

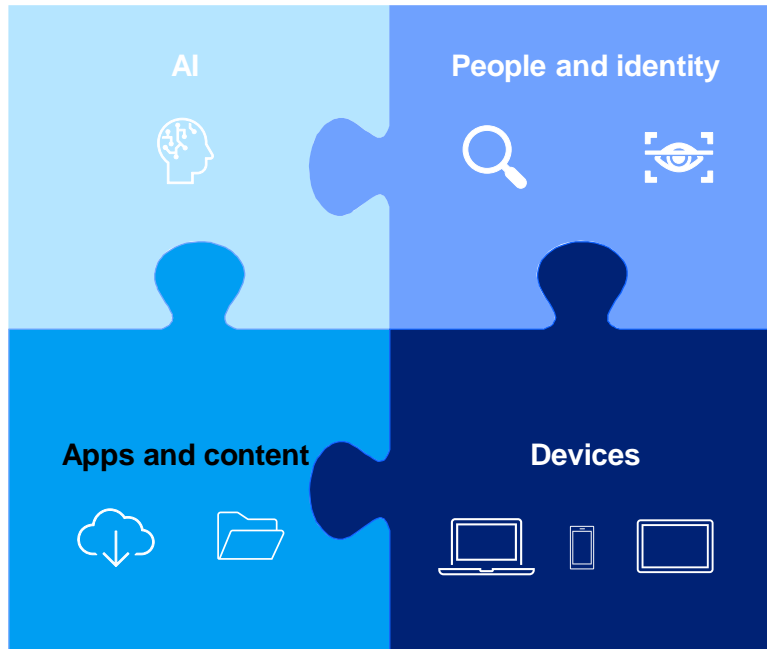
MaaS360 – Non GMS Device Management

—
Dhanasekar Varadarajan
Senior Product Manager, IBM MaaS360
IBM Software



IBM Security MaaS360 with Watson

Unifies, secures, and manages devices and users



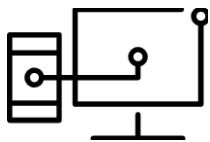
Unified Endpoint Management

- Provide best in class UEM/Modern Management coverage across all endpoints
- Enable co-existence with traditional endpoints management tools for laptop/desktop management
- Enable support for purpose built and industry focused use cases
- Expand admin and enable end user experience management
- Expand Device, App and end user Analytics and Automation

Zero Trust Endpoint Security

- Expand security detection, prevention and response on mobile endpoints
- Expand Security Analytics to enable response based on User and Device risk posture
- Enable Zero Trust and XDR use cases via integrations with IBM Security stack

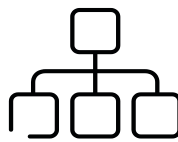
What sets IBM MaaS360 with Watson apart?



Complete UEM
of mobile devices,
laptops & things



Best-in-class cloud
on a mature, trusted
platform



**Open
platform**
for integration with
leading IT systems



**Industry-best user
interfaces**
for app catalogs & workplace
container



**Dedicated to your
success**
with 24x7x365 support by
chat, phone, email



**With
Watson™**

for actionable insights &
cognitive analytics



Fast deployment

Simple, self-service provisioning
process designed for maximum
configurability

Effortless scalability

Trial instantly becomes production
environment with ability turn up new
devices, users, apps

Automatic upgrades

Continuously updated daily with new
capabilities and same day OS support for
the latest platform

What is a Non-GMS Device?

- Android devices that does not have access to Google APIs (Non-GMS)
- Android devices that are in countries where Android Play Store is not available
- Built from Android Open Source Project (ASOP) for specific use-cases
- Few of Non-GMS examples
 - RealWear
 - Amazon FireOS devices
 - Santok



Industries and Examples

- A manufacturing company uses a wearable device to take snapshot of manufacturing errors
- A healthcare company that gives Android devices to its trial participants to track the progress of medicine trial.
- A non-GMS device is used in meeting rooms for video conferencing and show the room booking information.
- A company in China that uses the Android devices for its employees' mail access. Android play store is not available in China



Enrollment Modes

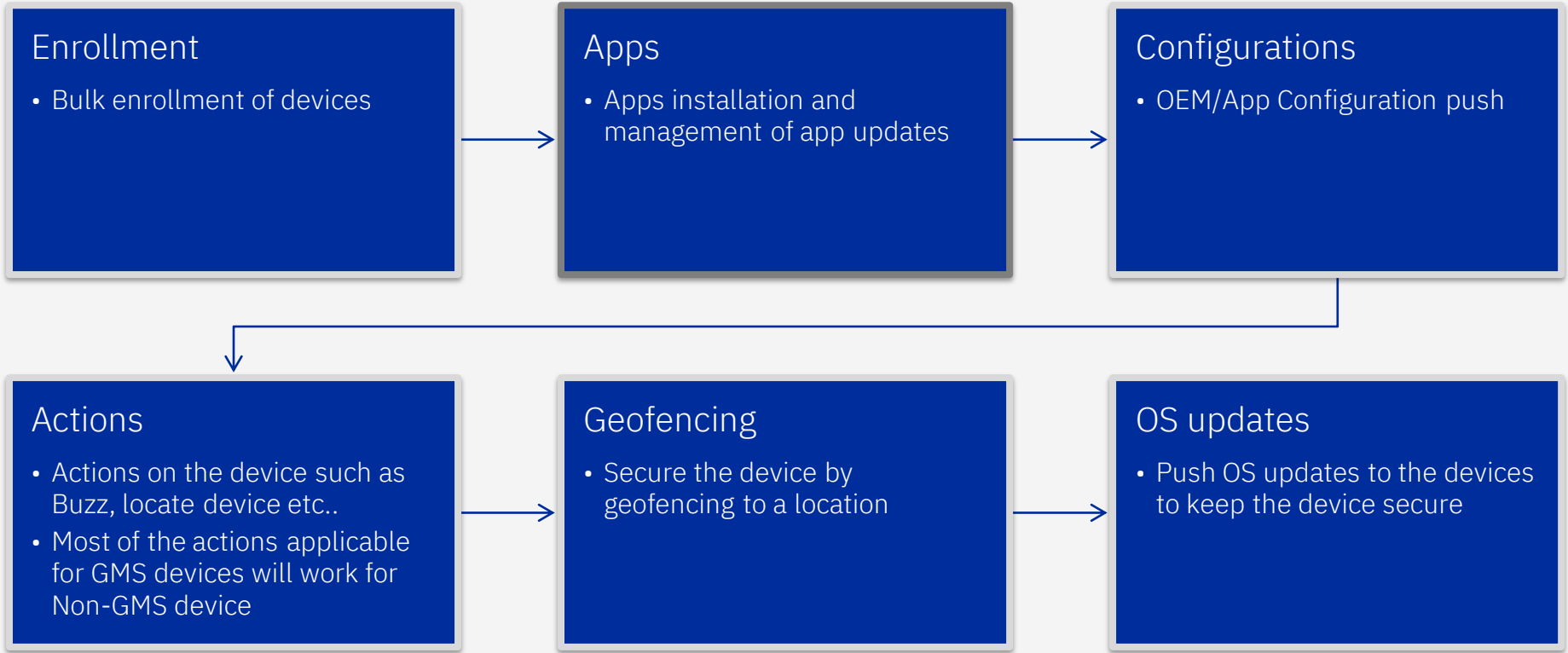


QR Code Based Enrollment

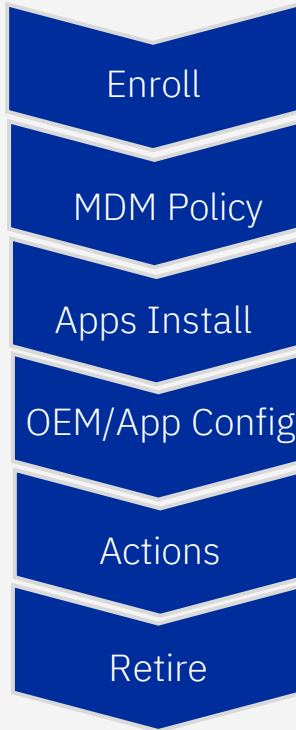
adb devices	lists connected devices
adb root	restarts adbd with root permissions
adb start-server	starts the adb server
adb kill-server	kills the adb server
adb reboot	reboots the device
adb devices -l	list of devices by product/model
adb shell	starts the background terminal
exit	exits the background terminal
adb help	list all commands
adb -s <deviceName> <command>	redirect command to specific device
adb -d <command>	directs command to only attached USB device

ADB Command

Use-cases for Non-GMS Devices



Example – RealWear Devices

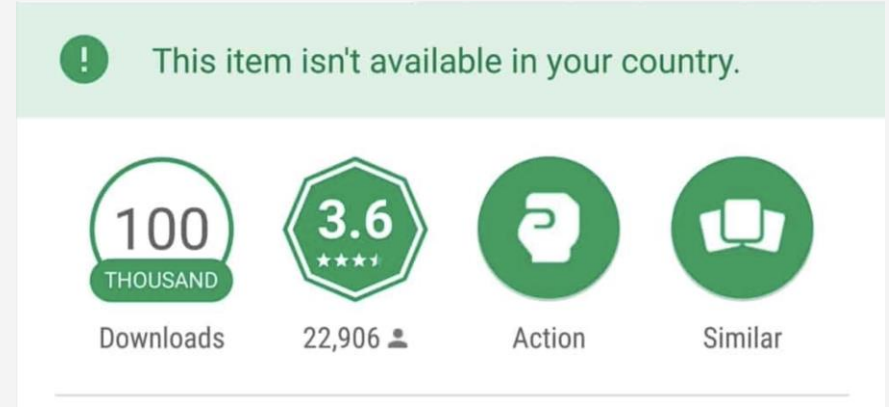


Difference between Non-GMS and GMS

Enrollment	MDM Policy	OEM/App Config	App Distributions	Notifications
<ul style="list-style-type: none">• Supports only QR Code and ADB enrollments	<ul style="list-style-type: none">• MDM policies are applied to the device through MaaS360 app	<ul style="list-style-type: none">• Configurations are pushed directly to the OS directly through MaaS360 app	<ul style="list-style-type: none">• Enterprise apps distributions and installation are supported• MaaS360 App Catalog can be used by users for installation of enterprise apps	<ul style="list-style-type: none">• Device heartbeat is used to let the device know for waiting commands

Non-GMS Device Countries

- There are countries where Play Store and Google Services are not available
- For example, China does not have Play Store
- MaaS360 app is pushed to the device from CDN directly for enrollment.
- Google server-side APIs are not used and instead all device APIs are used as alternative.



How it works?

Enrollment

Android Enterprise QR Code Provisioning

Enrollment Settings

Wi-Fi Settings

Corporate ID

MaaS360

Android Enterprise mode

☐ Device Owner (DO) mode

☐ Work Profile on Corporate Owned

☒ Device Owner without Google Managed Services (Non-GMS)

Ownership

☒ Corporate Owned

☐ Corporate Shared

Enrollment Email ID

For bulk enrollments using device account, specify a common email address

Username

For bulk enrollments using device account, specify a common username


Password

Domain

Back

Next

Device Detail


 a [redacted]

Summary ▾

Locate

Message

Hardware Inventory

Username	[redacted]	Email Address	[redacted]@k.com
Operating System	Android	Manufacturer	samsung
Model	SM-N960F	IMEI/MEID	[redacted]243
Device ID	AndroidUser26062112330	Ownership	Not Defined 
Device Enrollment Mode	Android Debug Bridge	Container Type	Device Owner - Non GMS

Enterprise App Addition

Enterprise App for Android

Available forAll

App Details

Policies and Distribution

Wrapping Configuration

Wrapping and Signing

Advanced

App*

Upload .apk file

Browse

Provide URL

Description

Up to 10000 characters.

Enter App Description

Category

Enter Comma Separated Categories

Screenshot(s)

Browse

Attach More

Review App for Risk Management

☐

Cancel

Add

App Configurations Upload



IBM Wearable [↗](#)

App: IBM Wearable Platform: Android Last publish: -

Configuration

Distributions

Note:

- 1. Configurations for Gmail, Exchange, Active Sync or other VPN apps will override similar settings distributed to devices by Android MDM policy.
- 2. Custom attributes like username(%username%), domain(%domain%) etc. can be used to configure following settings.
- 3. Configurations of type bundle array are supported on Android 6.0+ only.

Upload XML template file

Max file size is 500kb. Supported file types are .xml

Upload

Configuration settings

Base URL Base URL	<input type="text"/>
Username Username	<input type="text"/>

Cancel

Save as draft

Next

Device Heartbeat

Policies / Workshop MDM Policy (Test)

Workshop MDM Policy (Test)

Published Type: Android MDM Version: 2 Last published: Apr 21, 2022 1:21 PM

Configure settings Review changes Assignments

- ActiveSync
- Wi-Fi
- VPN
- Certificates
- Browser
- COSU (Kiosk mode)
- Wallpapers
- System Update Settings
- Device Management**
- Trusteer Threat Management

🔍 Search		
Data Collection Frequency (in Minutes) Reducing this will increase battery usage on the device. Minimum allowed value: 60 mins Android 5.0+ (PO & DO)	240	- +
Device Heartbeat Frequency (in Minutes) * Reducing this will increase battery usage on the device. Minimum allowed value: 15 mins Android 5.0+ (PO & DO)	15	- +
Use strict scheduler for device heartbeat and data collection. Enabling this will drain more device battery due to frequent alarms on device. Strict scheduler for data collection is supported from Agent version 7.60 and above. Android 5.0+ (PO & DO)	<input type="checkbox"/>	
Usage Data Collection Frequency (in Minutes) * Reducing this will increase battery usage on the device. Minimum allowed value: 15 mins Android 5.0+ (PO & DO)	15	- +

Others..

Limitation

- Realtime notifications to the device
- Currently it depends on heartbeat frequency

How to Enable?

- Reach out to support to enable this feature

Thank you

<https://www.ibm.com/maas360>

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

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

youtube.com/ibmsecurity

© Copyright IBM Corporation 2022. 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 *[insert other IBM trademarks listed on the [IBM Trademarks List](#)—and use serial commas]*, are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

