

Android enterprise

Work-Managed enrolment DPC identifier provisioning



MobileIron Core



Android 7.x

September 2017

Enterprise Mobility documentation by bou



In order to proceed, you must have:

- Android 6.0 or later installed on the devices to be provisioned. Android 7.0+ recommended.
- A functional MobileIron EMM solution in place.
- Android enterprise fully configured on your EMM platform.

DPC identifier provisioning is simple, but may cause confusion for end-users as requesting they type a token into the Google account prompt may result in typos and/or misunderstandings. Consider as an alternative QR enrolment or NFC enrolment.





For DPC identifier provisioning there are no special initial steps.

You must work through the first few steps of the Wizard, until a Google account is requested.

To begin, tap LET'S GO.





Copying data from another device will result in an inability to provision the device again without undertaking a factory reset.

Tap Set up as new.

	L
	L.
-	

a

Welcome to your Nexus 5X

Copy your data

From an iPhone® or Android device, or the cloud

Set up as new Get a fresh start

 \bigtriangledown

Continue device setup

The device requires connectivity in order to download the DPC and, later, policies & configs.

Connect to a WiFi network. The device will automatically progress once a connection has been made.

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 when complete.

Ð

Checking for updates...

This may take a minute or two



* 🕩 💎 🛯 💈



At the Google account sign in screen, input the following DPC identifier:

afw#mobileiron.core

Each EMM provider has one or more of these unique tokens, each depicting the DPC that will be downloaded for enrolment.

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

Google Sign in with your Google Account. Learn more Email or phone afw#mobileiron.core Forgot email? NEXT More options \triangleleft



The device will now prompt you to install the chosen DPC – Mobile@Work in this instance – and will begin to download in order to do so once **INSTALL** is tapped.

Ð

Android for Work

This account requires mobile device management. Install the Mobile@Work app to enforce security policies required by the account.



Mobile@Work

SKIP

INSTALL



* 🕩 💎 🖹 月



The device will now download the DPC and automatically move to the next step in the process.



* 🕕 💎 🗶 🖡



Unlike other provisioning options (NFC, QR), using token enrolment prompts you to install the DPC manually.

Tap INSTALL in order to continue.

MobileIron

Do you want to install this application? It does not require any special access.

CANCEL INSTALL



 \triangleleft

* 🕩 💎 🖹 🛙



Following installation, the device will prompt you to confirm you're aware that the organisation has full control over the device.

Tap **NEXT** to continue.

0

Set up work device

Your organization will control this device and keep it secure.

The following app will manage your device:



MobileIron

NEXT



The device being provisioned will again display a prompt with an overview of monitoring capabilities.

You must accept the device being managed by the organisation in order to begin provisioning.

Tap **OK** to proceed.

Your admin has the ability to monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this device, including network activity and your device's location information.

To use theft-protection features, you must have a password-protected screen lock for your device.

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

CANCEL OK

* 🛛

oauton

* 🗢 🖹 🛔



The device will set the device owner and continue the provisioning process.

This may take a few minutes.

The following prompts may include license acceptance, agreement to services or finishing the setup Wizard. This varies between OEMs, however when complete the device will display a sparse home screen before the DPC launches. 0

Set up work device

Setting the device owner...





Shortly after Android enterprise provisioning is complete, the DPC will automatically launch and begin enrolment.

There is no need to manually open the DPC from the home screen.





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.





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.

Tap CONTINUE.

💶 🗟 🖻 🗉 📉 🦻 23:24 **Device Configuration Status** 0000 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. CONTINUE \bigcirc \triangleleft

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		

bayton

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.



bayton

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

bayton



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