

Android Enterprise Best Practices

White Paper



Contents

Introduction	3
What is Android Enterprise?	3
Researching Suitable Hardware.....	4
Choosing Android Enterprise Features	4
Work Profile.....	5
Fully Managed Device	6
Recommended Policies for Android Enterprise	7
Work Profile.....	7
Fully Managed Device	8
Password Policies	10
Recommended App Management.....	11
Importing Apps & App Updates.....	12
Configuring Applications	12
Conclusion	12

Introduction

We have prepared a detailed set of tips and recommendations to help you choose, configure and manage devices with **Android Enterprise**. Included in this white paper are three sets of different device policy recommendations that are ready for you to implement, offering varying levels of usability and security.

Also inside is a tip if you want to use hardware that is not on the Android Recommended list, a summary of the advantages and disadvantages of Android Enterprise's features, and a further selection of configurations and guidelines for best practice app management. All of these recommendations, based on our experience in Enterprise Mobility Management, can be easily integrated using a compatible MDM/MAM solution, such as Cortado MDM.

What is Android Enterprise?

The total share of devices running Android remained a dominant 85% in 2018¹. While there may be contrasting studies showing that 82% of mobile enterprise use takes place on iOS², it is safe to assume that the integration of Android devices into enterprises will accelerate in the future.

Android Enterprise, the Google-led initiative previously known as Android for Work, will likely contribute to this shift. It describes a collection of MDM tools and APIs (application programming interfaces) that were gradually released after 2014 and are now found on all devices that meet Google's Android compatibility requirements – i.e. classified as Google Mobile Services (GMS) certified. With Android Enterprise, IT admins have greater control over enterprise devices, allowing for instance the easy separation of personal and work-based data across the fleet.

Originally, Android APIs were not included with the operating system, leaving Android less manageable in terms of providing room for EMM platforms to manage devices that matched the demands of enterprises. The collection of MDM features in Android Enterprise now includes a common set of device management APIs and complements existing EMM-solutions within companies. Selecting Android enterprise devices is now easier, and two main features – “Android Work Profile” and “Fully Managed Device” – will be explained in greater detail below.

¹ International Data Corporation (IDC). (2018). Smartphone Market Share. Retrieved from International Data Corporation: <https://www.idc.com/promo/smartphone-market-share/os> (08.02.2019)

² Evans, J. (2017, August 30). Apple's iOS dominates enterprise mobility, data shows. Retrieved from Computerworld: <https://www.computerworld.com/article/3220988/apple-ios/apples-ios-dominates-enterprise-mobility-data-shows.html> (08.02.2019)

Researching Suitable Hardware

If Android is to be operating system of choice in your enterprise, you will have to consider what hardware to use. You might already have your preferences, but we ask you not to be biased. Unlike the iOS ecosystem, the OEM partners of Google change certain aspects of the Android operating system that is used in their hardware product lines, leading to a fragmentation and possible incompatibility with MDM systems. This circumstance should be a strong motivator to take a closer look at certain things when ordering new Android Hardware.

Luckily, Google offers a decision aid called **Android Enterprise Recommended**. On this website, a complete list of Android hardware with a compatibility guarantee for Android Enterprise can be found. Additionally, you can find out what Android Enterprise Features you can use with specific hardware.

We know that some devices are compatible even though they not included on the list. If there is a need to implement a device that is not on the Android Enterprise Recommended list, you can contact us at Cortado Mobile Solutions and ask us if we have experience with that particular hardware. Please understand, however, that we can only speak from experience and cannot predict (or guarantee) device behavior when OS updates arrive for them. Thus, it is best to stick to the Enterprise Recommended lists whenever possible.

Choosing Android Enterprise Features

As mentioned above there are currently two main Android Enterprise features called “Work Profile” and “Fully Managed Device”. These two features are mutually exclusive, meaning, that you can only select one of these features on each device.

These features are enabled by enrolling the device in different ways. We have assessed each of them and looked at how they are activated, what makes them unique, what their advantages and drawbacks are and what our recommendation is – depending on typical use cases.

Work Profile

Android's Work Profile is activated by enrolling a compatible Android device without any further preparation by using the Fast Enrollment Feature (QR-Code, Self Service Link, etc.).

What makes this feature unique is that a device configured with the work profile will have a private and a business container. These containers are decoupled from one another but are presented to the user in the same GUI.

As the admin you will be able to:

- › push configurations (like Exchange Mail Configurations)
- › push applications from the Play Store
- › distribute APKs (like Microsoft Word or an application that your organization has developed) over the Managed Google Play Store
- › push security policies to this business container

In order to make it easier for the end user to distinguish business from private apps, apps that you pushed to the business container will be marked with a little suitcase. Some security policies, like password restrictions (i.e. setting a min. length for a device's lock screen pin) will be used for the whole device. In general, though, your degree of control will be limited here to the business container.

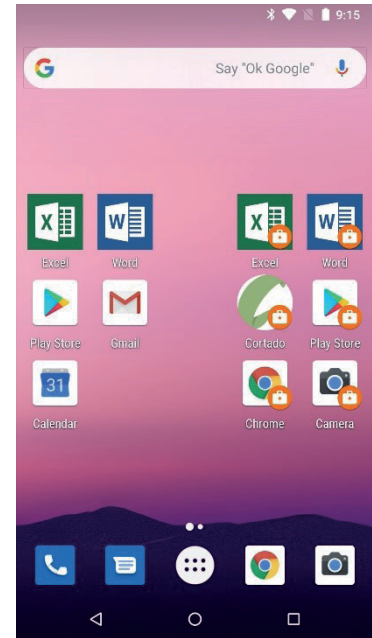


Fig.1 Android Work Profile

Work Profile Advantages:

- › No need for further preparation on the device
- › Good compatibility for Android Devices running Android 5.1.1 and newer
- › Business content is safely encapsulated within the business container (suitable for GDPR in the European Union, explained in more detail in [this white paper](#))
- › End users can use their private devices to work with business data securely and without having to change their private apps or settings, which makes on-boarding and off-boarding devices easy.
- › End users can continue to use WhatsApp in the private container without putting business contacts at risk

Drawbacks:

- › Scope of control is limited to the business container
- › No option to deactivate the installation of third-party apps in the private container, which can be a security risk and needs to be countered by improving user awareness. Although the risks of compromising the work profile via rogue apps in the private container are very slim, this aspect needs to be considered.
- › End users can delete the work profile and change connection settings for Wi-Fi/VPN, which could increase help-desk workload

Android Enterprise Best Practices

Work Profile is recommended for the following scenarios, if:

- you think your end users are at least somewhat aware of the risks involved in manually activating developer options and installing applications from non-official stores
- you have a good idea of what android devices your end users are using and know that they are compatible
- your end users have a strong desire to use their own personal devices for work purposes.
- your end users are using WhatsApp or other messengers that usually sync contact details to unsanctioned cloud providers

Fully Managed Device

The second main Android Enterprise feature is called Fully Managed Device. It is important to bear in mind that some preparations are needed before activating this feature. For one, you will need to do a factory reset on every device you would like to set up in this mode. Check out [our manual](#) regarding what enrollment options we support from that point forward.

What distinguishes this feature from the work profile is that there is no longer any private space on the device. The whole device and its manageable functions are controlled by the MDM admin, hence the name “Fully managed device”.

Advantages:

- You have extended, in-depth control over the mobile device
- Many security features are available to harden the device against attacks (i.e. no manual installation of non-market apps anywhere on the device)
- Manual (mis)configuration of settings (like Wi-Fi, etc.) can be disabled by the admin

Disadvantages:

- Fully Managed Devices are not suitable for BYOD scenarios
- Since there is no separation through containers, the use of apps such as WhatsApp is not recommended

Fully Managed Device is recommended in the following scenarios, if:

- You have end users that are new to smartphones or who may lack the experience needed to make appropriate judgments regarding device security
- You have high security requirements that requires you to sacrifice some end user freedom
- You have a fleet of company owned devices or you are about to order devices that should be used for specific, narrow purposes without allowing any, or very limited, private use.
- You do not use Facebook/WhatsApp in a corporate context

Recommended Policies for Android Enterprise

After choosing your devices, Android Enterprise feature and enrollment method the next step is determining what policies you want to enforce on them. Choosing policies for your Android devices should be done carefully. Please do not forget that dissatisfied end users are more likely to try to circumvent your measures if you configure mobile devices solely for optimal security, and that the resulting shadow IT is real problem for many companies.

We put together 3 sets of Android policies that make sense in different circumstances. The first will favor usability over maximum device lock down, the second favors a balanced approach and the last set is a no-compromise security set that utilizes all available measures to increase the security of an Android Device. Since the available policy APIs differ between the Android Enterprise features Work Profile and Fully Managed Device, we also grouped them accordingly.

Work Profile

Policy	Usability Focus	Balanced	Security Focus
Camera	On	On	On
Modify Accounts	On	Off	Off
Chrome	On	On	Off
Cross-profile Copy & Paste	Off	Off	Off
Google Play Store	On	On	On
Installation of Non-market Apps	Off	Off	Off
Screen Capture	On	Off	Off
Skip First-time User Hints	Off	Off	Off
Display Caller ID Information	On	On	On
Allow Parent Profile App Linking	Off	Off	Off
Bluetooth Contact Sharing	On	On	Off

Android Enterprise Best Practices

Policy	Usability Focus	Balanced	Security Focus
System Behavior for App Permissions	Auto Grant	Auto Grant	Prompt
Display Contacts Search	On	On	On
Fingerprint	On	On	On
Trust Agents	Off	Off	Off
Unredacted notifications	On	Off	Off

Fully Managed Device

Policy	Usability Focus	Balanced	Security Focus
ADB	Off	Off	Off
Auto Time and Date	On	On	Off
Auto Time Zone	On	On	Off
Data Roaming	On	Off	Off
USB Mass Storage	On	Off	Off
Location mode	Off	Off	Off
Wi-Fi Sleep Policy	Default	Default	Default
Config Bluetooth	On	On	Off
Config Cell Broadcasts	On	Off	Off
Config Credentials	On	Off	Off
Config Tethering	On	Off	Off
Config VPN	On	On	Off
Config Wi-Fi	On	On	Off

Android Enterprise Best Practices

Policy	Usability Focus	Balanced	Security Focus
Apps Control	On	On	Off
Ensure Verify Apps	On	On	On
Install Apps	On	On	On
Install Unknown Sources	Off	Off	Off
Uninstall Apps	Off	Off	Off
Lock Screen Disable All Features	Off	Off	On
Lock Screen Secure Camera	On	Off	Off
Lock Screen Secure Notifications	On	Off	Off
Adjust Volume	On	On	On
Debugging Features	Off	Off	Off
Factory Reset	On	Off	Off
Master Volume	On	On	On
Microphone	On	On	On (Off)
Mount Physical Media	On	On (Off)	On (Off)
Android Beam	On	Off	Off
Outgoing Calls	On	On (off)	On (Off)
Share Location	On	On	On
SMS	On	On (off)	On (off)
USB File Transfer	On	Off	Off
Stay On			Never
Changes to Wi-Fi	On	On	Off

Android Enterprise Best Practices

Policy	Usability Focus	Balanced	Security Focus
Network reset	On	Off	Off
Safe Boot	Off	Off	Off
Status bar disabled	Off	Off	Off
Add user	Off	Off	Off
Remove User	Off	Off	Off

Password Policies

Policy	Usability Focus	Balanced	Security Focus
Force Password	On	On	On
Password Type	Device	Work Profile	Work Profile
Password Strength	Simple Password	Simple Password	Complex Password
Minimum password length	4	6	8
Minimum letters	N/A	N/A	1
Minimum lowercase letters	N/A	N/A	1
Minimum numeric characters	N/A	N/A	1
Minimum symbolic characters	N/A	N/A	1
Minimum uppercase letters	N/A	N/A	1
Password expiration	None	365	180
Maximum failed logins	10	10	10
Password history	N/A	5	10
Auto lock period (min)	5	1	1

Recommended App Management

Android Enterprise makes it easy to manage business applications. Combined with the app management features of **Cortado MDM**, the process of adding new applications to your application pool, from which you can assign and rollout software to the end users' devices, is further simplified.

Android Enterprise allows us to customize this process further, so it is both more convenient, reliable and secure when it comes to updating applications.

Recommended Apps

Before you add new applications to the pool, consider a few things first. Whenever possible we suggest you use applications from trusted, well known developers. Some text editors or open-source office programs might be free to download but often come with ads or in-app purchases that are detrimental to user experience and the security of the device.

This set up has proven to be sufficient for the everyday tasks of a mobile workforce:

Purpose	Recommended App
Email	Gmail or Nine Work or IBM Verse
Contacts	Google Contacts or Stock Contacts App
Calendar	Google Calendar or Stock Calendar App
Text Editing	Google Docs or Microsoft Word
Presentations	Google Slides or Microsoft PowerPoint
Spreadsheets	Google Sheets or Microsoft Excel
Browser	Google Chrome
PDF	Google PDF Viewer or Adobe Acrobat Reader
Camera	Open Camera

Please note: If you want to use pre-installed apps on the device you need to make sure that those stock applications are able to do what you want. For example, not every Stock PIM App allows bidirectional sync. Some Google Applications might not be compatible with every device, so you will not be able to roll out these applications and will need to fall back to either stock apps or alternatives. If you need guidance, please do not hesitate to contact us.

Importing Apps & App Updates

When approving Android applications, you will get the option to set up how the application and the Cortado MDM should behave in case there is an update to the application asking for a new app permission. In this case, the best option is keeping the app approved. If you have a very controlled environment you can opt for revoking the approval, however, since we recommend a small number of apps from trusted sources that update apps regularly this might be a bad tradeoff and requires you to regularly reapprove the app manually.

In any case we recommend making use of email notifications to a monitored admin inbox whenever there is an update for an app that requires additional permissions.

Configuring Applications

Android Enterprise offers a rather well-honed configuration for MDM admins. When you have imported an application, you can activate its checkbox in the left-hand frame and click “Configure” on the right-hand frame.

Here, you can:

- › set the states for permissions that the application requests upon install
- › control these permissions globally, via the policy „System behavior for app permissions“, or customize these at an app level

By default, these permissions are not managed by the MDM but instead the user is prompted to grant or deny permissions on install. Unless your users are particularly tech-savvy, we recommend only granting permissions for the applications that we recommend. The benefit is end-users cannot make errors upon setup, like denying an important permission.

We recommend refraining from denying permissions unless you really know the consequence this has on the app’s behavior. For example, some applications might accept a denied access to storage, however, some might break and not start up, or produce errors that the end user will not be able to understand.



Conclusion

Overall, Android Enterprise represents a step forward towards the optimal management of Android devices for enterprise use. Integration into EMM-solutions has been simplified, meaning more companies can take advantage of the affordable Android devices available on the market.

..... Headquarters

Cortado Mobile Solutions GmbH

Alt-Moabit 91a/b
10559 Berlin, Germany
Tel.: +49 (0)30 408 198 500
Fax: +49 (0)30 408 198 501
E-Mail: info@cortado.de
www.cortado.de

Cortado Pty Ltd.

..... Australia

Level 12, Plaza Building,
Australia Square, 95 Pitt Street
NSW 2000 Sydney, Australia
Tel.: +61-(0)2-8079 2989

..... USA (Colorado)

Cortado, Inc.

3858 Walnut Street, Suite 130
Denver, CO 80205, USA
Tel.: +1-303-487-1302
E-mail: info@cortado.com
www.cortado.com

Cortado Japan

..... Japan

5F Yaesu Dori Building,
3-4-15 Nihonbashi,
Chuo-ku Tokyo
Tokyo 103-0027
Tel.: +81-(0)3-6870 3467



All names and trademarks are the names and trademarks of the respective manufacturers.

Follow Cortado at:



facebook



twitter



youtube



linkedin