

Enterprise Mobility Management (EMM)

Agenda

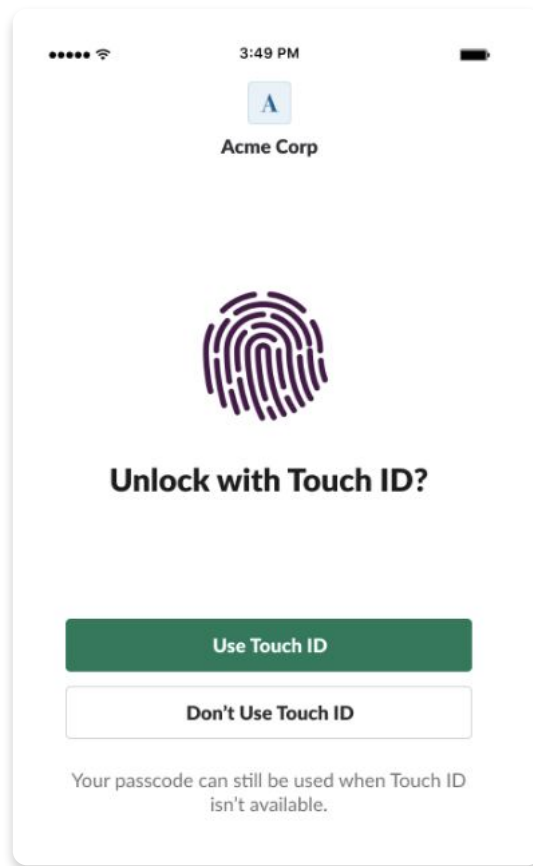
- **Slack-native mobile security features**
- **EMM @ Slack**
- **Setting up EMM**
- **What happens next?**
- **How does it work?**

Slack-native mobile security features



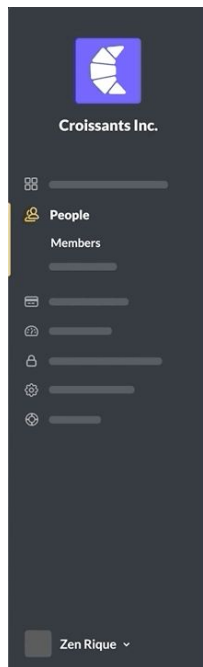
Secondary authentication

Ability to require employees to use additional authentication via Face ID, Touch ID, or passcode











Session management

Remotely wipe mobile and/or desktop sessions associated with a specific user



Organization Members (13)

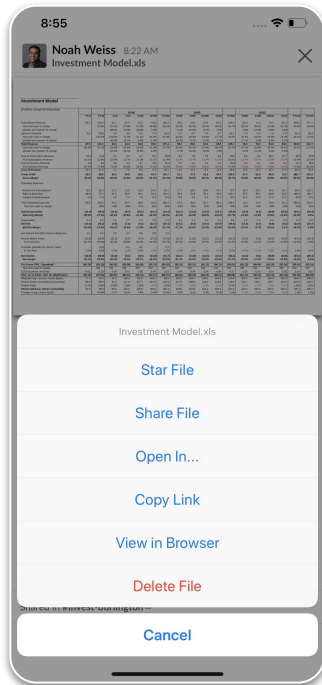
[View Deactivated Members](#)

Q Search members		All Members (13) ▾
Name	Account Type	
<input type="checkbox"/>  Kate Feeney kf@croissants.com	Member	
<input type="checkbox"/>  Erica Engle ee@croissants.com	Single-Channel Guest	
<input type="checkbox"/>  Amy Zhang az@croissants.com	Member	
<input type="checkbox"/>  Pooja Mehta pm@croissants.com	Primary Org Owner	
<input type="checkbox"/>  Nikhil Rao nr@croissants.com	Org Admin	
<input type="checkbox"/>  Josh Cartmell jc@croissants.com	Multi-Channel Guest	
<input type="checkbox"/>  Ian Ndicu in@croissants.com	Member	
<input type="checkbox"/>  Lauren Yearly ly@croissants.com	Member	

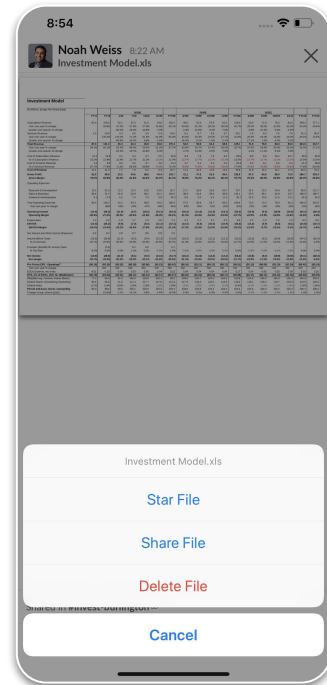
SLACK-NATIVE MOBILE SECURITY

Block files downloads and message copying on mobile devices

Ensure sensitive
corporate data is not
downloaded or shared
on unmanaged mobile
devices



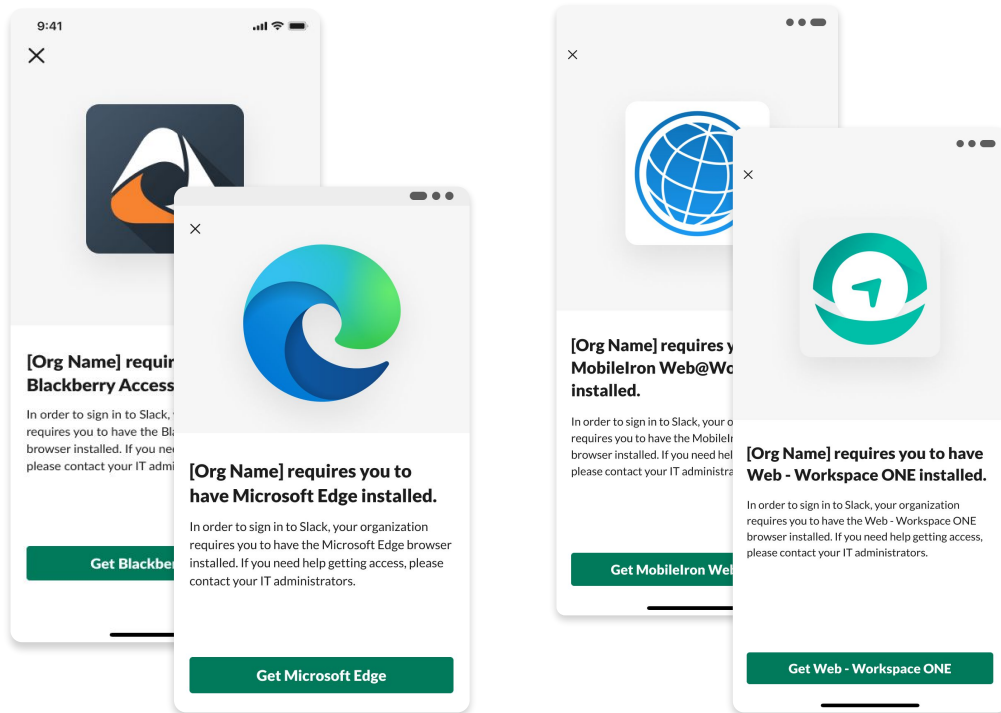
Feature disabled



Feature enabled

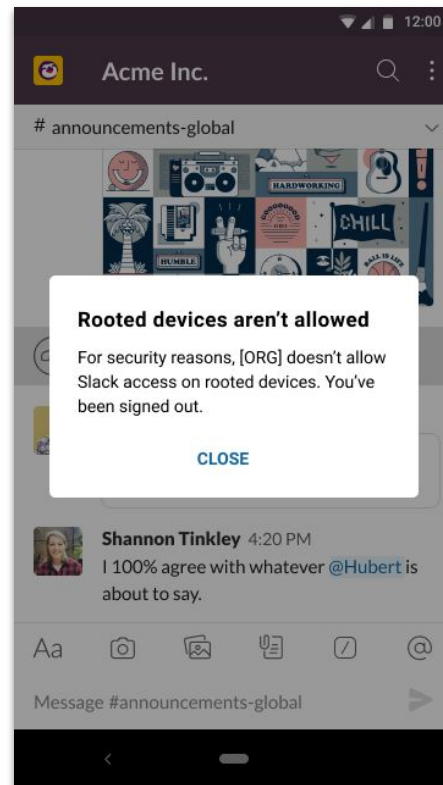
Default browser control

Control how Slack is used with the browser included in your MAM container

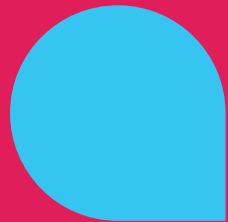


Block jailbroken or rooted devices

Detect if a device is
jailbroken (iOS) or rooted
(Android) and block
Slack access if so



EMM @ Slack



What is EMM at Slack?

Enterprise mobility management (EMM) is a suite of software that allows organizations to securely enable employee use of mobile devices and applications.

Mobile Device Management (MDM) is a subset of EMM, which focuses on the device management and device security policies.

MDM can include password protection, data loss prevention settings, device whitelisting and blacklisting, encryption and/or remote wipe technology, administrative controls to delete all data from a misplaced device.



Why EMM?



Restrict access to only managed/approved devices

Admins are able to restrict access to only approved and compliant devices that comply with their internal policies



Auto-discovery of the Slack organization

Admins can pre-configure the Slack app with the organization domain and the value is pre-populated for the user on the app after downloading it

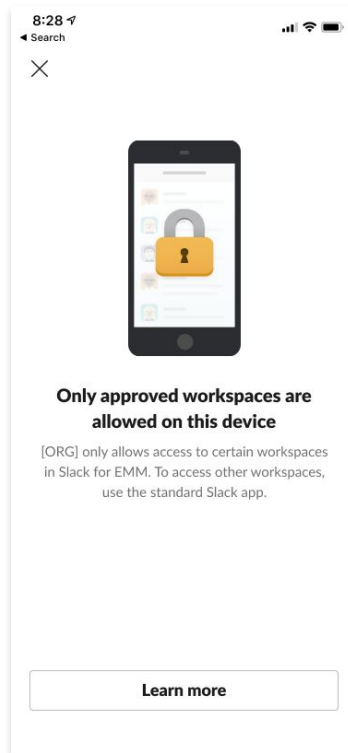
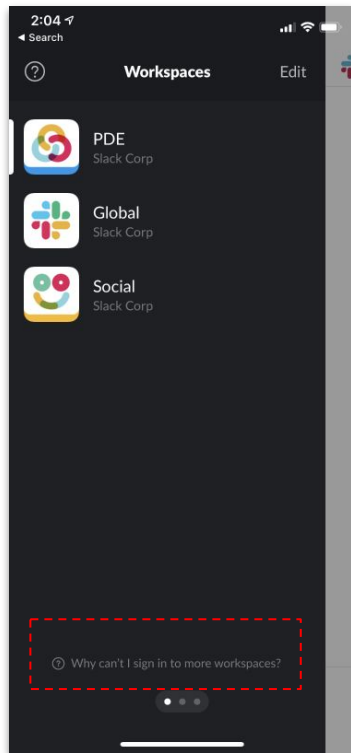


Whitelisting only corporate workspaces

Admins can restricts users from signing into personal/non-corporate workspaces by whitelisting the organization domain

Domain Whitelisting

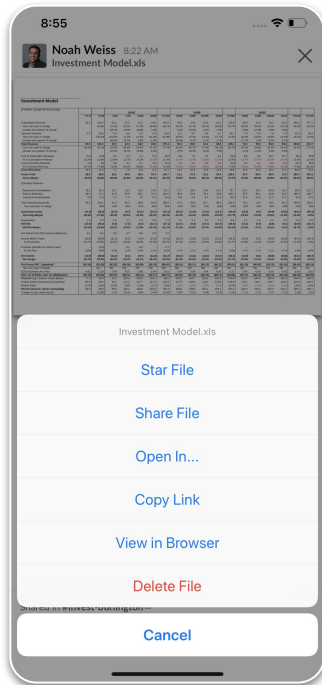
Allow your users to do work from anywhere and drive more adoption of Slack without sacrificing security



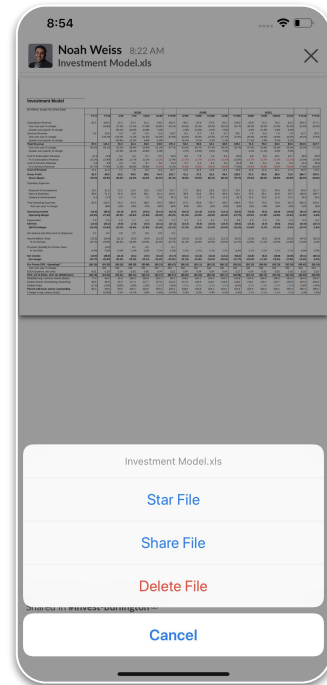
EMM @ Slack

Block files downloads and message copying on mobile devices

Ensure sensitive
corporate data is not
downloaded or shared
on unmanaged mobile
devices



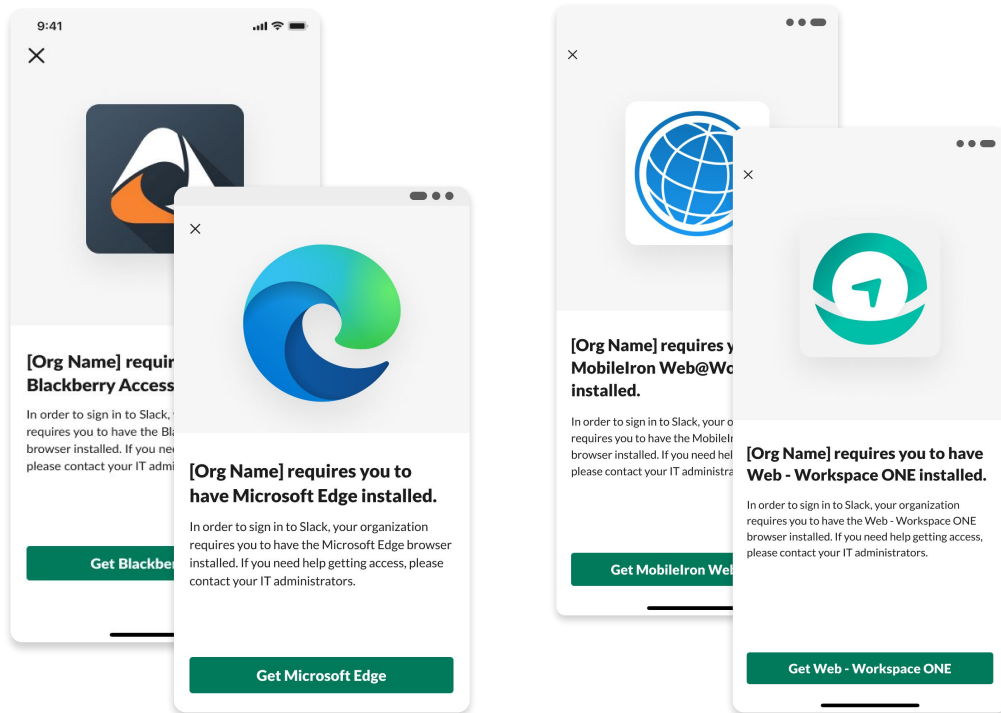
Feature disabled



Feature enabled

Default browser control

Control how Slack is used with the browser controlled by your EMM/MDM vendor

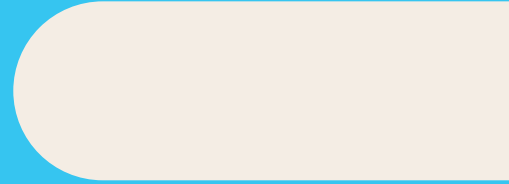


Compatibility

Slack integrates with several EMM providers via the [AppConfig community](#) as well as Microsoft Intune



Setting up EMM



Setting up EMM

Requirements for setting up EMM



Slack Enterprise Grid Subscription



Slack Enterprise Grid Sandbox Instance for Testing



EMM vendor Admin console



Slack for EMM application for iOS devices



Android for Work for Android devices



Slack AppConfig to be configured on EMM console

Configure who EMM applies to

Choose Configuration

When Enterprise Mobility Management is required, only users on approved devices will be able to access [REDACTED] on Slack.

☒ **Required for full members, but not guests**

All full organization members will be subject to Enterprise Mobility Management. Guests will be able to sign in from any device.

☐ **Required for everyone in the organization**

All full members **and** guests will be subject to Enterprise Mobility Management, and must use an approved device to access Slack.

☐ **Optional for all members**

Full members and guests can choose whether to enroll in Enterprise Mobility Management. Some Slack functionality may be limited on unmanaged devices.

EMM setup & rollout plan

1. [Customer] Org Owner reaches out to the CE/CSM team
2. [Customer] provides the message content, that will be sent to the end users
3. [Customer] identifies who EMM should apply to
4. [Customer] configures Slack for EMM app on the EMM portal
5. Slack enables EMM at the Org level
6. An email and a Slackbot message will be sent to the impacted users. This message contains the content provided in step 2
7. Users have **72 hours** to enroll the device into EMM and set up Slack for EMM portal

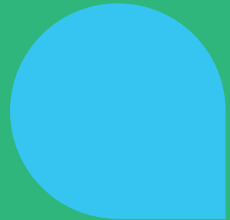
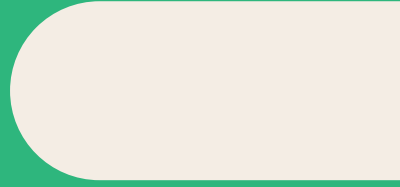


Once EMM is enabled, the message content cannot be modified or disabled.

Slack -> AppConfig values

1. Login to your EMM Admin Console
2. Enter a name for your configuration (this is for identification purposes)
3. Enter the configuration key **ApprovedDevice** and the corresponding value **SlackAppConfig**
4. To fast-forward users to directly sign on to the official corporate Slack, enter the configuration key **OrgDomain** and for the corresponding value, enter your org subdomain: (e.g. if your org Slack domain is acme.enterprise.slack.com, just enter **acme.enterprise**)
5. (Optional) If you want to restrict users from signing into non-company workspaces, enter the configuration key **WhitelistedDomains** and for the corresponding value, your org subdomain. (Note: you can currently only enter one value for this)
6. (Optional) If you want to disable copying and pasting messages from Slack, as well as restrict file downloads, enter the configuration key **DisableCopy** and the corresponding value **true** (or **false** to turn this off)

What happens next?



What happens next?

Immediate actions

- All users affected by the setting will get both a Slackbot message and email
- Within 72 hours, ALL mobile sessions will end for the affected users
- After 72 hours, no users from the affected setting will be able to access their org from an unapproved device
- The users can use the email at anytime (before or after the 72 hour cutoff) to find the link to the EMM Marketplace

What happens next?

Sample email message



Using Slack on mobile at [REDACTED]

Your organization ([REDACTED]) has updated its mobile security settings, to help keep all your work data secure. Starting on **April 24th at 4:09 PM** only approved mobile devices will be able to access Slack.

Details about how to set up your device are included below. You can also learn more about [mobile security](#) in Slack's Help Center.

A message from [REDACTED]:

Please refer to Acme's internal documentation at <https://wiki.acme.com/slack/emm-config> for detailed information.

Made by [Slack Technologies, Inc](#) • [Our Blog](#)

500 Howard Street • San Francisco, CA 94105 • United States

What happens next?

Sample Slackbot message



Slackbot 4:09 PM

Greetings! Your organization has updated its [mobile security settings](#), to help keep all your work data secure. Starting on **April 24th, 2019 at 4:09 PM PDT**, only approved mobile devices will be able to access Slack.

Details about how to set up your device are included below, and we'll also send you an email with this information, just in case.

A message from [REDACTED]:

Please refer to Acme's internal documentation at <https://wiki.acme.com/slack/emm-config> for detailed information.



Slack Help Center

[Enable Enterprise Mobility Management for your org](#)

Enterprise Mobility Management (EMM) — also known as Mobile Device Management — gives organizations control over how their company data is used and accessed on mobile devices. Step 1: Choose an E...



Confirmation of setup in admin console



Organization



Billing



Analytics



Security

SSO Configuration

SSO Preferences

Security

Mobile Security

Key Management



Settings

Mobile Security

Some organizations limit access to work software and data to approved mobile devices. If you use an enterprise mobility management tool, you can view your settings here.



Contact Slack to add or change your mobile security settings

Enterprise mobility management settings at the organization level require a two-step confirmation to ensure Slack is set up with your EMM tool correctly.

[Contact Slack](#) to change your mobile security settings.



Enterprise Mobility Management

Mobile Device Approval



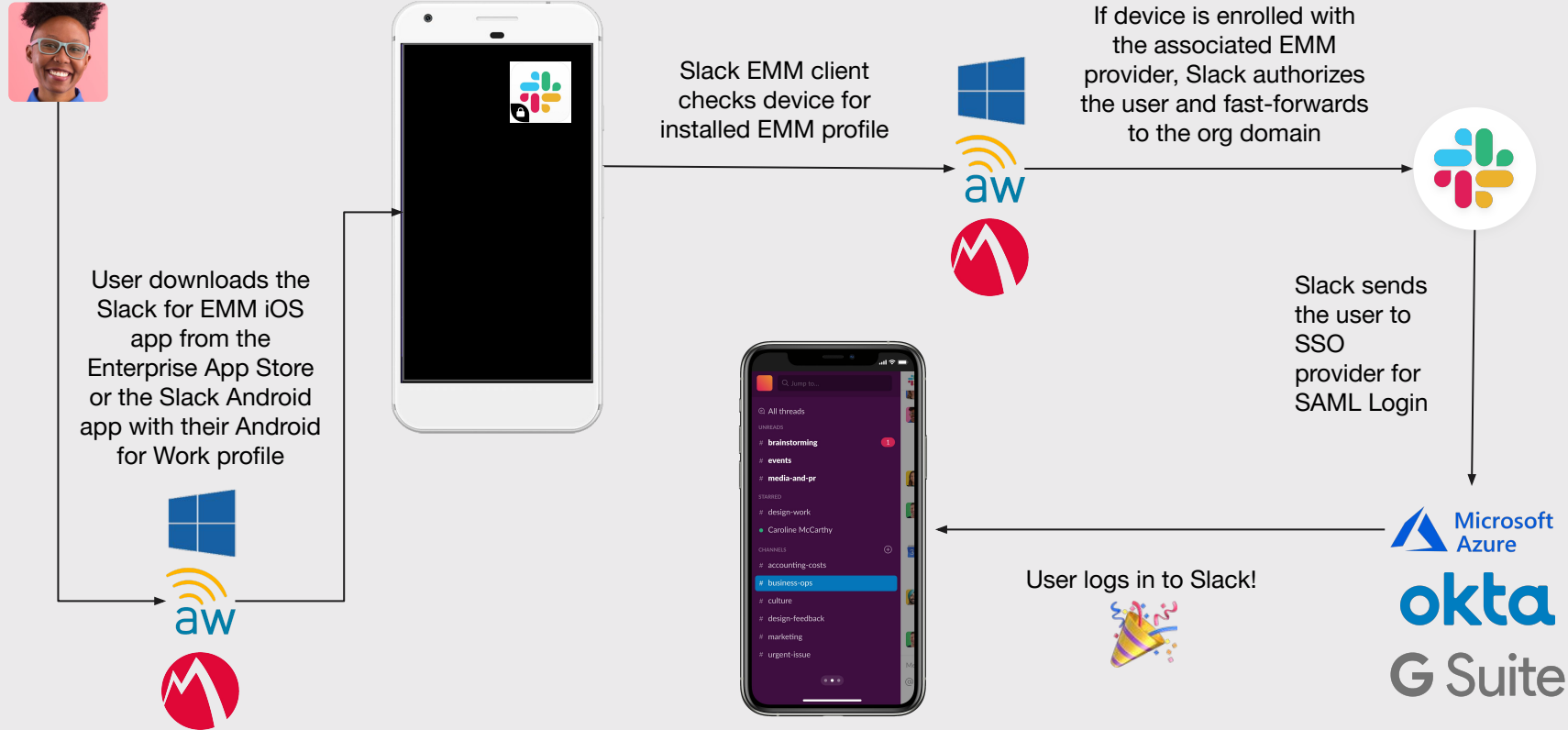
Required for all users, except guests

All users must use an approved mobile device, except guest accounts

How does it work?



How does it work on an approved device?



How does it work on an unapproved device?



Thank you!

Appendix

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