

# Android enterprise

Work-Managed enrolment  
NFC provisioning



MobileIron Core



Android 7.x

September 2017

Enterprise Mobility documentation by bayton

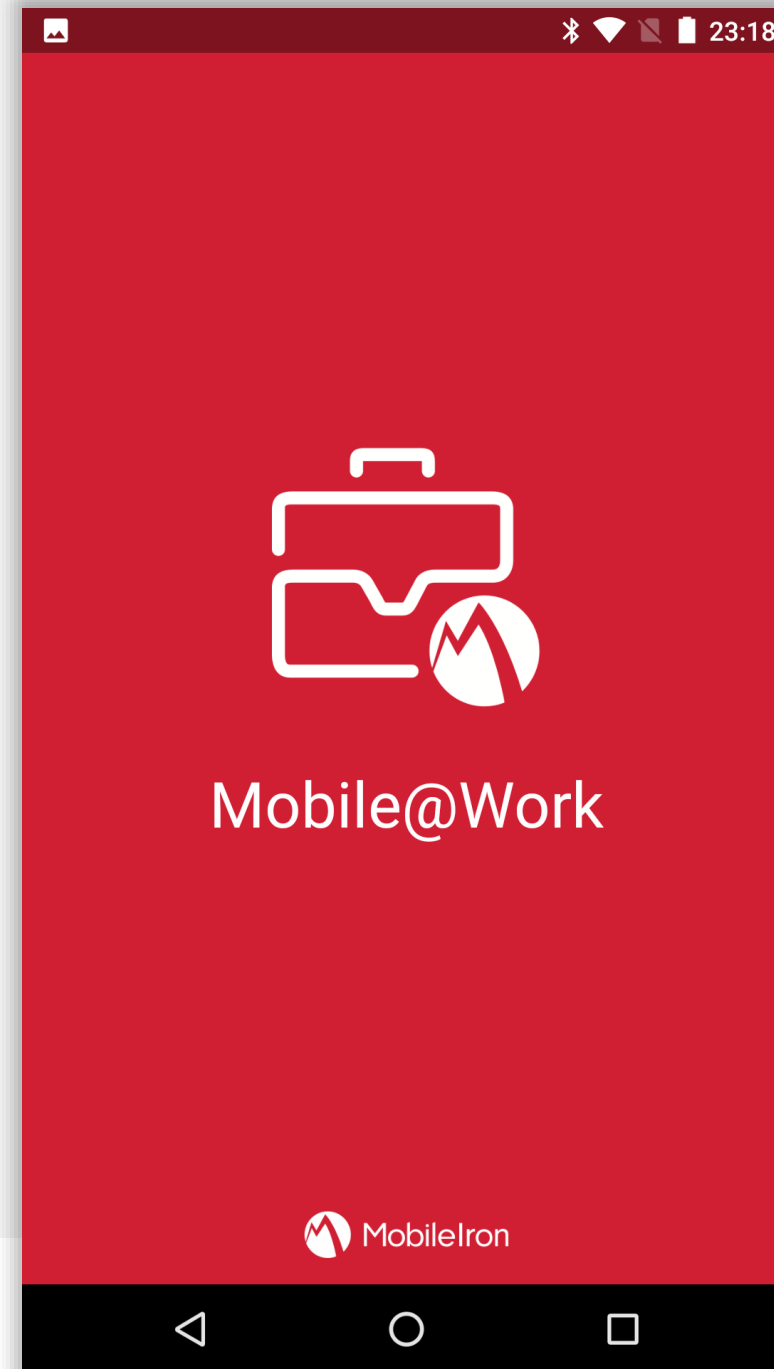


# Requirements

In order to proceed, you must have:

- Android 6.0 or later installed on the devices to be provisioned. Earlier Android versions are less likely to reliably work. Android 7.0+ recommended.
- A spare device with NFC to “bump” the devices to be provisioned.
- NFC functionality enabled out of the box for devices to be provisioned.
- A functional MobileIron EMM solution in place.
- Android enterprise fully configured on your EMM platform.

NFC provisioning is the earliest form of Android enterprise Work-Managed enrolment and cannot be done remotely. Consider as an alternative QR enrolment or DPC identifier enrolment; these do allow enrolment remotely.





# Configure the provisioner

The provisioner app must be installed on a spare device that is not going to be enrolled onto the EMM platform.

Once downloaded from Google Play, open the Provisioner app, then set the following:

- App for Provisioning (Mobile@Work, MobileIron Go, etc).
- WiFi SSID.
- WiFi Security Type.
- WiFi Password.

All of these fields are mandatory, the time zone and locale are normally automatically set.

Tap **CONTINUE** to begin the provisioning process.

The screenshot shows the 'Provisioner' app interface on a mobile device. At the top, there's a red header with the title 'Provisioner' and a menu icon. Below the header, a message states: 'Provision work-managed devices using NFC bump: fill out the information below to prepare this device to be the provisioner.' The form contains several fields: 'Select App For Provisioning' with 'Mobile@Work' selected; 'Wi-Fi Network SSID' with 'WIFINET' entered; 'Wi-Fi Security Type' with 'WPA' selected; 'Wi-Fi Password' with a masked password '.....'; 'Time Zone' with 'GMT+01:00 British Summer Time'; and 'Locale' with 'English (United Kingdom)'. At the bottom, there is a red 'CONTINUE' button. The Android navigation bar is visible at the very bottom.

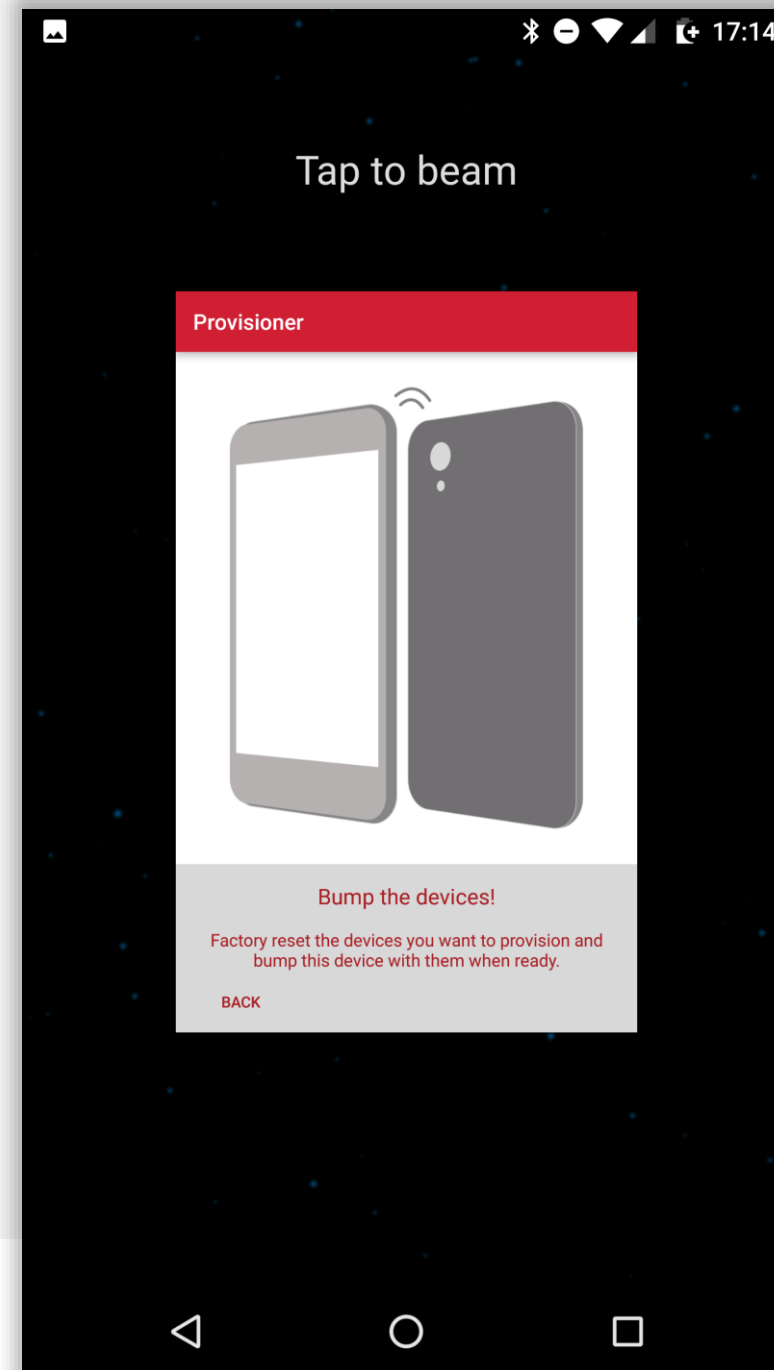


# Bump the devices

Locate the NFC radios on both the provisioning device and the device to be provisioned.

Touch the two devices together until a sound is heard and an animation played on the provisioning device. The device to be provisioned should also indicate a successful connection has been made.

Tap the screen on the provisioning device in order to transmit the NFC payload.





# Begin provisioning

---

Once the NFC payload has been transmitted, the device being provisioned will 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

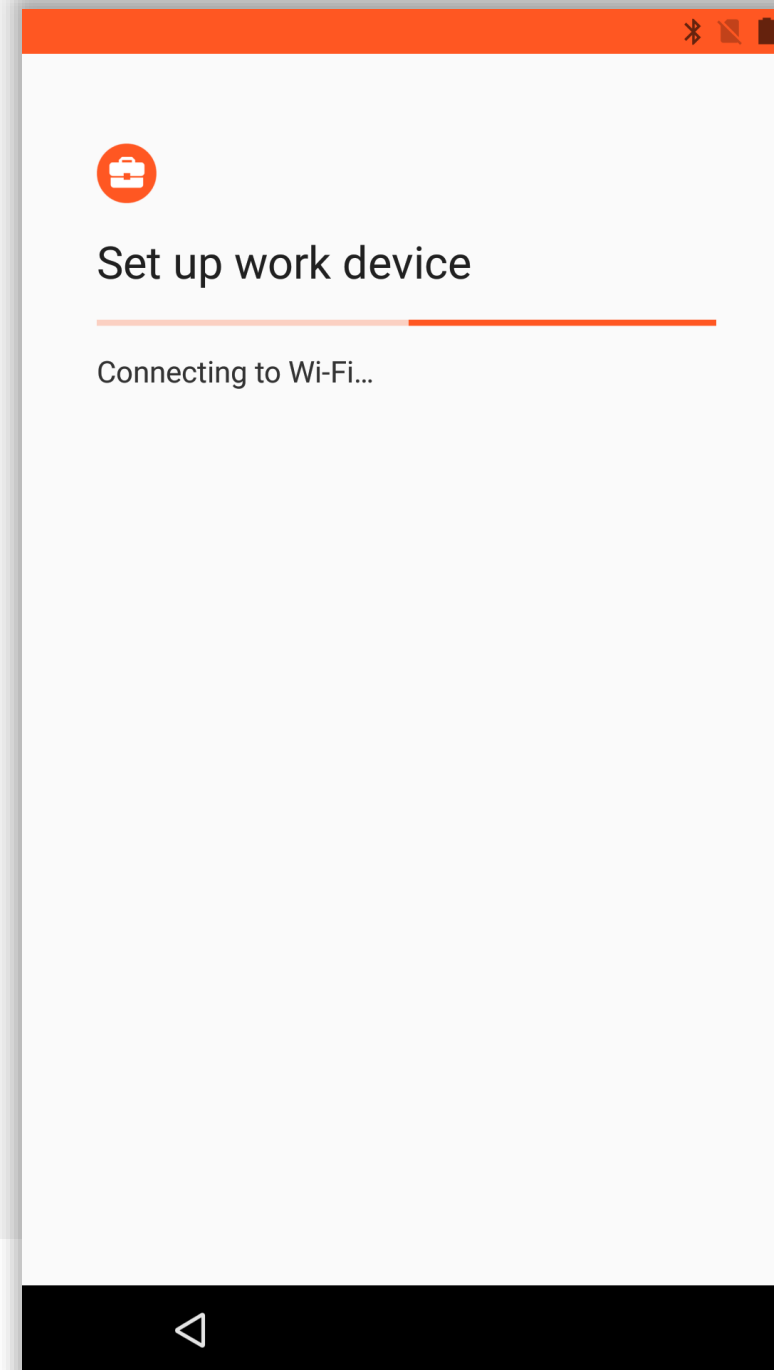


# The device will provision

---

The device will attempt to connect to the WiFi network provided in the NFC payload and begin the provisioning process.

This may take a few minutes.



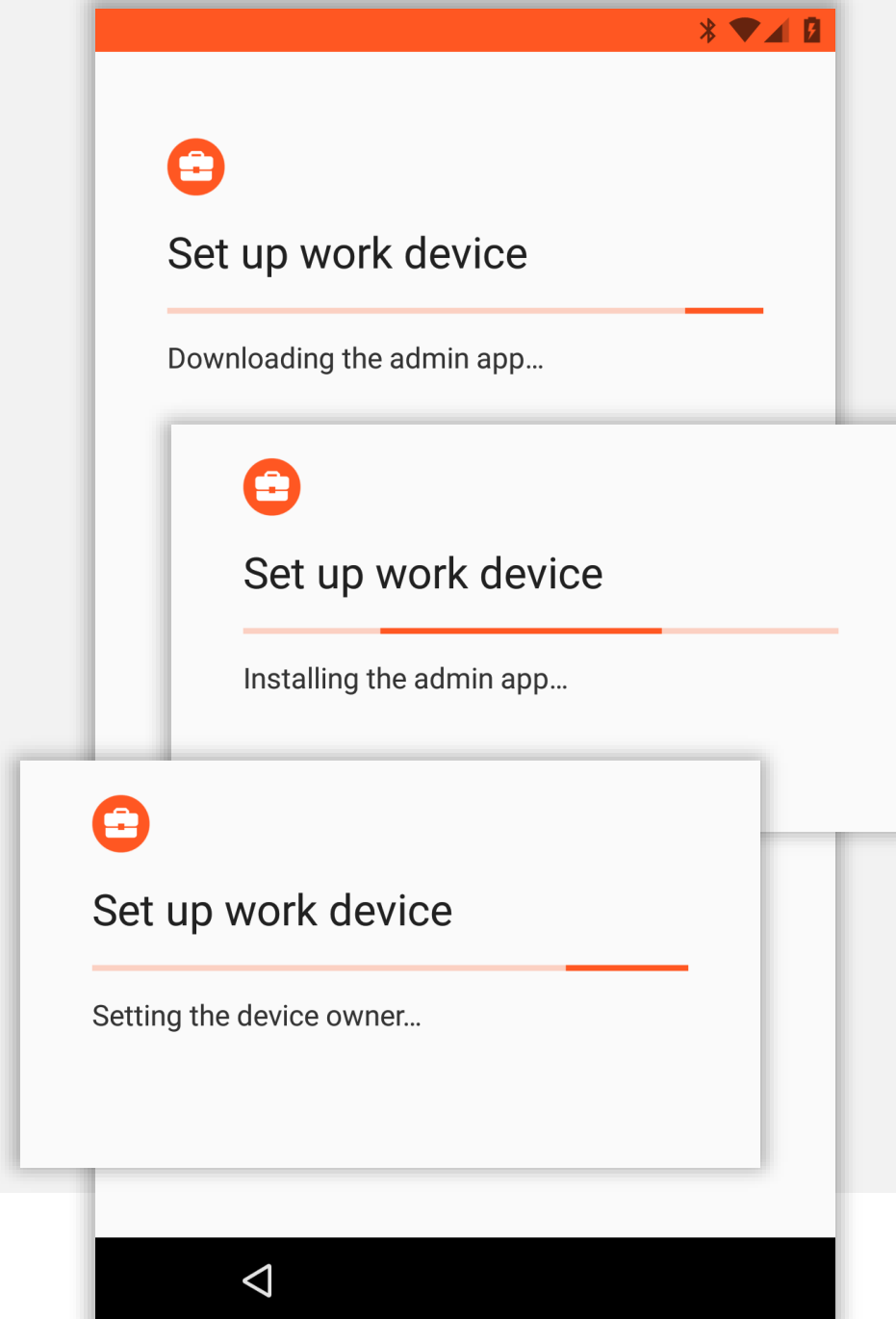


# The device will provision

The device will attempt to download the DPC provided in the NFC payload, install it and set MobileIron as the device owner.

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.

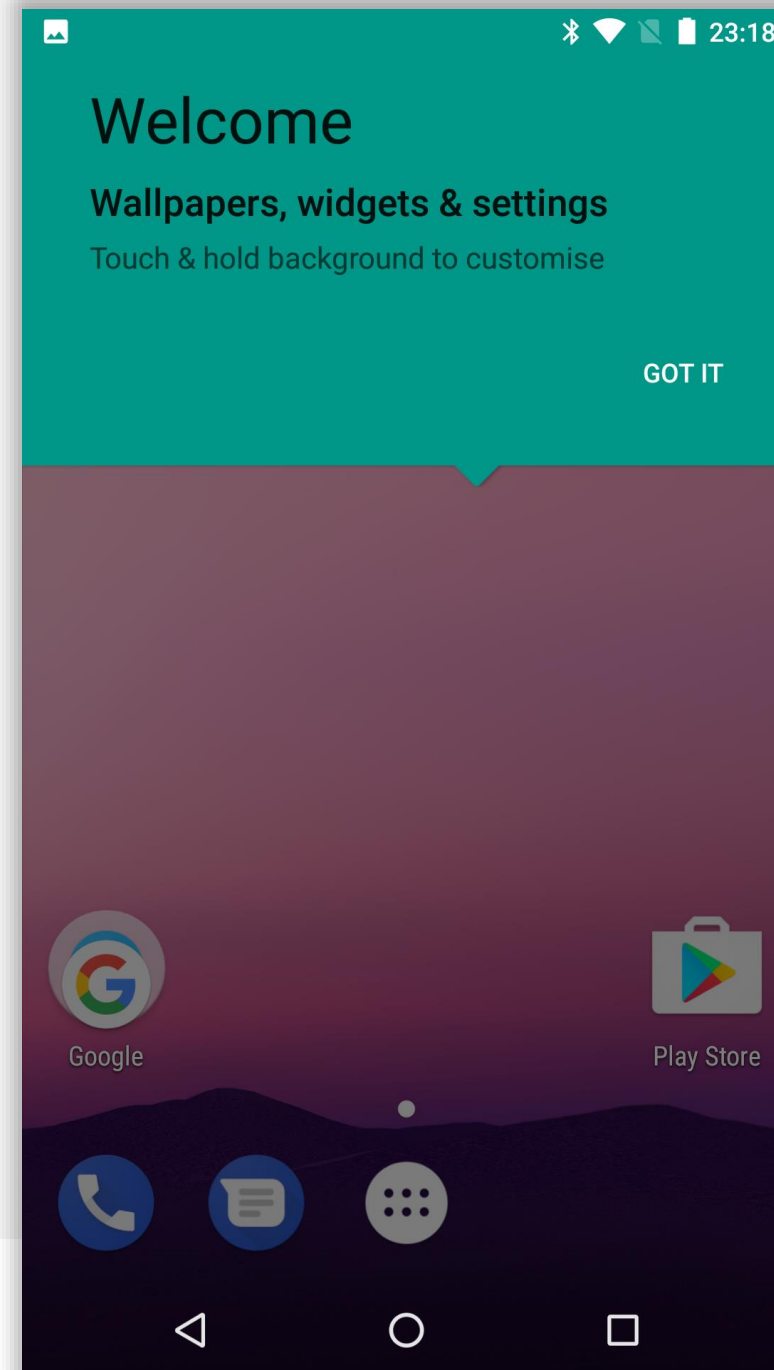




# Provisioning complete

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.








# Begin enrolment

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



10:44

## Get Ready for Work with MobileIron

To configure and secure your device, enter your company email

COMPANY EMAIL

Email

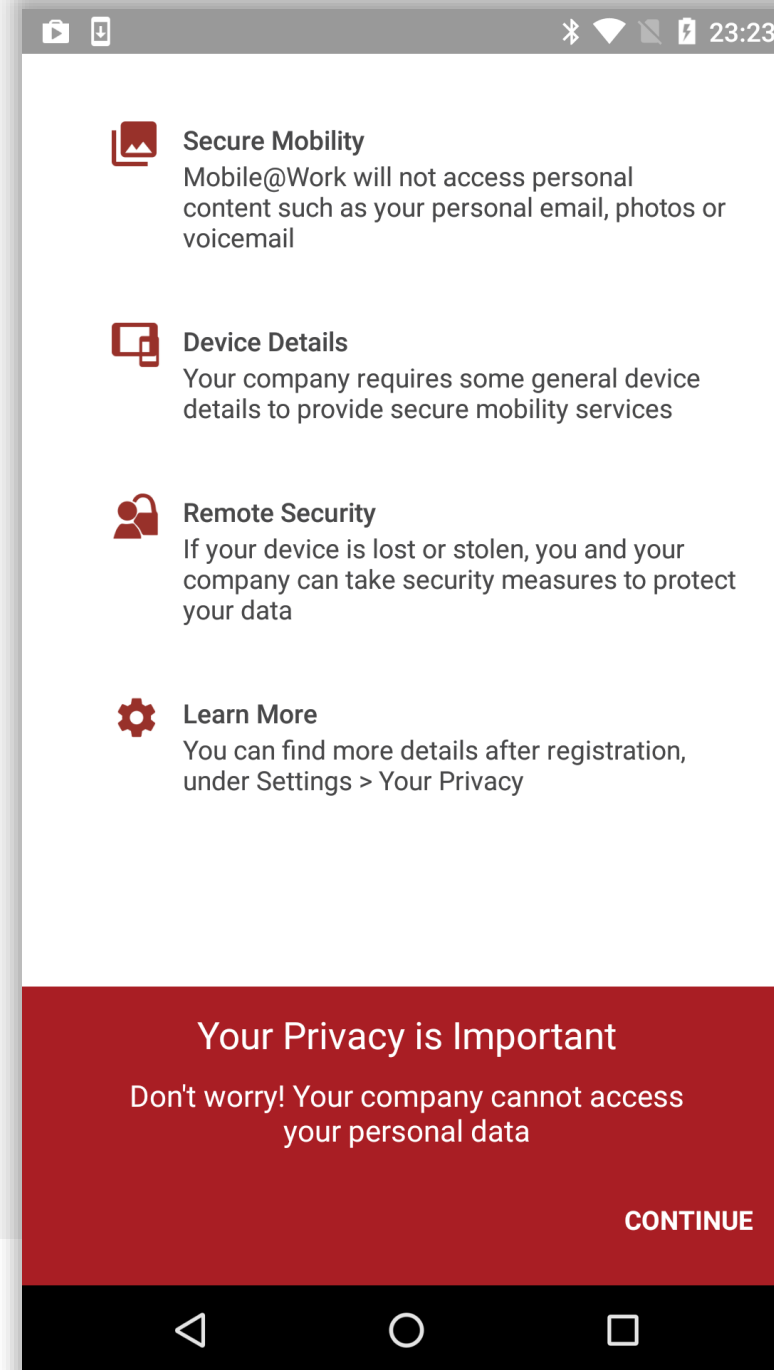
[Or register with server URL](#)

NEXT



# Continue enrolment

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





# Continue enrolment

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

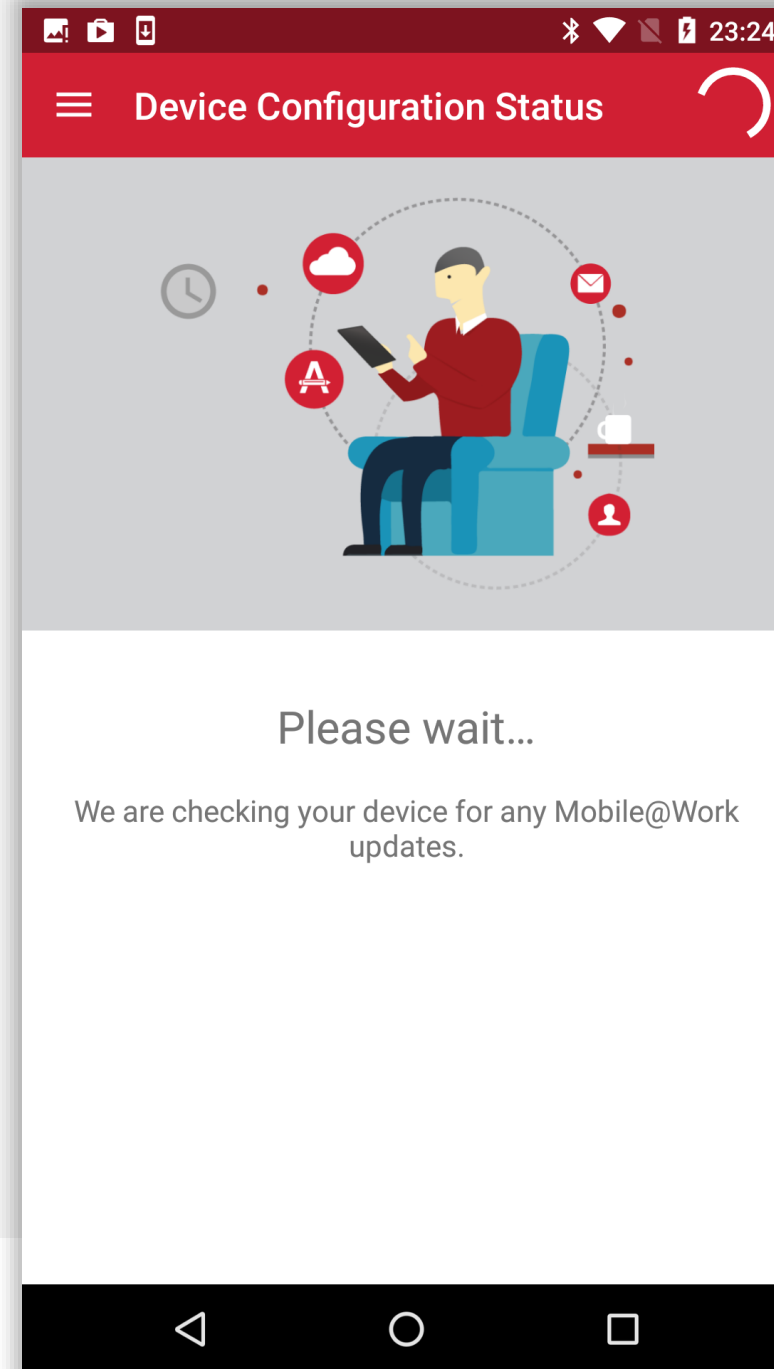
Enter the required fields and tap **SIGN IN**.

The screenshot shows a mobile application interface for signing in. At the top, there is a header illustration of a person sitting at a desk and another person standing and holding a phone. Below the header, there are two input fields: "COMPANY EMAIL" with the text "jason@bayton.org" and "PASSWORD" with the text "Password". A red "SIGN IN" button is located to the right of the password field. Below the input fields is a QWERTY keyboard with a green checkmark button on the right. The status bar at the top shows "LTE" and "10:46".



# Device configuration

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





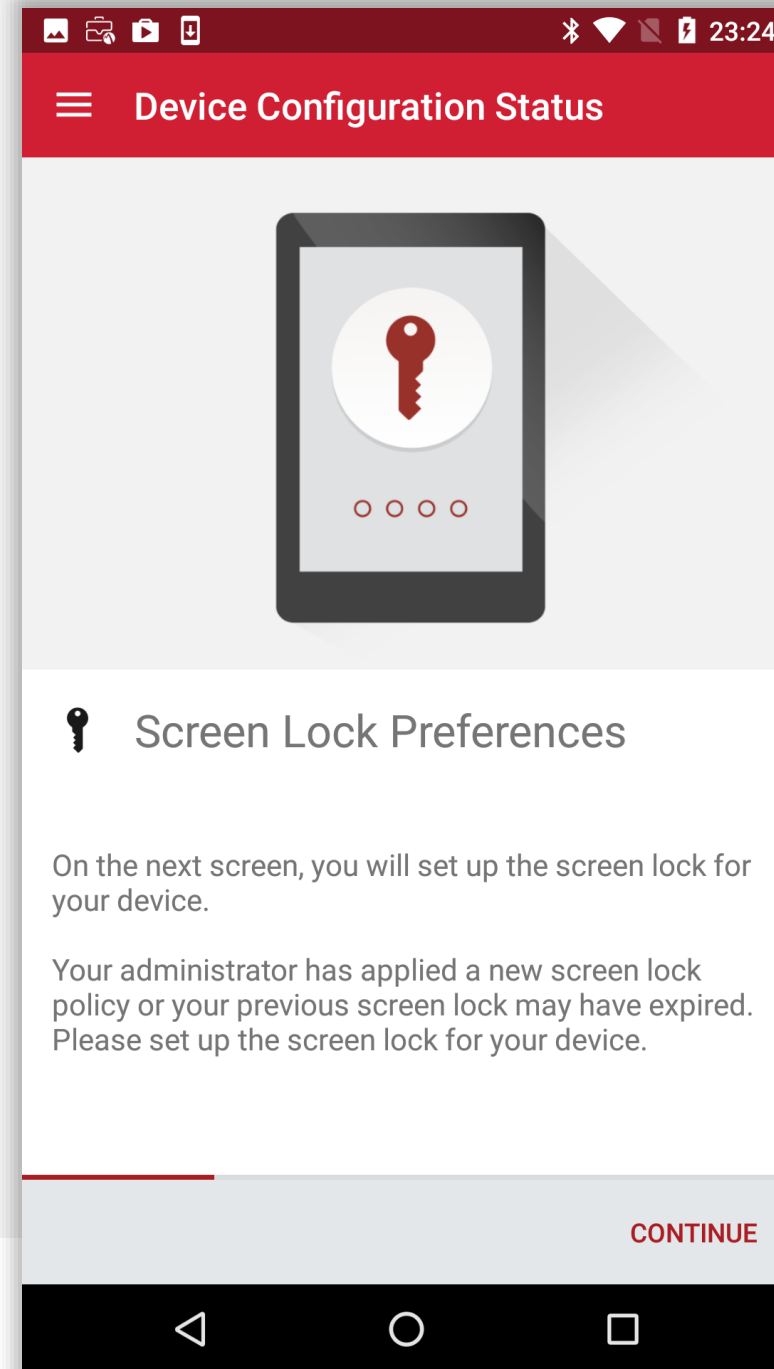
# Device configuration

---

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.

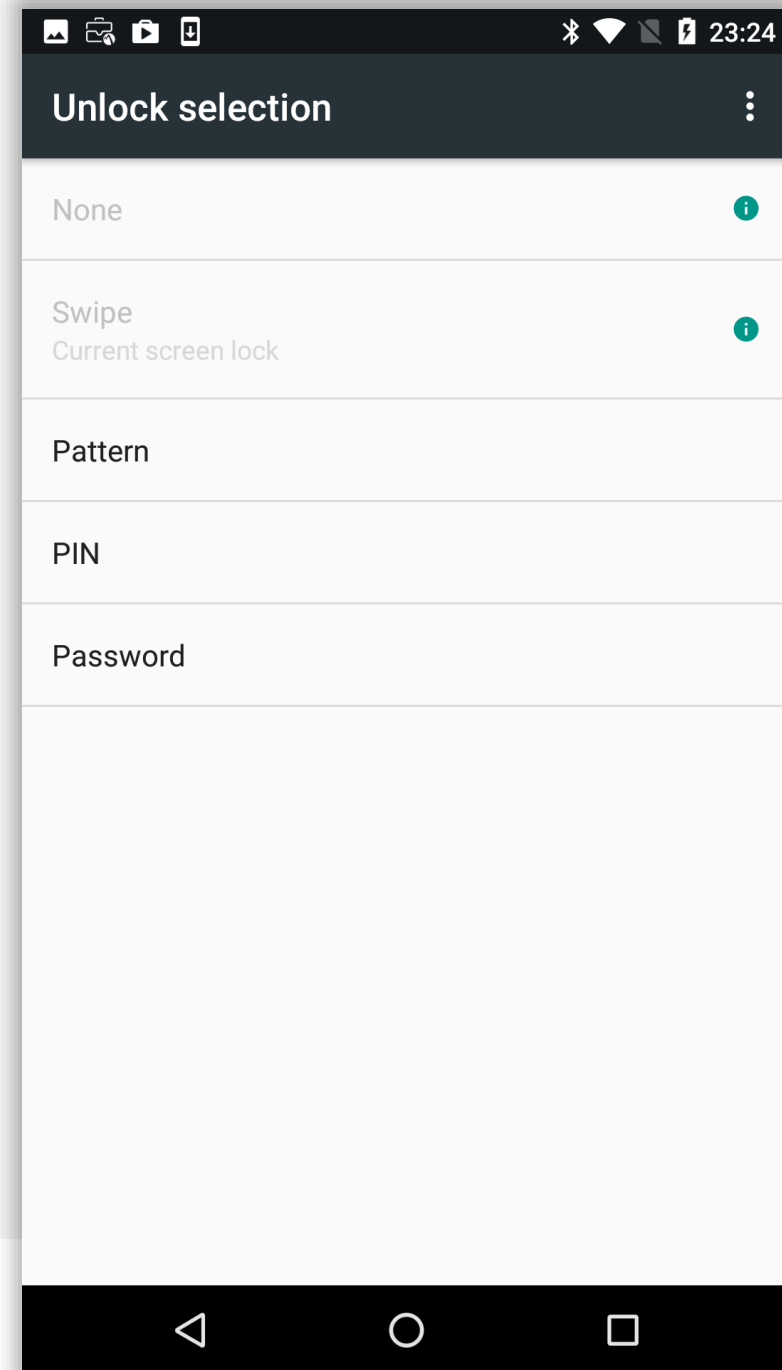
Tap **CONTINUE**.





# Device configuration

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

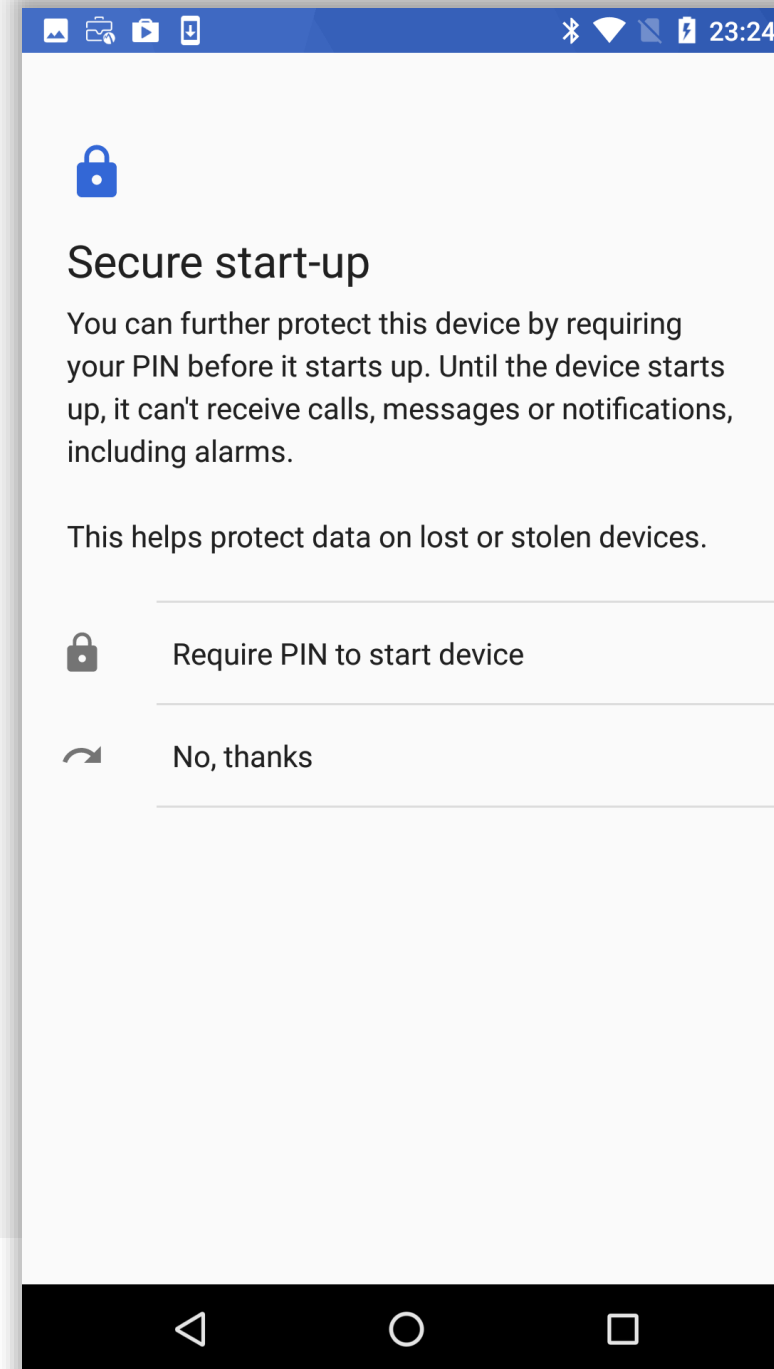




# Device configuration

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.





# Device configuration

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





## Choose your PIN

---

PIN must be at least 4 characters

[Cancel](#) **CONTINUE**

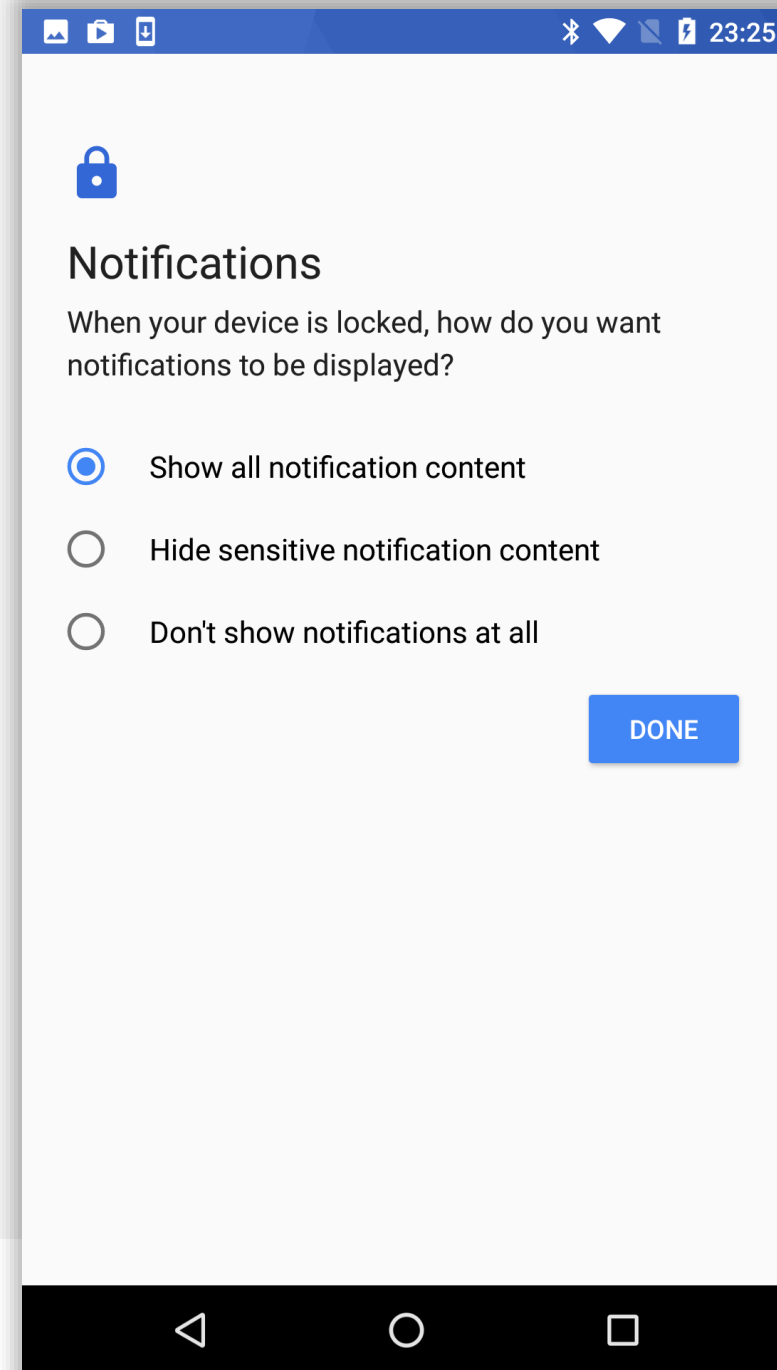
1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PRQS	8 TUV	9 WXYZ
	0	





# Device configuration

Permit or prohibit notification content and tap **DONE**.



The image shows a screenshot of an Android phone's notification settings. At the top, there is a blue status bar with icons for camera, gallery, and a lock icon, along with the time 23:25. Below the status bar is a white header with a blue lock icon. The main title is "Notifications" in bold. Below the title is a question: "When your device is locked, how do you want notifications to be displayed?". There are three radio button options: "Show all notification content" (selected), "Hide sensitive notification content", and "Don't show notifications at all". A blue "DONE" button is located at the bottom right of the settings area. At the very bottom of the screen is a black navigation bar with three white icons: a back arrow, a circle, and a square.

**Notifications**

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

- ☒ Show all notification content
- ☐ Hide sensitive notification content
- ☐ Don't show notifications at all

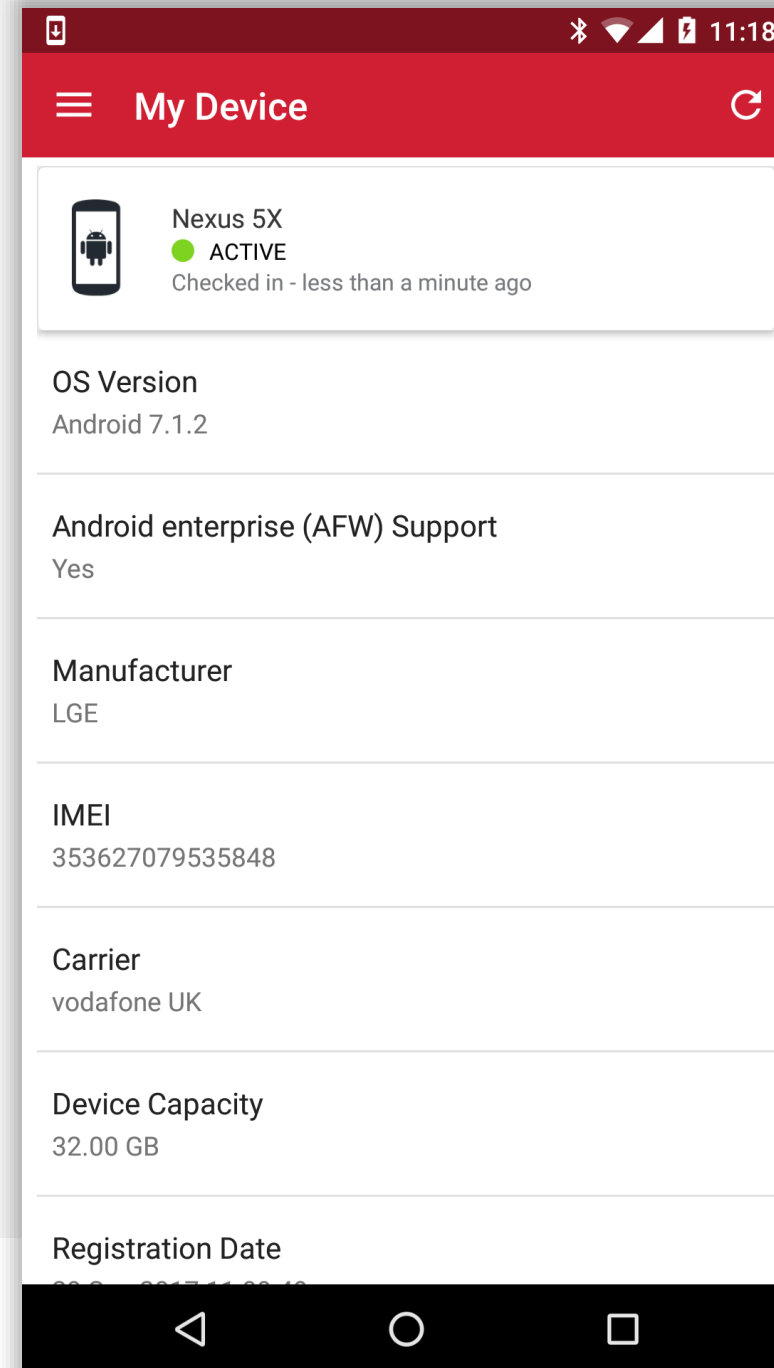
**DONE**



# Configuration complete

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.



# bayton



Jason Bayton



bayton.org



/in/jasonbayton



@jasonbayton



+JasonBaytonX



jason@bayton.org

Updates to this document can be found here:

[Android enterprise provisioning guides](#)

