

IBM Security MaaS360



**With
Watson™**

Virtual User Group – To Be or Not BYOD

January, 2020

Agenda

- Virtual User Group Goals
- Topic: To BYOD or Not To BYOD
 - >> Vaishnavi Thotieam
Offering Management - IBM Security MaaS360
 - >> Dhanasekar Varadarajan
Offering Management - IBM Security MaaS360
 - >> Mitt Sharma
Offering Management – IBM Security MaaS360
 - Q&A
- Wrap Up & Resources

Virtual User Group Goals

- Collaboration
- Community
- Customer Advocacy
- Feedback

The Case for BYOD

Your employees want to use their own devices for work

- 59% of employees use personal devices at work [Tech Pro Research]

Let them work from anywhere, anytime with a bring-your-own-device (BYOD) policy

- Personal device use [...] saves employees *58 minutes per day*—a 34% increase in productivity! [Frost & Sullivan]



The Case for BYOD

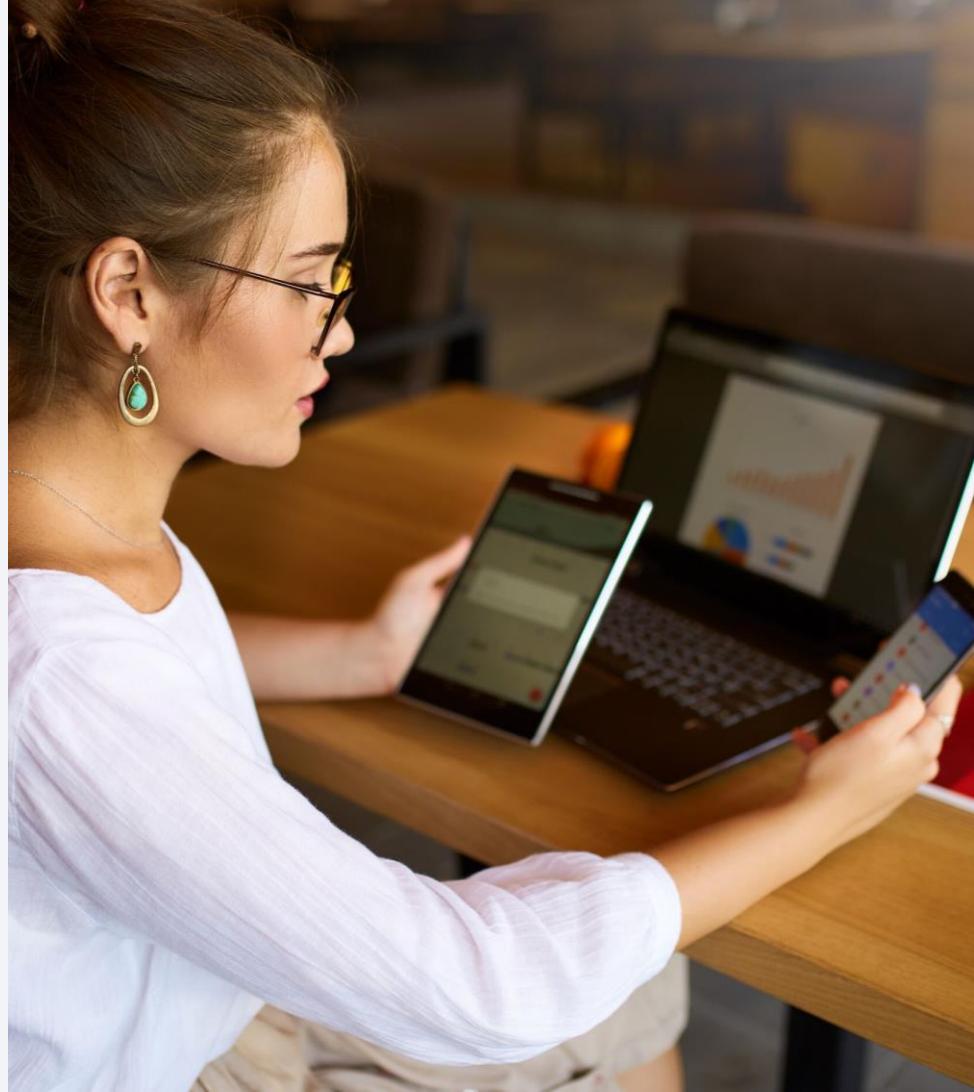
BYOD...

...boosts morale

More choice/new
technology
means employee
flexibility

...reduces cost

No IT spend on
procuring devices



Worried about BYOD in your organization?

87% of companies allow employees to access business apps on personal devices...
[Syntonic]

...but that doesn't mean it isn't a security risk.

We want to hear your concerns. **Take the survey!**

Current BYOD program issues



Device control

- Admin can control the entire personal device
- Can perform actions such as a full factory reset

Privacy problems

- Admin can see *all personal* apps installed
- Info such as UDID and carrier are visible to admins

No data separation

- No native partition between personal and corporate data
- Admins can end up wiping personal data along with corporate
- User confusion occurs over Apple/Android T&C, which presents privacy concerns to IT

BYOD with MaaS360

Inbuilt Security

Native containerization & DLP via Android Enterprise/iOS User Based Enrollment

Applications on Demand

Manage only corporate applications & container

License Management

Limit devices and device licenses per employee

Uniformity in experience

Deploy MaaS360 PIM, Browser & Content Suite for unified end user app experience within the native container

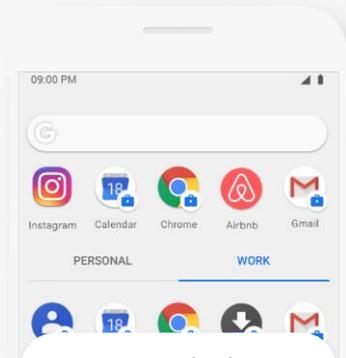


Android Enrollment Modes

Android Enterprise Enrollment Modes

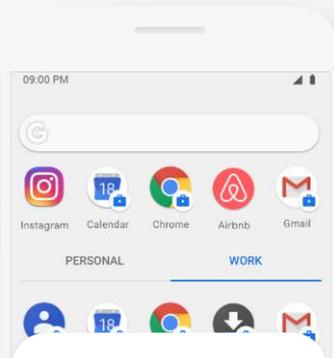
Personally-owned

Work profile



BYOD (PO)

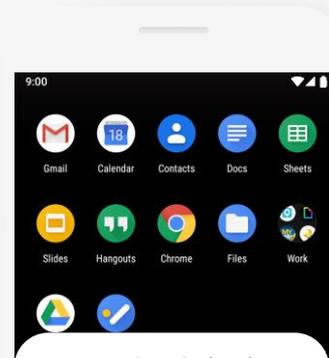
Fully managed device with work profile



Personally enabled (COPE)*

Company-owned

Fully managed device



Work only (DO)

Fully managed device in lock task mode



Dedicated Device (COSU)

*Available with MaaS360 in closed BETA

Android Enterprise (Profile Owner)

Native containerization

Dual persona for Personal and Work Profiles

Managed Google Play

Robust app deliver—silent installs & on-demand

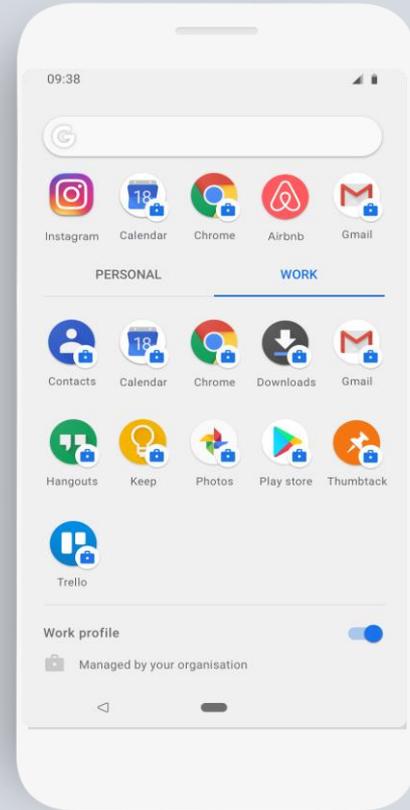
App Management

Private and alpha/beta publishing, no wrapping, managed config

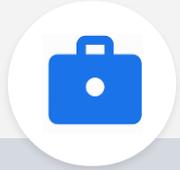
Device Management

Limit only to corporate apps and work container

Recommended to use on Android OS 7.0+



How to deploy Android Enterprise via MaaS360?



Setup AE

Bind your MaaS360 tenant to Android Enterprise using a service account (free)



Setup Device Policy

Configure Android Enterprise policy section within MDM policies



Setup Approved Apps

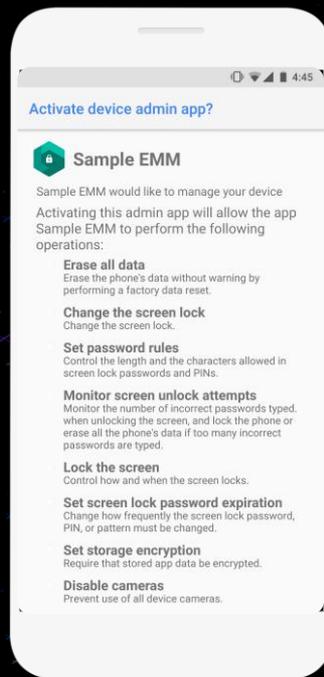
Select, approve, and distribute from a list of apps on the Managed Play Store



Allow Self-Enrollment

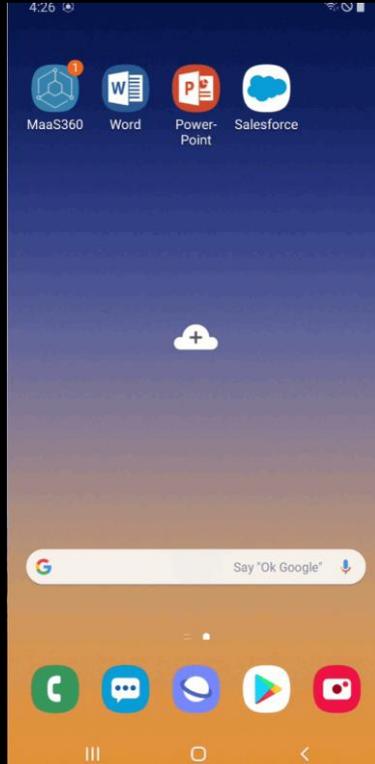
Allow users to self-enroll via employee credentials (enforce a minimum OS version)

Stuck with legacy
Android enrolled
via Device Admin?



Migrate to a work
profile with the
MaaS360 Migration
Tool!

Work Profile migration tool



Admin initiates "Migrate to Work Profile"

User navigates to "Migrate to Android Enterprise"

Device level policies are removed and restrictions apply to work profile

Work profile created

WiFi, email, and VPN moved to work profile

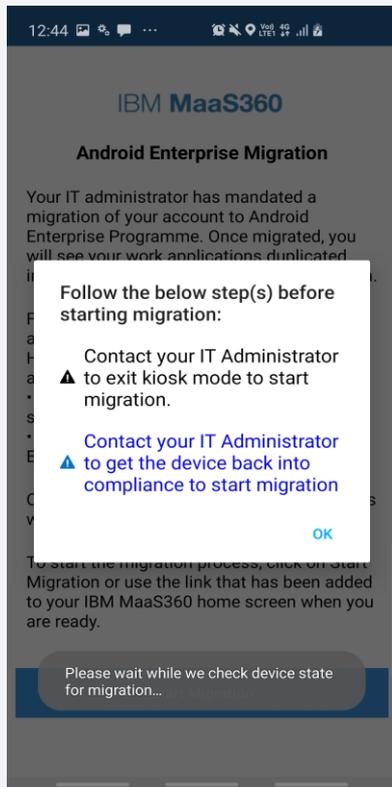
Apps removed and redeployed on work profile

MaaS360 app moved to work profile

MaaS360 Browser, Docs, User-created corporate docs, move to work profile

MaaS360 Email (if used) moves into Work Profile

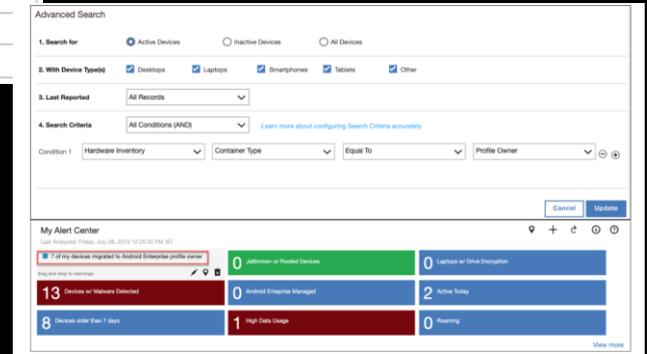
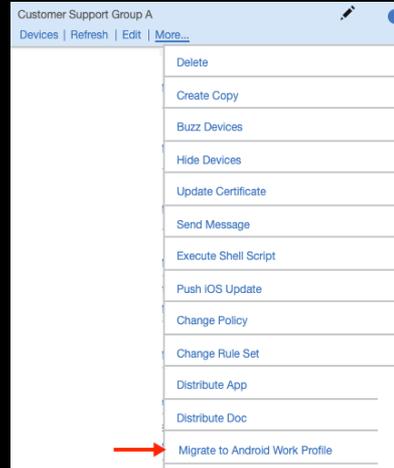
Pre-requisites for migration



- Device has battery charge of 30% or higher
- Device is connected to the internet
- Device is encrypted if running OS version < 7.0
- Device time & server time are synchronized
- Device Play Store Services are up-to-date
- If shared, should be on the sign-in screen
- Device is in compliance
- Device is not in a selective wipe state
- Device is not in kiosk mode

Schedule & track migration

- Prepare groups of devices with “Container Type = Device Administrator”
 - Create an Alert Center Watchlist
 - Send “Migrate to Work Profile” action
-
- Goal is to convert “Container Type = Profile Owner” for all migrated devices
 - As devices migrate, progress can be tracked in Global Action History with granular status.
 - Results can be exported into .csv or .pdf



Device Name	Platform	Device ID	Action Date	Action	Action By	Status
829357183-SM-G970W	Android	Android742b5d44e20313f	07/22/2019 15:22 EDT	Migrate to Work Profile	focus09p	Completed
DM17348-SM-G960U	Android	Androidca29e34b687be9	07/18/2019 07:48 EDT	Migrate to Work Profile	focus09p	Completed
455341008-SM-G975W	Android	Androidc3be84233ca4b27	07/16/2019 14:24 EDT	Migrate to Work Profile	focus09p	Completed

Jump To Page | Displaying 1 - 3 of 3 Records | Show 25 Records | Reset Filters | Customize Columns | CSV | Export

iOS Enrollment Modes

DEP Enrollment

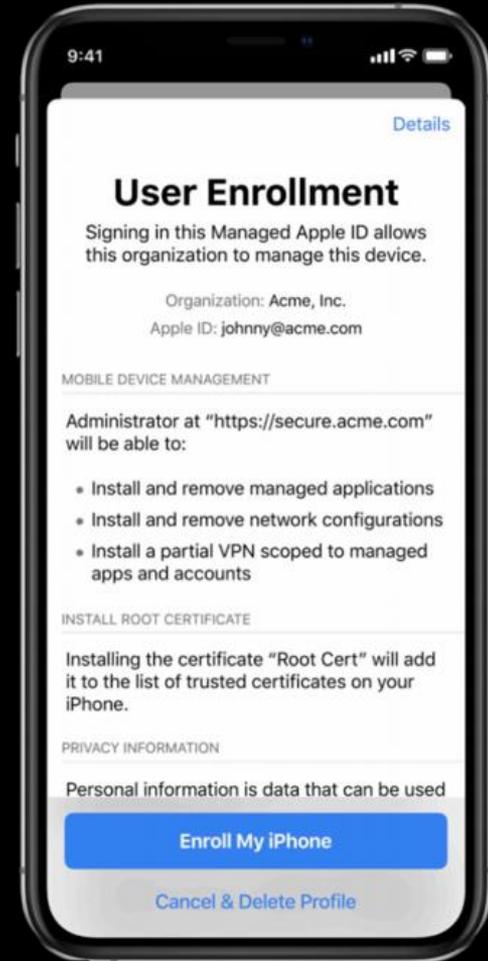
- Used in Corporate owned devices.
- Administrator gets additional device controls
- Device gets enrolled into MaaS360 upon boot-up and factory reset

Management Profile Enrollment

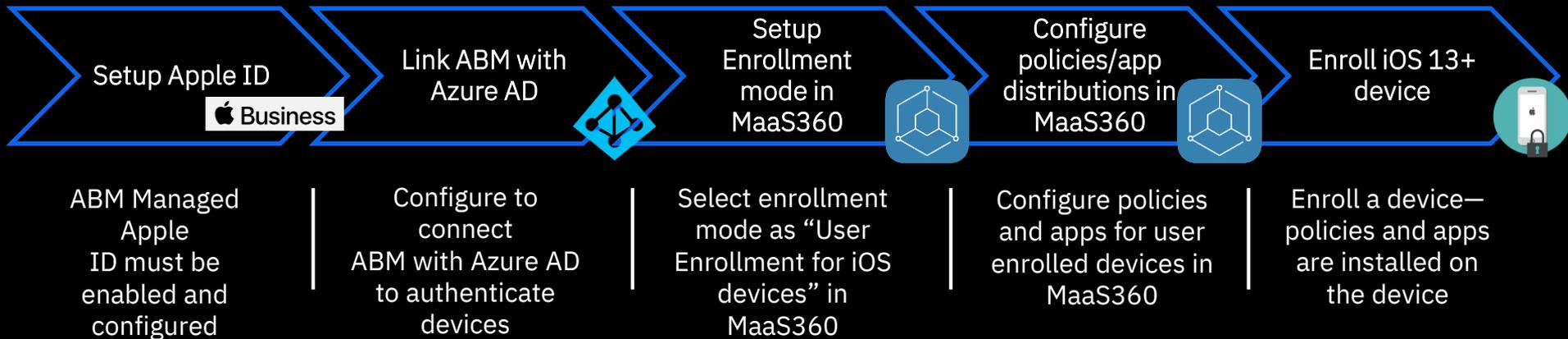
- Currently used in BYOD scenarios
- Administrator gets access to the whole device—not as extensive as DEP
- Device needs to be enrolled by the user manually; user can remove control

User Enrollment for iOS

- Separate disk partitions for personal and corporate apps
- Administrator cannot apps installed in personal partition
- Sensitive device information (UDID, CSN) is not visible to admins
- Secure way to distribute and install corporate apps
- Admins cannot perform actions (factory reset, reset passcode)
- Restrictions/policies apply to corporate file system and apps only
- Azure AD as managed Apple ID is used for enrollment



How User Enrollment works



Who needs iOS User Enrollment?

Organizations who...

- *...want to enable employees' personal devices for corporate use*
- *...need to secure corporate apps and content*
- *...would like to limit the amount of devices employees need*
- *...aim to reduce IT spending on employee devices*
- *...deal with employee privacy concerns*



iOS User Enrolment Launch

GA Target Date

End of Q2 2020

Q & A

Resources

MaaS360 Security User Community:

<https://community.ibm.com/community/user/security/communities/community-home?CommunityKey=9d8b7835-e47a-4850-b400-d8c77708af84>

MaaS360 Resources

- [MaaS360 Product Hub](#)
- [IBM MaaS360 Login](#)
- [MaaS360 Support Home](#)
- [IBM Security Request for Enhancement Community](#)
- [IBM MaaS360 Knowledge Center](#)
- [IBM MaaS360 Security Learning Academy](#)
- [Develop a MaaS360 Integration](#)
- [IBM Security Product Notifications Subscription](#)
- [IBM VIP Rewards for Security](#)

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.