appdome

Appdome for Mobile Enterprise Access

No-Code Mobile Integration to Enable
Android and iOS Apps with Secure Access
To Corporate Resources

Appdome for Mobile Enterprise Access makes it easy and convenient to add secure access services to any app. Developers and non-developers alike can add MicroVPN, behind-the-firewall resource governing proxy policies, server access paths and more to any Android and iOS app in seconds, no code or coding required.

Appdome provides customers ultimate flexibility to add secure access services integrated with an app, eliminating the need for per-app VPNs and VPN-client-based solutions. Encryption and other Appdome Mobile Enterprise Access services improve the mobile end user experience without compromising data-in-motion security. For example, Appdome Mobile Enterprise Access gives organizations using Microsoft Intune secure access to protected resources without having to rely on the Intune managed browser or specific gateway.

SECURE ACCESS WITHOUT CODING

Mobile apps are equipped with native support for different secure access solutions, leaving customers on their own to manually integrate these services or compromise network architecture to solve for a use case involving a custom-developed app. And if the use case involves a third party ISV app, getting access to the source code to manually code support is impossible.

Appdome's no-code mobile integration platform enables customers to use secure access services to any mobile app easily and without coding. This allows customers to leverage existing network and security investments to manage access to corporate resources from any Android and iOS app on-demand (including third party apps).

APPDOME FUSION PROCESS

To enable any Appdome for Mobile Enterprise Access integrations to any mobile app, simply upload an app binary to Appdome, select the desired Access service, click the "Fuse My App" button and you're done! In about a minute, the platform generates a new app binary which includes everything the mobile app needs to authenticate against the Secure Access services and securely connect to the desired enterprise resources. Then, sign the new binary and deploy the app using your existing workflow.

Appdome works with all Android and iOS apps (native, hybrid and non-native apps), developed in any framework, out of the box. No changes are required to mobile apps in order to work with Appdome, and enterprises do not need to change their app server or enterprise infrastructure. Appdome doesn't require source code and doesn't change the app's behavior or your workflow. Fused apps can be deployed through any public or private Appstore.

APPDOME FOR MOBILE ENTERPRISE ACCESS

Appdome for Mobile Enterprise Access offers customers several options for ensuring that apps, needing to access corporate resources, can do so securely. These options include MicroVPN, proxies and app configuration and setup.

MICROVPN BY APPDOME

Appdome's home-grown MicroVPN solution allows mobile applications to establish direct and seamless access to corporate resources without requiring device level or per-App VPN. Appdome MicroVPN is a flexible, all-in-one, mobile enterprise connectivity solution that supports any enterprise standard network gateway such as an SSL gateway, proxy, reverse proxy, or industry standard VPN, all without any change to enterprise network infrastructure.

Appdome MicroVPN provides two modes of operation. **Direct Connection Mode** enables a direct connection between an app and a protected resource (1-to-1 mapping), leveraging a gateway function built into the fusion layer of an app. Alternatively, customers can use a **Transparent Connection Mode**, whereby Appdome reroutes connections to internally resolved protected resources (many-to-many mapping) via standard secure gateways.
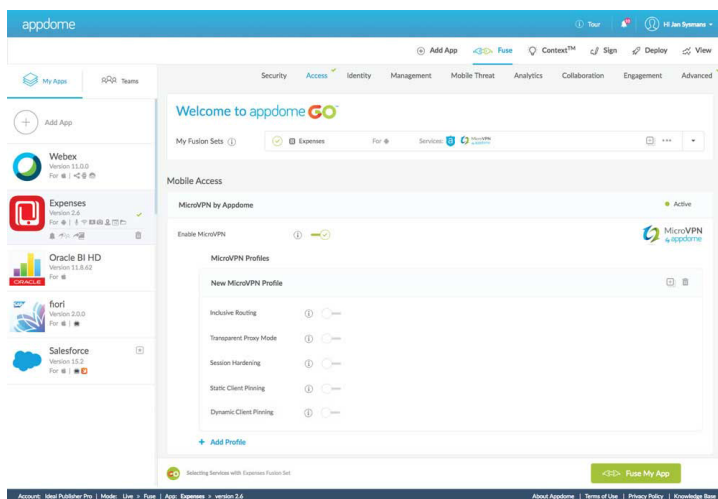

Image: Fuse Appdome MicroVPN to Oracle Expenses for iOS App

THIRD PARTY PROXIES

Appdome also includes implementations for third party secure gateways, including those from F5 Networks and Microsoft.

F5 Access Manager enables enterprises to connect any mobile app to F5 Access Manager natively. Any mobile app then can authenticate to F5 as an identity provider or as a proxy or gateway, and also receive authorization services inside the app's existing workflow. Appdome supports all F5 access methods and authentication types out of the box.

Microsoft's Azure AD Application Proxy (AppProxy) provides secure remote access for on-premise web apps. With Appdome, Microsoft AppProxy can be extended to Android and iOS apps, for controlled authentication. Enterprises can Fuse Appdome for Microsoft AppProxy, enabling Appdome-Fused mobile apps to tunnel traffic using either a transparent or reverse proxy mode.

APPDOME ACCESS SUITE

Appdome Mobile Enterprise Access also includes the Appome Access Suite. These capabilities provide the ability to fuse app configuration information, removing the burden for mobile end users having to copy and paste (or manually enter) server locations and other resource data. This includes private URLs, custom config files and custom values. Customers can also add private certificates and authorities, proxy PAC files and more to ensure app requests and data can successful traverse complex enterprise network environments.

Learn more about Appdome at **www.appdome.com** or open a free Appdome account at **fusion.appdome.com.**