IBM Security MaaS360

With Watson™

Frank Gentile

Virtual User Group – To Be or Not BYOD

January, 2020

IBM **Security**

IBM

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

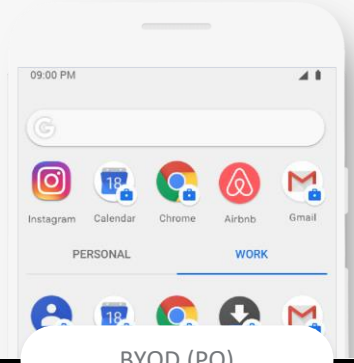
Android Enrollment Modes

Android Enterprise Enrollment Modes

Personally-owned

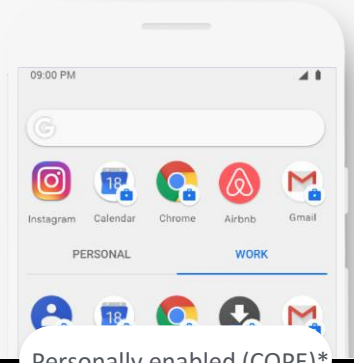
Company-owned

Work profile



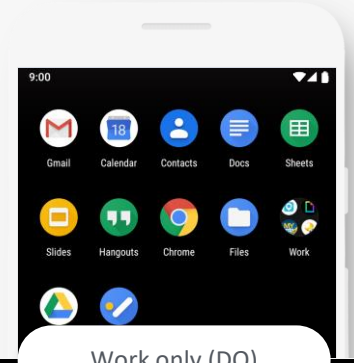
BYOD (PO)

Fully managed device with work profile



Personally enabled (COPE)*

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)

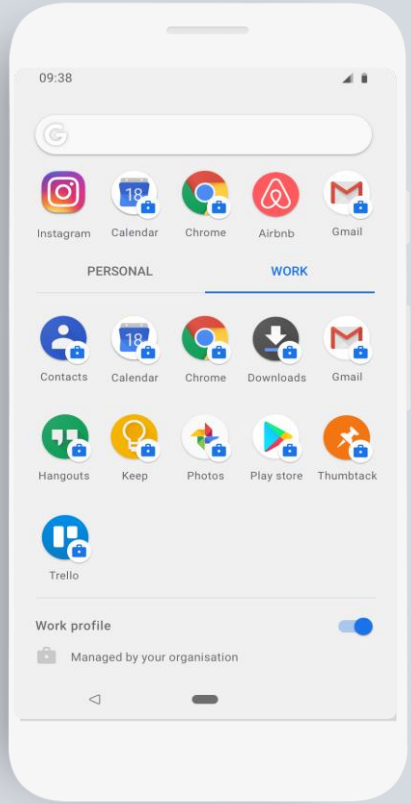
Native containerization
Dual persona for Personal and Work Profiles

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

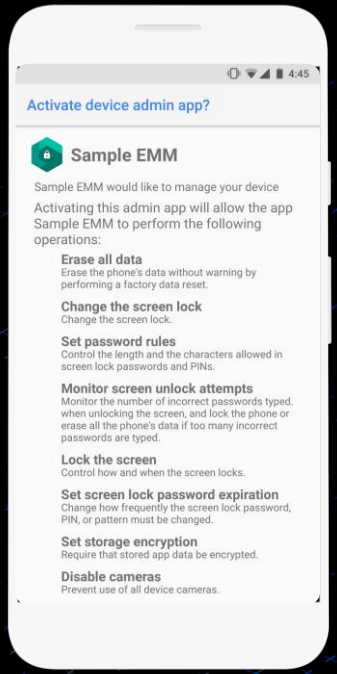
Setup Approved Apps

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

Allow Self-Enrollment

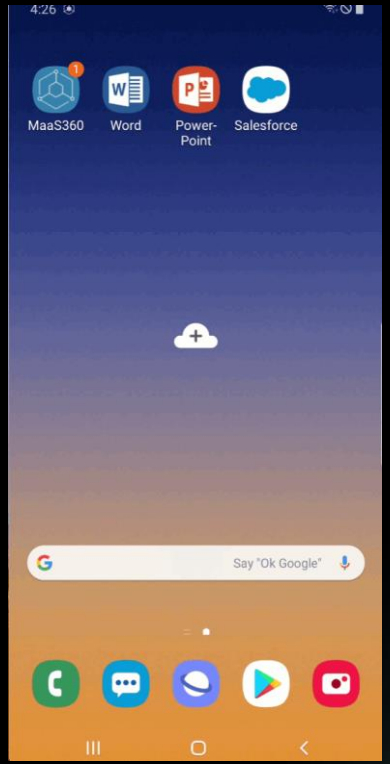
Allow users to self-enroll via employee credentials (enforce a minimum OS version)

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

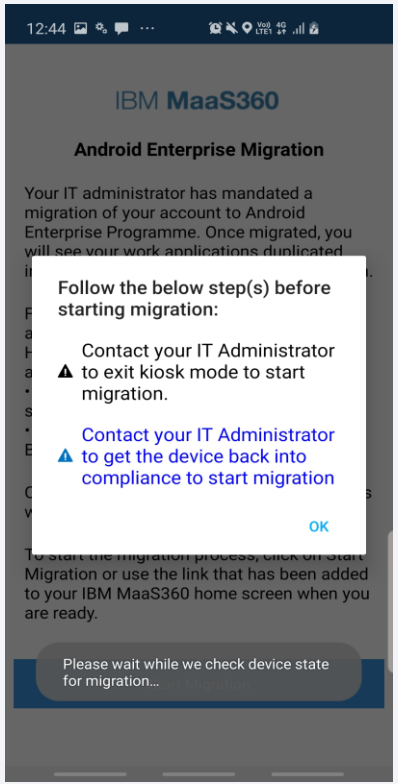
- WiFi, email, and VPN moved to work profile
- Apps removed and redeployed on work profile

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

Supported on Android OS 5.1+ | MaaS360 for Android app 6.70+ | G-Suite (optional)

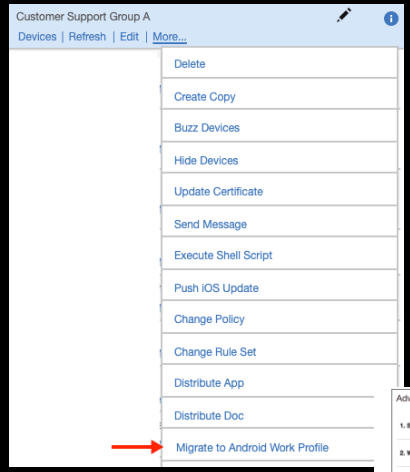
Pre-requisites for migration

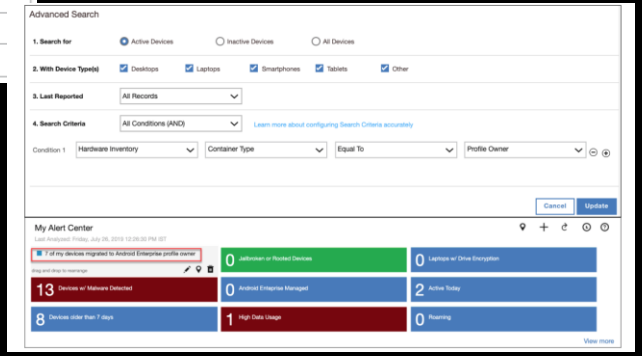


- Device has battery charge of 30% or higher
- Device is connected to the internet
- Device is encrypted if running OS version < 7.0
- Device time & server time are synchronized
- Device Play Store Services are up-to-date
- If shared, should be on the sign-in screen
- Device is in compliance
- Device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

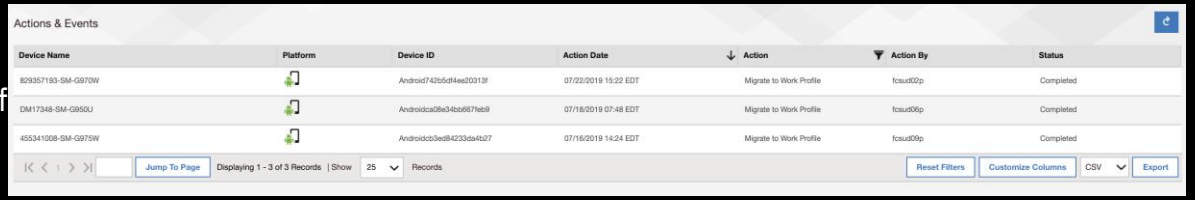
Schedule & track migration

- 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



iOS Enrollment Modes

DEP Enrollment

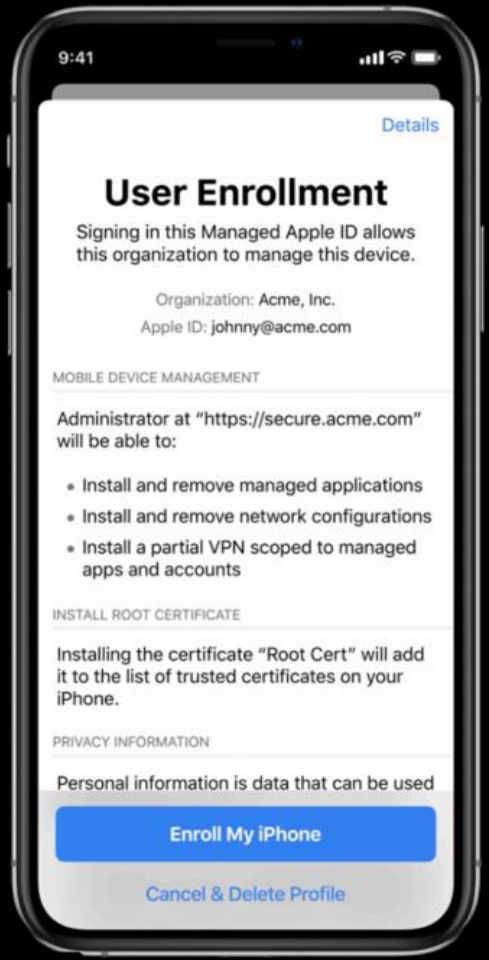
- Used in Corporate owned devices.
- Administrator gets additional device controls
- Device gets enrolled into MaaS360 upon boot-up and factory reset

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

ABM Managed Apple ID must be enabled and configured

Configure to connect ABM with Azure AD to authenticate devices

Select enrollment mode as “User Enrollment for iOS devices” in MaaS360

Configure policies and apps for user enrolled devices in MaaS360

Enroll a device—policies and apps are installed on the device

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

youtube/user/ibmsecuritysolutions