

Android legacy

Traditional enrolment
Factory-reset state



MobileIron Core



Android 7.x

September 2017

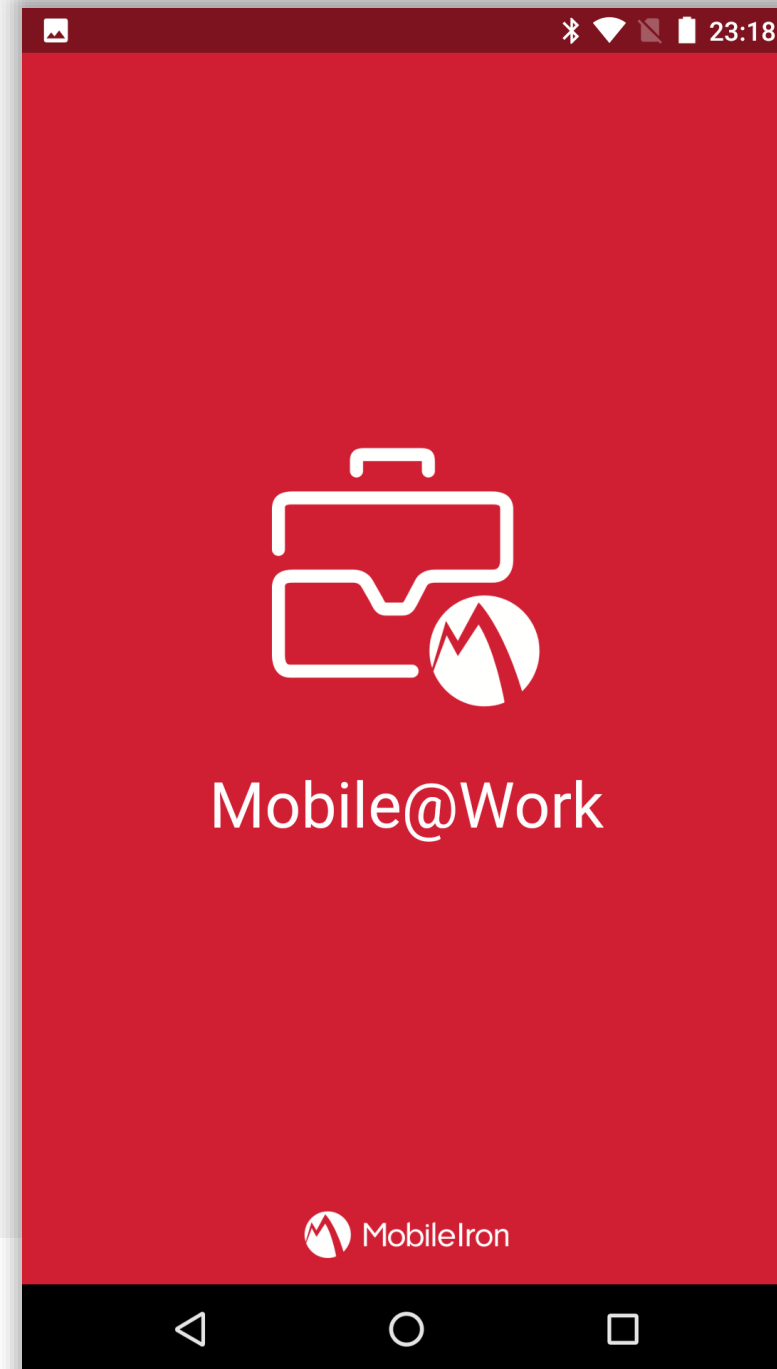




Requirements

In order to proceed, you must have:

- Android 4.x or later installed on the devices to be enrolled. Anything other than Samsung is unlikely to support more than minimal EMM capabilities.
- A functional MobileIron EMM solution in place.
- A Google account.



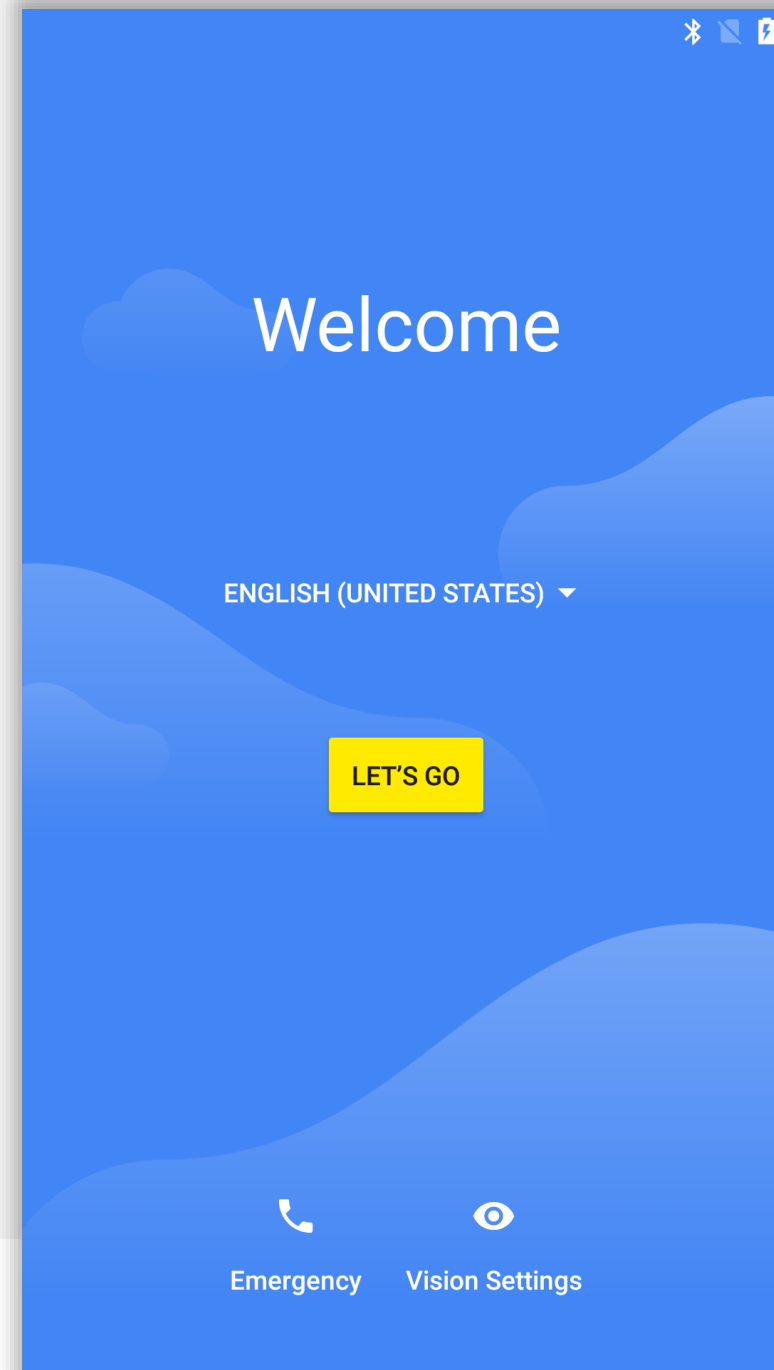


Begin device setup

For legacy 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**.

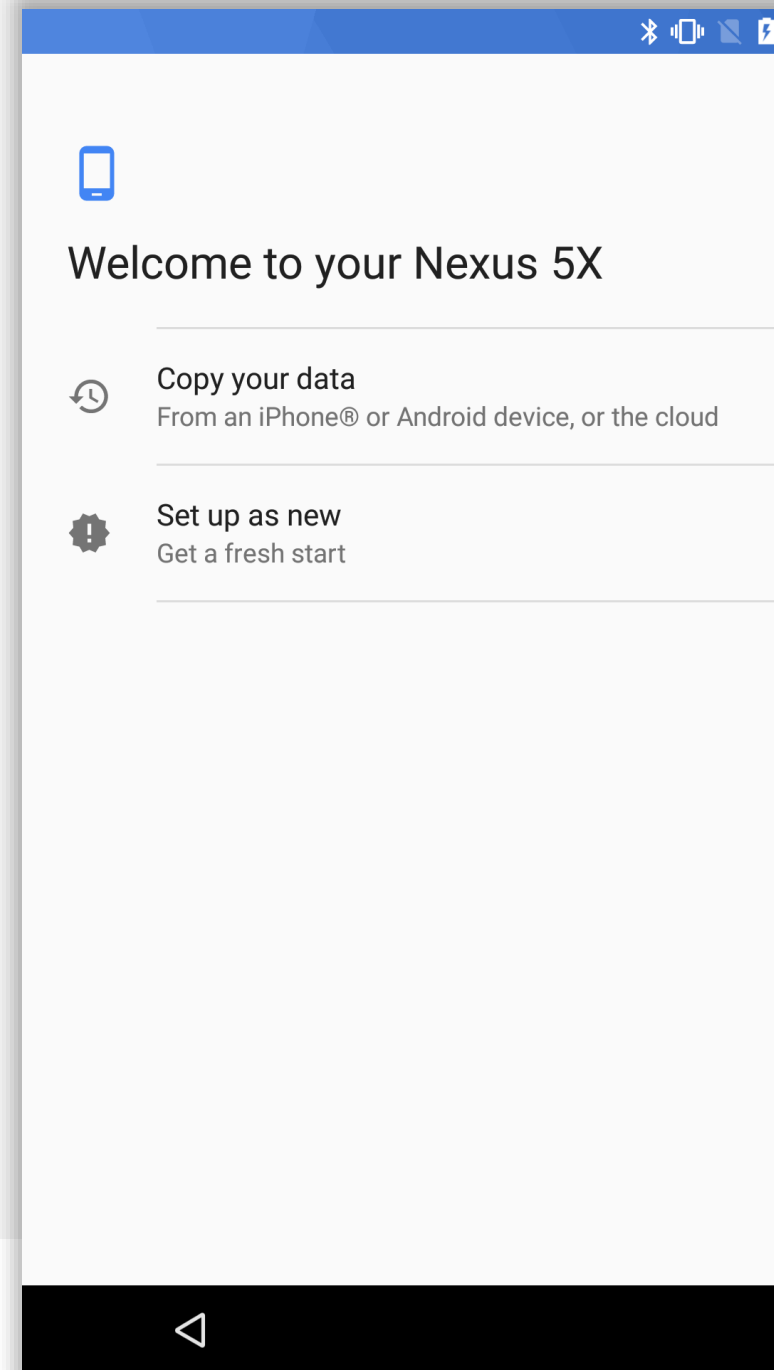




Continue device setup

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

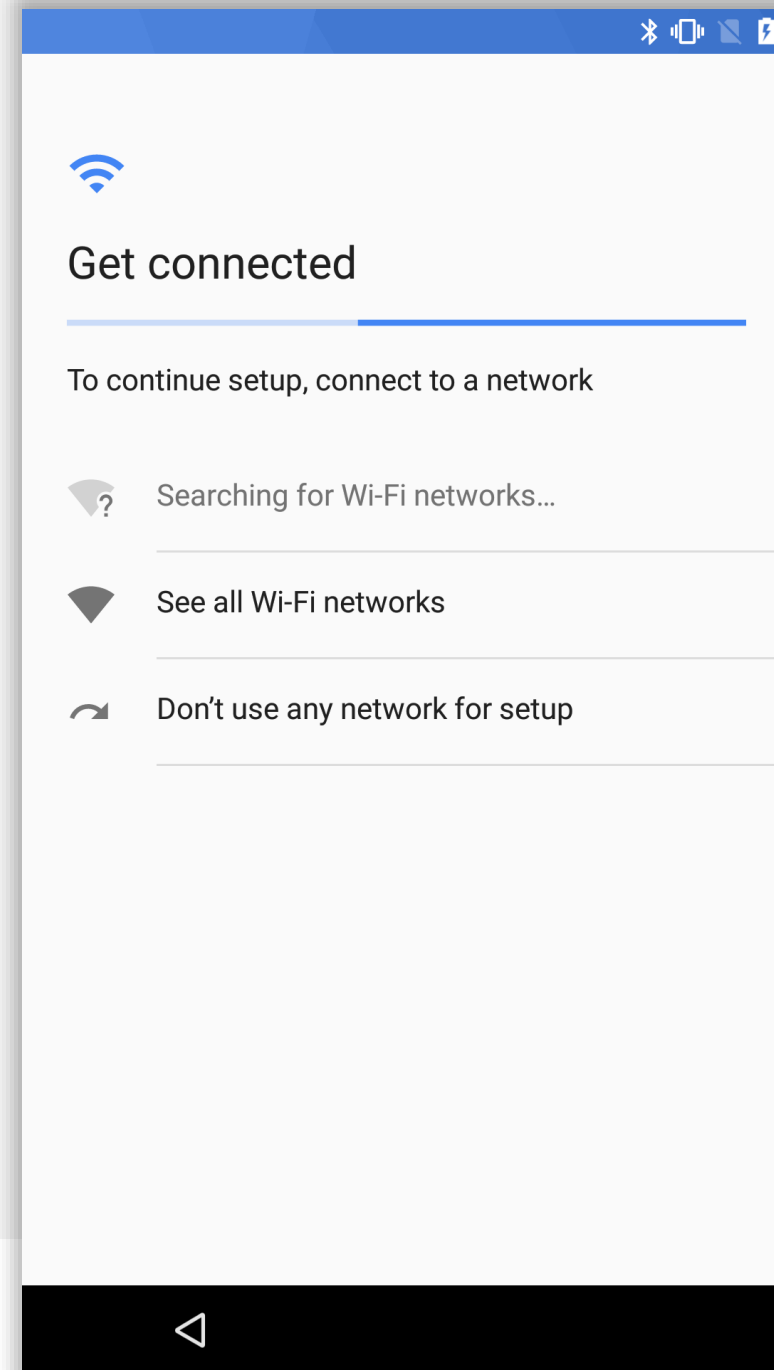




Continue device setup

Connect to a suitable WiFi network to continue.

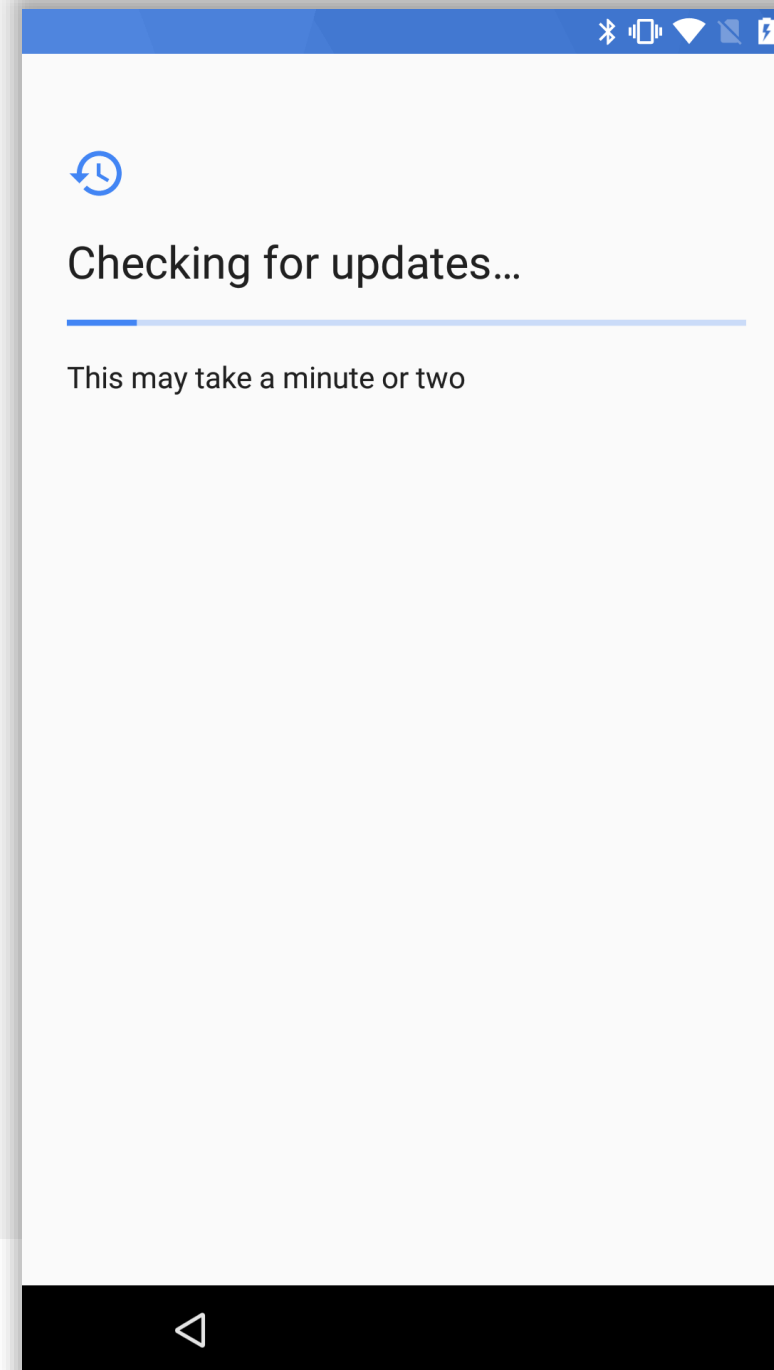
Alternatively, for devices with an active data connection, WiFi can be skipped by selecting **Use mobile network for setup**.





Continue device setup

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





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](#)

emm.setup@gmail.com

[Forgot email?](#)

[More options](#)

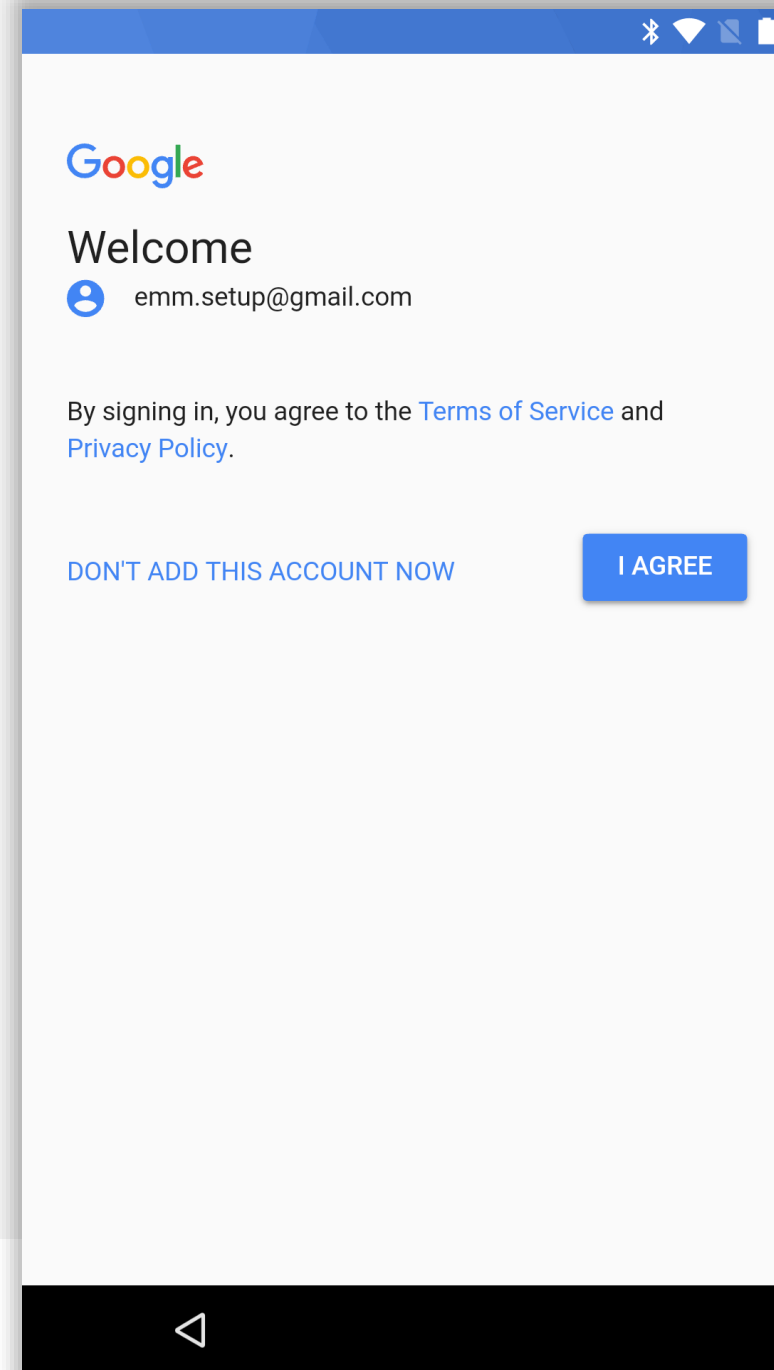
NEXT



Continue device setup

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

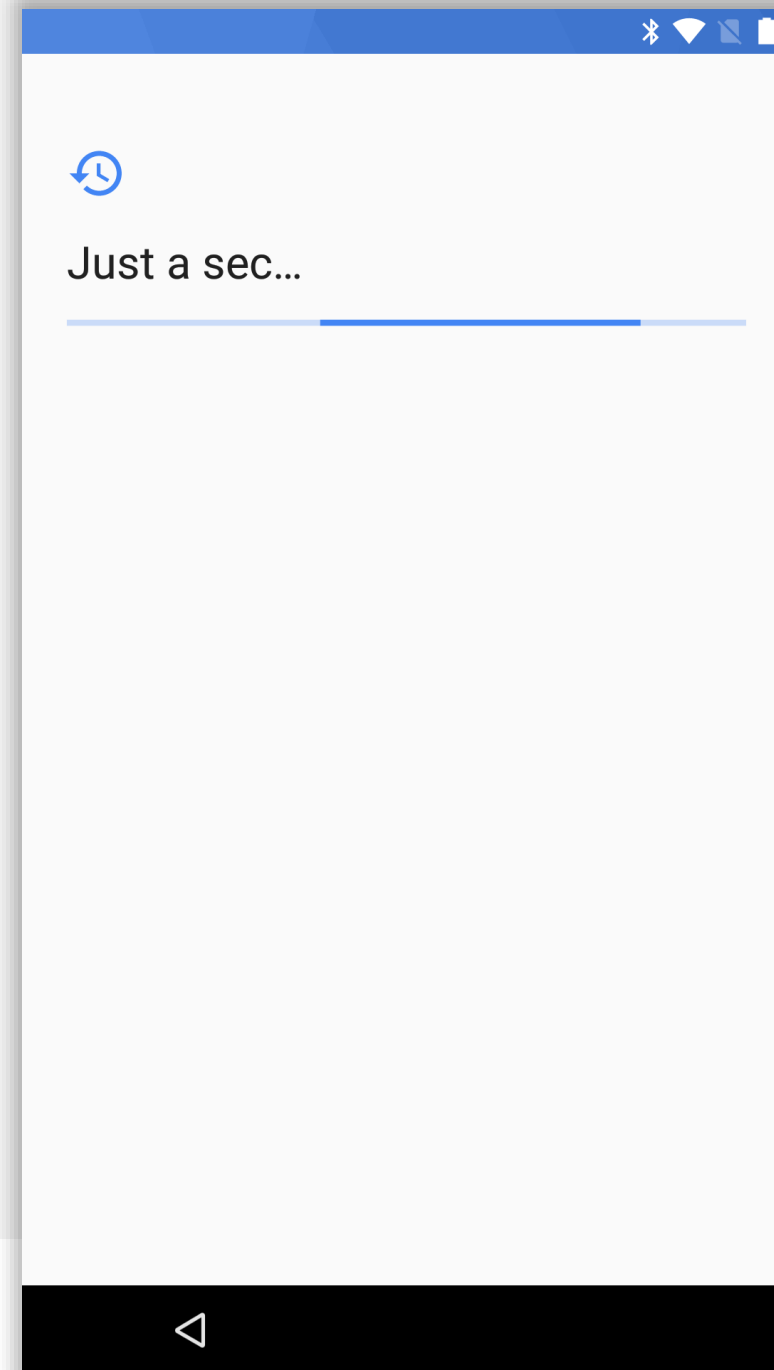
(After reading the ToS and Privacy Policy, naturally).





Continue device setup

The device will now add the account 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.



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](#).

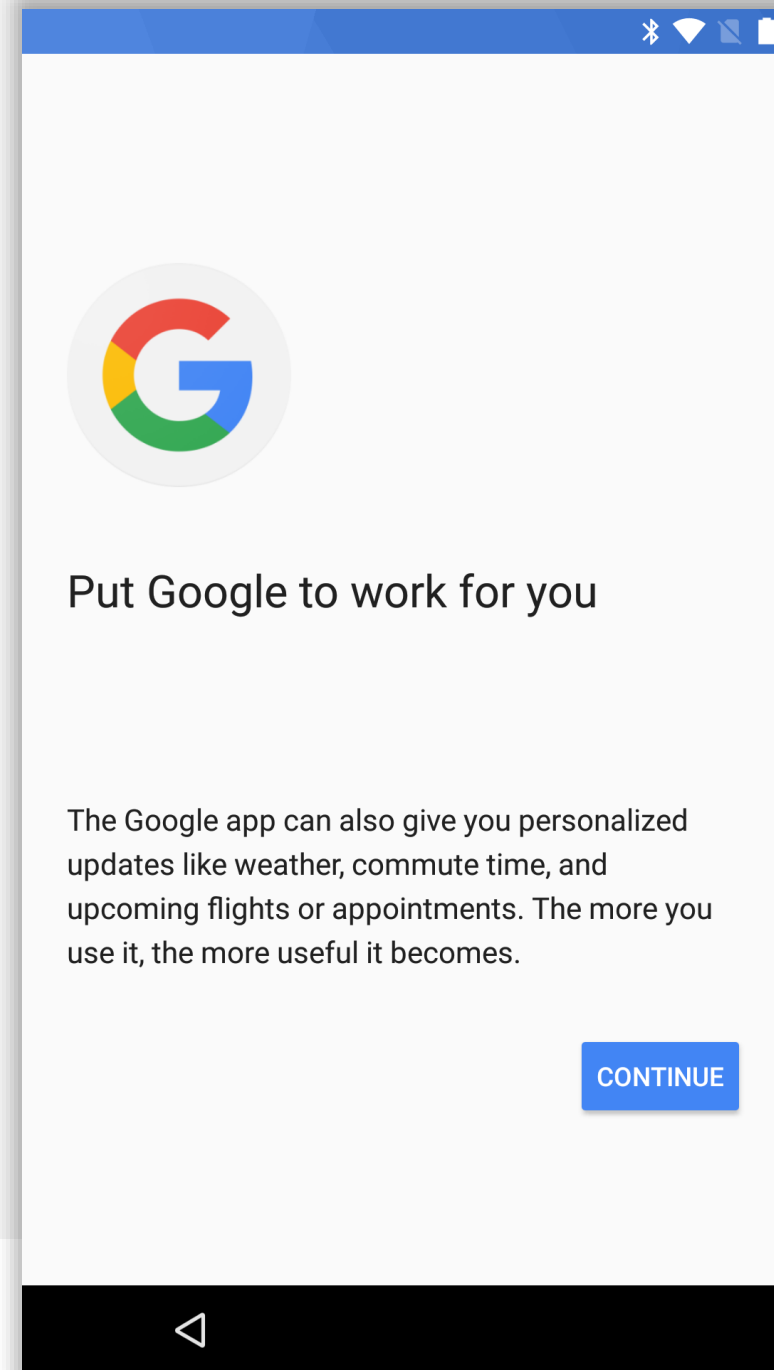
If you want to learn more, you can tap each service.

-  **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



Continue device setup

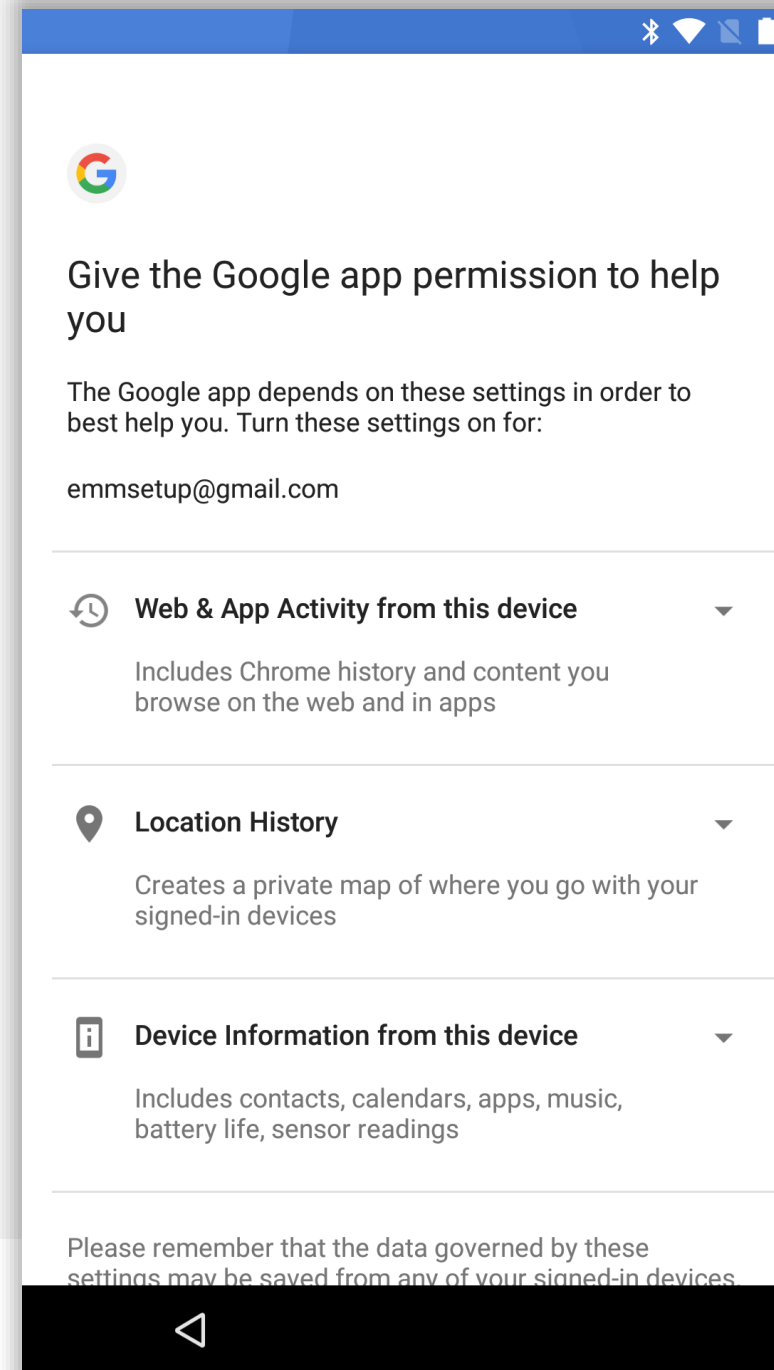
Tap **CONTINUE** to progress to the next step.





Continue device setup

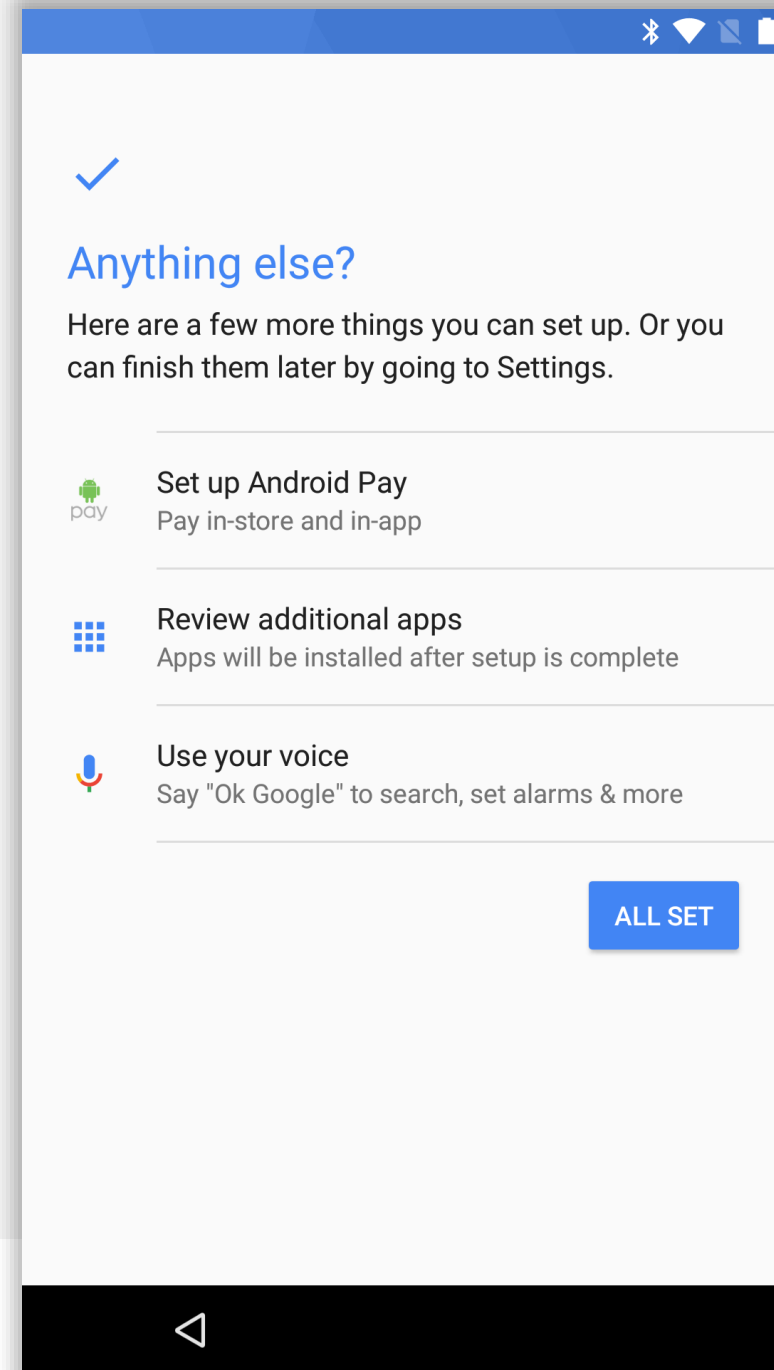
If the Google app is desired, tap **YES I'M IN**, otherwise tap **No Thanks** to continue to the next step.





Continue device setup

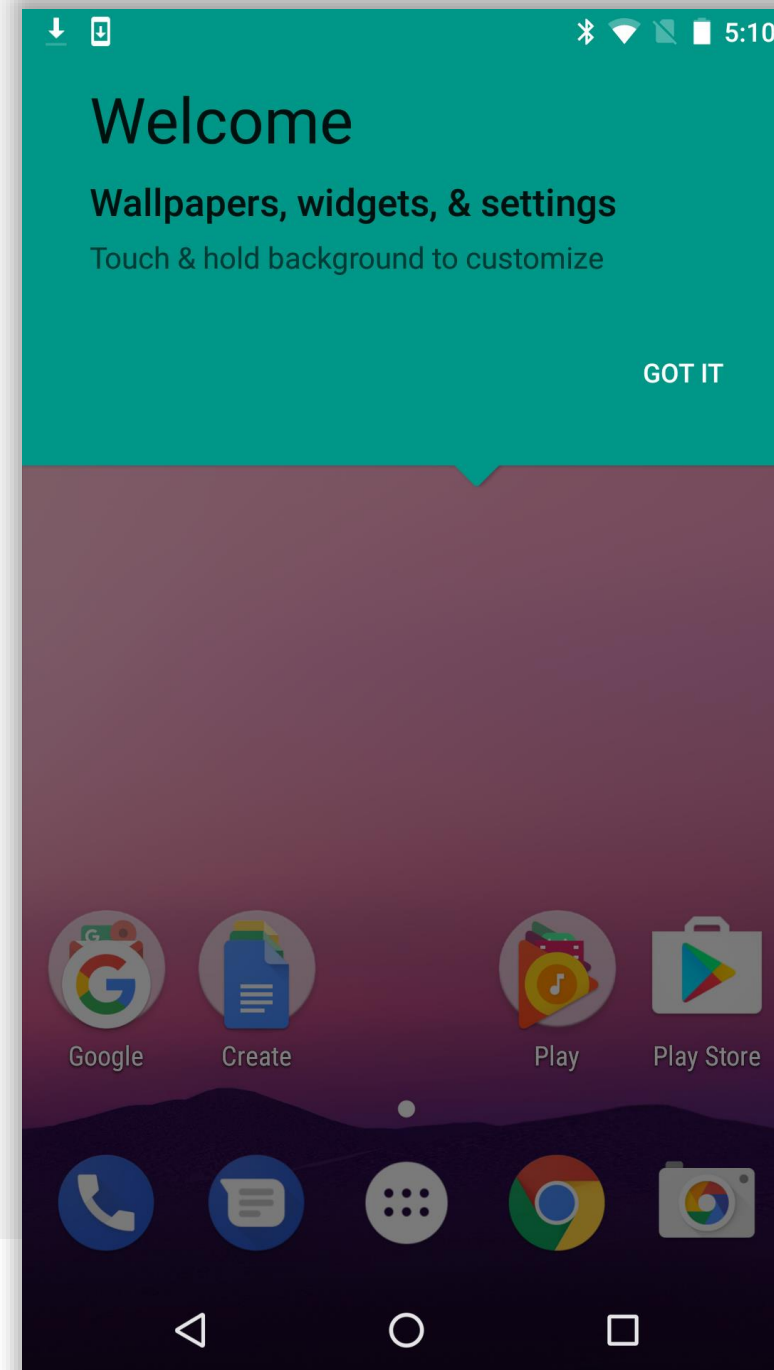
Tap **ALL SET** to exit the Wizard.





Device setup complete

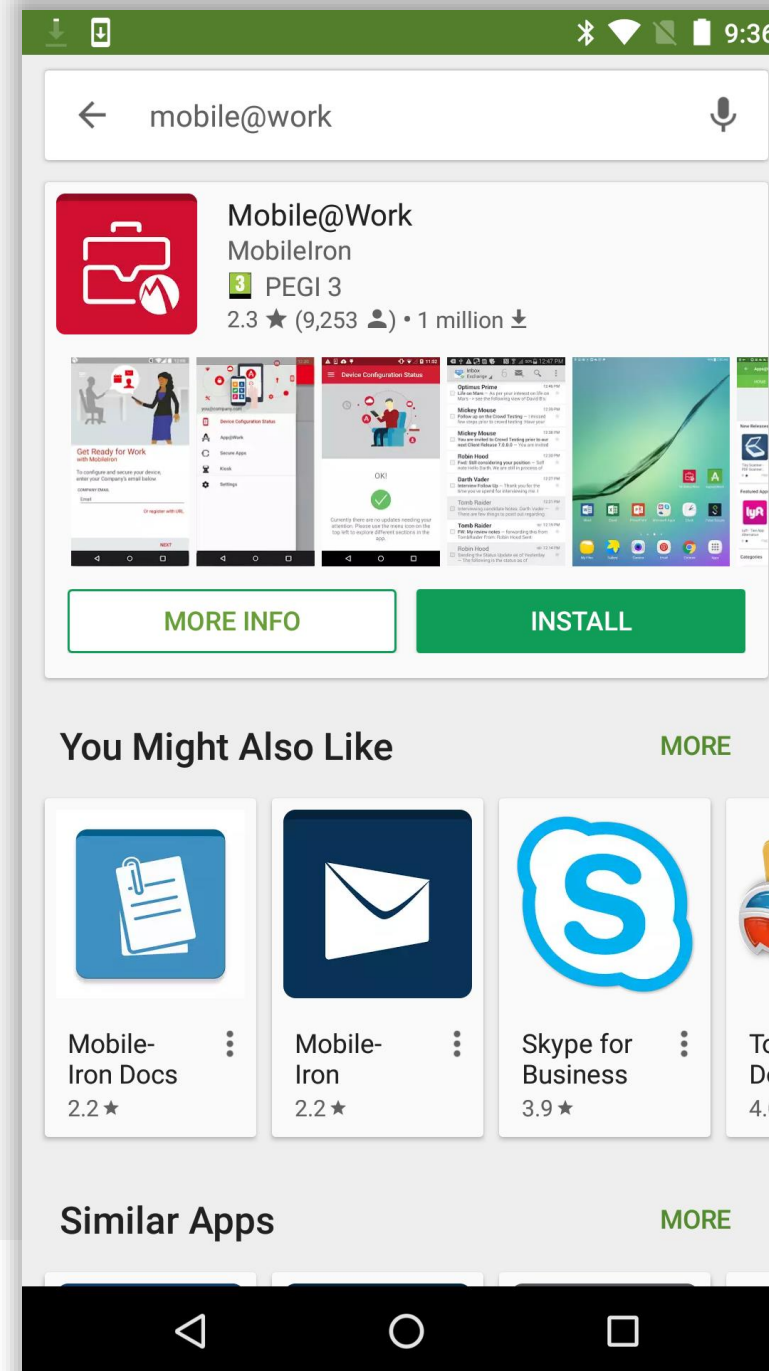
From the home screen, tap **GOT IT**, then open the Play Store.





Install the DPC

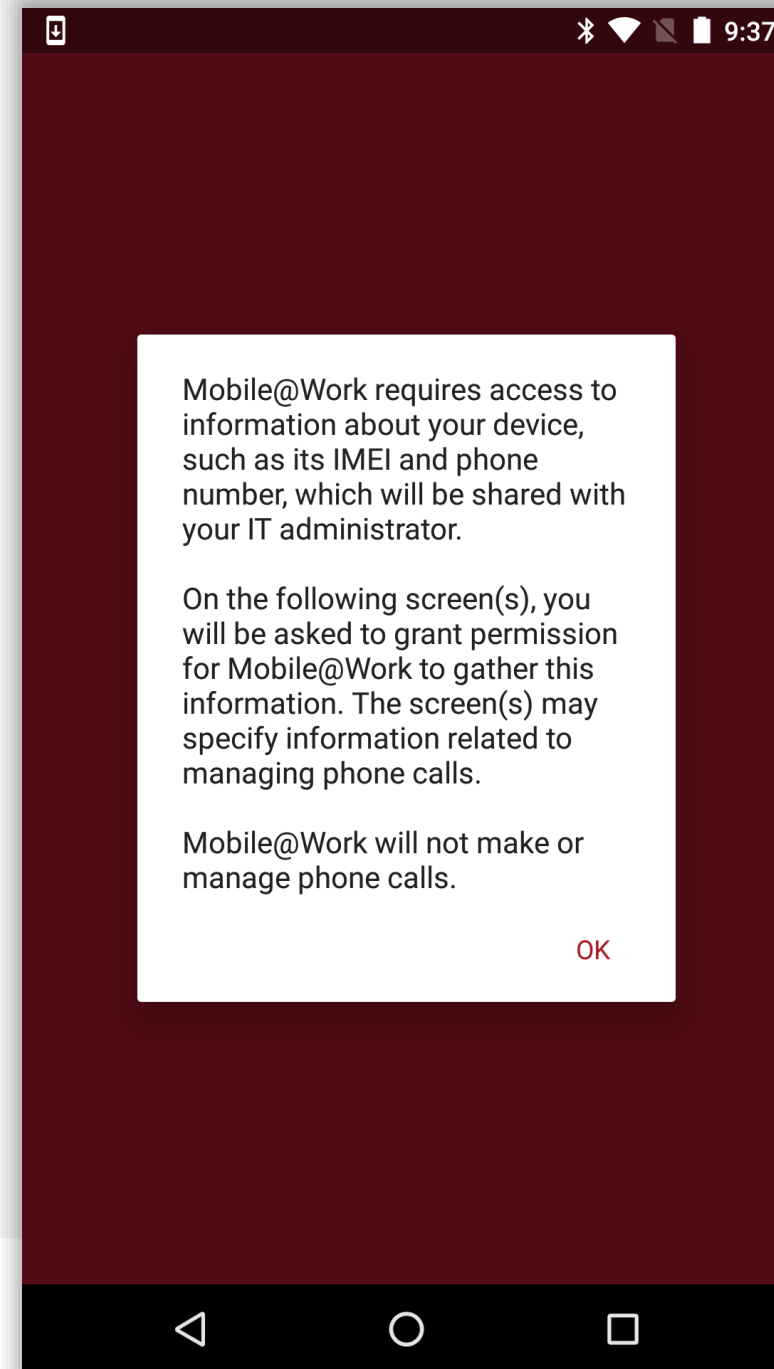
Search for Mobile@Work and tap **INSTALL** when located.





Open the DPC

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

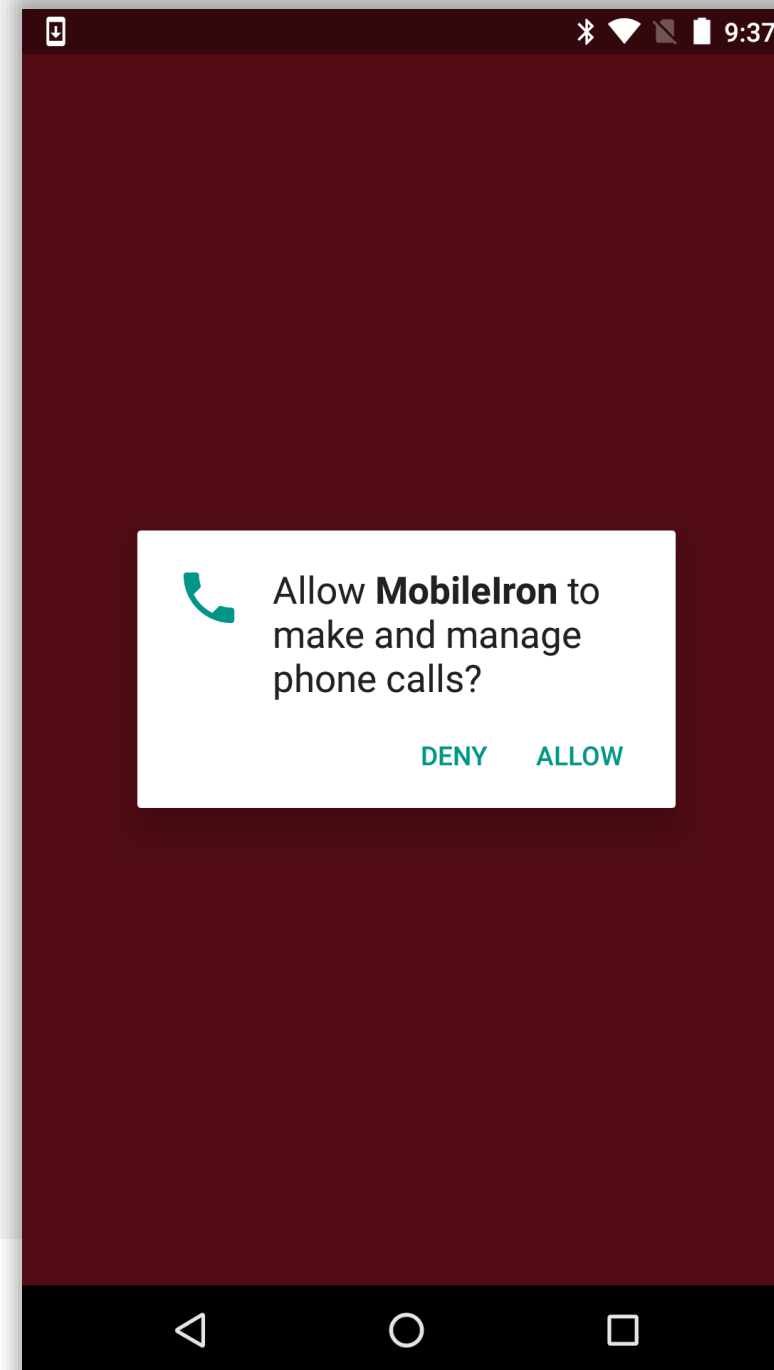




Grant permissions

Grant MobileIron the requested permissions.


Tap **ALLOW**.





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

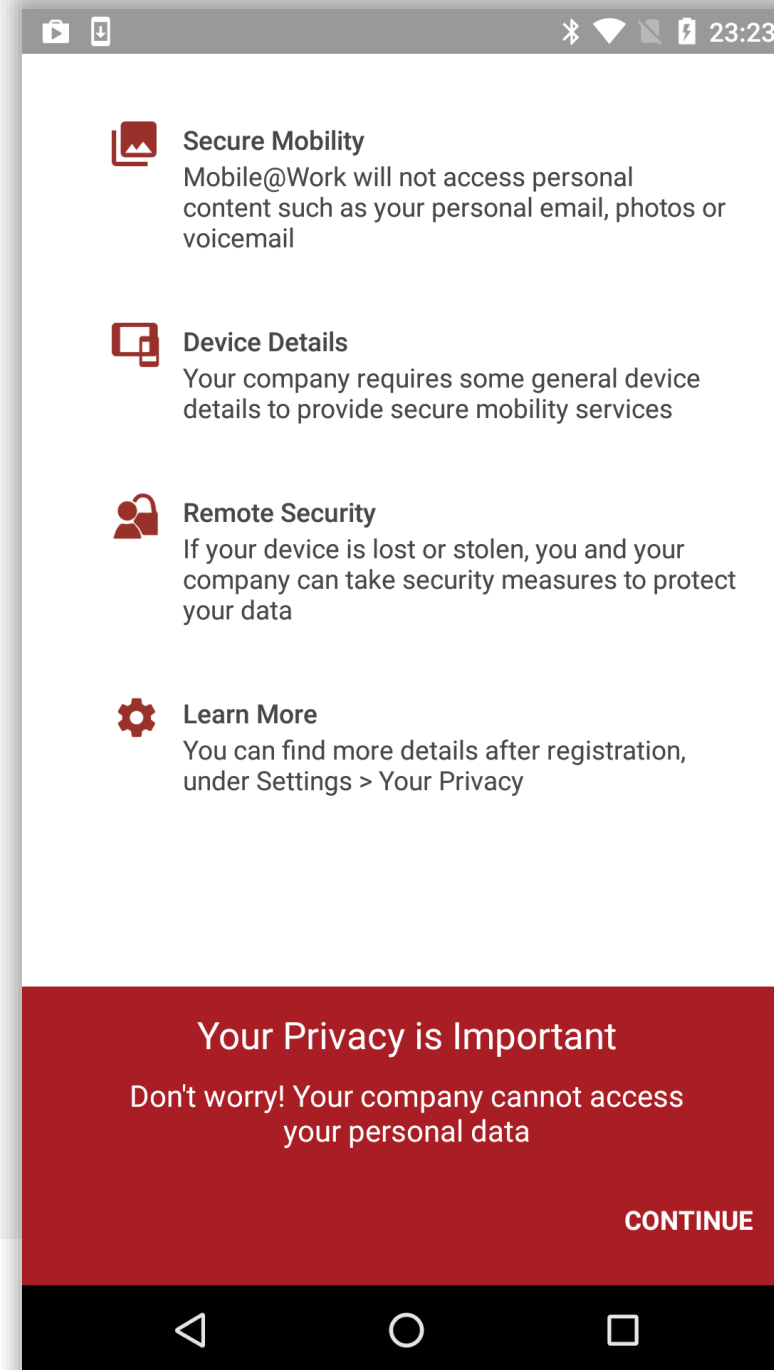
Or register with server URL

NEXT



Continue enrolment

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





Continue enrolment

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

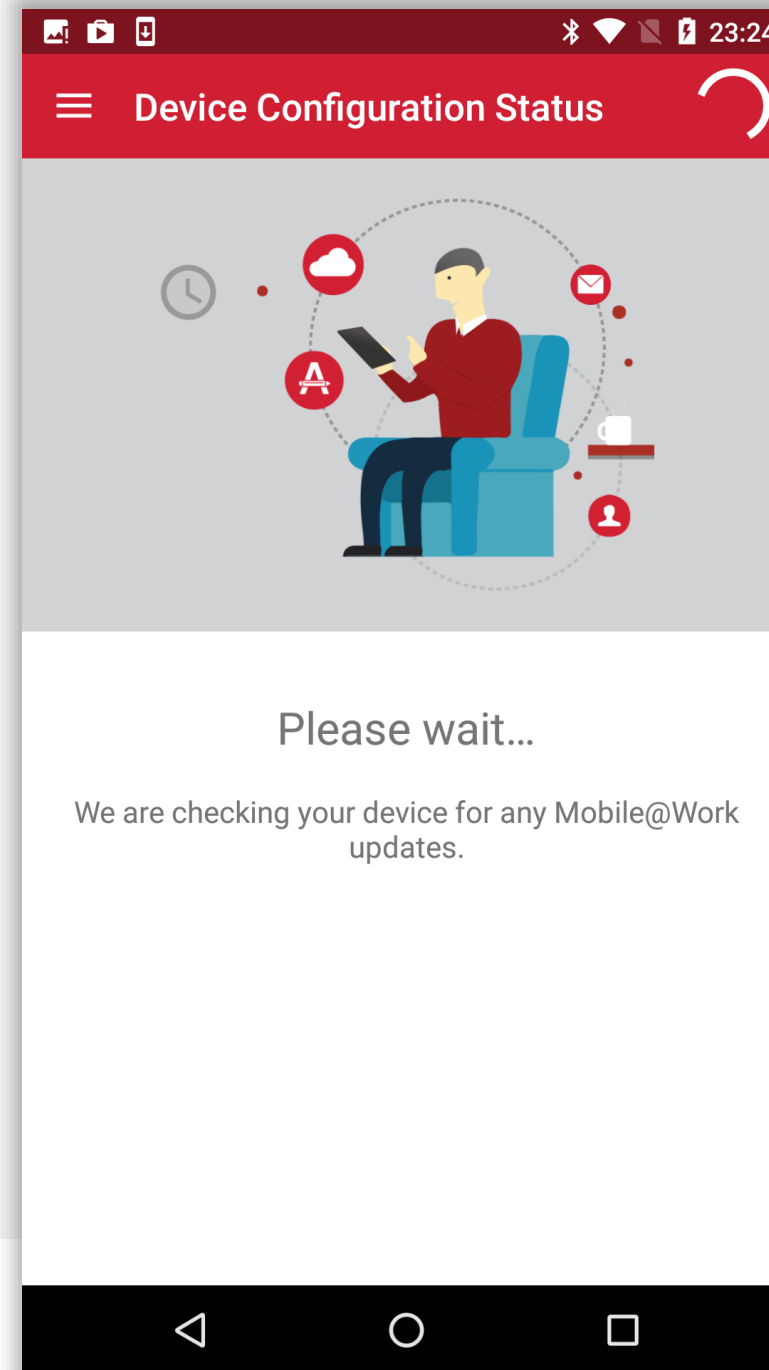
Enter the required fields and tap **SIGN IN**.

The screenshot shows a mobile application interface for a sign-in screen. At the top, there is a header image showing 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 value "jason@bayton.org" and "PASSWORD" with the value "Password". A red "SIGN IN" button is located to the right of the password field. Below the input fields is a QWERTY keyboard. The status bar at the top shows the time as 10:46 and the battery level. The Android navigation bar is visible at the bottom.



Device configuration

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

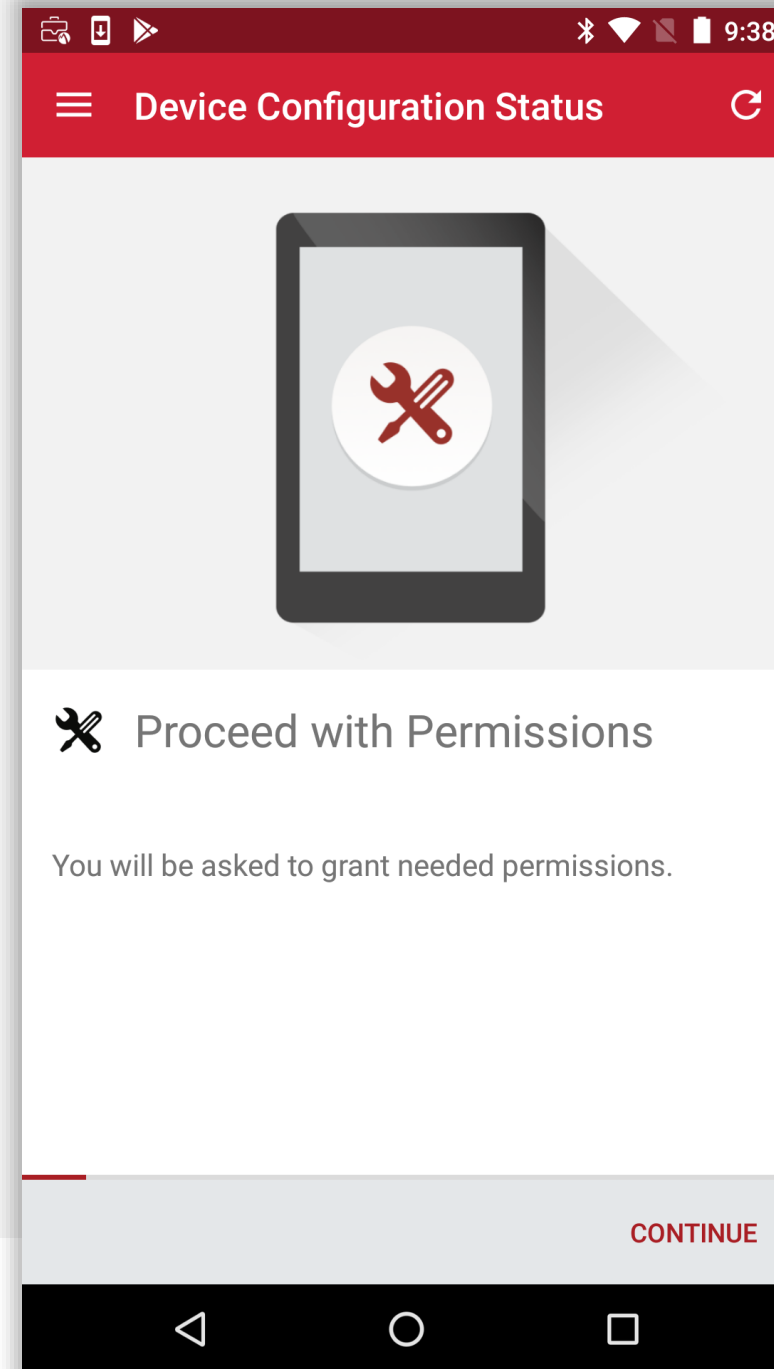




Device configuration

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

Tap **CONTINUE**.

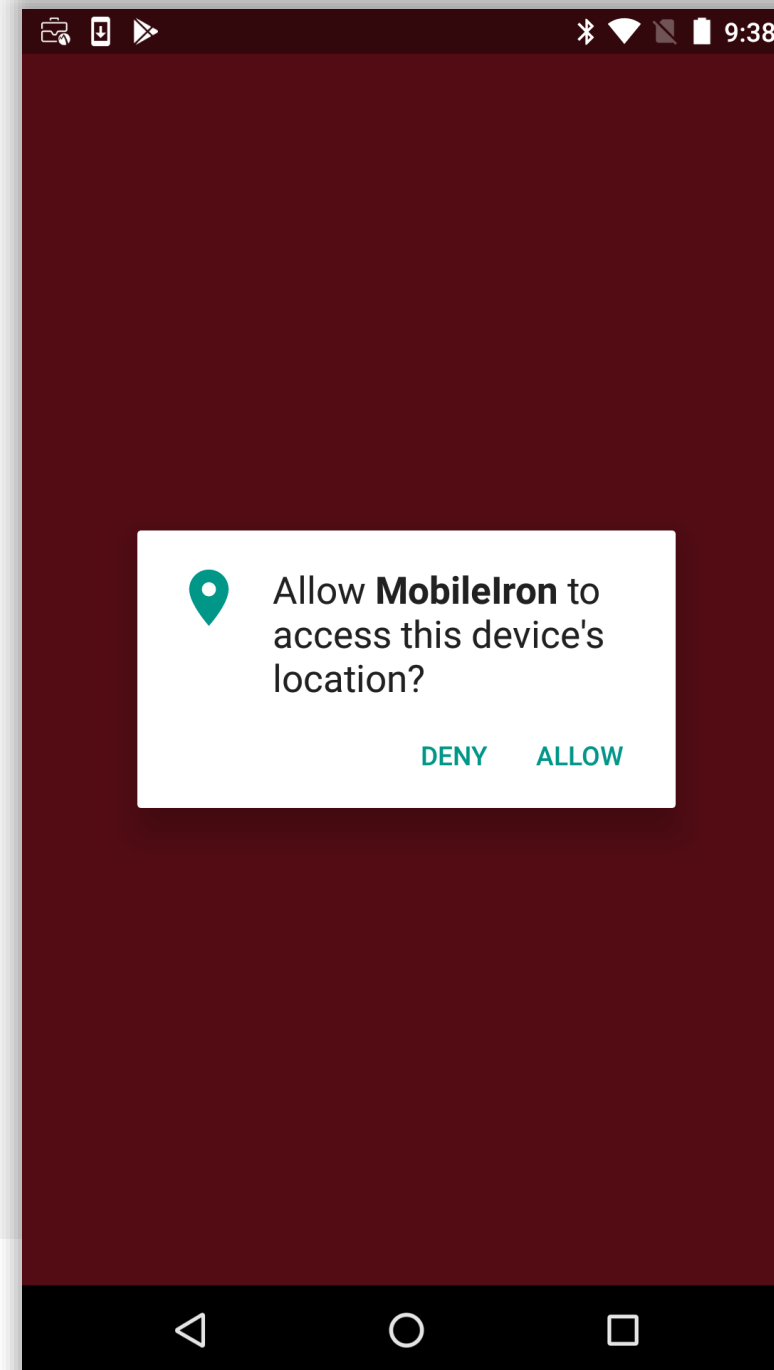




Grant permissions

Grant MobileIron the requested permissions.

Tap **ALLOW**.



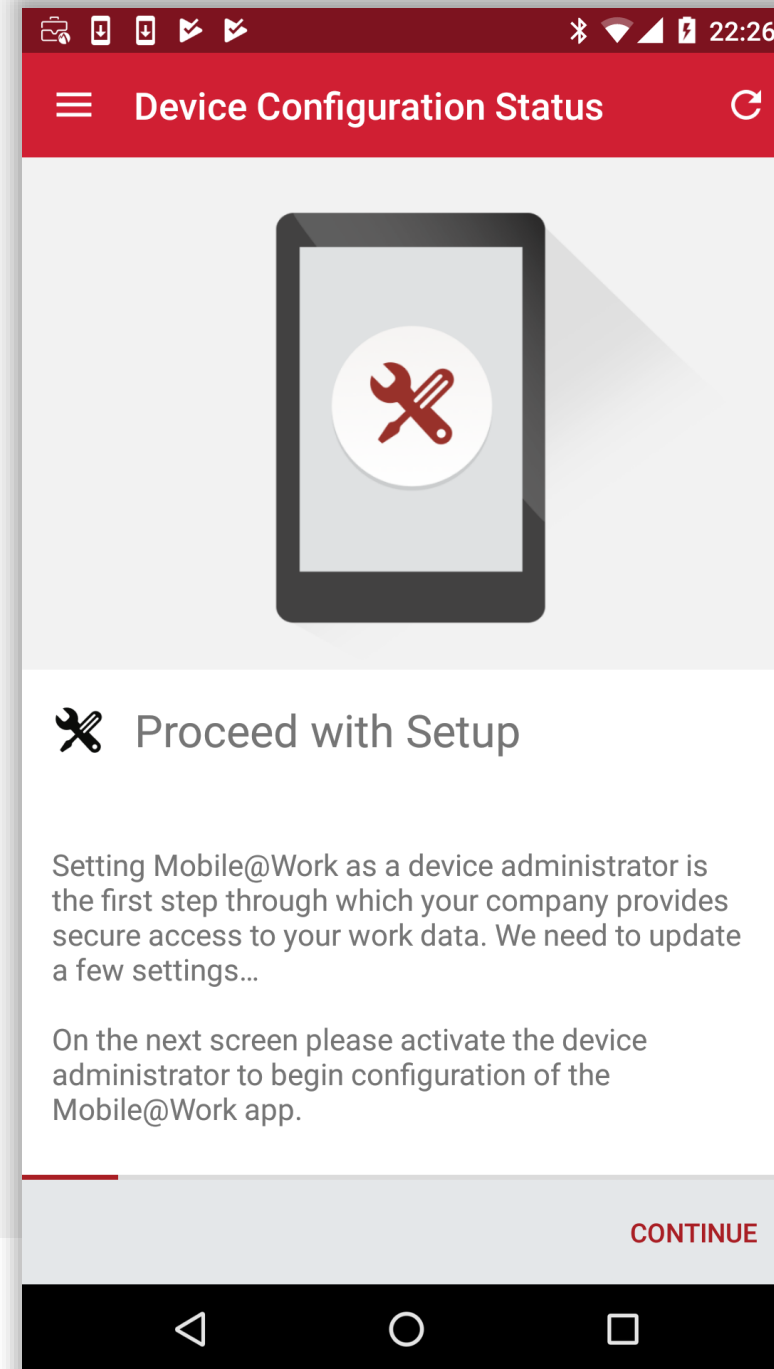


Device configuration

MobileIron requires device administrator permissions in order to effectively manage the device.

If this is not granted, or the administrator permission is later revoked, device management will not function.

Tap **CONTINUE**.



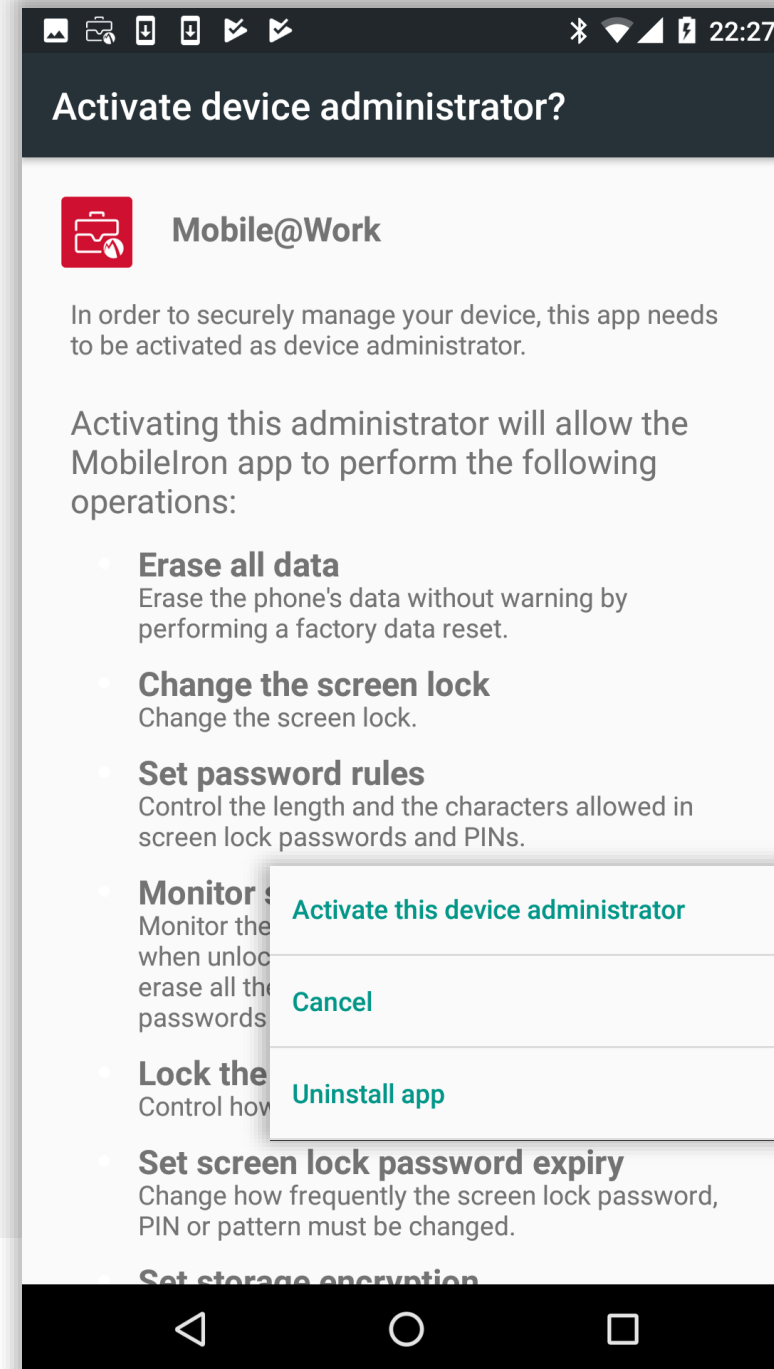


Activate administrator

MobileIron, like all EMMs, requires a number of permissions in order to effectively manage the device.

Scroll through the list of permissions until you reach the bottom.

Tap **Activate this device administrator** to continue.

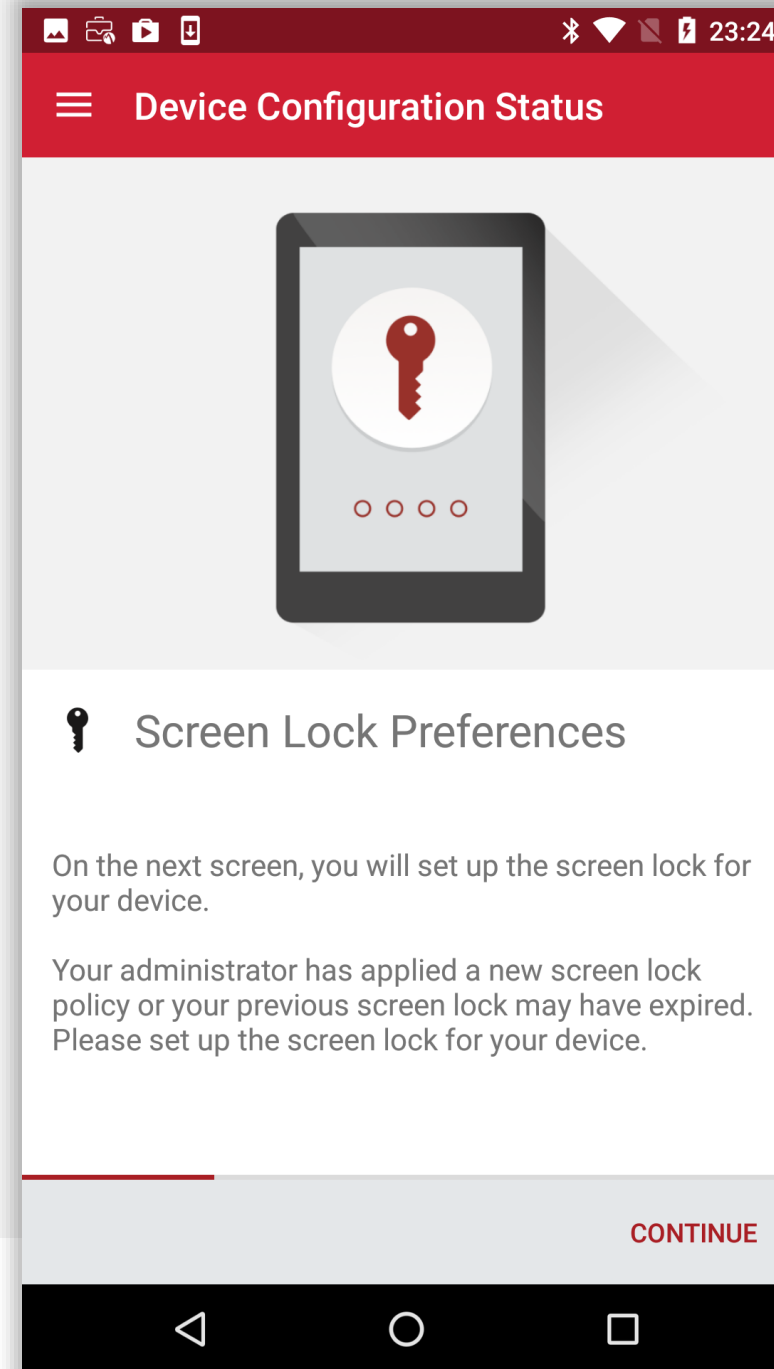




Device configuration

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

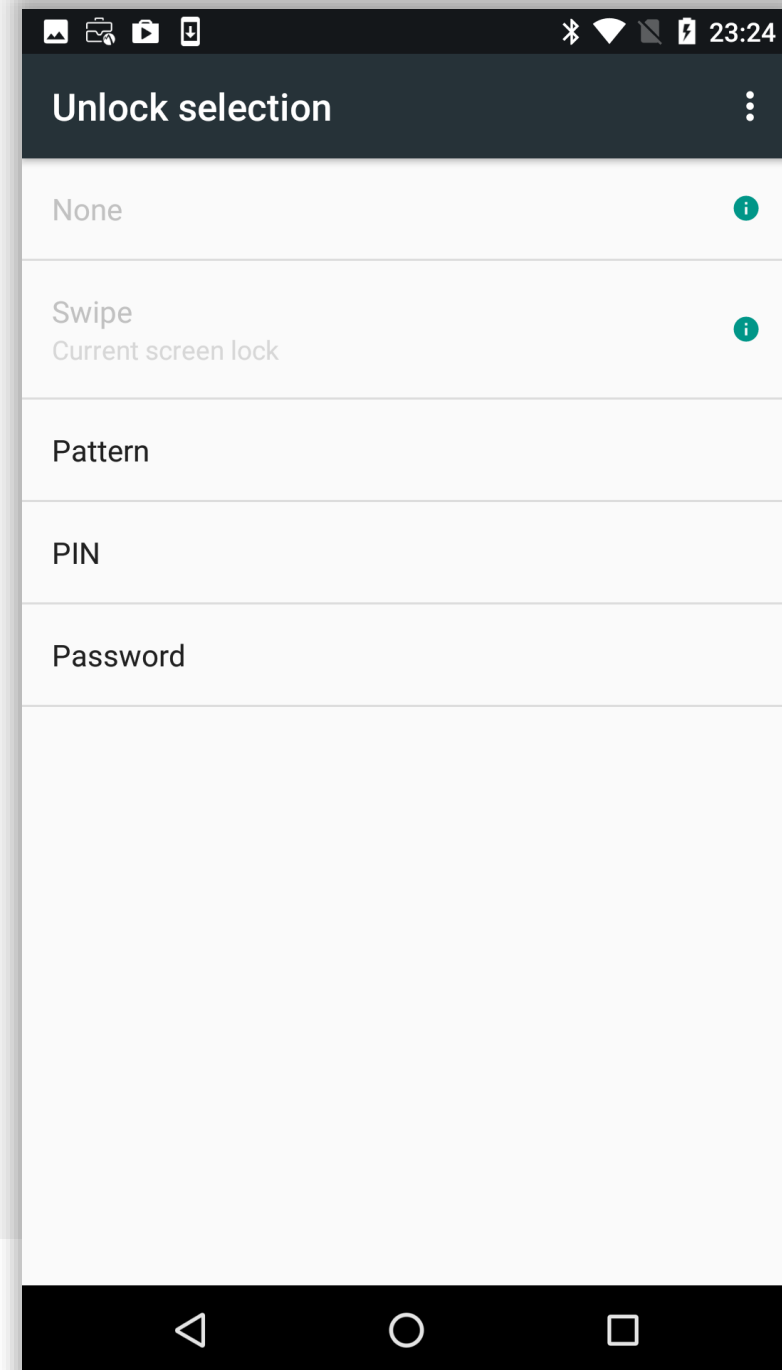
The type of passcode mandated may not be a PIN as depicted in the following steps. The process however is similar for all alpha/numeric passcode options.





Device configuration

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

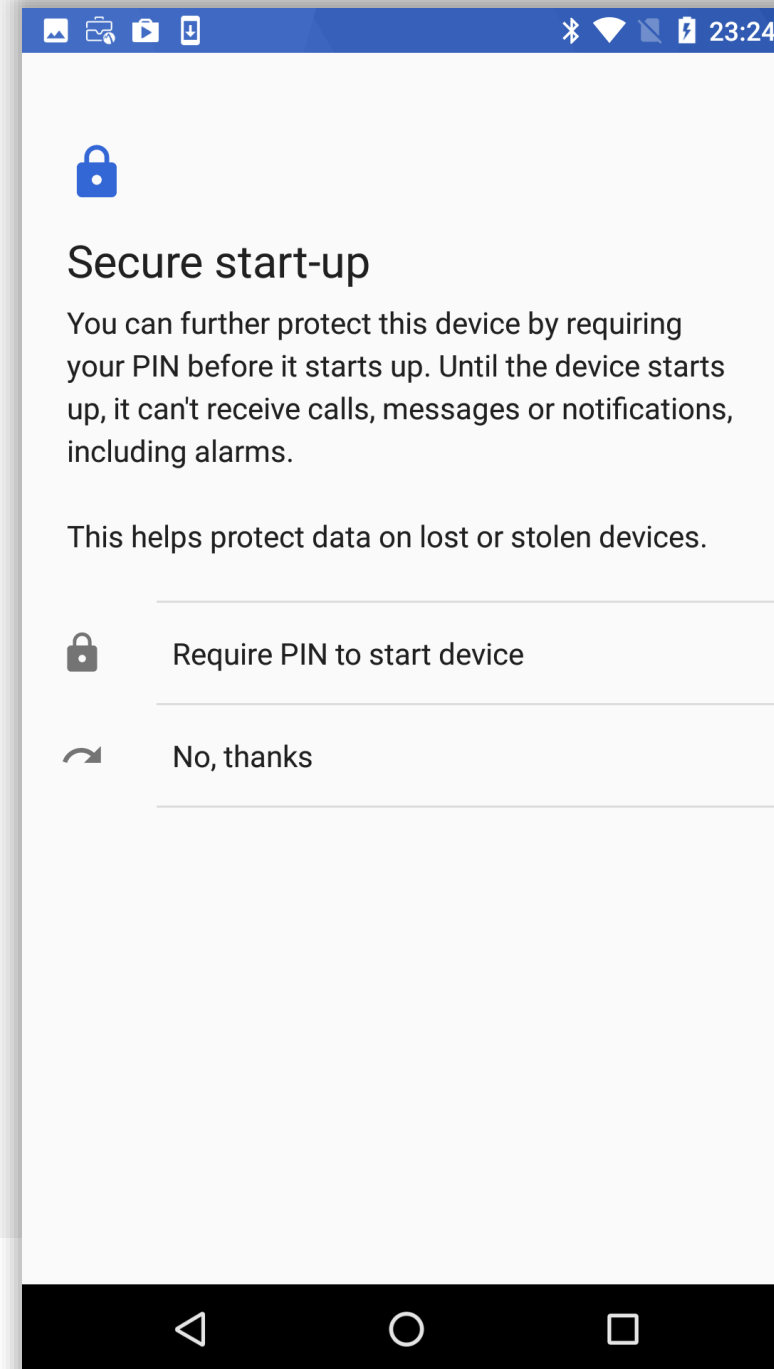




Device configuration

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

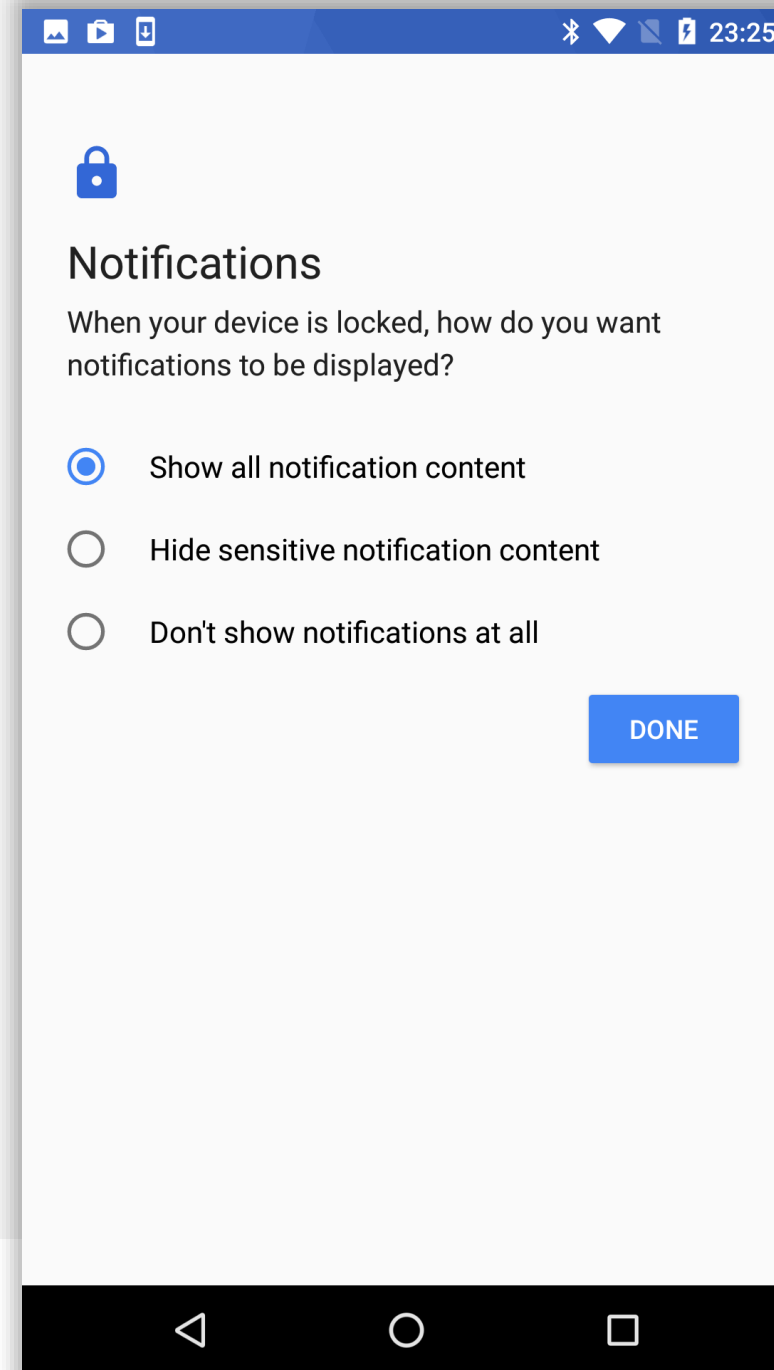
[Cancel](#) **CONTINUE**


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**.

A screenshot of an Android phone's notification settings screen. The screen has a blue header bar with icons for gallery, camera, and a lock, and status icons for Bluetooth, Wi-Fi, and battery. The main content area is white and features a blue lock icon at the top. Below it, the title 'Notifications' is followed by the question 'When your device is locked, how do you want notifications to be displayed?'. Three radio button options are listed: '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. The bottom of the screen shows the standard Android navigation bar with back, home, and recent apps buttons.



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

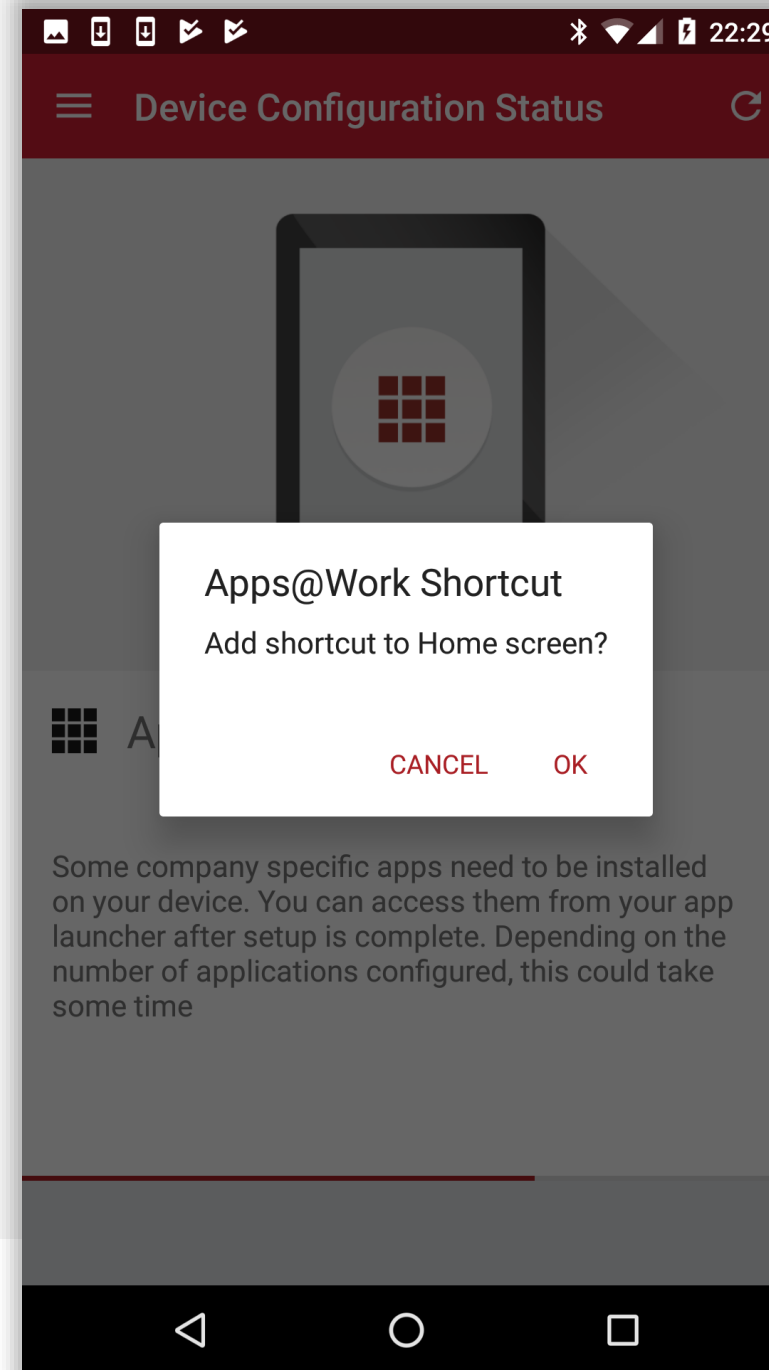
DONE



Device configuration

Legacy Android enrolment requires an EMM app catalogue on the device in order to install assigned applications.

Tap **OK** to add the Apps@Work shortcut to your home screen.

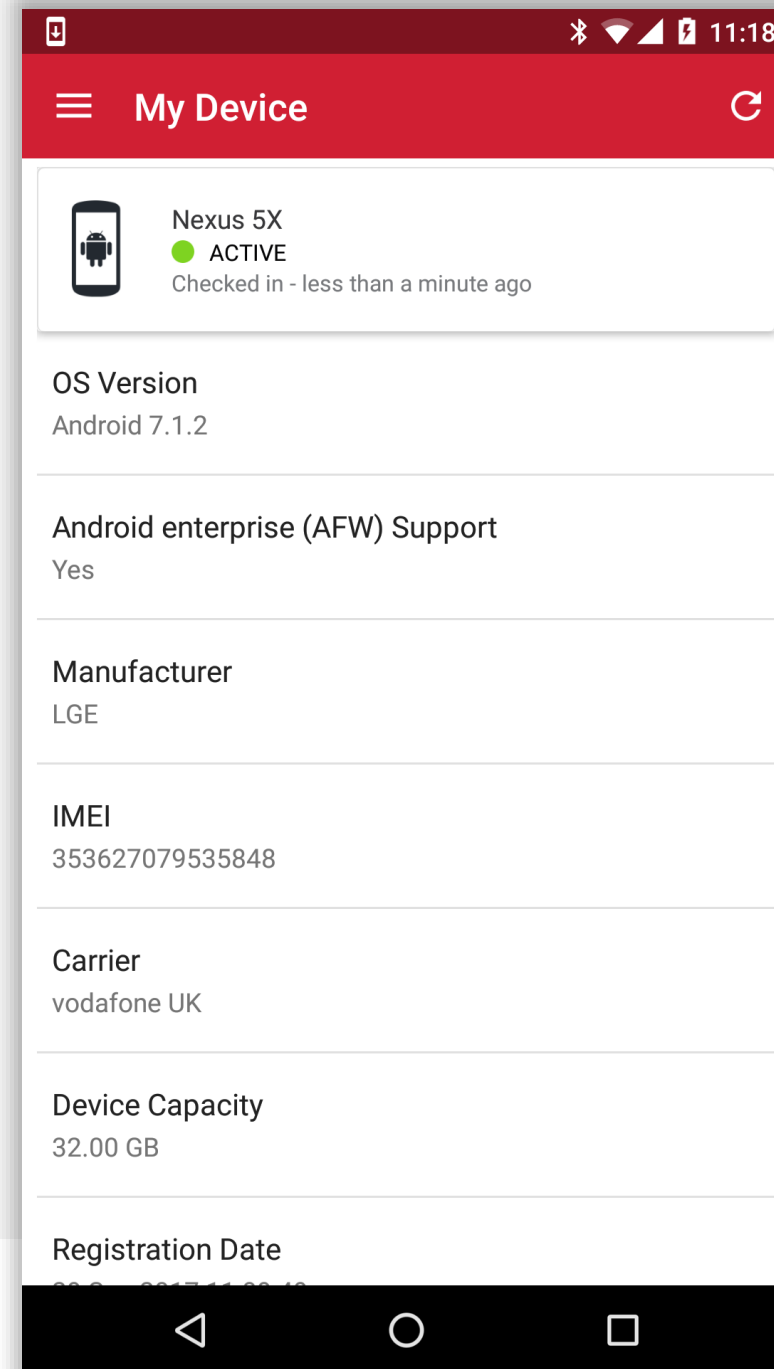




Configuration complete

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

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



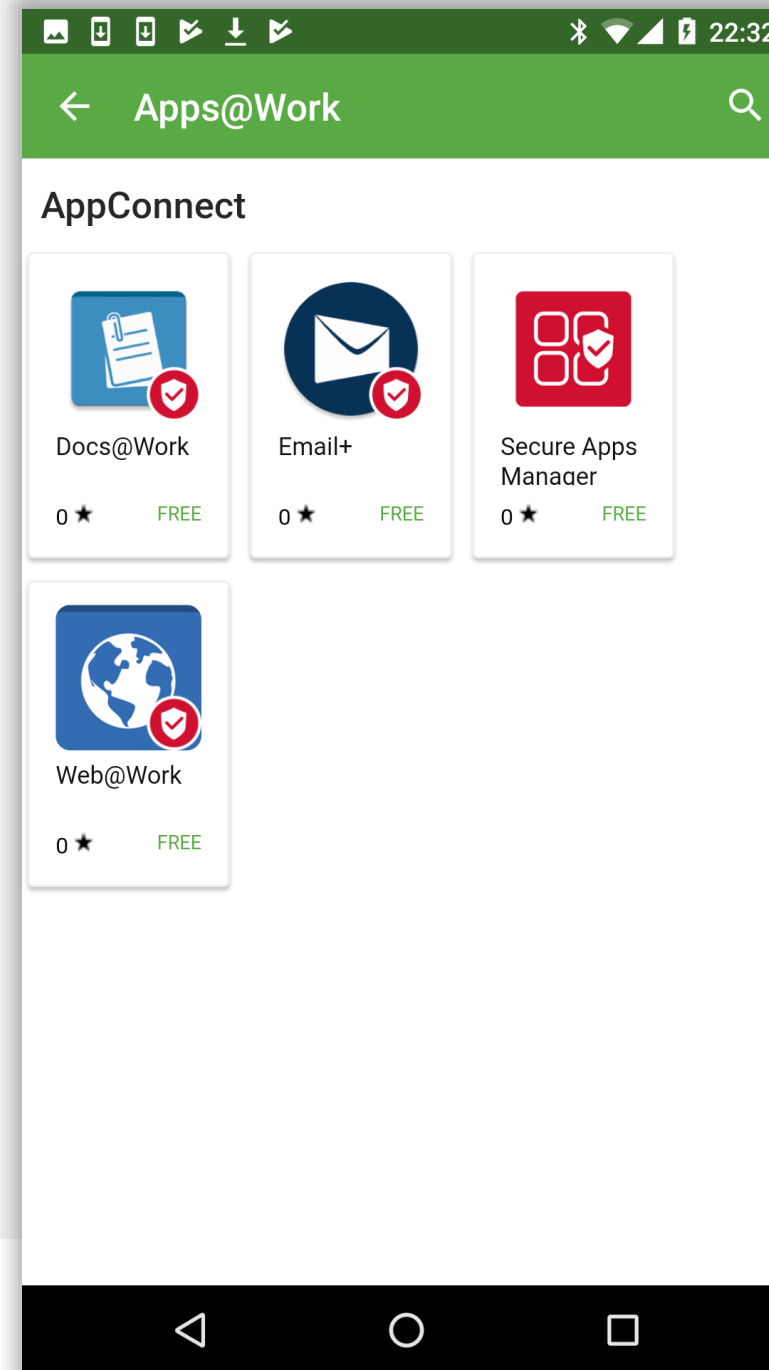


Installing applications

If you use a Samsung device, EMM-hosted applications like the AppConnect selection in the right-hand screenshot can be pushed down silently.

If you use any other device, such as the Nexus used for this guide, applications will not push and require you open the app catalogue in order to pull them down.

Public applications will redirect you to the Play Store for installation. They can't be installed silently.

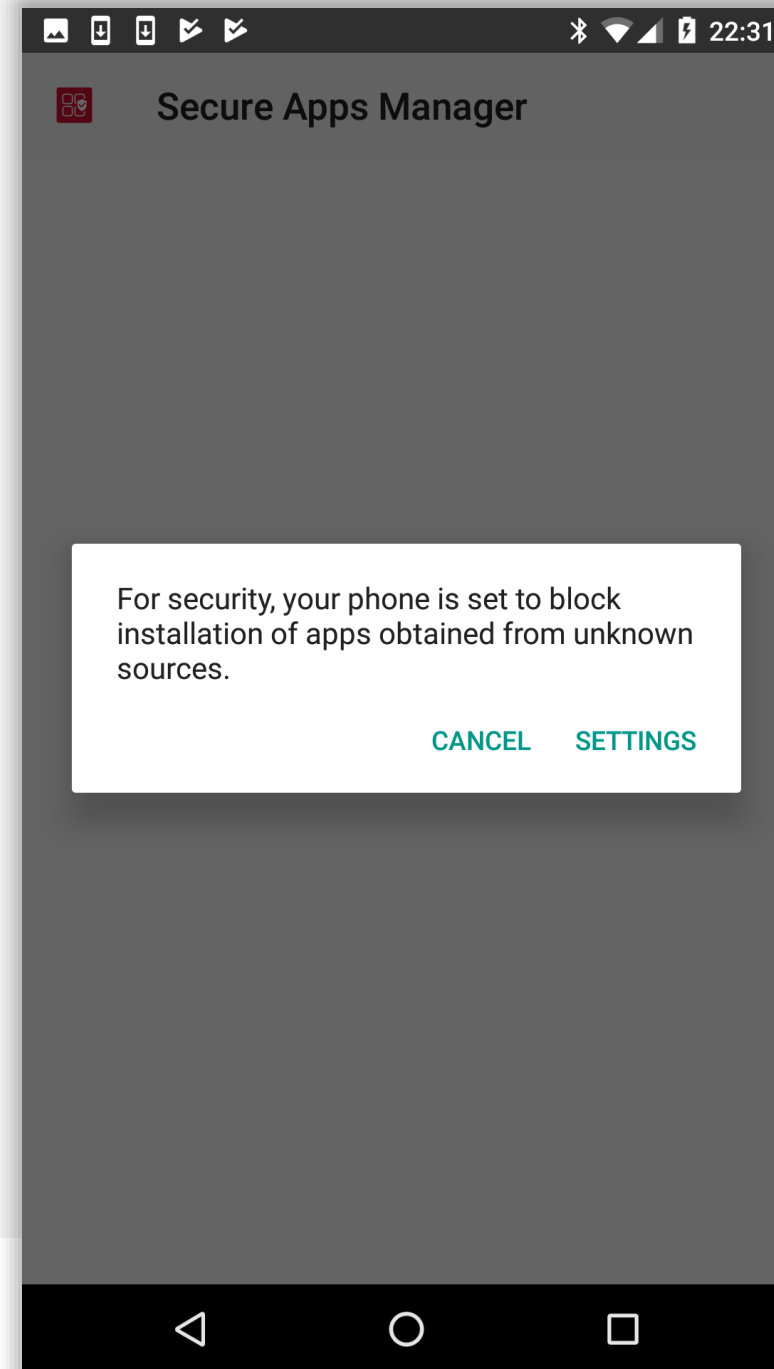




Installing applications

If installing in-house applications hosted and distributed through the EMM platform, unknown sources must be enabled on the device.

Tap **SETTINGS** to continue.



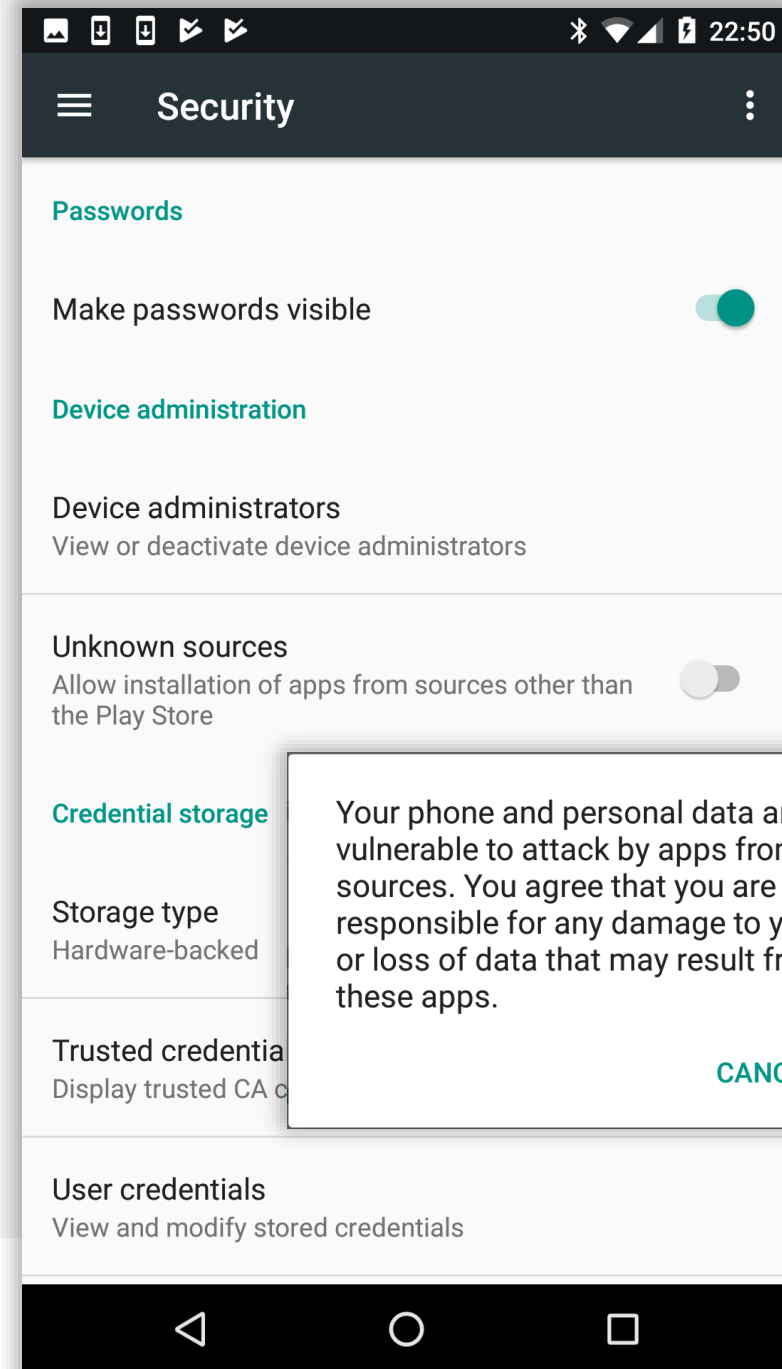


Installing applications

Scroll through settings until **Unknown sources** comes into view.

Tap the switch to enable unknown sources, then tap **OK** on the security warning that pops up to confirm you wish to continue.

You may now return to Apps@Work and tap to install the selected application once again.



bayton



Jason Bayton



bayton.org



/in/jasonbayton



@jasonbayton



+JasonBaytonX



jason@bayton.org

Updates to this document can be found here:

[Android enterprise provisioning guides](#)

