions of their apps. Appdome for AppConfig users also enjoy choice-driven integrations, offering faster and more agile implementations of AppConfig in minutes.

What is Appdome for AppConfig?

Appdome for AppConfig is a best practice implementation of the AppConfig standard, including native-OS features, that anyone can add to an app. Without Appdome, developers could spend weeks or months manually creating features and implementing AppConfig in their apps. On top of implementation challenges, developers also faced maintenance challenges. With every single release of the app, OS, and each new feature in the AppConfig standard itself, developers would have to update or redo manual implementations. Appdome for AppConfig enables anyone to complete integrations and delivers faster development and deployment of apps for the enterprise by using technology to implement AppConfig to apps.

Why did Appdome join AppConfig?

Appdome mission is to support leading standards in mobile development across use cases. Mobile device management (MDM) and managed-BYOD are critical use cases in enterprise mobility. AppConfig makes apps enterprise ready, allowing apps to be managed by MDM vendors. By transforming AppConfig into a click-to-implement service, Appdome intends to accelerate the adoption of AppConfig among all ISVs and mobile app makers. By making the service available to all app makers, Appdome makes it easier for enterprises to bring more apps into the workplace and enables employees to fully leverage mobile apps in their day-to-day work.

How do I use Appdome for AppConfig?

The ease of use of Appdome for AppConfig empowers anyone to add AppConfig to any app without code or coding. The entire process works in just a few clicks and in a few minutes. Appdome users simply upload a final app package (.ipa or .apk) to the Appdome platform, select the desired Appdome for AppConfig services and click “Fuse my App.” The cloud-based integration process is completed automatically within minutes, integrating the full AppConfig standard to any app. You can find Appdome for AppConfig at the top of the management category on the Appdome platform (shown below).

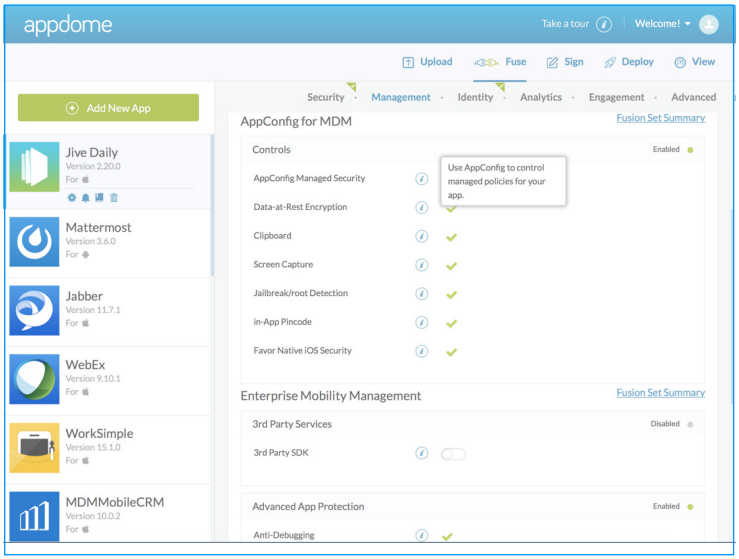

Figure 1: AppConfig standard on the Appdome platform

Features in Appdome for AppConfig

Appdome's AppFusion technology replaces manual development with automation, offering enterprise customers and publishers the ability to add new services and features to existing iOS or Android apps via a simple cloud based workflow, requiring zero development or engineering effort. All services added via Appdome for AppConfig are per app without development and without code or coding.

Feature	Android	IOS
App Configuration	Fuse Android for Work App Restrictions into any native and hybrid Android mobile app.	Fuse iOS Managed Configuration into any native and hybrid iOS mobile app.
App Tunnel / Per-App VPN	Fuse "Per-app VPN" capability available in most commercial VPN solutions and Android 5.0+ to any Android app.	Fuse "Per-app VPN" capability available in most commercial VPN solutions and iOS 9+ to any iOS app.
Single Sign-On Login Hint	Appdome supports automatic tenant discovery for any standard single sign-on protocol, such as OAuth or OpenID Connect, and **automatically** invoke the identity provider login page in a web view.	Appdome supports multiple single sign on protocols such as SAML and others, allowing Fused iOS apps to **automatically** invoke the identity provider login page in a web view.
App Security: **Passcode (TouchID)**	Fuse **app specific** pincode and fingerprint authentication, without custom implementation or coding app-specific restrictions, to enable admin configuration of the passcode settings and requirements.	Fuse app specific pincode and TouchID and use iOS Managed Configuration to set the pincode or TouchID settings on the application.
App Security: **Managed Open-In Document Sharing**	Fuse full document sharing and synching capabilities to **any** Android app and use Android for Work / Android 5.0+ managed profile to enforce files to open only in managed apps or only in apps under the managed profile. There is no need to ensure apps are using Content URIs and not File URIs.	Fuse full document sharing and synching capabilities to **any** iOS app and set the "managed open in" control available by the EMM provider to restrict the native open in capability or use iOS Managed Configuration to set the document sharing and syncing policy on the application.
App Security: **Prevent App Backup**	Fuse "prevent app backup" to **any** Android app and any app deployed under Android for Work / Android 5.0+ managed profiles will not participate in any backup and restore infrastructure.	Fuse full "prevent app backup" feature-set to **any** iOS app and set the "prevent app backup" security control available by the EMM provider to prevent app data backup in iTunes.
App Security: **Disable Screen Capture**	Fuse "prevent screen capture" security control to **any** Android app and use Android for Work / Android 5.0+ managed profile to prevent screenshots.	Fuse "prevent screen capture" security control to **any** iOS app and set the "prevent screen capture" security control available by the EMM provider with iOS 9+ to restrict the native screenshot capability.
App security-**Enforce App Encryption**	Fuse **per app** data at rest encryption plus enable the use of Android for Work device encryption.	Fuse **per app** data at rest encryption plus enable use of native iOS data protection encryption.
App security-**Remote Wipe App**	Fused apps that leverage an EMM to remote wipe an app from a device and distribute the app to the device as a managed application using the EMM tool.	Fused Apps leverage EMM to remote wipe an app from a device and distribute the app to the device as a managed application using the EMM tool.
App security-**Disable Copy-Paste**	Fuse copy/paste prevention to **any** Android app and use an Android for Work / Android 5.0+ managed profile to containerize copy and pasting to only managed applications.	Fuse copy/paste prevention to **any** iOS app and use iOS Managed Configuration to set the copy/paste policy on the application.

Appdome strives to deliver the following benefits to the AppConfig community:

- **Accelerate the adoption of AppConfig**
  Appdome automates the implementation of AppConfig, filling the gaps for app makers that lack the development and engineering resources to implement the standard manually. Now, app makers can add AppConfig to an app by selecting the desired functionality on Appdome and clicking "Fuse my App." After the app is built, app makers can sign and publish their AppConfig-enabled app via their app store of choice.

- **Eliminate manual development required to implement AppConfig**
  Appdome makes it simple and easy to implement AppConfig to any app. The no-code service eliminates the software development and maintenance burden that use to accompany an app maker's decision to adopt and support the standard. In the past, developers would need to manually code and validate AppConfig to each build of each app. Appdome's mobile service integration platform eliminates this work and provides a fully automated experience that adds AppConfig to apps.

- **Encourage better Appconfig-enabled apps**
  Developers will be excited to reclaim precious engineering time that might otherwise go to manually implementing AppConfig in every single release of the app and OS, freeing core development efforts to proceed on pace and without delay. This allows app-makers to remain heads down developing great features that customers want. In fact, by using Appdome for AppConfig, enterprise customers get the best of both worlds – better apps enabled by AppConfig.

- **Facilitate the evolution of AppConfig as an important industry standard**
  By enabling all app makers to easily and quickly implement AppConfig without code or coding, Appdome allows the standard to evolve without the burden of manual implementation associated with new features. Appdome for AppConfig allows the rapid evolution of the standard, promising a greater range of features developers can "AppConfig-in". Appdome for AppConfig works across OS platforms and is framework independent. That means app makers get cross-platform support (Android and iOS) without any additional effort, along with a consistent implementation that requires just a few clicks in a few minutes.

Advanced app protection from Appdome

Each app that is fused on Appdome includes critical app hardening to ensure the highest levels of protection for users, application, and data:

- **Anti-debugging**
  Prevent malicious parties from debugging an app, attaching malicious code in real time, and understanding how the app works. This way, app makers can ensure their apps are much safer running on mobile devices.

- **Obfuscation**
  Ensure all critical and sensitive areas of an app is protected from prying eyes through source code obfuscation, so no one but the app maker will understand how the app works underneath the hood. Appdome utilizes anti-reversing with code obfuscation to confuse and slow hackers so that they cannot ascertain how an app actually works internally.

- **Anti-tampering**
  Appdome uniquely protects an app from being tampered with. By sealing the app and actively detecting modifications at run-time, Appdome makes sure no one can modify the app or re-distribute it without permission.

- **Checksum Validation**
  Checksum validation is a technique used in the security industry to calculate a unique hash or fingerprint of information, binary data, and assets. By creating checksums and validating them at run-time, Appdome prevents changes to an app, its resources, code, configuration and more.

- **Jailbreak and Root Protection**
  Jailbreak and Root will detect if a device has been jailbroken (iOS) or rooted (Android). Appdome will alert the app user and exits the app based on the EMM provider settings.

To learn more about Appdome or AppConfig, visit www.appdome.com or open a free Appdome account and start your free Mobile Services trial today!

About Appdome. Appdome is the industry's first codeless mobile integration service, providing developers and others an easy to use cloud based workflow to complete mobile integration projects. To use Appdome, no source code, coding, or development expertise is required. Likewise, no modifications to an app or an SDK are required for Appdome's technology to complete the full integration of services that are selected by users of the Appdome platform. The solution is currently used by the world's leading financial, healthcare and e-commerce companies to support productivity, compliance, and security for consumers and employees. Appdome was rated a Cool Vendor in Mobile Security by Gartner in 2015. For more information, visit **www.appdome.com**

appdome