APPCONFIG COMMUNITY

ISEC7 Mobile Exchange Delegate

AppConfig Technical Capabilities

Introduction

The following document describes the technical capabilities and deployment the native mobile ISEC7 Mobile Exchange Delegate 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 ISEC7 Mobile Exchange Delegate 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 ISEC7 Mobile Exchange Delegate application requires configuration of user, server and license information. 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
ISEC7UserName (iOS) username (Android)	Username for the user	username	String	Yes	Yes
ISEC7UserEmail (iOS) email (Android)	Email for the user	email	String	Yes	Yes
ISEC7Server (iOS) server (Android)	Hostname for the Microsoft Exchange Server	Hostname	String	Yes	Yes

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.

Access Control

For security reasons, enterprises may want to prevent users from downloading ISEC7 Mobile Exchange Delegate to their unmanaged or unapproved device. The following approaches of preventing access to the ISEC7 Mobile Exchange Delegate 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 ISEC7 Mobile Exchange Delegate 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 ISEC7 Mobile Exchange Delegate 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	Not supported	Y (Android for Work policy)
Screenshot Control	Not supported	Y (Android for Work policy)