APPCONFIG
COMMUNITY

Slack (for EMM)

AppConfig Technical Capabilities

Introduction

The following document describes the technical capabilities and deployment the native mobile Slack (for EMM) 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. Please reach out to your Sales representative for a copy of Slack's XML file.

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 Slack (for EMM) 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 Slack (for EMM) application requires creating a team at slack.com. 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 (Y/N)	Android for Work Support (Y/N)
OrgDomain	Ability to enter the Organization's URL domain in order to fast forward users directly to Sign On Note: this does not prevent users from signing into other orgs; for this, see WhitelistedDomains below	Eg for acme.enterprise.slack.com; enter `acme.enterprise`	String	Y	Y

App Tunnel

EMM vendors who participate in the 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

SAML-based single sign-on (SSO) gives members access to Slack through an identity provider (IDP) of your choice. A list of the identity providers that we've partnered with can be found on our App Directory under Security and Compliance.

Access Control

For security reasons, enterprises may want to prevent users from downloading Slack to their unmanaged or unapproved device. The following approaches of preventing access to the Slack app on unapproved devices is supported:

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

Security Policies

Some organizations may require the Slack (for EMM) 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 Slack (for EMM) 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
Screenshot Control	N	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
ApprovedDevice	Verification that the device is approved.	Provided by your Slack Sales representative	String	Yes	Yes
DisableCopy	Ability to prevent users from copy/pasting Slack messages.	Yes or No	Boolean	Yes	Yes
WhitelistedDomains	Ensures that users can only log in to the whitelisted organization. Currently only a single domain is supported.	e.g. for acme.enterprise.slack.com; enter `acme.enterprise`	String	Yes	Yes

BrowserControl	Enforces the use of the specified browser when signing into Slack or opening links from Slack. Only the listed browsers are supported at this time.	`Web@Work`
		`Workspace One`
		`Microsoft Edge`
		`Blackberry Access`
		`Chrome`
			String	Yes	Yes

EndSessionLink	Private beta, do not use.	Please leave blank or omit key/value pair from config.	String	n/a	n/a