App Name Here

AppConfig Technical Capabilities

**Instructions for App Vendors:**

Please fill in the appropriate field for each section below. If you do not have capabilities for a specific section, you do not need to fill it out.We have broken up app management capabilities in the following ways: Deployment (all apps supported), Configuration, Tunneling (all apps supported), SSO, Access Control, and Security Policies. Fields that are already populated and not highlighted are native operating system and/or EMM capabilities. You can leave these as is. Once completed, include this in your submission to the AppConfig.org website. Before submission, please remove these instructions, any highlighting in the document, and save as a PDF. We will then make the PDF available on the AppConfig Community website.

# Introduction

The following document describes the technical capabilities and deployment the native mobile [app name] 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 [app name] 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

For some customers, the first time use of the [app name] application requires [insert requirments here. For example: domain, etc]. 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** |
| Fill in here |  |  |  |  |  |
| Fill in here |  |  |  |  |  |

## 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

[app name] 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 [app name] app:

|  |  |  |
| --- | --- | --- |
| **SSO Support** | **iOS Support (Y/N)** | **Android Support (Y/N)** |
| Certificate based authentication to SAML identity provider | Fill in here | Fill in here  |
| Kerberos based authentication to SAML identity provider | Fill in here | Fill in here  |

When using the certificate based authentication approach, the following App Configuration key/value pairs must be used to initiate the SSO process:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Configuration Key** | **Description** | **Value** | **Type** | **iOS Support** | **Android for Work Support** |
| Fill in here | Fill in here | Fill in here | Fill in here | Fill in here | Fill in here |
| Fill in here | Fill in here | Fill in here | Fill in here | Fill in here | Fill in here |

## Access Control

For security reasons, enterprises may want to prevent users from downloading [app name] to their unmanaged or unapproved device. The following approaches of preventing access to the [app name] 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 | Fill in here (If no specific capability, write “Not supported”) | Fill in here (If no specific capability, write “Not supported”) |

## Security Policies

Some organizations may require the [app name] 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 [app name] 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 (App Configuration key/value required) or “Not supported” | Y (Android for Work policy) |
| Screenshot Control | Yes or “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** |
| Fill in here |  |  |  |  |  |