Appdome for AppConfig

AppConfig Technical Capabilities

Introduction

The following document describes the technical capabilities and deployment of a native mobile app , integrated with AppConfig using the Appdome for AppConfig codeless integration service, to devices based on the best practices documented by the AppConfig Community. Reference EMM vendor specific setup documentation available on the AppConfig Community site for details on how to configure each of these capabilities with the EMM vendor of your choice.

App Deployment

EMM solutions have the capability to deploy native applications that live on the public app stores to devices. Operating systems such as iOS, Android, and Windows provide EMM vendors native built-in APIs as part of the MDM "Mobile Device Management" protocols documented by the operating systems to make this possible. Using this capability, an app integrated with AppConfig using the Appdome for AppConfig service that is in the public app store can be installed automatically or via a self-service catalog with EMM platforms participating in AppConfig Community.

App Configuration

An app, integrated with AppConfig using the Appdome for AppConfig service may require configuration including private URLs, tokens and other customizations to enable use, all of which can be completed on Appdome. EMM vendors participating in AppConfig Community have the ability to auto-configure these settings. The end user no longer has to input these values themselves. Please reference the matrix below for more information.

Configuration Key	Description	Value	Type	iOS Support	Android for Work Support
All	Available from the ISV	All	All	Y	Y

App Tunnel

Appdome, and EMM vendors who participate in AppConfig Community, have the ability to enable native app tunneling features on supported mobile devices using a protocol called per-app VPN. Appdome and many EMM vendors provide customers a built-in per-app VPN or App Tunneling solution as part of their offering, as well as integrate with 3rd party per-app VPN providers such as Cisco, Palo Alto Networks, F5, and Pulse Secure. In addition, Appdome allows for split tunneling based on class of traffic used by an app.

Single Sign On

An app that supports delegating the login process to a company's SAML identity provider will be able to work with EMM vendors participating in AppConfig Community after its integrated with AppConfig using the Appdome for AppConfig service. EMM vendors have the ability to auto-deploy the appropriate certificates and credentials to the mobile device to auto-login the user into this SAML identity provider that has been setup.

Note: The SAML identity provider that is used must support the native SSO capabilities that are documented in the AppConfig Community. Visit the SSO section of the AppConfig Community dev center for an up to date list of identity providers that have been tested to work successfully with single sign-on.

The following SSO protocols are supported in the Appdome for AppConfig service to allow an app with these capabilities to perform properly:

SSO Support	iOS Support (Y/N)	Android Support (Y/N)
Certificate based authentication to SAML identity provider	Y	Y
Kerberos based authentication to SAML identity provider	Y	Y

Appdome supports a variety of certificate based authentication approaches, including private and public certs. The App Configuration key/value pairs needed to initiate the SSO process is determined the app integrated with AppConfig using the Appdome for AppConfig service.

Configuration Key	Description	Value	Type	iOS Support	Android for Work Support
All	Determined by ISV	All	All	Y	Y

Access Control

For security reasons, enterprises may want to prevent users from downloading an app integrated using the Appdome for AppConfig service to their unmanaged or unapproved device. The following approaches of preventing access to the app on unapproved devices is supported:

Access Control Support Type	iOS Support (y/n)	Android Support (y/n)
SAML Identity provider based access control	Y	Y
App Config Based Access Control	Y	Y

Security Policies

Appdome allows organizations that require an app integrated with AppConfig using the Appdome for AppConfig service to have more granular security and data loss protection within itself to prevent sensitive data and documents from leaking outside company control. Lastly, with apps integrated with AppConfig using the Appdome for AppConfig service organizations with EMM can leverage the native OS protocols to wipe and remove all corporate data on the device and uninstall the integrated app.

Security Policy	iOS Support (Y/N)	Android Support (Y/N)
Native OS Encryption	Y (enforced with device pincode)	Y (enforced with device pincode)
Managed Open In	Y (iOS managed open in policy)	Y (Android for Work policy)
Copy / Paste Control	Y	Y (Android for Work policy)
Screenshot Control	Y	Y (Android for Work policy)

The following config key/value pairs correspond to any security controls above that are implemented via app configuration keys.

Key	Description	Value	Type	iOS Support	Android for Work Support
blurApplicationScreen	Protects app on screen information while in the background		Boolean	Yes	No
disableScreenCapture	Block screenshot functionality in the protected app and blur application screenshot in switchboard		Boolean	No	Yes
inAppPinCode	Locks the app with an embedded local Pincode set by the user app launch		Boolean	Yes	Yes
copyAndPasteProtection	Resticts clipboard functionality to non protected applications		Boolean	Yes	Yes
dataAtRestEncryption	Sets up a secure and encrypted file container for application data		Boolean	Yes	Yes
jailBreakDetection	Disables app launch on Jailbroken devices		Boolean	Yes	No
rootDetection	Disables app launch on rooted devices		Boolean	No	Yes