Symphony.com

AppConfig Technical Capabilities

Introduction

The following document describes the technical capabilities and deployment the native mobile Symphony app 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, the Symphony app that is in the public app store can be installed automatically or via a self-service catalog with EMM platforms participating in AppConfig Community. Alternatively, some customers may choose to build a custom app built using the Force.com development platform. In this case, the resulting app will likely be deployed as an internal or in-house app. EMM vendors participating in AppConfig Community have the capability to deploy these types of apps as well.

App Configuration

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
pod_domain	The domain name of your pod. (In version 1.43+ this value is unused.)	<blank>	String	Y	Y
enable_photo_picker	Set to false to prohibit attaching photos from camera roll to messages sent within the application.	TRUE	Boolean	Y	Y

enable_webview	Set to false to prohibit viewing non-image attachments and URLs sent within the application.	TRUE	Boolean	Y	Y
enable_sharing	Set to false to prohibit users from sharing image attachments to other applications through OS installed share extensions.	TRUE	Boolean	Y	Y
enable_crash_reporting	Set to false to prohibit the recording of crashes for later analysis.	TRUE	Boolean	Y	Y
enable_analytics	Set to false to prohibit recording anonymous usage statistics.	TRUE	Boolean	Y	Y
enable_addressbook	Set to false to prohibit using OS Address Book to invite new contacts to application.	TRUE	Boolean	Y	Y
enable_copy	Set to false to prohibit users from copying the contents of messages.	TRUE	Boolean	Y	Y
enable_network_debugging	Set to true to emit logging for debugging network-related issues.	TRUE	Boolean	Y	Y
disable_pin	Set to true to hide the built-in Pincode feature	TRUE	Boolean	Y	Y
disable_introduction	Set to true to automatically skip the first-launch introduction screens	FALSE	Boolean	Y	Y
disable_sso	Set to true to prevent logging in through SSO	FALSE	Boolean	Y	Y

App Tunnel

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. Many EMM vendors provide customers a built-in per-app VPN or App Tunneling solution as part of the EMM offering, as well as integrate with 3rd party per-app VPN providers such as Cisco, Palo Alto Networks, F5, and Pulse Secure.

Single Sign On

Symphony supports delegating the login process to a company's SAML identity provider. EMM vendors participating in AppConfig Community 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 Symphony app:

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	N	N

Access Control

For security reasons, enterprises may want to prevent users from downloading Symphony to their unmanaged or unapproved device. The following approaches of preventing access to the Symphony 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	Not Supported	Not Supported

Security Policies

Some organizations may require the Symphony app to have more granular security and data loss protection within itself to prevent sensitive data and documents from leaking outside company control. Lastly, EMM can leverage the native OS protocols to wipe and remove all corporate data on the device and uninstall the Symphony 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	Not Supported	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
enable_copy	Set to false to prohibit users from copying the contents of messages.	TRUE	Boolean	Y	Y