

Android enterprise

Work Profile enrolment Factory-reset state



MobileIron Core



Android 7.x

September 2017

Enterprise Mobility documentation by boulon



In order to proceed, you must have:

- Android 5.0 or later installed on the devices to be provisioned. Android 6.0+ recommended.
- A functional MobileIron EMM solution in place.
- Android enterprise fully configured on your EMM platform.
- A Google account.





For Work Profile enrolment there are no special initial steps.

You must work through all steps of the Wizard, until presented with the home screen.

To begin, tap LET'S GO.





There is no requirement to select one option over the other here as this does not impact Work Profile enrolment.

If being configured on behalf of a user, tap **Set up as new** and utilise a unique Google account. The user can add in their own account at a later point if desired.



* 🕩 🖹 💈



Connect to a suitable WiFi network to continue.

Alternatively, for devices with an active data connection, WiFi can be skipped by selecting Use mobile network for setup.





Once connected, the device will check for updates and automatically continue to the next step.

Ð

Checking for updates...

This may take a minute or two



* 💎 🛚 📋

Continue device setup

At the Google account sign in screen, input an existing unique Google account address, or tap **More options** to create a new account.

When ready, tap **NEXT** to continue.

Why does a unique Google account matter?

By default, when adding a Google account to an Android device it is set to automatically sync account data. Though it can be disabled manually later, if it is re-enabled for any reason many users may inadvertently share their contacts, calendars, histories and more with one another. In addition, account tools allowing devices to be located can also be considered an invasion of privacy. Finally, It's against Google's ToS and may result in the account being closed.

Google

Sign in

with your Google Account. Learn more

Email or phone



* 💎 🕅

Continue device setup

Once authenticated with the unique Google account, tap I AGREE to continue.

(After reading the ToS and Privacy Policy, naturally).





The device will now add the account to the device and automatically continue.



* 🗢 🕱 📋

Continue device setup

Optionally configure fingerprint unlock, if supported. Keep in mind if the backup-passcode configured as part of fingerprint setup does not conform to corporate policies, you will be prompted to set a stronger passcode again later.

Tap **ADD FINGERPRINT** to begin this process, or **Skip** to continue.

Note: Fingerprint setup is not documented in this guide as it is assumed corporate passcode policies are in place which may block its use. Passcode setup is documented in the following pages and as such the next page in this guide assumes **Skip** has been tapped.

@

Unlock with fingerprint

Nexus Imprint uses your fingerprint to wake and unlock your phone, authorize purchases, or sign in to apps.

Be careful whose fingerprints you add. Any fingerprints added will be able to do these things.

Note: Your fingerprint may be less secure than a strong pattern or PIN.

Skip

ADD FINGERPRINT

* 💎 🛛 🗎

Continue device setup

Disable relevant services and tap **NEXT** to continue to the next step.

G

0

()

Google services

You can turn these services on or off at any time for emmsetup@gmail.com. Data will be used according to Google's **Privacy Policy**.

If you want to learn more, you can tap each service.

Automatically back up device data (such as Wi-Fi passwords and call history) and app data (such as settings and files stored by apps) to Google Drive.

Use Google's location service to help apps determine your location. Anonymous location data will be sent to Google when your device is on.

Improve location accuracy by allowing apps and services to scan for Wi-Fi and Bluetooth, even when these settings are off.

Help improve your Android experience by automatically sending diagnostic and

 \bigtriangledown



Tap **CONTINUE** to progress to the next step.



Put Google to work for you

The Google app can also give you personalized updates like weather, commute time, and upcoming flights or appointments. The more you use it, the more useful it becomes.

CONTINUE

oayton

•

Continue device setup

If the Google app is desired, tap **YES I'M IN**, otherwise tap **No Thanks** to continue to the next step.

G

Give the Google app permission to help you

The Google app depends on these settings in order to best help you. Turn these settings on for:

emmsetup@gmail.com

Web & App Activity from this device

Includes Chrome history and content you browse on the web and in apps

Location History

Creates a private map of where you go with your signed-in devices

i Device Information from this device

Includes contacts, calendars, apps, music, battery life, sensor readings

Please remember that the data governed by these settings may be saved from any of your signed-in devices.

 \bigtriangledown

* 💎 🛛 📋



Tap ALL SET to exit the Wizard.



J

Anything else?

Here are a few more things you can set up. Or you can finish them later by going to Settings.



Review additional apps Apps will be installed after setup is complete

Use your voice Say "Ok Google" to search, set alarms & more

ALL SET



From the home screen, tap GOT IT, then open the Play Store.





Search for Mobile@Work and tap INSTALL when located.

<u>⊥</u> ∎		* 🗢 🕱 🛙	9:36
← mobile@	ฏwork		Ŷ
	obile@Work obileIron PEGI 3 3 ★ (9,253 ≗) • 1 millio	on ±	
MORE I	NFO	INSTALL	
You Might Also Like		MORE	
		S	
Mobile- Iron Docs 2.2 ★	Mobile- Iron 2.2 *	Skype for Business 3.9 ★	Tou Dov 4.0 s
Similar Apps MORE		RE	
\triangleleft	0		





Once installed, open Mobile@Work and tap **OK** to agree to the prompt for permissions.

Mobile@Work requires access to information about your device, such as its IMEI and phone number, which will be shared with your IT administrator.

Ŧ

On the following screen(s), you will be asked to grant permission for Mobile@Work to gather this information. The screen(s) may specify information related to managing phone calls.

Mobile@Work will not make or manage phone calls.

 \bigcirc

 \triangleleft

OK



Grant MobileIron the requested permissions.

Tap ALLOW.





Input your email address (or switch to server URL if required). Tap **NEXT**.



Continue enrolment

Accept the privacy alert by tapping **CONTINUE**.

101

Secure Mobility

Mobile@Work will not access personal content such as your personal email, photos or voicemail

Device Details

Your company requires some general device details to provide secure mobility services

Remote Security

If your device is lost or stolen, you and your company can take security measures to protect your data

Learn More

You can find more details after registration, under Settings > Your Privacy

Your Privacy is Important

Don't worry! Your company cannot access your personal data

 \bigcirc

CONTINUE



 \triangleleft



When your account has been found and validated, you'll be prompted for your password, PIN or both.

Enter the required fields and tap SIGN IN.



Device configuration

The DPC will now configure the device, bringing down the relevant policies and configurations.





Once authenticated, MobileIron will request further permissions to effectively manage the device.

Tap CONTINUE.





Grant MobileIron the requested permissions.

Tap ALLOW.





At this point Android enterprise setup initiates. By tapping **CONTINUE**, a new, corporately-managed profile (not dissimilar to a secondary user profile) will be created.

ĉa 🖬 🖳 🕨

\equiv Device Configuration Status C



Create Work Profile

 \triangleleft

Android enterprise (AFW) creates a separate work profile to access work data and keeps it separate from your personal data. In the next steps, you will be guided to set up your Android enterprise (AFW) profile.

CONTINUE

9:38







Grant MobileIron the requested access.

Set up work profile

Your organization controls this profile and keeps it secure. You control everything else on your device.

The following app will need to access this profile:

0



 \triangleleft

MobileIron

NEXT





Tap **OK** to accept the privacy alert, or tap **Learn more** for more information about how it works and the monitoring/control capabilities the DPC has.

ā 🗉 🕨

0

Set up work profile

Vour organization controls this profile and

Your admin has the ability to monitor and manage settings, corporate access, apps, permissions, and data associated with this profile, including your network activity, as well as your device's location, call history, and contact search history.

Contact your admin for more information, including your organization's privacy policies.

 \bigcirc

Learn more

 \triangleleft

CANCEL OK



The Work Profile is being created. This will automatically progress to the next step.

Setting up your work profile...

 \bigtriangledown

Ο



At this point the DPC will disable on the personal profile and open automatically in the Work Profile. Expect the DPC to vanish and relaunch.

MobileIron will check for any further policies or configurations to be applied to the **device** (not the Work Profile) before the Work Profile configuration is completed.





If the relevant security policy has been deployed, a passcode will be required.

The type of passcode mandated may not be a PIN as depicted in the following steps. The process however is similar for all alpha/numeric passcode options.



Device configuration

Select the relevant passcode, some options may not be available depending on the security policy deployed.

🗖 č, 🖻 🗉		* 💎 🖹 🛿 23:24	
Unlock selection		:	
None		0	
Swipe Current screen lock		0	
Pattern			
PIN			
Password			
\bigtriangledown	0		

Device configuration

Before inputting a passcode, the device may display a prompt to opt in to secure start-up.

While it is more secure to require the passcode on device boot, it will result in a longer boot process.

💶 🗟 🖻 🗉

•

Secure start-up

You can further protect this device by requiring your PIN before it starts up. Until the device starts up, it can't receive calls, messages or notifications, including alarms.

This helps protect data on lost or stolen devices.





Input a PIN (or other passcode type) and tap **CONTINUE**. Repeat to confirm.



Device configuration

Permit or prohibit notification content and tap DONE.

🖂 🖻 🗉

Notifications

When your device is locked, how do you want notifications to be displayed?

- Show all notification content
- Hide sensitive notification content

Ο

 \triangleleft

O Don't show notifications at all

DONE



The Work Profile configuration will now finalise and automatically continue to the next step.





The device has now completed initial configuration and will continue to pull down applications and resources in the background if configured.

You may tap the home (O) button to leave the DPC.





Jason Bayton

bayton.org
/in/jasonbayton
@jasonbayton
+JasonBaytonX
jason@bayton.org

Updates to this document can be found here: Android enterprise provisioning guides