

Android enterprise

Work Profile enrolment Non 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.
- A fully set-up device with Play Store access.





Open the Play Store, search for Mobile@Work and tap INSTALL when located.

<u>↓</u> .		* 💎 🛚 🕻	9:36	
← mobile@v	work		Ļ	
Mol Mol 2.3	bile@Work bileIron PEGI 3 ★ (9,253 ♣) • 1 milli	on 🛨		
MORE INFO INSTALL				
You Might Also Like		MORE		
		S		
Mobile- Iron Docs 2.2 *	Mobile- Iron 2.2 ★	Skype for Business	Tou Dov 4.0 s	
Similar Apps		MORE		
\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.



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.

Tap NEXT.

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:

Ο



 \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 re-launch.

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.

For an already set-up device this prompt my not show if the existing passcode setup by you matches or exceeds the requirements of the security policy.

🖂 🗟 🖻 🖸

* 💎 🖹 💈 23:24

 \equiv Device Configuration Status



1 Screen Lock Preferences

On the next screen, you will set up the screen lock for your device.

Your administrator has applied a new screen lock policy or your previous screen lock may have expired. Please set up the screen lock for your device.

 \bigcirc

CONTINUE



 \langle



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		

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.



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